Qualys API (VM and PA)

User Guide
Version 10.40

September 7, 2026

Copyright 2018-2026 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Preface 10

Welcome 11

API Conventions 11
- Qualys User Account 11

Qualys API Server URL 12
Making API requests 13
API Limits 14
Tracking API usage by user 15
HTTP Response Headers 15
Activity Log 18
API Life Cycle - EOS/EOL 18

Authentication to your account 25

What do I need to know? 25
Using Basic HTTP Authentication 25
Using Session Based Authentication 26
Session Login 29
Session Logout 31
Token-based API Authentication Using IdP 32
- API Authentication using IdP Provider Tokens 32
- Onboarding IdP-based Authentication 33
- Generate IdP-based Authentication Token 34
- Access Qualys APIs with Authentication Token 35

Scans 37

VM Scans 38
- VM Scan List 38
- List Last 'N' Scan References for a Schedule 48
- Launch VM Scan 51
- Launch VM Scan on EC2 assets 53
- Manage VM Scans 56

Compliance Scans 59
- Compliance Scan List 60
- List Last 'N' Scan References for a Schedule 61
- SCAP Scan List 64
- Launch Compliance Scan 66
- Launch Compliance Scan on EC2 assets 67
- Manage Compliance Scans 69

Cloud Perimeter Scans 72
- Create/Update Cloud Perimeter Scan 72

Create/Update Cloud Perimeter Scan 75
Create/Update/Reset Cloud Perimeter Scan 77
Cloud Internal Scans 79
Create/Update Azure Internal Scan 80
Create/Update Azure and Google Cloud Platform Internal Scan 82
VM Scan Schedules 85
PC Scan Schedules 114
Scan List Parameters 124
Scan Parameters 126
Cloud Perimeter Scan Parameters 131
Azure Internal Scan Parameters 135
Google Cloud Platform Internal Scan Parameters 137
Scan Schedule Parameters 141
Azure and GCP Internal Scan Schedule Parameters 145
VM Scan Statistics 149
VM Scan Summary 153
Scan Summary 164
Scanner Details 167
Share PCI Scan 169
Discovery Scans (maps) 173

Scan Configuration 198

Scanner Appliance List 199
Manage Virtual Scanner Appliances 203
Update Physical Scanner Appliance 208
Replace Scanner Appliance 212
Scanner Appliance VLANs and Static Routes 214
Option Profile Export 219
Option Profile Import 262
Option Profiles for VM 297
Option Profiles for PCI 379
Option Profiles for Compliance 387
KnowledgeBase 477
KnowledgeBase QVS Download in JSON Format 541
Editing Vulnerabilities 556
Static Search Lists 559
Dynamic Search Lists 565
Vendor IDs and References 591
Manage Containerized Scanner Appliance 594
Create New Containerized Scanner Appliance 594
List Containerized Scanner Appliance 596
Update Containerized Scanner Appliance 600
Delete Containerized Scanner Appliance 602

Scan Authentication 605

User Permissions Summary 606
List Authentication Records 607
List Authentication Records by Type 615
Apache Cassandra Record 620
DataStax Record 626
Application Server Records 631
Azure MS SQL Record 636
Cisco APIC 4.x Authentication Record 641
DNS BIND Authentication Record 648
Docker Record 654
HTTP Record 657
IBM DB2 Record 660
InformixDB Record 665
Infoblox Record 670
JBoss Server record 676
Kubernetes Record 680
MariaDB Record 683
MarkLogic Record 687
Microsoft SharePoint Record 694
MongoDB Record 704
    System created MongoDB records 707
MS Exchange Server 714
MS SQL Record 719
MySQL Record 729
Neo4j Record 748
Nginx Record 753
Oracle Record 757
    System created Oracle records 763
Oracle Listener Record 765
Oracle WebLogic Server Record 767
Palo Alto Firewall Record 770
Pivotal Greenplum Record 774
PostgreSQL Record 781
SAP Hana Record 788
SAP IQ Record 793
SNMP Record 798
Sybase Record 803
Tomcat Server Records 815
Unix Record 829
Network SSH Record 902
VMware Record 909
VMware NSX Record 915
Windows Record 931
Oracle HTTP Server Record 939
vCenter - ESXi Mapping Records 949

Vault Support 955
Vault Support matrix 955
Vault Definition 962
List Vaults 969
Manage Vaults 972

Assets 983
IP List 984
Add IPs 987
Update IPs 990
Host List 995
Host Update 1115
Host List Detection 1119
Host List Detection - Normalized Data 1310
Host List Detection - Use Cases 1311
Host List Detection - Best Practices 1312
Excluded Host List 1313
Excluded Hosts Change History 1316
Manage Excluded Hosts 1319
Virtual Host List 1323
Manage Virtual Hosts 1325
Restricted IPs List 1327
Manage Restricted IPs 1329
Asset Group List 1332
Manage Asset Groups 1335
Purge Hosts 1340
Patch List 1347

IPv6 Assets 1349
API Support for IPv6 Asset Management and Scanning 1349
IPv6 Mapping Record List 1354
Add IPv6 Mapping Records 1355

Networks 1357
Network List 1357
Create Network 1358
Update Network 1360
Assign Scanner Appliance to Network 1361

Reports 1363
Report List 1364
Launch Report 1370
    Launching Reports Using Asset Tags 1383
    Launching and Fetching Compliance Reports in CSV Format 1384

Launching and Fetching Compliance Reports in XML Format 1387
Report Template List 1405
Launch Scorecard 1407
Cancel Running Report 1414
Download Saved Report 1417
Delete Saved Report 1431
Scheduled Reports List 1432
Launch Scheduled Report 1433
Asset Search Report 1433

VM Report Templates 1445

API Support for Report Templates 1445
Scan Template 1446
Cloud Asset Metadata Fields in CSV Format 1454
Cloud Asset Metadata Fields in XML Format 1455
Cloud Asset Metadata Fields in CSV Format 1468
Cloud Asset Metadata Fields in XML Format 1469
Cloud Asset Metadata Fields in CSV Format 1485
Cloud Asset Metadata Fields in XML Format 1485
Cloud Asset Metadata Fields in CSV Format 1506
Cloud Asset Metadata Fields in XML Format 1507
PCI Scan Template 1531
Patch Template 1533
Map Template 1541

VM Remediation Tickets 1559

Remediation Tickets overview 1559
Ticket Parameters 1561
View Ticket List 1563
Edit Tickets 1565
Delete Tickets 1567
View Deleted Ticket List 1569
Get Ticket Information 1570
Set Vulnerabilities to Ignore on Hosts 1572

Compliance 1578

Compliance Control List 1579
Compliance Policy List 1631
Compliance Policy - Export 1649
Compliance Policy - Import 1676
Compliance Policy - Merge 1681
Compliance Policy - Manage Asset Tags 1687
Compliance Policy - Manage Asset Groups 1691
Compliance Framework Reports 1694

GET Preferred Framework List API 1694
GET Policies List API 1695
GET Asset Groups List API 1695
GET Asset Tags List API 1696
GET Asset Sources List API 1696
Create Compliance Framework Report API 1697
GET Report Generation Status API 1700
Download Compliance Framework Report API 1700
Compliance Posture Information 1702
PC Posture Information APIs 1702
PC Posture Streaming APIs 1721
Get Policy List 1722
Resolve Host IDs 1728
Get Posture Info 1744
Control Criticality 1930
Exceptions 1931
List exceptions 1931
Request exception 1939
Update exceptions 1944
Delete exceptions 1947
SCAP Cyberscope Report 1950
SCAP ARF Report 1954
SCAP Policy List 1955
PCAS Policies 1958
Policy 1959
Lock Policy 1964
Policy Technology 1965
Policy Section 1967
Policy Section Control 1971
Policy Section Control Technology 1977
Policy Section Control Technology Evaluate 1981
PCAS Library Policy 1985
Library Label 1986
Library Label Technology 1987
Library Policy 1988
Library Policy Details 1991
Import Library Policy 1999

Users and Activity Log 2001

User List 2001
Add/Edit User 2003
Change Login Password 2012
User Registration Process 2013
Accept Qualys EULA 2015
Activate/Deactivate Users 2017

User Password Change 2018
Export User Activity Log 2021

Appendix A - API Documentation 2026

Appendix B - Ports used for scanning 2027

Appendix C - Scan Results JSON 2029

Appendix D - Error Codes / Descriptions 2035

Appendix E - Streaming Posture API Client Sample Code (Python) 2040

Index 2047

Preface

Using the Qualys API, third parties can integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. The APIs described in this guide are available to customers using Qualys Cloud Platform (VM, PC).

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.

Welcome

The Qualys API allows third parties to integrate their own applications with Qualys cloud security and compliance solutions using an extensible XML interface. APIs in this user guide are supported using Qualys Cloud Platform (VM, PC).

We recommend you join our Community and subscribe to our API Notifications RSS Feeds for announcements and discussions.

Get API Notifications

Join our Community

API Notifications RSS Feeds

API Conventions

Qualys User Account

Authentication with valid Qualys user account credentials is required for making Qualys API requests to the Qualys API servers. These servers are hosted at the Qualys platform, also referred to as the Security Operations Center (SOC), where your account is located. If you need assistance with obtaining a Qualys account, please contact your Qualys account representative.

Users with a Qualys user account may access the API functions. When a subscription has multiple users, all users with any user role (except Contact) can use the Qualys API. Each user's permissions correspond to their assigned user role.

Qualys user accounts that have been enabled with VIP two-factor authentication can be used with the Qualys API, however two-factor authentication will not be used when making API requests. Two-factor authentication is only supported when logging into the Qualys GUI.

Qualys API Server URL

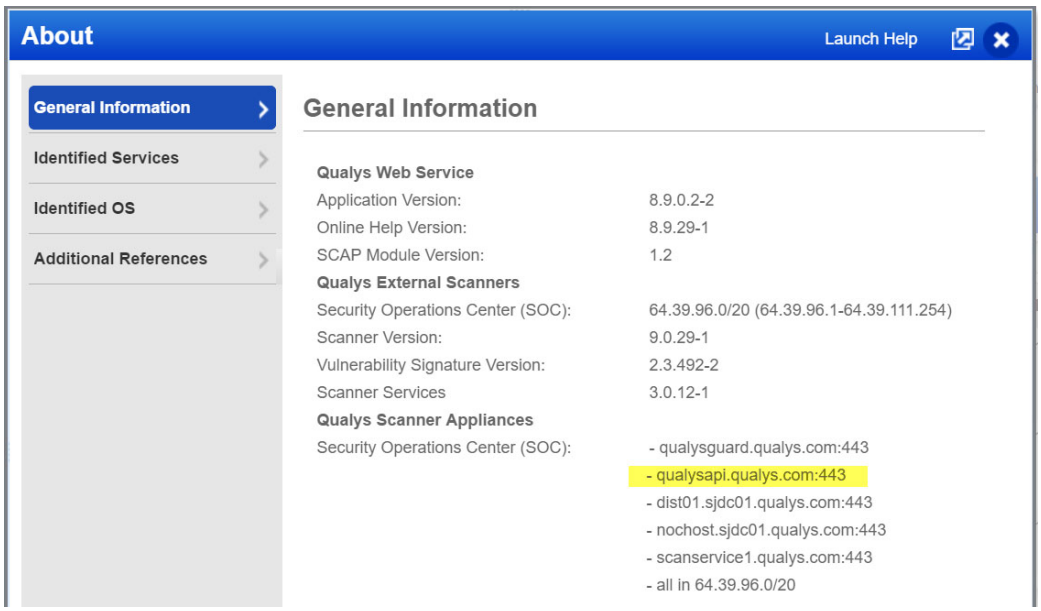
The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

Still have questions? You can easily find the API server URL for your account.

Just log in to your Qualys account and go to Help > About. You'll see this information under Security Operations Center (SOC).



Making API requests

Curl samples in our API docs

We use curl in our API documentation to show an example how to form REST API calls, and it is not meant to be an actual production example of implementation.

GET and POST Methods

Qualys API functions allow API users to submit parameters (name=value pairs) using the GET and/or POST method. There are known limits for the amount of data that can be sent using the GET method, and these limits are dependent on the toolkit used. Please refer to the individual descriptions of the API function calls to learn about the supported methods for each function.

Parameters in URLs

API parameters, as documented in this user guide, should be specified one time for each URL. In the case where the same parameter is specified multiple times in a single URL, the last parameter takes effect and the previous instances are silently ignored.

Additionally, when making API requests, ensure that all input parameters are enclosed in double quotes.

Date Format in API Results

The Qualys API has adopted a date/time format to provide consistency and interoperability of the Qualys API with third-party applications. The date format follows standards published in RFC 3339 and ISO 8601, and applies throughout the Qualys API.

The date format is:

yyyy-mm-dd**T**hh-mm-ss**Z**

This represents a UTC value (GMT time zone).

URL Encoding in API Code

You must URL encode variables when using the Qualys API. This is standard practice for HTTP communications. If your application passes special characters, like the single quote (‘), parentheses, and symbols, they must be URL encoded.

For example, the pound (#) character cannot be used as an input parameter in URLs. If “#” is specified, the Qualys API returns an error. To specify the “#” character in a URL you must enter the encoded value “%23”. The “#” character is considered by browsers and other Internet tools as a separator between the URL and the results page, so whatever follows an un-encoded “#” character is not passed to the Qualys API server and returns an error.

UTF-8 Encoding

The Qualys API uses UTF-8 encoding. The encoding is specified in the XML output header as shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
```

URL Elements are Case Sensitive

URL elements are case sensitive. The sample URL below will retrieve a previously saved scan report that has the reference code "scan/987659876.19876". The parameter name "ref" is defined in lower-case characters. This URL will return the specified scan report:

```
https://qualysapi.qualys.com/msp/scan_report.php?
ref=scan/987659876.19876
```

The sample URL below is incorrect and will not return the specified scan report because the parameter name "Ref" appears in mixed-case characters:

```
https://qualysapi.qualys.com/msp/scan_report.php?
Ref=scan/987659876.19876
```

Decoding XML Reports

There are a number of ways to parse an XML file. Select the method which is most appropriate for your application and its users. Qualys publishes DTDs for each report on its Web site. For example, the scan list output DTD is found at the URL shown:

```
https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd
```

The URLs to current report DTDs are included with the function descriptions in this document.

Occasionally Qualys updates the report DTDs. It is recommended that you request the most recent DTDs from the Qualys platform to decode your reports. The URLs to the report DTDs are included in this user guide.

Detailed information about each XML report is provided in the document Qualys API for VM and Compliance XML/DTD Reference

Some parts of the XML report may contain HTML tags or other special characters (such as accented letters). Therefore, many elements contain CDATA sections, which allow HTML tags to be included in the report. "High" ASCII and other non-printable characters are escaped using question marks.

API Limits

Qualys Cloud Platform enforces limits on the API calls subscription users can make. The limits apply to the use of all APIs, except "session" API (session login/logout).

API controls are applied per subscription based on your subscription's service level. Default settings are provided and these may be customized per subscription by Qualys Support.

There's 2 controls defined per subscription:

- Concurrency Limit per Subscription (per API). The maximum number of API calls allowed within the subscription during the configured rate limit period (as per service level).

- Rate Limit per Subscription (per API). The period of time that defines a window when API calls are counted within the subscription for each API. The window starts from the moment each API call is received by the service and extends backwards 1 hour or 1 day. Individual rate and count settings are applied (as per service level).

Click here to learn more about the controls and settings per service level.

How it works - Qualys checks the concurrency limit and rate limit each time an API request is received. In a case where an API call is received and our service determines a limit has been exceeded, the API call is blocked and an error is returned (the concurrency limit error takes precedence).

Tracking API usage by user

You can track API usage per user without the need to provide user credentials such as the username and password. Contact Qualys Support to get the X-Powered-By HTTP header enabled. Once enabled, the X-Powered-By HTTP header is returned for each API request made by a user. The X-Powered-By value includes a unique ID generated for each subscription and a unique ID generated for each user. See sample headers below.

Click here to learn more.

HTTP Response Headers

Your subscription's API usage and quota information is exposed in the HTTP response headers generated by Qualys APIs (all APIs except "session" API).

The HTTP response headers generated by Qualys APIs are described below.

The HTTP status code "OK" (example: "HTTP/1.1 200 OK") is returned in the header for normal (not blocked) API calls. The HTTP status code "Conflict" (example: "HTTP/1.1 409 Conflict") is returned for API calls that were blocked.

Header	Description
X-RateLimit-Limit	Maximum number of API calls allowed in any given time period of <number-seconds> seconds, where <number-seconds> is the value of X-RateLimit-Window-Sec.
X-RateLimit-Window-Sec	Time period (in seconds) during which up to <number-limit> API calls are allowed, where <number-limit> is the value of X-RateLimit-Limit.
X-RateLimit-Remaining	Number of API calls you can make right now before reaching the rate limit <number-limit> in the last <number-seconds> seconds.
X-RateLimit-ToWait-Sec	The wait period (in seconds) before you can make the next API call without being blocked by the rate limiting rule.
X-Concurrency-Limit-Limit	Number of API calls you are allowed to run concurrently.

Header	Description
X-Concurrency-Limit-Running	Number of API calls that are running right now (including the one identified in the current HTTP response header).
X-Powered-By	This header is only returned when the X-Powered-By header is enabled for your subscription. It includes a unique ID generated for each subscription and a unique ID generated for each user. Click here to learn more.

Sample HTTP Response Headers

Sample 1: Normal API call (API call not blocked)

Returned from API call using HTTP authentication.

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2018 00:13:18 GMT
Server: qweb
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 1
X-RateLimit-ToWait-Sec: 0
X-RateLimit-Remaining: 4
Transfer-Encoding: chunked
Content-Type: application/xml
```

Sample 2: API Call Blocked (Rate Limit exceeded)

Returned from API call using HTTP authentication.

```
HTTP/1.1 409 Conflict
Date: Fri, 22 Apr 2018 00:13:18 GMT
Server: qweb
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 1
X-RateLimit-ToWait-Sec: 181
X-RateLimit-Remaining: 0
Transfer-Encoding: chunked
Content-Type: application/xml
```

Sample 3: API Call Blocked (Concurrency Limit exceeded)

Returned from API call using API session authentication.

```
HTTP/1.1 409 Conflict
Date: Fri, 22 Apr 2018 00:13:18 GMT
Server: qweb
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 3
Transfer-Encoding: chunked
Content-Type: application/xml
```

In case where the concurrency limit has been reached, no information about rate limits will appear in the HTTP headers.

Sample 4: Tracking API usage through the X-Powered-By HTTP header

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2018 00:13:18 GMT
Server: qweb
   X-Powered-By: Qualys:USPOD1:d9a7e94c-0a9d-c745-82e9-
980877cc5043:f178af1e-4049-7fce-81ca-75584feb8e93
X-RateLimit-Limit: 15
X-RateLimit-Window-Sec: 360
X-Concurrency-Limit-Limit: 3
X-Concurrency-Limit-Running: 1
X-RateLimit-ToWait-Sec: 0
X-RateLimit-Remaining: 4
Transfer-Encoding: chunked
   Content-Type: application/xml
```

Once X-Powered-By HTTP header is enabled, information is returned in the following format:

X-Powered-By Qualys:<POD_ID>:<SUB_UUID>:<USER_UUID>

Where,

POD_ID is the shared POD or a PCP. Shared POD is USPOD1, USPOD2, etc.

SUB_UUID is the unique ID generated for the subscription

USER_UUID is the unique ID generated for the user

For example,

```
X-Powered-By: Qualys:USPOD1:d9a7e94c-0a9d-c745-82e9-
980877cc5043:f178af1e-4049-7fce-81ca-75584feb8e93
```

You can use the USER_UUID to track API usage per user.

Activity Log

You can view the Activity Log using the Qualys user interface and the Activity Log API (/api/2.0/fo/activity_log). The Activity Log shows details about user actions taken.

To view the Activity Log, log into your Qualys account. Go to Users and click the Activity Log tab. Select Filters > Recent API Calls. You'll see the API Processes list showing the API calls subject to the API limits (all APIs except "session" API) made by subscription users and/or updated by the service in the past week.

Tip - You can search the processes list to find API processes. You can search by process state (Queued, Running, Expired, Finished and/or Blocked), by submitted date and by last updated date. You can search for API processes that were blocked due to exceeding the API rate limit and/or the API concurrency limit.

API Life Cycle - EOS/EOL

API Versioning Standards and Deprecation Timelines

Introduction

API versioning is vital for maintaining seamless communication and data exchange between applications during software development. This is a strategic enhancement designed to give you greater control, improved stability, and smoother integration processes.

Need for API Versioning

APIs serve as the backbone of modern software ecosystems, enabling diverse applications to interact with each other and share data seamlessly. However, as platforms evolve, managing changes without disrupting existing systems becomes a challenge.

- API versioning is our strategic response to this challenge, and provides the following benefits:

- Backward compatibility: Existing integrations continue to function without interruption, ensuring operational continuity.

- Transparent updates: New features and improvements are introduced in a controlled, predictable, and transparent manner.

- Choice and flexibility: You can select the API version that best aligns with your operational needs and compatibility requirements.

Deprecation Strategies for Earlier API Endpoints

As part of these strategies, we have come up with End of Support (EOS) and End of Life (EOL) policies for the earlier released APIs, and you will observe this for all earlier and upcoming new endpoints.

EOS and EOL timelines:

For API endpoints supporting versioning standards, customers get an overall 12 months to shift to the latest versions.

End of Support (EOS): Six months after the latest deployment for your respective POD. During this EOS period, new enhancements will not be supported. Any identified bugs will be addressed only. In the API response output, you will notice the EOS timelines for the respective endpoint.

End of Life (EOL): An Additional six months' lead time starting from the EOS timelines is available to switch to the latest versions. During this EOL period, new enhancements will not be supported, and bugs will be addressed in the latest versions. After this lead time, the API endpoint will be decommissioned. In the API response output, you will notice the past due of EOS and the EOL timelines for the respective endpoint.

EOS-EOL Timelines for VM API Endpoints

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Search list	Dynamic Search list API	/api/2.0/fo/qid/search_list/dynamic/index.php	/api/3.0/fo/qid/search_list/dynamic/index.php	August 2026	February 2027
Knowledge Base	Knowledge Base Vulnerability API	/api/2.0/fo/knowledge_base/vuln/index.php	/api/4.0/fo/knowledge_base/vuln/index.php	December 2025	December 2026
		/api/3.0/fo/knowledge_base/vuln/index.php	/api/4.0/fo/knowledge_base/vuln/index.php	August 2025	February 2027
	Knowledge Base QVS API	/api/2.0/fo/knowledge_base/qvs/index.php	/api/3.0/fo/knowledge_base/qvs/index.php	December 2025	December 2026

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Scan	Cloud Internal Scan API	/api/2.0/fo/scan/cloud/internal/job/index.php	/api/3.0/fo/scan/cloud/internal/job/index.php	December 2025	December 2026
	Schedule Scan API	/api/2.0/fo/schedule/scan/index.php	/api/5.0/fo/schedule/scan/index.php	December 2025	December 2026
	Schedule Scan API	/api/3.0/fo/schedule/scan/index.php	/api/5.0/fo/schedule/scan/index.php	December 2025	December 2026
	Schedule Scan API	/api/4.0/fo/schedule/scan/index.php	/api/5.0/fo/schedule/scan/index.php	December 2025	December 2026
	Scan API	/api/2.0/fo/scan/index.php	/api/3.0/fo/scan/index.php	December 2025	December 2026
	Cloud Perimeter Scan API	/api/2.0/fo/scan/cloud/perimeter/job/index.php	/api/4.0/fo/scan/cloud/perimeter/job/index.php	December 2025	December 2026
		/api/3.0/fo/scan/cloud/perimeter/job/index.php	/api/4.0/fo/scan/cloud/perimeter/job/index.php	December 2025	December 2026

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Option Profile	Option Profile API	/api/2.0/fo/subscription/option_profile/index.php	/api/6.0/fo/subscription/option_profile/index.php	December 2025	December 2026
		/api/3.0/fo/subscription/option_profile/index.php	/api/6.0/fo/subscription/option_profile/index.php	December 2025	December 2026
		/api/4.0/fo/subscription/option_profile/index.php	/api/6.0/fo/subscription/option_profile/index.php	December 2025	December 2026
		/api/5.0/fo/subscription/option_profile/index.php	/api/6.0/fo/subscription/option_profile/index.php	July 2025	January 2027
	VM Option Profile API	/api/2.0/fo/subscription/option_profile/vm/index.php	/api/4.0/fo/subscription/option_profile/vm/index.php	December 2025	December 2026
		/api/3.0/fo/subscription/option_profile/vm/index.php	/api/4.0/fo/subscription/option_profile/vm/index.php	December 2025	December 2026

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Asset	Asset Host API	/api/2.0/fo/asset/host/index.php	/api/5.0/fo/asset/host/index.php	December 2025	December 2026
		/api/3.0/fo/asset/host/index.php	/api/5.0/fo/asset/host/index.php	December 2025	December 2026
		/api/4.0/fo/asset/host/index.php	/api/5.0/fo/asset/host/index.php	December 2025	December 2026
	VM Detection API	/api/2.0/fo/asset/host/vm/detection/index.php	/api/5.0/fo/asset/host/vm/detection/index.php	December 2025	June 2027
		/api/3.0/fo/asset/host/vm/detection/index.php	/api/5.0/fo/asset/host/vm/detection/index.php	December 2025	June 2027
		/api/4.0/fo/asset/host/vm/detection/index.php	/api/5.0/fo/asset/host/vm/detection/index.php	December 2025	June 2027
Report	Report Template Scan API	/api/2.0/fo/report/template/scan/index.php	/api/7.0/fo/report/template/scan/index.php	December 2025	December 2026
		/api/3.0/fo/report/template/scan/index.php	/api/7.0/fo/report/template/scan/index.php	December 2025	December 2026
		/api/4.0/fo/report/template/scan/index.php	/api/7.0/fo/report/template/scan/index.php For more information, refer to Scan Template API	December 2025	December 2026
	Report API	/api/2.0/fo/report/index.php	/api/3.0/fo/report/index.php	December 2025	December 2026

EOS-EOL Timelines for PA API Endpoints

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Option Profile	PA Option Profile API	/api/2.0/fo/subscription/option_profile/pc/index.php	/api/5.0/fo/subscription/option_profile/pc/index.php	December 2025	December 2026
		/api/3.0/fo/subscription/option_profile/pc/index.php	/api/5.0/fo/subscription/option_profile/pc/index.php	December 2025	December 2026
		/api/4.0/fo/subscription/option_profile/pc/index.php	/api/5.0/fo/subscription/option_profile/pc/index.php	December 2025	December 2026
Control	Control List	/api/2.0/fo/compliance/control/index.php	/api/4.0/fo/compliance/control/index.php	December 2025	December 2026
		/api/3.0/fo/compliance/control/index.php	/api/4.0/fo/compliance/control/index.php	December 2025	December 2026
Posture	Posture Info	/pcrs/1.0/posture/postureInfo	/pcrs/5.0/posture/postureInfo	November 2026	May 2027
	Resolve Host IDs	/pcrs/1.0/posture/hostids	/pcrs/5.0/posture/hostids	November 2026	May 2027
Exception	Compliance Exception	/api/2.0/fo/compliance/exception/index.php	/api/3.0/fo/compliance/exception/index.php	December 2025	December 2026

Module	Category	API Path	New API Path (Recommended	End of Service (EOS)	End of Life (EOL)
Authentication	MySQL Authentication API	/api/2.0/fo/auth/mysql/index.php	/api/3.0/fo/auth/mysql/index.php	December 2025	December 2026
	Sybase Authentication API	/api/2.0/fo/auth/sybase/index.php	/api/3.0/fo/auth/sybase/index.php	December 2025	December 2026
	Authentication API	/api/2.0/fo/auth/index.php	/api/3.0/fo/auth/index.php	December 2025	December 2026

Authentication to your account

Authentication with valid Qualys account credentials is required for making Qualys API requests to the Qualys API servers. When calling the V2 APIs (i.e. APIs with /2.0/ as URL element), users have the option to choose between session based authentication (using login and logout operations) and basic HTTP authentication (method supported for V1 APIs (i.e. APIs with /msp/ as URL element).

What do I need to know?

Using the API Session Resource

Session Login

Session Logout

Token-based API Authentication Using IdP

What do I need to know?

Here's some things to know about making authenticated API requests to Qualys API servers.

Required Header Parameter

The following header parameter must be included in all API calls using basic HTTP authentication and session based authentication:

```
"X-Requested-With: <user description, like a user agent>"
```

Specifying the required "X-Requested-With" parameter helps to protect Qualys API users from cross-site request forgery (CSRF) attacks.

Using Basic HTTP Authentication

Using this method, Qualys account credentials are transmitted using the "Basic Authentication Scheme" over HTTPS for each API call. For information, see the "Basic Authentication Scheme" section of RFC #2617:

```
http://www.faqs.org/rfcs/rfc2617.html
```

The exact method of implementing authentication will vary according to which programming language is used.

A sample asset/host API request (Curl) using basic HTTP authentication:

```
curl -H "X-Requested-With: Curl Sample" -u "acme_ab12:passwd"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list"
```

Using Session Based Authentication

Using this method, the user makes a sequence of API requests as follows (supported for V2 API calls):

Step 1: Make session login request

Use the Qualys API **session** resource to make a login request. Upon success, the request returns a session ID in the Set-Cookie HTTP header:

```
curl -H "X-Requested-With: Curl Sample" -D headers
-d "action=login&username=acme_ab12&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/session/"
```

Note: When you make the session login request, use an alphanumeric password that must always contain numbers and letters.

Step 2: Make resource requests

Use the API resources to make API requests, as described in this user guide, and include the session ID in the cookie header for each request.

You'll notice the session cookie (QualysSession) was extracted from the "headers" file contents returned from the session login API call (Step 1 above):

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" -d "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Step 3: Make session logout request

Once logged in to Qualys you can make multiple API requests. Use the Qualys API **session** resource to logout of the current session. Logging out of the session closes the open session and ensures secure, ongoing access to your account. Access may be denied if a user makes too many session login requests without closing sessions properly:

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=10b8eb6d4553b4d1ecb860c2b3c247d4; path=/api;
secure" -d "action=logout"
"https://qualysapi.qualys.com/api/2.0/fo/session/"
```

Using the API Session Resource

Sessions created using the Qualys API via the **session** resource are equivalent in every way to sessions created by users logging into the Qualys user interface. Too many open sessions, whether created via the API and/or via user interface login, will lock out new session login attempts from both interfaces (user and API).

The request URL has several elements. The following elements appear in every request URL based on the API V2 architecture.

URL element	Description
qualysapi.qualys.com:443	FQDN of the Qualys API server and option port (443 if specified).
api	Qualys Application component name.
2.0	Qualys API version number.
fo	Qualys interface component name.
session|scan|report or other component name	Qualys API resource name, i.e. session or some other component like scan or report etc.
action={value}	Qualys API resource-specific action. In the sample session login URL above, the action is "login".

Session Login Request

The session login request includes the Qualys user login credentials, the request URL, and the location where the HTTP response headers will be saved.

The sample API call below saves the HTTP headers in a local file named "headers":

```
curl -H "X-Requested-With: Curl Sample" -D headers
-d "action=login&username=acme_ab12&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/session/"
```

If you do not wish to store this information in the "headers" file, you can save the HTTP header in a cookie as shown below:

```
curl -H "X-Requested-With: Curl Sample" -c cookie.txt
-d "action=login&username=acme_ab12&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/session/"
```

Upon success, the sample Qualys API call returns an XML response with the message "Logged in" and the Qualys API session ID in the Set-Cookie HTTP header. See "HTTP Response Headers" for further information.

Resource Requests

When session based authentication is used, the session cookie returned in the XML response from the session login request must be included in the cookie header of subsequent API requests. Multiple API requests can be made using the same session cookie (this is supported using V2 API requests).

The resource request includes the Qualys user login credentials, the Qualys API session ID, the request URL, and the location where the HTTP response headers are saved.

The sample API request below is used to request a list of reports in the user's Report Share storage space. You'll notice the session cookie (QualysSession) was extracted from the "headers" file contents returned from the session login API call.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=list"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

If you saved the HTTP response headers (from the session login request) in a cookie file, make an API request to obtain the cookie from the cookie file as shown below:

```
curl -H "X-Requested-With: Curl Sample"
-d "action=list"
-b "cookie.txt" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Upon success, the sample report list API call returns an XML response listing the reports in the user's Report Share. In progress and completed reports are included.

HTTP Response Headers

These API requests return HTTP response headers: session login requests, session logout requests, and fetch (download) report requests. These requests provide information to the third party application about the XML output.

Sample XML output showing HTML response headers returned from a session logout request:

```
HTTP/1.1 200 OK
Date: Wed, 20 Jun 2007 16:21:03 GMT
Server: qweb/3.3h
Set-Cookie: QualysSession=71e6cda2a35d2cd404cddaf305ea0208;
path=/api; secure
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/xml
```

Sample XML output showing HTML response headers returned from a fetch (download) report request, where the report format is HTML:

```
HTTP/1.1 200 OK
Date: Wed, 20 Jun 2007 16:36:42 GMT
Server: qweb/3.3h
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
Content-Disposition: attachment;
filename=scan_report__1182357402.zip
Content-length: 98280
Connection: close
```

```
Content-Type: application/zip
```

Expires HTTP Header - For the Expires header, Qualys complies with RFC #2109 and sets the Expires date to an old date (a date long in the past). Currently Qualys sets the Expires date to "Mon, 24 Oct 1970 07:30:00 GMT". Note that Qualys cookie expiration is managed on the server side, and Qualys does not rely on clients to drop their expired cookies.

Session Logout Request

A sample session logout request (POST method) is shown below. Upon success, the sample Qualys API call returns an XML response with the message "Logged out".

```
curl -H "X-Requested-With: Curl Sample"
-d "action=logout"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/session/"
```

See "Session Logout" below for further information.

Session Timeout

Every Qualys user account has a session timeout setting. This setting is configurable at the subscription level by Manager users in the Qualys user interface (go to Users > Setup > Security). For a new subscription, this is set to 60 minutes.

The session timeout applies to sessions started using the user interface and sessions started using the Qualys APIs, including APIs based on the new API architecture.

When you launch a scan or report (using Report Share), the task is launched in the background, and processing does not timeout until the task has completed.

Session Login

/api/2.0/fo/session/?action=login

[POST]

Make a request to Qualys API server for session login.

A session login request is used to authenticate to the Qualys API and receive a Qualys API session ID, which must be included in the cookie header of subsequent API resource requests.

Input Parameters

Parameter	Description
action=login	(Required) A flag used to make a session login request.
username	(Required) The user name (login) of a Qualys user account.

Parameter	Description
password	(Required) The password of a Qualys user account. When using -d in the curl request for login, you must URL encode any special characters in the password. For example, if your password is Peas+Carrots then you must specify it as password=Peas%2BCarrots or authentication will not be successful. When using -u in the curl request for login, you can enter the password as is without URL encoding special characters. Using the same example, you'd specify password=Peas+Carrots as part of the request.
echo_request={0|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

A sample session login request (POST method) is shown below. Upon success, the sample Qualys API call returns an XML response with the message "Logged in" and the Qualys API session ID as shown.

```
curl -H "X-Requested-With: Curl Sample" -D headers.4
-d "action=login&username=acme_ab12&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/session/"

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">

<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2007-06-20T16:21:04Z</DATETIME>
    <TEXT>Logged in</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>

cat headers.4

HTTP/1.1 200 OK
Date: Wed, 20 Jun 2007 16:21:03 GMT
Server: qweb/3.3h
Set-Cookie: QualysSession=71e6cda2a35d2cd404cddaf305ea0208;
path=/api; secure
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
```

```
Connection: close
Transfer-Encoding: chunked
Content-Type: text/xml
```

Session Logout

/api/2.0/fo/session/?action=logout

[POST]

Make a request to Qualys API server for session logout.

When you're done making V2 API resource requests, the third party application must make a session logout request. This results in closing the session ID for the user's account, preventing future API requests from running.

Input Parameters

Parameter	Description
action=logout	(Required) A flag used to make a session logout request.
echo_request={0|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

A sample session logout request (POST method) is shown below. Upon success, the sample Qualys API call returns an XML response with the message "Logged out" as shown.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=logout"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/session/"

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2007-06-20T21:50:37Z</DATETIME>
    <TEXT>Logged out</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>

cat headers.18

HTTP/1.1 200 OK
```

```
Date: Wed, 20 Jun 2007 21:50:36 GMT
Server: qweb/3.3h
Expires: Mon, 24 Oct 1970 07:30:00 GMT
Cache-Control: post-check=0,pre-check=0
Pragma: no-cache
Set-Cookie: QualysSession=71e6cda2a35d2cd404cddaf305ea0208;
expires=Wed, 13-Jun-2007 21:50:37 GMT; path=/fo
Connection: close
Transfer-Encoding: chunked
Content-Type: text/xml
```

Token-based API Authentication Using IdP

API Authentication using IdP Provider Tokens

The API Authentication using Identity provider (IdP) tokens adds an extra layer of protection to your APIs. When this method is implemented for API authentication , IdP is used for user authentication and JWT token generation. This document covers onboarding and implementation details of IdP-based API Authentication.

Note: Once you enable IdP-based API authentication, you can use either basic authentication or JWT tokens to access Qualys APIs.

Key Highlights

- Seamless integration of OpenID Connect to enhance API authentication and authorization measures.

- Compatibility with current identity providers and authentication to facilitate a seamless integration experience.

- This authentication is supported by all Qualys APIs, /api/2.0/ and onward versions.

msp API also supports Passwordless (JWT)token authentication.

- Eliminates the need for users to provide a username and password. This streamlines Qualys API access by allowing users to use JWT tokens, bypassing the hassle associated with usernames and passwords.

Enable IdP-based API Authentication

This feature is not available by default. Refer to the Onboarding Process to onboard with IdP-based API authentication.

To set up this feature you must have an IdP.

Important: Along with IdP Provider Tokens, you can use the Qualys Managed Tokens to access Qualys APIs. Refer API Authentication using Qualys Managed Tokens to learn more.

Benefits

Enhanced API security

OpenID Connect (OIDC) uses tokens to establish a user's identity and grant access.

Standardized access control

OpenID Connect (OIDC) provides a standardized way to manage user identities and access control.

Centralized Authentication

By enabling IDP-initiated SSO, users can authenticate once through your organization's Identity Provider (IDP) and gain access to all the necessary APIs without needing to log in again. This simplifies the user experience and reduces password fatigue, making access faster and more secure.

Compliance and Security

Helps to meet compliance requirements by ensuring that user authentication processes adhere to established security protocols like SAML and OIDC.

Onboarding IdP-based Authentication

Prerequisites

To enable OpenID Connect API authentication support, you need to contact Qualys Support. Provide the following information to Qualys Support to get onboarded with IdP-based API authentication:

Certificates/JWKS URL: You can provide the certificates or JWKS URL in one of the following ways:

Share the Certificates Directly - You can directly share the KIDs and corresponding public signing certificates to be used. The certificates must be in X.509 format (typically .pem or .cer files). You can add up to 5 certificates/public keys for OIDC configuration.

OR

Share the JWKS URL - Confirm if your organization plans to rotate certificates, public keys, or key IDs (KIDs) on a regular basis. If so, provide the JWKS (JSON Web Key Set) URL.

This URL hosts an organization's current set of certificates/public keys along with their KIDs. It is usually managed by the IT or Identity team. We will configure this URL in our setup to support IdP-based authentication.

Once configured, Qualys periodically retrieves the latest keys from the JWKS endpoint, helping maintain up-to-date authentication credentials without requiring manual updates.

Prerequisites Audience and Issuer Values or JWT Token: The audience and issuer values are important to set up the IdP-based authentication. You can,

- Provide the audience and issuer values directly,

OR

- Share a JWT token with us, from which we can extract these values and use them to configure certificates for IdP-based authentication.

Share the External ID: The External ID represents the unique identifier assigned to the user by the customer's IdP. This identifier could be an alphanumeric value, an email address, or any unique ID generated by the IdP. This External ID is stored in the Qualys user management system and is mandatory for mapping the JWT token to the correct user, with the correct permissions.

Important:

The External ID can be used for Custom Claim support. Refer to Custom Claim for Token-based Authentication to learn more.

Onboarding Steps

To onboard IdP-based API authentication, complete the following onboarding process:

1. Contact Qualys Support to activate IdP-based API authentication your subscription.

2. Qualys Support requests the necessary technical information to enable IdP-based authentication. See the Prerequisites for details.

3. Once we receive the required technical information, we will enable IdP-based API authentication support.

API Authentication Workflow

Once activated, you can leverage password less authentication for Qualys API using an IdP-provided access token. The following is the basic workflow for IdP-based API authentication.

1. Use the Authentication API to generate the JSON Web Token (JWT) for API access.

2. Use this JWT token in the API requests. Qualys verifies if the correct JWT token is provided or not.

3. Upon successful verification, you are allowed to access the Qualys APIs.

Support for Certificate Rotation

Currently we support certificate, public key, and Key ID (KID) rotation using JWKS URL. If you opt in for certificate rotation, Qualys periodically (every 30 minutes) retrieves the latest certificate, public key, and KID details. This ensures that the authentication is done with the latest credentials.

Enhancement for Certificate Rotation

We have introducesd real-time dynamic JWKS URL rotation. This helps you authenticate using the latest certificates immediately, without waiting for the next scheduled interval for retrieving the authentication credentials.

Generate IdP-based Authentication Token

The following sample illustrates generating JWT tokens required for accessing Qualys APIs.

API Request

```
curl --location '<<token generation url>>' JWT Token
```

```
--header 'Content-Type: application/x-www-form-urlencoded' JWT Token
--data-urlencode 'grant_type=password' JWT Token
--data-urlencode 'username=<<Qualys_okta_sandbox_user_id>>' JWT Token
--data-urlencode 'password=<<Qualys_okta_sandbox_password>>' \
--data-urlencode
'client_id=<<Qualys_okta_sandbox_application_client_id>>' \
--data-urlencode 'scope=openid profile'
```

Note: The token generation URL may vary based on the IdP application you are using. This sample illustrates the request and response for Okta.

API Response

```
{
  "token_type": "Bearer",
  "expires_in": 3600,
  "access_token": "<JWT token value",
  "scope": "profile openid",
  "id_token": "<JWT token value>"
}
```

Access Qualys APIs with Authentication Token

Once the onboarding process is complete and the token-based authentication is enabled, generate a JWT token and use it for accessing Qualys APIs. Learn more about generating a JWT Token.

The following samples illustrate using a JWT token to access the Qualys APIs.

Sample - Execute API using JWT Token

API Request

```
curl --location --request POST 'https://
<qualys_base_url>/api/2.0/fo/asset/ip/?action=add&enable_vm=1&ips=
10.10.10.10&echo_request=1' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer <JWT token value>'\
--header 'X-Requested-With: curl Autodemo' \
--header 'Accept: */*' \
--header 'Content-Length: 0'
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://
<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <REQUEST>
        <DATETIME>2024-11-06T07:32:58Z</DATETIME>
        <USER_LOGIN>username</USER_LOGIN>
        <RESOURCE>https://
```

```
<qualys_base_url>/api/2.0/fo/asset/ip/</RESOURCE>
        <PARAM_LIST>
            <PARAM>
                <KEY>action</KEY>
                <VALUE>add</VALUE>
            </PARAM>
            <PARAM>
                <KEY>enable_vm</KEY>
                <VALUE>1</VALUE>
            </PARAM>
            <PARAM>
                <KEY>ips</KEY>
                <VALUE>10.10.10.10</VALUE>
            </PARAM>
            <PARAM>
                <KEY>echo_request</KEY>
                <VALUE>1</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2024-11-06T07:33:05Z</DATETIME>
        <TEXT>IPs successfully added to Vulnerability
Management</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Scans

Launch and manage vulnerability scans, compliance scans, discovery scans (maps).

VM Scans | Compliance Scans | Cloud Perimeter Scans | Cloud Internal Scans

VM Scan Schedules | PC Scan Schedules

Scan List Parameters | Scan Parameters | Cloud Perimeter Scan Parameters | Azure Internal Scan Parameters | Scan Schedule - Occurrence | Azure and GCP Internal Scan Schedule Parameters

VM Scan Statistics

VM Scan Summary | Scan Summary

Scanner Details

Share PCI Scan

Discovery Scans (maps) | Domain List | Add/Edit Domain

VM Scans

The VM Scan API (/api/2.0/fo/scan/) is used to obtain a list of vulnerability scans in your account and to take actions on them like cancel, pause, resume, and fetch (download) finished results.

Express Lite: This API is available to Express Lite users.

Permissions

User Role	Permissions
Manager	Manage scans on all IPs in the subscription.
Unit Manager	Launch, list and fetch scans on IPs in the user's business unit. And take actions on scans launched by users in the same business unit (cancel, pause, resume and delete)
Scanner	Launch, list and fetch scans on IPs in the user's account. And take actions on scans that the user owns (cancel, pause, resume and delete).
Reader	View scans with targets containing IPs in the user's account. Download scan results when the target includes at least one IP in the user's account.
Auditor	No permissions.

VM Scan List

For API version information, refer to the API Version History section.

V2.0 | V3.0

V2.0

/api/2.0/fo/scan/?action=list

[GET] [POST]

List vulnerability scans in the user's account. By default the XML output lists scans launched in the past 30 days.

Note:

- When the Unit Manager runs the API for the scan list, the count differs from what appears on the Scan List page in the UI (Scans > Scans). This discrepancy occurs due to the in-scope scan list enabled by default in the API and the Show in Scope Scan List option disabled in the VM UI.

- You can generate a scan based report for a paused scan. The scan reports still reflects all data processed prior to the pause

Input Parameters

The input parameters for requesting a VM scan list are shown below. See Scan List Parameters for complete details.

Type	Parameter List
Request	action=list (required), echo_request
Scan List Filters	scan_ref, state, processed, type, target, user_login, launched_after_datetime, launched_before_datetime, scan_type=certview, scan_type=ec2certview, client_id and client_name (only for Consultant type subscriptions)
Show/Hide Information	show_ags, show_op, show_status, show_last, ignore_target

Samples

List all scans in the user account.

API Request:

```
curl --location
'<qualys_base_url>//api/2.0/fo/scan/?action=list&show_ags=1&show_o
p=1' \
--header 'X-Requested-With: badsawewbu' \
--header 'User-Agent: xx_xx/1.0.0 (https://xxxx.com)' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Accept: /' \
--header 'Host: <qualys_base_url>.com:43000' \
--header 'Connection: keep-alive'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/scan/scan_list_output.dtd">
<SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T10:21:25Z</DATETIME>
        <SCAN_LIST>
            <SCAN>
                <REF>scan/1736361211.27337</REF>
                <TYPE>Scheduled</TYPE>
                <TITLE>
                  <![CDATA[Cloud Perimeter Scan 20250106-141228]]>
                </TITLE>
                <USER_LOGIN>vmsp_ag1</USER_LOGIN>
                <LAUNCH_DATETIME>2025-01-
08T18:33:31Z</LAUNCH_DATETIME>
                <DURATION>00:29:43</DURATION>
                <PROCESSING_PRIORITY>0 - No
Priority</PROCESSING_PRIORITY>
                <PROCESSED>1</PROCESSED>
                <STATUS>
                    <STATE>Finished</STATE>
                    <SUB_STATE>No_Vuln</SUB_STATE>
                </STATUS>
                <TARGET>
                    <![CDATA[abc.com]]>
                </TARGET>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
```

```
                    </TITLE>
                    <DEFAULT_FLAG>0</DEFAULT_FLAG>
                </OPTION_PROFILE>
            </SCAN>
        <SCAN_LIST>
    <RESPONSE>
<SCAN_LIST_OUTPUT>
```

List all running scans that were launched by the user with the login ID “acme_ab”:

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/
?action=list&state=Running&user_login=acme_ab"
```

List all scheduled scans that were launched after June 5, 2018.

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/
?action=list&type=Scheduled&launched_after_datetime=2018-06-05"
```

List all scans for AFCO Company client (only for Consultant type subscriptions).

```
curl -u "USERNAME:PASSWORD" -H "content-type:
text/xml""https://qualysapi.qualys.com/api/2.0/fo/scan/?action=lis
t&client_name=AFCO Company"
```

DTD

<platform API server>/api/2.0/fo/scan/scan_list_output.dtd

V3.0

/api/3.0/fo/scan/?action=list

[GET] [POST]

List vulnerability scans in the user’s account. By default the XML output lists scans launched in the past 30 days.

Note:

- When the Unit Manager runs the API for the scan list, the count differs from what appears on the Scan List page in the UI (Scans > Scans). This discrepancy occurs due to the in-scope scan list enabled by default in the API and the Show in Scope Scan List option disabled in the VM UI.

- You can generate a scan based report for a paused scan. The scan reports still reflects all data processed prior to the pause.

Input Parameters

The input parameters for requesting a VM scan list are shown below. See Scan List Parameters for complete details.

Type	Parameter List
Request	action=list (required), echo_request
Scan List Filters	scan_ref, state, processed, type, target, user_login, launched_after_datetime, launched_before_datetime, scan_type=certview, scan_type=ec2certview, client_id and client_name (only for Consultant type subscriptions)
Show/Hide Information	show_ags, show_op, show_status, show_last, ignore_target

Samples

List all scans in the user account.

API Request:

```
curl --location
'<qualys_base_url>//api/3.0/fo/scan/?action=list&show_ags=1&show_o
p=1' \
--header 'X-Requested-With: badsawewbu' \
--header 'User-Agent: xx_xxx/1.0.0 (https://xxxx.com)' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Accept: /' \
--header 'Host: <qualys_base_url>.com:43000' \
--header 'Connection: keep-alive'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/scan/scan_list_output.dtd">
<SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T10:21:25Z</DATETIME>
        <SCAN_LIST>
            <SCAN>
                <REF>scan/1736361211.27337</REF>
                <TYPE>Scheduled</TYPE>
                <TITLE>
                  <![CDATA[Cloud Perimeter Scan 20250106-141228]]>
                </TITLE>
                <USER_LOGIN>vmsp_ag1</USER_LOGIN>
                <LAUNCH_DATETIME>2025-01-
08T18:33:31Z</LAUNCH_DATETIME>
                <DURATION>00:29:43</DURATION>
                <PROCESSING_PRIORITY>0 - No
Priority</PROCESSING_PRIORITY>
                <PROCESSED>1</PROCESSED>
                <STATUS>
                    <STATE>Finished</STATE>
                    <SUB_STATE>No_Vuln</SUB_STATE>
                </STATUS>
                <TARGET>
                    <![CDATA[abc.com]]>
                </TARGET>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
                    </TITLE>
```

```
                    <DEFAULT_FLAG>0</DEFAULT_FLAG>
                </OPTION_PROFILE>
            </SCAN>
        <SCAN_LIST>
    <RESPONSE>
<SCAN_LIST_OUTPUT>
```

List all running scans that were launched by the user with the login ID “acme_ab”:

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/3.0/fo/scan/
?action=list&state=Running&user_login=acme_ab"
```

List all scheduled scans that were launched after June 5, 2018.

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/3.0/fo/scan/
?action=list&type=Scheduled&launched_after_datetime=2018-06-05"
```

List all scans for AFCO Company client (only for Consultant type subscriptions).

```
curl -u "USERNAME:PASSWORD" -H "content-type:
text/xml""https://qualysapi.qualys.com/api/3.0/fo/scan/?action=lis
t&client_name=AFCO Company"
```

Sample - List Azure internal scan

API Request:

```
curl --location '<qualys_base_url>/api/3.0/fo/scan/?action=list' \
--header 'X-Requested-With: badsawewbu' \
--header 'User-Agent: xx_xx/1.0.0 (https://xxxx.com)' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Accept: /' \
--header 'Host: qualys_base_url:43000' \
--header 'Connection: keep-alive'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/scan/scan_list_output.dtd">
<SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-12-09T09:11:17Z</DATETIME>
        <SCAN_LIST>
            <SCAN>
```

```
                <REF>scan/1735543972.16308</REF>
                <TYPE>Scheduled</TYPE>
                <TITLE>
                    <![CDATA[Azure Scan Internal Test]]>
                </TITLE>
                <USER_LOGIN>vmsp_ag1</USER_LOGIN>
                <LAUNCH_DATETIME>2024-12-
30T07:32:52Z</LAUNCH_DATETIME>
                <DURATION>00:00:27</DURATION>
                <PROCESSING_PRIORITY>2 -
Ultimate</PROCESSING_PRIORITY>
                <PROCESSED>1</PROCESSED>
                <STATUS>
                    <STATE>Finished</STATE>
                    <SUB_STATE>No_Host</SUB_STATE>
                </STATUS>
                <TARGET>
                    <![CDATA[65188eb1-02b7-405e-861c-
fb44c98a20d7,cc681b26-8899-4ca8-bedd-b187bdbb8bdb,86c32f80-df08-
4d55-883d-dc1be958b404,4518d470-2c51-4b36-a2f8-
c160b84a3145,b119496c-008c-44cb-845a-928f22368776,e79b48ab-e76d-
4ce0-a2c7-f55cafb8214b,2fad044a-5a20-408d-a24c-
ec82db6b480a,8332f07d-ae8c-4ecf-81b1-b518b9c93b73,06ac9d58-bac5-
452c-b7d9-2bcc6a65f462,ee50296b-bd55-4806-ae44-
a741a8429980,01140268-3adf-48fb-87c3-e7f267ba06b8,7d97c6e6-94c1-
4dfb-834b-1372bed7f460,c24f8498-b2a9-4eb6-90be-
a2a1cce1c8fe,abf4867d-7d9a-49e2-af91-74a0a07ad78e,8040afd7-faae-
48cc-8721-0effdba065d9,806d9fbd-b3c5-47e6-b75d-
af452c85d52c,de9edb26-9fd6-48a9-82bd-0563e6c73c8c,45ecfa8b-5761-
44e3-ba19-7c5a1c5b5fd1,e2ef6795-79ef-45ff-a6d2-
c6f23498578c,81deef30-3247-4617-8539-98ff74b4b809,86258819-4965-
406b-87b7-c171dfa27740,8debc341-ddfc-4ceb-a505-
293092ee0235,3a6121a9-52ff-4c9a-a4cb-c998f8e1128b,8a1feb05-6bd1-
447b-9d81-a9df8d08fc6a,da029994-08ed-4fe9-9d18-
730e52668724,46cdd666-ed4d-4caa-a4f8-dc0de9840e33,a6b86d01-86d4-
4e33-9966-6223c6f26577,cbaeb49d-a885-4fc1-ac19-
fe65bcc92e58,ba47a438-a5ef-4487-a457-00624bd98fe7,0ad0ef2b-e4bd-
462b-be2e-9d363f03c8a4,209e9fad-455d-4755-b884-
87f538daa76d,2019b43a-155f-49b8-bf43-52092b87a6ab,1523ecc7-fb13-
4320-99c8-09800730fec9,57b01662-8754-4764-842f-
c9ce982924c6,c6419606-a6f0-4340-84f3-1be040384a54,3ee18bbf-54cf-
4466-9c51-08cde3f43b1a,a24ab800-6752-440e-b15f-
f8d652f56325,e60ab9f6-45f7-47d3-aeee-f2f6848a9137,8cc39bd5-42ef-
4cfc-a671-446228bdcd56,c97a9971-a52a-48fa-a202-
af3c2f76b623,aa887200-c6a9-435b-91bd-4fd8aa7b3166]]>
                </TARGET>
            </SCAN>
        </SCAN_LIST>
```

```
    </RESPONSE>
</SCAN_LIST_OUTPUT>
```

Sample - To fetch a specific launched Azure internal scan

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/scan/index.php?action=fetch&scan_ref
=scan%2F1725961482.79886&output_format=json' \
--header 'X-Requested-With: badsawewbu' \
--header 'User-Agent: xx_xx/1.0.0 (https://xxxx.com)' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Accept: /' \
--header 'Host: <qualys_base_url>:43000' \
--header 'Connection: keep-alive'
```

JSON Output:

```
[{&quot;ip&quot;:&quot;11.11.1.11&quot;,&quot;dns&quot;:&quot;27f8
6f78-8dc2-4093-abed-
1ce3b648c241&quot;,&quot;netbios&quot;:null,&quot;qid&quot;:38711,
&quot;instance&quot;:null,&quot;result&quot;:&quot;Hops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMPHops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMP&quot;},
{&quot;ip&quot;:&quot;11.11.1.11&quot;,&quot;dns&quot;:&quot;27f86
f78-8dc2-4093-abed-
1ce3b648c241&quot;,&quot;netbios&quot;:null,&quot;qid&quot;:14013,
&quot;instance&quot;:null,&quot;result&quot;:&quot;Port\tIANA
Assigned Ports\/Services\tDescription\tService
Detected\n111\tsunrpc\tSUN Remote Procedure Call\trpc
udp\n2049\tshilp\tshilp\tnfsPort\tIANA Assigned
Ports\/Services\tDescription\tService Detected\n111\tsunrpc\tSUN
Remote
Procedure Call\trpc udp\n2049\tshilp\tshilp\tnfs&quot;},
{&quot;ip&quot;:&quot;11.11.1.11&quot;,&quot;dns&quot;:&quot;27f86
f78-8dc2-4093-abed-
1ce3b648c241&quot;,&quot;netbios&quot;:null,&quot;qid&quot;:20220,
&quot;instance&quot;:null,&quot;result&quot;:&quot;Hops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMPHops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMP&quot;},
```

{"ip":"11.11.1.11","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":45266,
"instance":null,"result":"Port\tIANA
Assigned Ports\/Services\tDescription\tService
Detected\n111\tsunrpc\tSUN Remote Procedure Call\trpc
udp\n2049\tshilp\tshilp\tnfsPort\tIANA Assigned
Ports\/Services\tDescription\tService Detected\n111\tsunrpc\tSUN
Remote
Procedure Call\trpc udp\n2049\tshilp\tshilp\tnfs"},
{"ip":"11.11.1.11","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":48074,
"instance":null,"result":"Hops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t10.14.9.80\t1.91ms\tICMPHops\tIP\tRound
Trip
Time\tProbe\n1\t10.40.1.2\t0.19ms\tICMP\n2\t10.10.0.10\t0.26ms\tIC
MP\n3\t10.14.9.80\t1.91ms\tICMP"},
{"ip":"10.14.9.80","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":45268,
"instance":null,"result":"Hops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMPHops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t11.11.1.11\t1.91ms\tICMP"},
{"ip":"11.11.1.11","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":45304,
"instance":null,"result":""},
{"ip":"11.11.1.11","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":242738
,"instance":null,"result":"Hops\tIP\tRoun
d
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI
CMP\n3\t10.6.1.36\t1.91ms\tICMP"},
{"ip":"11.11.1.11","dns":"27f86
f78-8dc2-4093-abed-
1ce3b648c241","netbios":null,"qid":45376,
"instance":null,"result":"Hops\tIP\tRound
Trip
Time\tProbe\n1\t11.11.1.11\t0.19ms\tICMP\n2\t11.11.1.11\t0.26ms\tI

```
CMP\n3\t11.11.1.11\t1.91ms\tICMP&quot;}]
```

DTD

<platform API server>/api/3.0/fo/scan/scan_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/scan/?action=list	Active	Active
/api/2.0/fo/scan/?action=list	December 2025	December 2026

List Last 'N' Scan References for a Schedule

api/2.0/fo/scan/schedules/runhistory/?action=list

[GET]

Provides a list of the most recent "N" scan references associated with a particular schedule ID, allowing you to monitor and track automated scans initiated for that schedule.

Note: This API does not work for MAP schedule scan ids.

Input Parameters

Parameter	Description
action=list	(Required)
schedule_scan_ids	(Required) Specify schedule ids in a comma-separated list. Maximum 500 schedule ids are supported.
output_format	(Optional) Specify output file format. Default value is "xml" format. Supported values are "xml" & "json".
schedule_executions_count	(Optional) Specify a schedule execution count. You can specify a value form 1 to 50. When not specified, 3 is taken as the default.

Sample

List the last 'n' scan references for the given schedule IDs.

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/scan/schedules/runhistory/?action=li
st&output_format=xml&schedule_executions_count=4&schedule_scan_ids
=99446%2C85403%2C144180%2C144181%2C6666%2C657657%2C125485' \
--header 'X-Requested-With: test' \
```

```
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE SCHEDULES_RUN_HISTORY SYSTEM
"<platform_API_server>/api/2.0/fo/scan/schedules/runhistory/output
.dtd">
<SCHEDULES_RUN_HISTORY>
   <RESPONSE>
      <DATETIME>2023-01-09T14:57:51Z</DATETIME>
      <SCHEDULE_LIST>
         <SCHEDULE id="85403">
            <SCHEDULE_ID>85403</SCHEDULE_ID>
            <SCHEDULE_RUN_HISTORY>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99408</SCAN_ID>

<SCAN_REFERENCE>scan/1634824016.99408</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-21
13:46:56</LAUNCH_DATETIME>
                     <TITLE>test9090</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>86 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
            </SCHEDULE_RUN_HISTORY>
         </SCHEDULE>
         <SCHEDULE id="99446">
            <SCHEDULE_ID>99446</SCHEDULE_ID>
            <SCHEDULE_RUN_HISTORY>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99561</SCAN_ID>

<SCAN_REFERENCE>scan/1635442781.99561</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
17:39:41</LAUNCH_DATETIME>
                     <TITLE>test_555</TITLE>
```

```
                     <TARGET>list of target ips</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>434 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99554</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99554</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                     <TITLE>test_898</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>9 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99553</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99553</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                     <TITLE>test9090</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>79 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
```

```
            </SCHEDULE_RUN_HISTORY>
          </SCHEDULE>
        </SCHEDULE_LIST>
      </RESPONSE>
    </SCHEDULES_RUN_HISTORY>
```

DTD

<platform_API_server>/api/2.0/fo/scan/schedules/runhistory/output.dtd

Launch VM Scan

/api/2.0/fo/scan/?action=launch

[POST]

Launch vulnerability scan in the user's account.

Good to Know

- The Launch Scan API is asynchronous. When you make a request to launch a scan using this API, the service will return a scan reference ID right away and the call will quit without waiting for the complete scan results.

- When you launch a VM scan using the API, we check to see if the IPs in the scan target are available to the user making the scan request. To determine this, we check that each IP is in the subscription, in the VM license, and in the user's assigned scope. If any IP in the target is not available to the user, then it will be skipped from the scan job.

For example, let's say you specify the IP range 10.10.10.100-10.10.10.120, but IPs 10.10.10.115 and 10.10.10.120 are not available to you. In this case, we will launch the scan on 10.10.10.100-10.10.10.114, 10.10.10.116-10.10.10.119, and we'll skip 10.10.10.115 and 10.10.10.120.

- Using networks? Choose the Global Default Network to scan IPs on your network perimeter.

- A validation message displays during scan launch from both the VM and PCI portals. If the asset group or FQDN contains DNS entries exceeding 4000 characters, users are notified before the scan is initiated. This proactive check prevents scan sharing failures and improves user experience.

Input Parameters

The input parameters for launching a VM scan are shown below. See Scan Parameters for complete details.

Type	Parameter List
Request	action=launch (required), echo_request, runtime_http_header
Scan Title	scan_title

Type	Parameter List
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id or iscanner_name, ec2_instance_ids
Processing Priority	priority
Asset IPs/Groups	ip, asset_group_ids, asset_groups, exclude_ip_per_scan, default_scanner, scanners_in_ag
Asset Tags	target_from=tags, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include
Network	ip_network_id (when the Network Support feature is enabled)
Client	client_id and client_name (only for Consultant type subscriptions)

Sample - Launch scan on IP address

API request:

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -X "POST"
-d
"action=launch&scan_title=My+Vulnerability+Scan&ip=10.10.10.10&opt
ion_id=43165&iscanner_name=scanner1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/" > outputfile.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2013-01-15T21:32:40Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1358285558.36992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch Scan Samples

API request (FQDN only):

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWD" -X "POST" -d
"action=launch&option_title=Initial+Options&fqdn=domain.qualys.com
&iscanner_name=scanner_us"
"https://qualysapi.qualys.com/api/2.0/fo/scan/" > outputfile.txt
```

API request (FQDN and asset group):

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWD" -X "POST" -d
"action=launch&option_title=Initial+Options&fqdn=domain.qualys.com
&iscanner_name=scanner_us&scan_title=My+Scan&asset_groups=My+AG"
"https://qualysapi.qualys.com/api/2.0/fo/scan/" > outputfile.txt
```

Sample - Launch scan using asset tags

API request:

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWD" -X "POST" -d
"action=launch&scan_title=My+Vulnerability+Scan&target_from=tags&t
ag_set_by=name&tag_set_include=Windows&option_id=43165&iscanner_na
me=scanner1" "https://qualysapi.qualys.com/api/2.0/fo/scan/" >
file.txt
```

Sample - Launch scan using All Scanners in Network

API request:

```
curl -u "username:password" -H "X-Requested-With:curl demo" -d
"action=launch&scan_title=scan3&option_title=Initial+Options&ip_ne
twork_id=12807913&scanners_in_network=1&asset_groups=AG1-GDN"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Launch VM Scan on EC2 assets

/api/2.0/fo/scan/?action=launch

[POST]

Launch vulnerability scan on your Amazon EC2 hosts (in your Amazon Web Services account).

A few things to consider...

- EC2 Scanning must be enabled for your Qualys account.

- Managers and Unit Managers can launch EC2 scans.

- Before scanning you'll need to complete some set up steps. See Securing Amazon Web Services with Qualys

Input Parameters

The input parameters for launching an EC2 scan are shown below. See Scan Parameters for complete details.

Type	Parameter List
Request	action=launch (required), echo_request
Scan Title	scan_title
EC2 environment	connector_name (required), ec2_endpoint (required)
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id or iscanner_name
Processing Priority	priority
Target Hosts Note: You can use either ec2_instance_ids or tags parameter or both	target_from=tags Use tags to select the EC2 hosts you want to scan.
	These parameters provide separate options for including and excluding tags for network IP ranges. use_ip_nt_range_tags_include={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning. use_ip_nt_range_tags_exclude={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning. This parameter has been replaced with the include/exclude options above but it is still supported. use_ip_nt_range_tags={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning.
	These tag parameters are used to select tags: tag_set_include={tag1,tag2,...} (required) tag_set_exclude={tag1,tag2,...} (optional) tag_include_selector={**any**|all} (default in bold) tag_exclude_selector={**any**|all} (default in bold) tag_set_by={**id**|name} (default in bold)
	ec2_instance_ids={value} The ID of the target EC2 instance to launch the VM or compliance scan. Multiple ec2 instance ids are comma separated. You can add up to maximum 10 instance Ids.

Sample - Launch EC2 Vulnerability scan

Launch an EC2 vulnerability scan using the connector "EC2_Connector" on assets that match tags with IDs 1558997 and 1559222.

API request:

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWD" -X "POST" -d
"action=launch&scan_title=My+EC2+Scan&connector_name=EC2_Connector
&ec2_endpoint=us-east-1&target_from=tags&use_ip_nt_range_tags=0
&tag_include_selector=any&tag_set_by=id&tag_set_include=1558997,15
59222&option_id=43165&iscanner_name=EC2-1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/" > outputfile.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-02-25T21:32:40Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1358285558.36992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch EC2 Vulnerability scan for EC2 instance

Launch a VM scan on EC2 instances using the parameter ec2_instance_ids.

This sample is for a vulnerability scan with a mix of valid and invalid instance IDs. The scan is launched on the valid instance IDs and the invalid instance IDs are listed in the output with the reasons they were considered invalid. Some did not belong to the EC2 environment and some were not activated for VM.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample2&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-
01f234ce567ae890f,i-
0be12cb3da4567e8a,i-0d1f23d4ba5c67e8b,i-0123e456f7890f123,i-
012f3ceb4a5d6789d,i-0c123e4f567890123,i-012345a67bba89012,i-
01ba23a45cba678af,i-012345678dfc90efe,i-0ab12e3456baadeb7"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/dtd/launch_output.dt
d">
```

```
<SIMPLE_RETURN>
<RESPONSE>
<DATETIME>2021-11-19T09:13:21Z</DATETIME>
<TEXT>New vm scan launched</TEXT>
<NOTIFICATION>The following instances were skipped because they do
not belong to the selected EC2 environment: i-012f3ceb4a5d6789d,i-
0c123e4f567890123, i-012345a67bba89012. The following instances
were skipped because they are not activated for VM: i-
01ba23a45cba678af, i-012345678dfc90efe, i-
0ab12e3456baadeb7.</NOTIFICATION>
<ITEM_LIST>
<ITEM>
<KEY>ID</KEY>
<VALUE>1140800</VALUE>
</ITEM>
<ITEM>
<KEY>REFERENCE</KEY>
<VALUE>scan/1637313199.40800</VALUE>
</ITEM>
</ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

Manage VM Scans

/api/2.0/fo/scan/?action={action}

Take actions on vulnerability scans in their account, like cancel, pause, resume, delete and fetch completed scan results.

Parameter	Description
action={action}	(Required) One action required for the request: cancel - Stop a scan in progress (POST method) pause - Stop a scan in progress and change status to “Paused” (POST method) resume - Restart a scan that has been paused (POST method) delete - Delete a scan in your account (POST method) fetch - Download scan results for a scan with status of “Finished”, “Canceled”, “Paused” or “Error” (GET or POST method)
echo_request={**0**|1}	(Optional) Specify 1 to echo the input parameters in the XML output. When unspecified, parameters are not listed in the XML output.
scan_ref={value}	(Required) The scan reference for a vulnerability scan. This will have the format: scan/nnnnnnnnnn.nnnnn

Input Parameters

Parameter	Description
action={action}	(Required) An action for the request: cancel - stop a scan in progress, “Running” or “Paused” pause - stop a scan in progress and change status to “Paused” resume - restart a scan that has been paused fetch - download scan results for a scan with the status “Finished”, “Canceled”, “Paused” or “Error”.
echo_request={**0**|1}	(Optional) Specifies whether to echo the request’s input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
scan_ref={value}	(Required) Specifies a scan reference. A scan reference has the format “scan/987659876.19876”.
ips={value}	(Optional for a fetch request) Show only certain IP addresses/ranges in the scan results. One or more IPs/ranges may be specified. A range entry is specified using a hyphen (for example, 10.10.10.1-10.10.10.20). Multiple entries are comma separated.
mode={**brief**|extended}	(Optional for fetch request) The verbosity of the scan results details: brief (the default) or extended. The brief output includes this information: IP address, DNS hostname, NetBIOS hostname, QID and scan test results if applicable. The extended output includes the brief output plus this extended information: protocol, port, an SSL flag (“yes” is returned when SSL was used for the detection, “no” is returned when SSL was not used), and FQDN if applicable.
output_format={**csv**|json| csv_extended| json_extended}	(Optional for fetch request) The output format of the vulnerability scan results. A valid value is: csv (the default), json (for JavaScript Object Notation(), csv_extended, json_extended. Click here for information on Scan Results JSON
client_id={value}	(Optional for fetch request) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional for fetch request) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.

Samples - Take actions on scans

Cancel a scan (POST method) is shown below.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=cancel&scan_ref=234234234.12345"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Pause a scan (POST method) is shown below.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=pause&scan_ref=234234234.12345"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Resume a scan (POST method) is shown below.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=resume&scan_ref=234234234.12345"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Fetch/download a scan result is shown below.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=fetch&scan_ref=234234234.12345"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Compliance Scans

The Compliance Scan API (/api/2.0/fo/scan/compliance/) is used to launch compliance scans, get a list of compliance scans in your account and manage them. The SCAP Scan API (/api/2.0/fo/scan/scap/) is used to get a list of SCAP scans in your account.

Permissions

Note: The Compliance Scan APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Role-based user permissions are described below.

User Role	Permissions
Manager	Manage compliance scans on all compliance IPs in the subscription.
Unit Manager	When the "Manage compliance" permission is enabled in the user's account settings: 1) ability to launch, list and fetch compliance scans on IPs in the user's business unit, 2) ability to take actions on scans launched by users in the same business unit (cancel, pause, resume and delete).
Scanner	When the "Manage compliance" permission is enabled in the user's account settings: 1) ability to launch, list and fetch compliance scans on IPs in the user's account, 2) ability to take actions on scans that the user owns (cancel, pause, resume and delete).
Reader	No permissions to manage compliance scans.
Auditor	No permissions to manage compliance scans.

Compliance Scan List

/api/2.0/fo/scan/compliance/ with action=list

[GET] [POST]

List of compliance scans in your account. By default the XML output lists scans launched in the past 30 days.

The input parameters for requesting a PC scan list are below. See Scan List Parameters for complete details.

Type	Parameter List
Request	action=list (required), echo_request
Scan List Filters	scan_id (compliance scan ID), scan_ref, state, processed, type, target, user_login, launched_after_datetime, launched_before_datetime, client_id and client_name (only for Consultant type subscriptions)
Show Information	show_ags, show_op, show_status, show_last

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=list&state=Finished&scan_ref=compliance/1344842952.1340"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd
">
<SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-12T07:28:46Z</DATETIME>
    <SCAN_LIST>
      <SCAN>
        <ID>3332486</ID>
        <REF>compliance/1344842952.1340</REF>
        <TYPE>Scheduled</TYPE>
        <TITLE><![CDATA[MY PC Scan]]></TITLE>
        <USER_LOGIN>USERNAME</USER_LOGIN>
        <LAUNCH_DATETIME>2018-05-13T07:30:09Z</LAUNCH_DATETIME>
        <DURATION>00:06:29</DURATION>
        <PROCESSED>1</PROCESSED>
        <STATUS>
          <STATE>Finished</STATE>
```

```
            </STATUS>
            <TARGET><![CDATA[10.10.25.50]]></TARGET>
          </SCAN>
        </SCAN_LIST>
      </RESPONSE>
    </SCAN_LIST_OUTPUT>
```

DTD:

<platform API server>/api/2.0/fo/scan/scan_list_output.dtd

List Last 'N' Scan References for a Schedule

api/2.0/fo/scan/schedules/runhistory/?action=list

[GET]

Provides a list of the most recent "N" scan references associated with a particular schedule ID, allowing you to monitor and track automated scans initiated for that schedule.

Note: This API does not work for MAP schedule scan ids.

Input Parameters

Parameter	Description
action=list	(Required)
schedule_scan_ids	(Required) Specify schedule ids in a comma-separated list. Maximum 500 schedule ids are supported.
output_format	(Optional) Specify output file format. Default value is "xml" format. Supported values are "xml" & "json".
schedule_executions_count	(Optional) Specify a schedule execution count. You can specify a value form 1 to 50. When not specified, 3 is taken as the default.

Sample

List the last 'n' scan references for the given schedule IDs.

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/scan/schedules/runhistory/?action=li
st&output_format=xml&schedule_executions_count=4&schedule_scan_ids
=99446%2C85403%2C144180%2C144181%2C6666%2C657657%2C125485' \
--header 'X-Requested-With: test' \
--header 'Authorization: Basic <token>'
```

API request:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE SCHEDULES_RUN_HISTORY SYSTEM
"<platform_API_server>/api/2.0/fo/scan/schedules/runhistory/output
.dtd">
<SCHEDULES_RUN_HISTORY>
   <RESPONSE>
      <DATETIME>2023-01-09T14:57:51Z</DATETIME>
      <SCHEDULE_LIST>
         <SCHEDULE id="85403">
            <SCHEDULE_ID>85403</SCHEDULE_ID>
            <SCHEDULE_RUN_HISTORY>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99408</SCAN_ID>

<SCAN_REFERENCE>scan/1634824016.99408</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-21
13:46:56</LAUNCH_DATETIME>
                     <TITLE>test9090</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>86 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
            </SCHEDULE_RUN_HISTORY>
         </SCHEDULE>
         <SCHEDULE id="99446">
            <SCHEDULE_ID>99446</SCHEDULE_ID>
            <SCHEDULE_RUN_HISTORY>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99561</SCAN_ID>

<SCAN_REFERENCE>scan/1635442781.99561</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
17:39:41</LAUNCH_DATETIME>
                     <TITLE>test_555</TITLE>
                     <TARGET>list of target ips</TARGET>
                     <STATUS>FINISHED</STATUS>
```

```
                     <DURATION>434 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99554</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99554</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                     <TITLE>test_898</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>9 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
               <SCHEDULE_RUN>
                  <SCAN_LAUNCH_INFO>
                     <SCAN_ID>99553</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99553</SCAN_REFERENCE>
                     <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                     <TITLE>test9090</TITLE>
                     <TARGET>10.20.30.40</TARGET>
                     <STATUS>FINISHED</STATUS>
                     <DURATION>79 Seconds</DURATION>
                     <NBHOST>0</NBHOST>
                     <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                     <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                     <IS_PROCESSED>1</IS_PROCESSED>
                  </SCAN_LAUNCH_INFO>
               </SCHEDULE_RUN>
            </SCHEDULE_RUN_HISTORY>
         </SCHEDULE>
```

```
        </SCHEDULE_LIST>
    </RESPONSE>
</SCHEDULES_RUN_HISTORY>
```

DTD

<platform_API_server>/api/2.0/fo/scan/schedules/runhistory/output.dtd

SCAP Scan List

/api/2.0/fo/scan/scap/ with action=list

[GET] [POST]

List SCAP scans in your account. By default the XML output lists scans launched in the past 30 days.

The input parameters for requesting a SCAP scan list are below. See Scan List Parameters for complete details.

Type	Parameter List
Request	action=list (required), echo_request
Scan List Filters	scan_id (compliance scan ID), scan_ref, state, type, target, user_login, launched_after_datetime, launched_before_datetime
Show Information	show_ags, show_op, show_status, show_last

API request 1: all SCAP scans

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/scan/scap/"
```

API request 2: SCAP scan by reference number

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&scan_ref=qscap/1402642816.80342"
"https://qualysapi.qualys.com/api/2.0/fo/scan/scap/"
```

API request 3: On Demand SCAP scans only

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&type=On-Demand"
"https://qualysapi.qualys.com/api/2.0/fo/scan/scap/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scap/qscap_scan_list
_output.dtd">
<SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-13T22:56:19Z</DATETIME>
    <SCAN_LIST>
      <SCAN>
        <ID>6980366</ID>
        <REF>qscap/1402694682.80366</REF>
        <TYPE>On-Demand</TYPE>
        <TITLE><![CDATA[<IMG
SRC="http://www.google.com/images/logos/ps_logo2.png">]]></TITLE>
        <POLICY>
          <ID>39298</ID>
          <TITLE><![CDATA[Policy A]]></TITLE>
        </POLICY>
        <USER_LOGIN>acme_ab</USER_LOGIN>
        <LAUNCH_DATETIME>2018-06-13T21:24:42Z</LAUNCH_DATETIME>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <TARGET><![CDATA[10.10.30.244, 10.10.34.222]]></TARGET>
...
    </SCAN_LIST>
  </RESPONSE>
</SCAN_LIST_OUTPUT>
```

DTD:

<platform API server>/api/2.0/fo/scan/qscap_scan_list_output.dtd

Launch Compliance Scan

/api/2.0/fo/scan/compliance/?action=launch

[POST]

Launch compliance scan in the user's account.

Using networks? Choose the Global Default Network to scan IPs on your network perimeter.

Input Parameters

The input parameters for launching a compliance scan are shown below. See Securing Amazon Web Services with Qualys

Type	Parameter List
Request	action=launch (required), echo_request, runtime_http_header
Scan Title	scan_title
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id or iscanner_name
Asset IPs/Groups	ip, asset_group_ids, asset_groups, exclude_ip_per_scan, default_scanner, scanners_in_ag
Asset Tags	target_from=tags, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include
Network	ip_network_id (when the Network Support feature is enabled)
Client	client_id and client_name (only for Consultant type subscriptions)

Sample - Launch a Compliance Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=launch&ip=10.10.25.52&iscanner_name=iscan_er5&option_title
=Initial+PC+Options&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/" >
apiOutputScan.txt
```

Sample - Launch a compliance scan using all scanners in network

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo 2" -d
"action=launch&scan_title=pc+scan+API&option_id=3262&ip_network_id
=12807913&scanners_in_network=1&ip=10.10.10.10,10.10.10.11"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-15T21:55:36Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>18198</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1473976536.18198</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Launch Compliance Scan on EC2 assets

/api/2.0/fo/scan/compliance/?action=launch

[POST]

Launch a compliance scan on your Amazon EC2 hosts (in your Amazon Web Services account).

A few things to consider...

- EC2 Scanning must be enabled for your Qualys account.

- Managers and Unit Managers can launch EC2 scans.

- Before scanning you'll need to complete some set up steps. See Securing Amazon Web Services with Qualys

Input Parameters

The input parameters for launching an EC2 scan are shown below. Please see Scan Parameters for complete details.

Type	Parameter List
Request	action=launch (required), echo_request
Scan Title	scan_title
EC2 environment	connector_name (required), ec2_endpoint (required)
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id or iscanner_name
Target Hosts	target_from=tags (required) Use tags to select the EC2 hosts you want to scan.
	These parameters provide separate options for including and excluding tags for network IP ranges. use_ip_nt_range_tags_include={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning. use_ip_nt_range_tags_exclude={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning. This parameter has been replaced with the include/exclude options above but it is still supported. use_ip_nt_range_tags={**0**|1} (default in bold) Important - This cannot be set to "1" for EC2 scanning.
	These tag parameters are used to select tags: tag_set_include={tag1,tag2,...} (required) tag_set_exclude={tag1,tag2,...} (optional) tag_include_selector={**any**|all} (default in bold) tag_exclude_selector={**any**|all} (default in bold) tag_set_by={**id**|name} (default in bold)

Sample - Launch EC2 compliance scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=launch&scan_title=My+EC2+Scan+via+API&connector_name=EC2-
Connector-Lab&ec2_endpoint=us-east-
1&target_from=tags&tag_include_selector=any&tag_set_by=id&tag_set_
include=270325&option_id=61769&iscanner_name=my-ec2-scanner"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
```

```
  <REQUEST>
    <DATETIME>2018-06-24T10:10:51Z</DATETIME>
    <USER_LOGIN>USERNAME</USER_LOGIN>
<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/
</RESOURCE>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2018-06-24T10:10:57Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2222345</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1347771234.36444</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Manage Compliance Scans

/api/2.0/fo/scan/compliance/?action={action}

Take actions on compliance scans in their account, like cancel, pause, resume, delete and fetch completed scan results.

Parameter	Description
action={action}	(Required) One action required for the request: cancel - Stop a scan in progress (POST method) pause - Stop a scan in progress and change status to "Paused" (POST method) resume - Restart a scan that has been paused (POST method) delete - Delete a scan in your account (POST method) fetch - Download scan results for a scan with status of "Finished", "Canceled", "Paused" or "Error" (GET or POST method)
echo_request={**0**|1}	(Optional) Specify 1 to echo the input parameters in the XML output. When unspecified, parameters are not listed in the XML output.
scan_ref={value}	(Required) The scan reference for a compliance scan. This will have the format: compliance/nnnnnnnnnn.nnnnn

Sample - Fetch PC Scan Results

API request:

```
curl -u USERNAME:PASSWORD -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/?
action=fetch&scan_ref=compliance/1347709693.37303" >
apiOutputScanFetch.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCAN_RESULT_OUTPUT SYSTEM

"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/complianc
e_scan_result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-17T10:23:53Z</DATETIME>
    <COMPLIANCE_SCAN>
      <HEADER>
        <NAME><![CDATA[Compliance Scan Results]]></NAME>
        <GENERATION_DATETIME>2012-09-
17T10:23:53Z</GENERATION_DATETIME>
        <COMPANY_INFO>
          <NAME><![CDATA[Qualys]]></NAME>
          <ADDRESS><![CDATA[1600 Bridge Parkway]]></ADDRESS>
          <CITY><![CDATA[Redwood Shores]]></CITY>
          <STATE><![CDATA[California]]></STATE>
          <COUNTRY><![CDATA[United States]]></COUNTRY>
          <ZIP_CODE><![CDATA[94065]]></ZIP_CODE>
        </COMPANY_INFO>
        <USER_INFO>
          <NAME><![CDATA[NAME]]></NAME>
          <USERNAME>USERNAME</USERNAME>
          <ROLE>Manager</ROLE>
        </USER_INFO>
        <KEY value="USERNAME">USERNAME</KEY>
        <KEY value="COMPANY"><![CDATA[Qualys]]></KEY>
        <KEY value="DATE">2018-06-15T11:49:08Z</KEY>
        <KEY value="TITLE"><![CDATA[My PC Scan]]></KEY>
        <KEY value="TARGET">10.10.10.29</KEY>
        <KEY value="EXCLUDED_TARGET"><![CDATA[N/A]]></KEY>
        <KEY value="DURATION">00:01:00</KEY>
        <KEY value="SCAN_HOST">10.10.21.122 (Scanner 6.6.28-1,
Vulnerability Signatures 2.2.215-2)</KEY>
        <KEY value="NBHOST_ALIVE">1</KEY>
        <KEY value="NBHOST_TOTAL">1</KEY>
```

```
        <KEY value="REPORT_TYPE">Scheduled</KEY>
        <KEY value="OPTIONS">File Integrity Monitoring: Enabled,
Scanned Ports: Standard Scan, Hosts to Scan in Parallel - External
Scanners: 15, Hosts to Scan in Parallel - Scanner Appliances: 30,
Total Processes to Run in Parallel: 10, HTTP Processes to Run in
Parallel: 10,

Packet (Burst) Delay: Medium, Intensity: Normal, Overall
Performance: Normal, ICMP Host Discovery, Ignore RST packets: Off,
Ignore firewall-generated SYN-ACK packets: Off, Do not send ACK or
SYN-ACK packets during host discovery: Off</KEY>
        <KEY value="STATUS">FINISHED</KEY>
        <OPTION_PROFILE>
          <OPTION_PROFILE_TITLE
option_profile_default="0"><![CDATA[11412]]
></OPTION_PROFILE_TITLE>
        </OPTION_PROFILE>
      </HEADER>
      <APPENDIX>
        <TARGET_HOSTS>
          <HOSTS_SCANNED>10.10.10.29</HOSTS_SCANNED>
        </TARGET_HOSTS>
        <TARGET_DISTRIBUTION>
          <SCANNER>
            <NAME><![CDATA[iscan_sx]]></NAME>
            <HOSTS>10.10.10.29</HOSTS>
          </SCANNER>
        </TARGET_DISTRIBUTION>
        <AUTHENTICATION>
          <AUTH>
            <TYPE>Windows</TYPE>
            <SUCCESS>
              <IP>10.10.10.29</IP>
            </SUCCESS>
          </AUTH>
        </AUTHENTICATION>
      </APPENDIX>
    </COMPLIANCE_SCAN>
  </RESPONSE>
</COMPLIANCE_SCAN_RESULT_OUTPUT>
```

Cloud Perimeter Scans

For API version information, refer to the API Version History section.

V2.0 | V3.0 | V4.0

V2.0

/api/2.0/fo/scan/cloud/perimeter/job/

[POST]

Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

The input parameters for requesting a Cloud Perimeter scan are below. See Cloud Perimeter Scan Parameters for complete details.

Type	Parameter List
Request	action={create|update}
Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, scanner_id, iscanner_name, platform_type, region_code, vpc_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, elb_dns, schedule

Create/Update Cloud Perimeter Scan

We allow you to create/update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&tag_set_by=name&tag_include_selector=any&tag_set_include=e
c2-Virginia,Unassigned Business Unit&connector_name=conn1&region_code=us-
east-1&active=1&option_title=Initial
Options&module=vm&schedule=now&cloud_provider=aws&platform_type=classic&&
after_notify=1&after_notify_message=Scan Finished"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-11T04:06:01Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
```

```
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1352070</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Example - Create Cloud Perimeter Scan Job (Recurring Schedule)

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&tag_set_by=name&tag_include_selector=any&tag_set_include=E
C2_Targets&tag_exclude_selector=any&tag_set_exclude=EC2_Test&connector_na
me=EC2 Connector&region_code=us-east-
1&active=0&occurrence=daily&start_date=04/02/2018&start_hour=10&start_min
ute=30&time_zone_code=IN&option_title=Initial
Options&frequency_days=364&observe_dst=no&module=vm&schedule=recurring&cl
oud_provider=aws&platform_type=classic&after_notify=1&recipient_group_ids
=4229"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-11T05:01:42Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1352071</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Example - Update Cloud Perimeter Scan Job

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=update&id=1352071&connector_name=EC2Connector-
2&platform_type=vpc_peered&region_code=us-west-1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-11T05:05:35Z</DATETIME>
    <TEXT>Scan has been updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1352071</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/fo/scan/simple_return.dtd

V3.0

/api/3.0/fo/scan/cloud/perimeter/job/

[POST]

Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

The input parameters for requesting a Cloud Perimeter scan are below. See Cloud Perimeter Scan Parameters for complete details.

Type	Parameter List
Request	action={create|update}
Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, scanner_id, iscanner_name, platform_type, region_code, vpc_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, elb_dns, schedule
include_app_gateway_lb_from_connector={0|1}	(Optional) Specify 1 to include public app gateway load balancers from selected connector, else 0. By default the value is set to 0.
include_lb_from_connector={0|1}	(Optional) Specify 1 to include public load balancers from selected connector, else 0. By default the value is set to 0.

Create/Update Cloud Perimeter Scan

We allow you to create or update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Example - Create Cloud Perimeter Scan Job

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/scan/cloud/perimeter/job/?action=create&sca
n_title=API%20Launch17&configured_from_source=connector_module&source_sca
n_type=custom&module=vm&active=1&schedule=now&option_title=Initial%20Opti
ons&priority=1&cloud_provider=azure&cloud_service=vm&connector_uuid=5fdec
014-0562-47fc-8029-
a90e7d87add9&include_lb_from_connector=1&include_app_gateway_lb_from_conn
ector=1' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer <JWT Tokens>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-03-13T06:12:28Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1431330</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Example - Update Cloud Perimeter Scan Job

API Request:

```
curl --location --request POST
'https://<qualys_base_url>/api/3.0/fo/scan/cloud/perimeter/job/?action=up
date&id=1431330&priority=1&connector_uuid=5fdec014-0562-47fc-8029-
a90e7d87add9&include_lb_from_connector=1&include_app_gateway_lb_from_conn
ector=1' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.p01.eng.sjc01.qualys.com/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-03-13T06:30:25Z</DATETIME>
        <TEXT>Scan has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1431330</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/3.0/fo/scan/simple_return.dtd

V4.0

/api/4.0/fo/scan/cloud/perimeter/job/

[POST]

Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

You can now reset the scheduled scan's pause/cancel and recurrence scheduling settings for cloud perimeter scans.

The input parameters for requesting a Cloud Perimeter scan are below. See Cloud Perimeter Scan Parameters for complete details.

Type	Parameter List
Request	action={create|update}
Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, scanner_id, iscanner_name, platform_type, region_code, vpc_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, elb_dns, schedule
include_app_gateway_lb_from_connector={0|1}	(Optional) Specify 1 to include public app gateway load balancers from selected connector, else 0. By default the value is set to 0.
include_lb_from_connector={0|1}	(Optional) Specify 1 to include public load balancers from selected connector, else 0. By default the value is set to 0.

Create/Update/Reset Cloud Perimeter Scan

We allow you to create or update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Example - Create Cloud Perimeter Scan Job

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/scan/cloud/perimeter/job/?action=create&sca
n_title=API%20Launch17&configured_from_source=connector_module&source_sca
n_type=custom&module=vm&active=1&schedule=now&option_title=Initial%20Opti
ons&priority=1&cloud_provider=azure&cloud_service=vm&connector_uuid=5fdec
014-0562-47fc-8029-
a90e7d87add9&include_lb_from_connector=1&include_app_gateway_lb_from_conn
ector=1' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dm1zcF9hZzE6UXVhbHlzQDEyMw=='
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-03-13T06:12:28Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1431330</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Example - Update Cloud Perimeter Scan Job

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/scan/cloud/perimeter/job/?action=update&id=
1431330&priority=1&connector_uuid=5fdec014-0562-47fc-8029-
a90e7d87add9&include_lb_from_connector=1&include_app_gateway_lb_from_conn
ector=1' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dm1zcF9hZzE6UXVhbHlzQDEyMw=='
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-03-13T06:30:25Z</DATETIME>
        <TEXT>Scan has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1431330</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Reset the scheduled scan duration and recurrence

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/4.0/fo/scan/cloud/perimeter/job/index.php?`action=u
pdate&id=1458384&active=1&remove_duration=1&remove_recurrence=1' \
--header 'X-Requested-With: postman' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T09:41:09Z</DATETIME>
        <TEXT>Scan has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1458384</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Create OCI Cloud Perimeter Scan

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/scan/cloud/perimeter/job/?action=create&mod
ule=vm&configured_from_source=connector_module&source_scan_type=custom&sc
hedule=now&active=1&cloud_provider=oci&cloud_service=compute_instance&inc
lude_lb_from_connector=0&connector_uuid=<connector_uuid>&option_id=<optio
n_id>&scan_title=<scan_title>' \
```

```
--header 'Accept: */*' \
--header 'X-Requested-With: NONE' \
--header 'Content-Length: 0' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-08-03T11:47:25Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>7663224</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/4.0/fo/scan/simple_return.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	API Status	Release Date
/api/4.0/fo/scan/cloud/perimeter/job/	Active	Active
/api/3.0/fo/scan/cloud/perimeter/job/	December 2025	December 2026
/api/2.0/fo/scan/cloud/perimeter/job/	December 2025	December 2026

Cloud Internal Scans

For API version information, refer to the API Version History section.

V2.0 | V3.0

V2.0

/api/2.0/fo/scan/cloud/internal/job/

[POST]

Azure cloud internal scans are available for only VM module. Only Managers and Unit Managers and Scanner role users have permission to configure Azure cloud internal scans.

The input parameters for requesting a Azure cloud internal scan are below. See Azure Internal Scan Parameters for complete details.

Type	Parameter List
Request	action={create|update}
Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, isscanner_id, iscanner_name, platform_type, region_code, virtual_network_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, cloud_resource_ids, schedule

Create/Update Azure Internal Scan

We allow you to create/update a Azure internal scan job through Azure Internal Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Sample - Create Azure Internal Scan Job

API Request:

```
curl --location --request POST '<qualys_base_url>/api/2.0/fo/scan/
cloud/internal/job/index.php?action=create&scan_title=Azure%20Scan%20Inte
rnal%20Test&
connector_uuid=1abcd111-1111-11ab-1111-a11b111aaa1&active=1&
option_title=Initial%20Options&
module=vm&schedule=now&cloud_provider=azure&iscanner_name=Azure_Internal_
Scanner_vmsp_ag1&`
region_code=eastus&priority=2&
platform_type=location&cloud_service=vm' \
--header 'X-Requested-With: xxxx' \
--header 'User-Agent: agentname/1.1.1 (https://agentname.com)' \
--header 'Authorization: Bearer< JWT Token>' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-11-26T05:17:19Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
```

```
                <VALUE>1395111</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Azure Internal Scan Job

API Request:

```
curl --location --request POST '<qualys_base_url>/api/2.0/fo/scan/cloud/
internal/job/index.php?action=update&
scan_title=Updated%20scan%20name&id=1395111&
iscanner_name=Azure_Internal_Scanner_New' \
--header 'X-Requested-With: qweabu' \
--header 'User-Agent: agentname/1.1.1 (https://agentname.com)' \
--header 'Authorization: Bearer< JWT Token>' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-11-26T05:20:01Z</DATETIME>
        <TEXT>Scan has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1395111</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/fo/scan/simple_return.dtd

V3.0

/api/2.0/fo/scan/cloud/internal/job/

[POST]

You can create/update the following internal instance based scans

- Azure cloud internal scans are available for only VM module.
- Google Cloud Platform (GCP) scan job for assets in the GCP cloud

Permisssions: Only Managers and Unit Managers and Scanner role users have permission to configure Azure cloud internal scans.

The input parameters for requesting a Azure and GCP internal scan are below. See Azure Internal Scan Parameters and Google Cloud Platform Internal Scan Parameters for complete details.

Cloud Internal Scan	Type	Parameter List
Azure/Google Cloud Platform	Request	action={create|update}
Azure	Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, isscanner_id, iscanner_name, platform_type, region_code, virtual_network_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, cloud_resource_ids, schedule
Google Cloud Platform	Scan List Filters	id, module, cloud_provider, cloud_service, connector_name, connector_uuid, scan_title, active, option_title, option_id, priority, isscanner_id, iscanner_name, region_code, virtual_network_id, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_include, tag_set_exclude, cloud_resource_ids, schedule

Create/Update Azure and Google Cloud Platform Internal Scan

You can create/update a Azure internal scan job through Azure Internal Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Sample - Create Azure Internal Scan Job

API Request:

```
curl --location --request POST '<qualys_base_url>/api/3.0/fo/scan/
cloud/internal/job/index.php?action=create&scan_title=Azure%20Scan%20Inte
rnal%20Test&
connector_uuid=1abcd111-1111-11ab-1111-a11b111aaa1&active=1&
option_title=Initial%20Options&
module=vm&schedule=now&cloud_provider=azure&iscanner_name=Azure_Internal_
Scanner_vmsp_ag1&`
region_code=eastus&priority=2&
platform_type=location&cloud_service=vm' \
--header 'X-Requested-With: xxxx' \
--header 'User-Agent: agentname/1.1.1 (https://agentname.com)' \
--header 'Authorization: Bearer< JWT Token>' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-11-26T05:17:19Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1395111</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Azure Internal Scan Job

API Request:

```
curl --location --request POST '<qualys_base_url>/api/3.0/fo/scan/cloud/
internal/job/index.php?action=update&
scan_title=Updated%20scan%20name&id=1395111&
iscanner_name=Azure_Internal_Scanner_New' \
--header 'X-Requested-With: qweabu' \
--header 'User-Agent: agentname/1.1.1 (https://agentname.com)' \
--header 'Authorization: Bearer< JWT Token>' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-11-26T05:20:01Z</DATETIME>
        <TEXT>Scan has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1395111</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create GCP Internal Scan Job

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/scan/cloud/internal/job/index.php?action=cr
```

```
eate&scan_title=GCP_Test_API3&connector_name=xxxxxx3&active=1&option_titl
e=Qualys%20Recommended%20Option%20Profile&module=vm&schedule=now&cloud_pr
ovider=gcp&iscanner_name=RM_GCP_SCANNER&cloud_service=compute_engine&virt
ual_network_id=projects%2Fqlys-devqa-qweb%2FvirtualNetworks%2Fvpc-qlys-
devqa-xxx' \
--header 'X-Requested-With: xxxx' \
--header 'User-Agent: Apidog/1.0.0 (https://apidog.com)' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-10T07:45:30Z</DATETIME>
        <TEXT>Scan has been created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>7469466</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update GCP Internal Scan Job

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/scan/cloud/internal/job/index.php?action=up
date&connector_name=CPSGLOBAL_clvautomationproject&active=1&option_title=
Qualys%20Recommended%20Option%20Profile&schedule=now&cloud_provider=gcp&i
scanner_name=RM_GCP_SCANNER&cloud_service=compute_engine&cloud_resource_i
ds=us-central1&virtual_network_id=projects%2Fqlys-devqa-
qweb%2FvirtualNetworks%2Fvpc-qlys-devqa-xx&id=7530283' \
--header 'X-Requested-With: xxxxx' \
--header 'User-Agent: Apidog/1.0.0 (https://apidog.com)' \
--header 'Accept: */*' \
--header 'Host: <qualys_base_url>' \
--header 'Connection: keep-alive' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-21T10:23:20Z</DATETIME>
```

```
            <TEXT>Scan has been updated successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>7530283</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

DTD

<platform API server>/api/3.0/fo/scan/simple_return.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/scan/cloud/internal/job	Active	Active
/api/2.0/fo/scan/cloud/internal/job	November 2026	May 2027

VM Scan Schedules

The Schedule Scan API (/api/2.0/fo/schedule/scan/) is used to define schedules for vulnerability scans in the user's account.

Permissions

User Role	Permissions
Manager	Create scan schedules for all assets in the subscription Remove all scan schedules View all scan schedules in the subscription
Unit Manager	Create scan schedules for assets in user's business unit Remove scan schedules in user's business unit. View scan schedules in the subscription*
Scanner	Create scan schedules for assets in user's account. Remove user's scan schedules View scan schedules in the subscription*
Readers	No permission to create or remove scan schedules View scan schedules in the subscription*

* Qualys includes an account permission setting that restricts Unit Managers, Scanners, and Readers from viewing scheduled tasks on unassigned assets.

List scan schedules

For API version information, refer to the API Version History section.

V2.0| V3.0| V4.0 | V5.0

V2.0

/api/2.0/fo/schedule/scan/?action=list

[GET] [POST]

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to display.
active={0|1}	(Optional) Specify 1 for active schedules only, or 0 for deactivated schedules only. **Note:** when you execute this endpoint with active=1 request, the response now include records with active=1, active=2, and active=3. This update ensures that all relevant active statuses are returned in the response.
show_notifications={**0**|1}	(Optional) Specify 1 to include the notification settings for each schedule in the XML output.

Parameter	Description
scan_type=certview	(Optional) Launch a CertView type VM scan. This option will be supported when CertView GA is released and enabled for your account.
scan_type=ec2certview	(Optional) Launch a CertView type VM scan for EC2 assets.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display the cloud details (Provider, Connector, Scan Type and Cloud Target) in the XML output. Otherwise the details are not displayed in the output.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
scan_type=perimeter	(Optional) List cloud perimeter scans only. **This option will be supported for Cloud Perimeter Scans in future release.**
show_cloud_details={**0**|1}	(Optional) Set to 1 to display cloud details in the XML output. The cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=lis
t&id=160642&show_notifications=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule_sc
an_list_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-12-01T19:26:50Z</DATETIME>
    <SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>160642</ID>
        <ACTIVE>1</ACTIVE>
        <TITLE><![CDATA[My Daily Scan]]></TITLE>
        <USER_LOGIN>qualys_ps</USER_LOGIN>
        <TARGET><![CDATA[10.10.10.10-10.10.10.20]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[External
Scanner]]></ISCANNER_NAME>
        <USER_ENTERED_IPS>
```

```
          <RANGE>
            <START>10.10.10.10</START>
            <END>10.10.10.20</END>
          </RANGE>
        </USER_ENTERED_IPS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial Options]]></TITLE>
          <DEFAULT_FLAG>1</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <SCHEDULE>
          <DAILY frequency_days="1" />
          <START_DATE_UTC>2017-11-30T00:30:00Z</START_DATE_UTC>
          <START_HOUR>16</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <NEXTLAUNCH_UTC>2017-12-02T00:30:00</NEXTLAUNCH_UTC>
          <TIME_ZONE>
            <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
            <TIME_ZONE_DETAILS>(GMT-0800) United States:
America/Los_Angeles</TIME_ZONE_DETAILS>
          </TIME_ZONE>
          <DST_SELECTED>1</DST_SELECTED>
        </SCHEDULE>
        <NOTIFICATIONS>
          <BEFORE_LAUNCH>
            <TIME>30</TIME>
            <UNIT><![CDATA[minutes]]></UNIT>
            <MESSAGE><![CDATA[This is my custom before scan email
message.]]></MESSAGE>
          </BEFORE_LAUNCH>
          <AFTER_COMPLETE>
            <MESSAGE><![CDATA[This is my custom after scan email
message.]]></MESSAGE>
          </AFTER_COMPLETE>
        </NOTIFICATIONS>
      </SCAN>
    </SCHEDULE_SCAN_LIST>
  </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Example: Users can filter the schedule scan list to only show cloud perimeter scan jobs. Also, when you include cloud details in the output, we'll show scan type "Cloud Perimeter".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=lis
t&id=1340788&scan_type=perimeter&show_cloud_details=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule_sc
an_list_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2018-04-12T12:57:03Z</DATETIME>
   <SCHEDULE_SCAN_LIST>
     <SCAN>
       <ID>1340788</ID>
       <ACTIVE></ACTIVE>
       <TITLE><![CDATA[My_External_Scan]]></TITLE>
       <USER_LOGIN>utwrx_mp</USER_LOGIN>
       <TARGET><![CDATA[Asset Tags Included]]></TARGET>
       <ISCANNER_NAME><![CDATA[External Scanner]]></ISCANNER_NAME>
       <EC2_INSTANCE>
         <CONNECTOR_UUID><![CDATA[8047abce-c3ac-42e0-ad49-
be4181d22c84]]></CONNECTOR_UUID>
         <EC2_ENDPOINT><![CDATA[1507b6c1-07a7-4d88-acf2-
8c6b63e749c4]]></EC2_ENDPOINT>
         <EC2_ONLY_CLASSIC><![CDATA[1]]></EC2_ONLY_CLASSIC>
       </EC2_INSTANCE>
       <CLOUD_DETAILS>
         <PROVIDER>AWS</PROVIDER>
         <CONNECTOR>
           <ID>37361</ID>
           <UUID>8047abce-c3ac-42e0-ad49-be4181d22c84</UUID>
           <NAME><![CDATA[EC2 Connector]]></NAME>
         </CONNECTOR>
         <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
         <CLOUD_TARGET>
           <PLATFORM>Classic</PLATFORM>
           <REGION>
             <UUID>1507b6c1-07a7-4d88-acf2-8c6b63e749c4</UUID>
             <CODE>us-east-1</CODE>
             <NAME><![CDATA[US East (N. Virginia)]]></NAME>
```

```
            </REGION>
            <VPC_SCOPE>None</VPC_SCOPE>
          </CLOUD_TARGET>
        </CLOUD_DETAILS>
        <ASSET_TAGS>
          <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>

<TAG_SET_INCLUDE><![CDATA[EC2_Targets]]></TAG_SET_INCLUDE>
          <TAG_EXCLUDE_SELECTOR>any</TAG_EXCLUDE_SELECTOR>
          <TAG_SET_EXCLUDE><![CDATA[EC2_Test]]></TAG_SET_EXCLUDE>
          <USE_IP_NT_RANGE_TAGS>0</USE_IP_NT_RANGE_TAGS>
        </ASSET_TAGS>
        <ELB_DNS>
          <DNS><![CDATA[abc.com]]></DNS>
          <DNS><![CDATA[abc123.com]]></DNS>
        </ELB_DNS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial Options]]></TITLE>
          <DEFAULT_FLAG>1</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <SCHEDULE>
          <DAILY frequency_days="364" />
          <START_DATE_UTC>2018-04-02T05:00:00Z</START_DATE_UTC>
          <START_HOUR>10</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <TIME_ZONE>
            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
          </TIME_ZONE>
          <DST_SELECTED>0</DST_SELECTED>
        </SCHEDULE>
      </SCAN>
    </SCHEDULE_SCAN_LIST>
  </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/schedule/scan/schedule_scan_list_output.dtd

V3.0

/api/3.0/fo/schedule/scan/?action=list

[GET] [POST]

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to display.
active={0|1}	(Optional) Specify 1 for active schedules only, or 0 for deactivated schedules only. **Note:** when you execute this endpoint with active=1 request, the response now include records with active=1, active=2, and active=3. This update ensures that all relevant active statuses are returned in the response.
show_notifications={**0**|1}	(Optional) Specify 1 to include the notification settings for each schedule in the XML output.
scan_type=certview	(Optional) Launch a CertView type VM scan. This option will be supported when CertView GA is released and enabled for your account.
scan_type=ec2certview	(Optional) Launch a CertView type VM scan for EC2 assets.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display the cloud details (Provider, Connector, Scan Type and Cloud Target) in the XML output. Otherwise the details are not displayed in the output.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
scan_type=perimeter	(Optional) List cloud perimeter scans only. This option will be supported for Cloud Perimeter Scans in future release.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display cloud details in the XML output. The cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/3.0/fo/schedule/scan/?action=lis
t&id=160642&show_notifications=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/3.0/fo/schedule/scan/schedule_sc
an_list_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-12-01T19:26:50Z</DATETIME>
    <SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>160642</ID>
        <ACTIVE>1</ACTIVE>
        <TITLE><![CDATA[My Daily Scan]]></TITLE>
        <USER_LOGIN>qualys_ps</USER_LOGIN>
        <TARGET><![CDATA[10.10.10.10-10.10.10.20]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[External
Scanner]]></ISCANNER_NAME>
        <USER_ENTERED_IPS>
          <RANGE>
            <START>10.10.10.10</START>
            <END>10.10.10.20</END>
          </RANGE>
        </USER_ENTERED_IPS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial Options]]></TITLE>
          <DEFAULT_FLAG>1</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <SCHEDULE>
          <DAILY frequency_days="1" />
          <START_DATE_UTC>2017-11-30T00:30:00Z</START_DATE_UTC>
          <START_HOUR>16</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <NEXTLAUNCH_UTC>2017-12-02T00:30:00</NEXTLAUNCH_UTC>
          <TIME_ZONE>
            <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
            <TIME_ZONE_DETAILS>(GMT-0800) United States:
America/Los_Angeles</TIME_ZONE_DETAILS>
          </TIME_ZONE>
          <DST_SELECTED>1</DST_SELECTED>
        </SCHEDULE>
        <NOTIFICATIONS>
          <BEFORE_LAUNCH>
            <TIME>30</TIME>
            <UNIT><![CDATA[minutes]]></UNIT>
            <MESSAGE><![CDATA[This is my custom before scan email
message.]]></MESSAGE>
          </BEFORE_LAUNCH>
```

```
          <AFTER_COMPLETE>
            <MESSAGE><![CDATA[This is my custom after scan email
message.]]></MESSAGE>
          </AFTER_COMPLETE>
        </NOTIFICATIONS>
      </SCAN>
    </SCHEDULE_SCAN_LIST>
  </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Example: Users can filter the schedule scan list to only show cloud perimeter scan jobs. Also, when you include cloud details in the output, we'll show scan type "Cloud Perimeter".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/3.0/fo/schedule/scan/?action=lis
t&id=1340788&scan_type=perimeter&show_cloud_details=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/3.0/fo/schedule/scan/schedule_sc
an_list_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2018-04-12T12:57:03Z</DATETIME>
   <SCHEDULE_SCAN_LIST>
     <SCAN>
       <ID>1340788</ID>
       <ACTIVE></ACTIVE>
       <TITLE><![CDATA[My_External_Scan]]></TITLE>
       <USER_LOGIN>utwrx_mp</USER_LOGIN>
       <TARGET><![CDATA[Asset Tags Included]]></TARGET>
       <ISCANNER_NAME><![CDATA[External Scanner]]></ISCANNER_NAME>
       <EC2_INSTANCE>
         <CONNECTOR_UUID><![CDATA[8047abce-c3ac-42e0-ad49-
be4181d22c84]]></CONNECTOR_UUID>
         <EC2_ENDPOINT><![CDATA[1507b6c1-07a7-4d88-acf2-
8c6b63e749c4]]></EC2_ENDPOINT>
         <EC2_ONLY_CLASSIC><![CDATA[1]]></EC2_ONLY_CLASSIC>
       </EC2_INSTANCE>
       <CLOUD_DETAILS>
         <PROVIDER>AWS</PROVIDER>
         <CONNECTOR>
           <ID>37361</ID>
```

```
            <UUID>8047abce-c3ac-42e0-ad49-be4181d22c84</UUID>
            <NAME><![CDATA[EC2 Connector]]></NAME>
          </CONNECTOR>
          <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
          <CLOUD_TARGET>
            <PLATFORM>Classic</PLATFORM>
            <REGION>
              <UUID>1507b6c1-07a7-4d88-acf2-8c6b63e749c4</UUID>
              <CODE>us-east-1</CODE>
              <NAME><![CDATA[US East (N. Virginia)]]></NAME>
            </REGION>
            <VPC_SCOPE>None</VPC_SCOPE>
          </CLOUD_TARGET>
        </CLOUD_DETAILS>
        <ASSET_TAGS>
          <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>

<TAG_SET_INCLUDE><![CDATA[EC2_Targets]]></TAG_SET_INCLUDE>
          <TAG_EXCLUDE_SELECTOR>any</TAG_EXCLUDE_SELECTOR>
          <TAG_SET_EXCLUDE><![CDATA[EC2_Test]]></TAG_SET_EXCLUDE>
          <USE_IP_NT_RANGE_TAGS>0</USE_IP_NT_RANGE_TAGS>
        </ASSET_TAGS>
        <ELB_DNS>
          <DNS><![CDATA[abc.com]]></DNS>
          <DNS><![CDATA[abc123.com]]></DNS>
        </ELB_DNS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial Options]]></TITLE>
          <DEFAULT_FLAG>1</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <SCHEDULE>
          <DAILY frequency_days="364" />
          <START_DATE_UTC>2018-04-02T05:00:00Z</START_DATE_UTC>
          <START_HOUR>10</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <TIME_ZONE>
            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
          </TIME_ZONE>
          <DST_SELECTED>0</DST_SELECTED>
        </SCHEDULE>
      </SCAN>
    </SCHEDULE_SCAN_LIST>
  </RESPONSE>
```

```
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Sample - Schedule list for Azure Internal Scans

API Request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/schedule/scan/index.php?action=list&
scan_type=internal&show_cloud_details=1&active=1&id=1396645' \
--header 'X-Requested-With: badsawewbu' \
--header 'User-Agent: agentname/1.0.0 (https://agentname.com)' \
--header 'Authorization: Bearer< JWT Token>' \
--header 'Accept: /' \
--header 'Host: <qualys_base_url>:43000' \
--header 'Connection: keep-alive'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/schedule/scan/schedule_scan_list_out
put.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-12-09T09:09:07Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1396645</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[Connector id]]>
                </TITLE>
                <USER_LOGIN>vmsp_ag1</USER_LOGIN>
                <TARGET>
                    <![CDATA[]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[Azure_Internal_Scanner_New]]>
                </ISCANNER_NAME>
                <CLOUD_DETAILS>
                    <PROVIDER>AZURE</PROVIDER>
                    <CONNECTOR>
                        <ID>1642552</ID>
                        <UUID>ddc52e7b-bcef-42f4-9243-
fb5747a23fc0</UUID>
```

```
                        <NAME>
                            <![CDATA[Azure VM Internal Scan]]>
                        </NAME>
                    </CONNECTOR>
                    <SCAN_TYPE>Cloud Internal</SCAN_TYPE>
                    <CLOUD_TARGET>
                        <PLATFORM>LOCATION</PLATFORM>
                        <REGION>
                            <UUID>080380ed-483e-45d7-8838-
c5e637750e54</UUID>
                            <CODE>eastus</CODE>
                            <NAME>
                                <![CDATA[East US]]>
                            </NAME>
                        </REGION>
                    </CLOUD_TARGET>
                </CLOUD_DETAILS>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
                    </TITLE>
                    <DEFAULT_FLAG>1</DEFAULT_FLAG>
                </OPTION_PROFILE>
                <PROCESSING_PRIORITY>2 -
Ultimate</PROCESSING_PRIORITY>
                <SCHEDULE>
                    <DAILY frequency_days="1" />
                    <START_DATE_UTC>2024-12-
04T10:28:00Z</START_DATE_UTC>
                    <START_HOUR>15</START_HOUR>
                    <START_MINUTE>58</START_MINUTE>
                    <NEXTLAUNCH_UTC>2024-12-
09T10:28:00</NEXTLAUNCH_UTC>
                    <TIME_ZONE>
                        <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                        <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                    </TIME_ZONE>
                    <DST_SELECTED>0</DST_SELECTED>
                </SCHEDULE>
            </SCAN>
        </SCHEDULE_SCAN_LIST>
    </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD

<platform API server>/api/3.0/fo/schedule/scan/schedule_scan_list_output.dtd

V4.0

/api/4.0/fo/schedule/scan/?action=list

[GET] [POST]

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to display.
active={0|1}	(Optional) Specify 1 for active schedules only, or 0 for deactivated schedules only. **Note:** when you execute this endpoint with active=1 request, the response now include records with active=1, active=2, and active=3. This update ensures that all relevant active statuses are returned in the response.
show_notifications={**0**|1}	(Optional) Specify 1 to include the notification settings for each schedule in the XML output.
scan_type=certview	(Optional) Launch a CertView type VM scan. This option will be supported when CertView GA is released and enabled for your account.
scan_type=ec2certview	(Optional) Launch a CertView type VM scan for EC2 assets.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display the cloud details (Provider, Connector, Scan Type and Cloud Target) in the XML output. Otherwise the details are not displayed in the output.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
scan_type=perimeter	(Optional) List cloud perimeter scans only. This option will be supported for Cloud Perimeter Scans in future release.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display cloud details in the XML output. The cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

API request:

```
curl --location
<qualys_base_url>/api/4.0/fo/schedule/scan/index.php?action=list&id=14409
22&show_cloud_details=1' \
--header 'X-Requested-With: e' \
--header 'Authorization: Bearer< JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/schedule/scan/schedule_scan_list_output.dtd
">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-04-17T06:10:18Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1440922</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[Azure Internal Scan now]]>
                </TITLE>
                <USER_LOGIN>scan_at3</USER_LOGIN>
                <TARGET>
                    <![CDATA[]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[Azure_Internal_Scanner]]>
                </ISCANNER_NAME>
                <CLOUD_DETAILS>
                    <PROVIDER>AZURE</PROVIDER>
                    <CONNECTOR>
                        <ID>1071626</ID>
                        <UUID>f4597cc6-4854-487a-85e3-15eb1595e40c</UUID>
                        <NAME>
                            <![CDATA[Azure_Connector_p01_scan_at]]>
                        </NAME>
                    </CONNECTOR>
                    <SCAN_TYPE>Cloud Internal</SCAN_TYPE>
                    <CLOUD_TARGET>
                        <PLATFORM>LOCATION</PLATFORM>
                        <REGION>
                            <UUID>080380ed-483e-45d7-8838-
c5e637750e54</UUID>
                            <CODE>eastus</CODE>
                            <NAME>
                                <![CDATA[East US]]>
                            </NAME>
                        </REGION>
                    </CLOUD_TARGET>
                </CLOUD_DETAILS>
```

```
                    <OPTION_PROFILE>
                        <TITLE>
                            <![CDATA[defaultOP_2025-04-11_00-49-54-751]]>
                        </TITLE>
                        <DEFAULT_FLAG>0</DEFAULT_FLAG>
                    </OPTION_PROFILE>
                    <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                    <SCHEDULE>
                        <DAILY frequency_days="1" />
                        <START_DATE_UTC>2025-04-11T04:23:00Z</START_DATE_UTC>
                        <START_HOUR>9</START_HOUR>
                        <START_MINUTE>53</START_MINUTE>
                        <NEXTLAUNCH_UTC>2025-04-17T06:24:35</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
                        <DST_SELECTED>0</DST_SELECTED>
                        <MAX_OCCURRENCE>1</MAX_OCCURRENCE>
                        <LAUNCH_TYPE>now</LAUNCH_TYPE>
                    </SCHEDULE>
                </SCAN>
            </SCHEDULE_SCAN_LIST>
        </RESPONSE>
    </SCHEDULE_SCAN_LIST_OUTPUT>
```

Note: The LAUNCH_TYPE tag indicates the type of scheduled scan - now or recurring and is included in all Cloud Perimeter Scans and Azure Internal Scans.

DTD

<platform API server>/api/4.0/fo/schedule/scan/schedule_scan_list_output.dtd

V5.0

/api/5.0/fo/schedule/scan/?action=list

[GET] [POST]

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to display.

Parameter	Description
active={0|1}	(Optional) Specify 1 for active schedules only, or 0 for deactivated schedules only. **Note:** when you execute this endpoint with active=1 request, the response now include records with active=1, active=2, and active=3. This update ensures that all relevant active statuses are returned in the response.
show_notifications={**0**|1}	(Optional) Specify 1 to include the notification settings for each schedule in the XML output.
scan_type=certview	(Optional) Launch a CertView type VM scan. This option will be supported when CertView GA is released and enabled for your account.
scan_type=ec2certview	(Optional) Launch a CertView type VM scan for EC2 assets.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display the cloud details (Provider, Connector, Scan Type and Cloud Target) in the XML output. Otherwise the details are not displayed in the output.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
scan_type=perimeter	(Optional) List cloud perimeter scans only. This option will be supported for Cloud Perimeter Scans in future release.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display cloud details in the XML output. The cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

API request:

```
curl --location
<qualys_base_url>/api/5.0/fo/schedule/scan/index.php?action=list&id=14409
22&show_cloud_details=1' \
--header 'X-Requested-With: e' \
--header 'Authorization: Bearer< JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/schedule/scan/schedule_scan_list_output.dtd
">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-04-17T06:10:18Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1440922</ID>
```

```
                    <ACTIVE>1</ACTIVE>
                    <TITLE>
                        <![CDATA[Azure Internal Scan now]]>
                    </TITLE>
                    <USER_LOGIN>scan_at3</USER_LOGIN>
                    <TARGET>
                        <![CDATA[]]>
                    </TARGET>
                    <NETWORK_ID>
                        <![CDATA[0]]>
                    </NETWORK_ID>
                    <ISCANNER_NAME>
                        <![CDATA[Azure_Internal_Scanner]]>
                    </ISCANNER_NAME>
                    <CLOUD_DETAILS>
                        <PROVIDER>AZURE</PROVIDER>
                        <CONNECTOR>
                            <ID>1071626</ID>
                            <UUID>f4597cc6-4854-487a-85e3-15eb1595e40c</UUID>
                            <NAME>
                                <![CDATA[Azure_Connector_p01_scan_at]]>
                            </NAME>
                        </CONNECTOR>
                        <SCAN_TYPE>Cloud Internal</SCAN_TYPE>
                        <CLOUD_TARGET>
                            <PLATFORM>LOCATION</PLATFORM>
                            <REGION>
                                <UUID>080380ed-483e-45d7-8838-
c5e637750e54</UUID>
                                <CODE>eastus</CODE>
                                <NAME>
                                    <![CDATA[East US]]>
                                </NAME>
                            </REGION>
                        </CLOUD_TARGET>
                    </CLOUD_DETAILS>
                    <OPTION_PROFILE>
                        <TITLE>
                            <![CDATA[defaultOP_2025-04-11_00-49-54-751]]>
                        </TITLE>
                        <DEFAULT_FLAG>0</DEFAULT_FLAG>
                    </OPTION_PROFILE>
                    <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                    <SCHEDULE>
                        <DAILY frequency_days="1" />
                        <START_DATE_UTC>2025-04-11T04:23:00Z</START_DATE_UTC>
                        <START_HOUR>9</START_HOUR>
                        <START_MINUTE>53</START_MINUTE>
                        <NEXTLAUNCH_UTC>2025-04-17T06:24:35</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
```

```
                        <DST_SELECTED>0</DST_SELECTED>
                        <MAX_OCCURRENCE>1</MAX_OCCURRENCE>
                        <LAUNCH_TYPE>now</LAUNCH_TYPE>
                    </SCHEDULE>
                </SCAN>
            </SCHEDULE_SCAN_LIST>
        </RESPONSE>
    </SCHEDULE_SCAN_LIST_OUTPUT>
```

Note: The LAUNCH_TYPE tag indicates the type of scheduled scan - now or recurring and is included in all Cloud Perimeter Scans and Azure Internal Scans.

Sample: To display the tags in Azure Cloud Perimeter Scan response

API request:

```
curl --location
'https://<qualys_base_url>/api/5.0/fo/schedule/scan/?action=list&id=14601
52&show_cloud_details=1' \
--header 'X-Requested-With: xxx' \
--header 'Authorization: Bearer< JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/schedule/scan/schedule_scan_list_output.dtd
">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-05-22T06:26:45Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1460152</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[sch_cps_azure_lb_appgtw]]>
                </TITLE>
                <USER_LOGIN>John</USER_LOGIN>
                <TARGET>
                    <![CDATA[Asset Tags Included]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[Azure_Internal_Scanner_John]]>
                </ISCANNER_NAME>
                <CLOUD_DETAILS>
                    <PROVIDER>AZURE</PROVIDER>
                    <CONNECTOR>
                        <UUID></UUID>
                        <NAME>
                            <![CDATA[]]>
                        </NAME>
```

```
                    </CONNECTOR>
                    <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>

<INCLUDE_LOAD_BALANCER_FROM_CONNECTOR>1</INCLUDE_LOAD_BALANCER_FROM_CONNE
CTOR>

<INCLUDE_APP_GATEWAY_LB_FROM_CONNECTOR>1</INCLUDE_APP_GATEWAY_LB_FROM_CON
NECTOR>
                </CLOUD_DETAILS>
                <ASSET_TAGS>
                    <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>
                    <TAG_SET_INCLUDE>
                        <![CDATA[xxx_Azure]]>
                    </TAG_SET_INCLUDE>
                    <USE_IP_NT_RANGE_TAGS>0</USE_IP_NT_RANGE_TAGS>

<USE_IP_NT_RANGE_TAGS_INCLUDE>0</USE_IP_NT_RANGE_TAGS_INCLUDE>
                </ASSET_TAGS>
                <ELB_DNS>
                    <DNS>
                        <![CDATA[abc.com]]>
                    </DNS>
                </ELB_DNS>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
                    </TITLE>
                    <DEFAULT_FLAG>1</DEFAULT_FLAG>
                </OPTION_PROFILE>
                <PROCESSING_PRIORITY>1 - Emergency</PROCESSING_PRIORITY>
                <SCHEDULE>
                    <DAILY frequency_days="1" />
                    <START_DATE_UTC>2025-05-16T09:51:00Z</START_DATE_UTC>
                    <MODIFIED_DATE_UTC>2025-05-
21T06:43:31Z</MODIFIED_DATE_UTC>
                    <START_HOUR>15</START_HOUR>
                    <START_MINUTE>21</START_MINUTE>
                    <NEXTLAUNCH_UTC>2025-05-22T09:51:00</NEXTLAUNCH_UTC>
                    <TIME_ZONE>
                        <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                        <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                    </TIME_ZONE>
                    <DST_SELECTED>0</DST_SELECTED>
                    <LAUNCH_TYPE>recurring</LAUNCH_TYPE>
                </SCHEDULE>
            </SCAN>
        </SCHEDULE_SCAN_LIST>
    </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Sample: Display the tags in EC2 Cloud Perimeter Scan Response

API Request:

```
curl --location
'https://<qualys_base_url>/api/5.0/fo/schedule/scan/?action=list&id=14601
51&show_cloud_details=1' \
--header 'X-Requested-With: John' \
--header 'Authorization: Bearer< JWT Token>’
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/5.0/fo/schedule/scan/schedule_scan_list_ou
tput.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-05-22T07:48:19Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1460151</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[sch_cps_ec2_lb]]>
                </TITLE>
                <USER_LOGIN>John</USER_LOGIN>
                <TARGET>
                    <![CDATA[]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[External Scanner]]>
                </ISCANNER_NAME>
                <EC2_INSTANCE>
                    <CONNECTOR_UUID>
                        <![CDATA[9a6b3e27-594e-4035-838c-5ab71e440365]]>
                    </CONNECTOR_UUID>
                    <EC2_ENDPOINT>
                        <![CDATA[1507b6c1-07a7-4d88-acf2-8c6b63e749c4]]>
                    </EC2_ENDPOINT>
                    <EC2_ONLY_CLASSIC>
                        <![CDATA[0]]>
                    </EC2_ONLY_CLASSIC>
                </EC2_INSTANCE>
                <CLOUD_DETAILS>
                    <PROVIDER>AWS</PROVIDER>
                    <CONNECTOR>
                        <ID>1752755</ID>
                        <UUID>9a6b3e27-594e-4035-838c-5ab71e440365</UUID>
                        <NAME>
                            <![CDATA[EC2_Connector_TB]]>
                        </NAME>
                    </CONNECTOR>
                    <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
```

```
<INCLUDE_LOAD_BALANCER_FROM_CONNECTOR>1</INCLUDE_LOAD_BALANCER_FROM_CONNE
CTOR>
                    <CLOUD_TARGET>
                        <PLATFORM>VPC</PLATFORM>
                        <REGION>
                            <UUID>1507b6c1-07a7-4d88-acf2-
8c6b63e749c4</UUID>
                            <CODE>us-east-1</CODE>
                            <NAME>
                                <![CDATA[US East (N. Virginia)]]>
                            </NAME>
                        </REGION>
                        <VPC_SCOPE>All</VPC_SCOPE>
                    </CLOUD_TARGET>
                </CLOUD_DETAILS>
                <ELB_DNS>
                    <DNS>
                        <![CDATA[abc.com]]>
                    </DNS>
                </ELB_DNS>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
                    </TITLE>
                    <DEFAULT_FLAG>1</DEFAULT_FLAG>
                </OPTION_PROFILE>
                <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                <SCHEDULE>
                    <DAILY frequency_days="1" />
                    <START_DATE_UTC>2025-05-16T09:50:00Z</START_DATE_UTC>
                    <MODIFIED_DATE_UTC>2025-05-
16T09:47:03Z</MODIFIED_DATE_UTC>
                    <START_HOUR>15</START_HOUR>
                    <START_MINUTE>20</START_MINUTE>
                    <NEXTLAUNCH_UTC>2025-05-22T09:50:00</NEXTLAUNCH_UTC>
                    <TIME_ZONE>
                        <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                        <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                    </TIME_ZONE>
                    <DST_SELECTED>0</DST_SELECTED>
                    <LAUNCH_TYPE>recurring</LAUNCH_TYPE>
                </SCHEDULE>
            </SCAN>
        </SCHEDULE_SCAN_LIST>
    </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Sample: Display the modified date in the scheduled Scan List

API Request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/schedule/scan/?action=list&id=1460801' \
```

```
--header 'X-Requested-With: John' \
--header 'Authorization: Bearer< JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/5.0/fo/schedule/scan/schedule_scan_list_ou
tput.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-05-21T11:38:34Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>1460801</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[Cloud Perimeter Scan111 20250519-153303]]>
                </TITLE>
                <USER_LOGIN>vmsp_ag1</USER_LOGIN>
                <TARGET>
                    <![CDATA[]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[External Scanner]]>
                </ISCANNER_NAME>
                <EC2_INSTANCE>
                    <CONNECTOR_UUID>
                        <![CDATA[9a6b3e27-594e-4035-838c-5ab71e440365]]>
                    </CONNECTOR_UUID>
                    <EC2_ENDPOINT>
                        <![CDATA[1507b6c1-07a7-4d88-acf2-8c6b63e749c4]]>
                    </EC2_ENDPOINT>
                    <EC2_ONLY_CLASSIC>
                        <![CDATA[0]]>
                    </EC2_ONLY_CLASSIC>
                </EC2_INSTANCE>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[Initial Options]]>
                    </TITLE>
                    <DEFAULT_FLAG>1</DEFAULT_FLAG>
                </OPTION_PROFILE>
                <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                <SCHEDULE>
                    <DAILY frequency_days="1" />
                    <START_DATE_UTC>2025-05-17T18:30:00Z</START_DATE_UTC>
                    <MODIFIED_DATE_UTC>2025-05-
19T10:12:38Z</MODIFIED_DATE_UTC>
                    <START_HOUR>0</START_HOUR>
                    <START_MINUTE>0</START_MINUTE>
```

```
                        <NEXTLAUNCH_UTC>2025-05-21T18:30:00</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
                        <DST_SELECTED>0</DST_SELECTED>
                        <LAUNCH_TYPE>recurring</LAUNCH_TYPE>
                    </SCHEDULE>
                </SCAN>
            </SCHEDULE_SCAN_LIST>
        </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD

<platform API server>/api/5.0/fo/schedule/scan/schedule_scan_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/schedule/scan/?action=list	Active	Active
/api/4.0/fo/schedule/scan/?action=list	December 2025	December 2026
/api/3.0/fo/schedule/scan/?action=list	December 2025	December 2026
/api/2.0/fo/schedule/scan/?action=list	December 2025	December 2026

Create scan schedule

/api/2.0/fo/schedule/scan/?action=create

[POST]

Create a scan schedule in the user's account.

Good to Know

A validation message displays during schedule scan from both the VM and PCI portals. If the asset group or FQDN contains DNS entries exceeding 4000 characters, users are notified before the scan is initiated. This proactive check prevents scan sharing failures and improves user experience.

Input Parameters

The input parameters for creating a scan schedule are below. For complete details see Scan Parameters and Azure Internal Scan Parameters.

Type	Parameter List
Request	action=create (required), echo_request
Scan	scan_title (required), active=0|1 (required)
Option Profile	option_id or option_title (one is required)
Scanner Appliance	iscanner_id or iscanner_name
Processing Priority	priority
Asset IPs/Groups	ip, asset_group_ids, asset_groups, exclude_ip_per_scan, default_scanner, scanners_in_ag
Asset Tags	target_from=tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags
Network	ip_network_id to filter IPs/ranges in "ip" parameter (valid when the networks feature is enabled)
EC2 Hosts	target_from=tags (required) use_ip_nt_range_tags_include=0 (optional) use_ip_nt_range_tags_exclude=0 (optional) use_ip_nt_range_tags=0 (optional) tag_set_include (required) More Asset Tags parameters (optional)
EC2 Environment	connector_name or connector_uuid (one is required) ec2_endpoint (required)
Scheduling	start_date (current date by default) start_hour, start_minute, time_zone_code, occurrence (required) observe_dst, recurrence, end_after, pause_after_hours, resume_in_days

Type	Parameter List
Daily Scan	occurrence=daily, frequency_days (required)
Weekly Scan	occurrence=weekly, frequency_weeks, weeks (required)
Monthly Scan	occurrence=monthly, frequency_months (required) Nth day of month: day_of_month (required) Day in Nth week: day_of_week, week_of_month (required)
Notifications	before_notify, before_notify_unit, before_notify_time, before_notify_message, after_notify, after_notify_message, recipient_group_ids, delay_notify, delay_notify_message, skipped_notify, skipped_notify_message, deactivate_notify, deactivate_notify_message

Sample - Create scan schedule

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: curl" -X "POST" -d
"scan_title=My+Scan+Schedule&active=1&option_id=3456&target_from=t
ags&tag_set_include=tag1,tag2,tag3&iscanner_name=scanner1&occurren
ce=daily&frequency_days=5&time_zone_code=US-CA&observe_dst=yes&sta
rt_hour=14&start_minute=0"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=cre
ate"
```

Sample - Create Scan Schedule, Cancel after 45 minutes

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&scan_title=My_Weekly_Scan&option_title=InitialOptio
ns&ip=10.20.31.73,10.20.31.106&active=1&occurrence=weekly&start_ho
ur=13&start_minute=30&time_zone_code=IN&frequency_weeks=1&weekdays
=Sunday&end_after=0&end_after_mins=45&iscanner_name=scanner1,scann
er2&before_notify=1&before_notify_unit=hours&before_notify_time=20
&recipient_group_ids=4228,5628"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-01-02T21:32:40Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
```

```
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create scan schedule using all scanners in network

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With:curl demo 2" -d
"action=create&scan_title=API+Schedule+scan&option_title=Initial+O
ptions&ip_network_id=12807913&scanners_in_network=1&ip=10.10.10.10
,10.10.10.11&occurrence=monthly&frequency_months=12&day_of_month=2
0&start_minute=00&start_hour=22&time_zone_code=IN&observe_dst=no&p
ause_after_hours=3&resume_in_days=4&recurrence=5&start_date=08/20/
2016&active=1"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-20T21:32:40Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create scan schedule (with FQDN and asset group)

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&scan_title=My+Schedule&active=1&time_zone_code=US-
OR&start_hour=18&start_minute=50&occurrence=daily&option_title=Ini
tial+Options&frequency_days=1&asset_groups=My+AG&fqdn=domain.qualy
s.com"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

Update a scan schedule

/api/2.0/fo/schedule/scan/?action=update

[POST]

Update a scan schedule in the user's account. During an update request you must specify target_from=assets when fqdn is specified in the same request. This is true for vulnerability scans and CertView type vulnerability scans.

When fqdn is not specified during an update request for a scheduled scan that already has fqdn defined, we will keep the existing value.

Input Parameters

The input parameters for updating a scan schedule are below. For complete details see Scan Parameters and Azure Internal Scan Parameters.

Type	Parameter List
Request	action=update (required), id (required), echo_request
Scan Title	scan_title
Status	active=0|1
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id, iscanner_name, default_scanner, scanners_in_ag, scanners_in_network, scanners_in_tagset
Processing Priority	priority
Asset IPs/Groups	ip, asset_group_ids or asset_groups, exclude_ip_per_scan
Asset Tags	target_from=tags, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include
EC2 Environment	connector_name or connector_uuid, ec2_endpoint, ec2_only_classic
Network	ip_network_id (when the Network Support feature is enabled)
Start Time	Must be specified together: set_start_time=1, start_date, start_hour, start_minute, time_zone_code, observe_dst
Recurrence	recurrence
Daily Scan	Must be specified together: occurrence=daily, frequency_days
Weekly Scan	Must be specified together: occurrence=weekly, frequency_weeks, weekdays
Monthly Scan	Must be specified together: occurrence=monthly, frequency_months, Nth day of month: day_of_month, Day in Nth week: day_of_week, week_of_month

Type	Parameter List
End	end_after, end_after_mins
Pause and Resume	pause_after_hours, pause_after_mins, resume_in_days, resume_in_hours
Notifications	before_notify, before_notify_unit, before_notify_time, before_notify_message, after_notify, after_notify_message, recipient_group_ids, delay_notify, delay_notify_message, skipped_notify, skipped_notify_message, deactivate_notify, deactivate_notify_message

Sample - Update scan schedule, Pause after 15 minutes

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=update&id=146754&pause_after_hours=0&pause_after_mins=15&r
esume_in_days=2&resume_in_hours=5"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-01-14T11:57:42Z</DATETIME>
    <TEXT>Edit scheduled Scan Completed successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>146754</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Delete scan schedule

/api/2.0/fo/schedule/scan/?action=delete

[POST]

Delete a scan schedule in the user's account.

Input Parameters

Parameter	Description
action=delete	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to delete.

Sample - Delete scan schedule

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: curl" -X "POST" -d
"id=123456"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=del
ete"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-05-30T21:32:40Z</DATETIME>
    <TEXT>Schedule scan deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>123456</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

PC Scan Schedules

The PC Schedule Scan API (/api/2.0/fo/schedule/scan/compliance) allows you to create, update, list, and delete schedule scans for Policy Compliance.

Permissions

Note: The PC Scan schedule APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

User Role	Permissions
Manager	Create scan schedules for all assets in the subscription Remove all scan schedules View all scan schedules in the subscription
Unit Manager	Create scan schedules for assets in user's business unit Remove scan schedules in user's business unit. View scan schedules in the subscription*
Scanner	Create scan schedules for assets in user's account. Remove user's scan schedules View scan schedules in the subscription*
Readers	No permission to create or remove scan schedules View scan schedules in the subscription*

*Qualys includes an account permission setting that restricts Unit Managers, Scanners, and Readers from viewing scheduled tasks on unassigned assets.

List compliance scan schedules

/api/2.0/fo/schedule/scan/compliance/?action=list

[GET]

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
id={value}	(Optional) The ID of the scan schedule you want to display.
active={0|1}	(Optional) Specify 1 for active schedules only, or 0 for deactivated schedules only.
show_notifications={**0**|1}	(Optional) Specify 1 to include the notification settings for each schedule in the XML output.
show_cloud_details={**0**|1}	(Optional) Set to 1 to display the cloud details (Provider, Connector, Scan Type and Cloud Target) in the XML output. Otherwise the details are not displayed in the output.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.
client_name={value}	(Optional) Name of the client (Consultant type subscription only). Parameter client_id or client_name may be specified for the same request.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
compliance_schedule_scan_list_output.dtd">
<COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-11-19T10:10:58Z</DATETIME>
        <COMPLIANCE_SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>57363</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
```

```
                        <![CDATA[My Scan Schedule api6]]>
                    </TITLE>
                    <USER_LOGIN>quays_sp1</USER_LOGIN>
                    <TARGET>
                        <![CDATA[10.10.10.185]]>
                    </TARGET>
                    <NETWORK_ID>
                        <![CDATA[0]]>
                    </NETWORK_ID>
                    <ISCANNER_NAME>
                        <![CDATA[pyscandsp]]>
                    </ISCANNER_NAME>
                    <ASSET_GROUP_TITLE_LIST>
                        <ASSET_GROUP_TITLE>
                            <![CDATA[policyred7]]>
                        </ASSET_GROUP_TITLE>
                    </ASSET_GROUP_TITLE_LIST>
                    <OPTION_PROFILE>
                        <TITLE>
                            <![CDATA[duplicate IO]]>
                        </TITLE>
                        <DEFAULT_FLAG>0</DEFAULT_FLAG>
                    </OPTION_PROFILE>
                    <SCHEDULE>
                        <DAILY frequency_days="5" />
                        <START_DATE_UTC>2019-11-
      19T22:00:00Z</START_DATE_UTC>
                        <START_HOUR>14</START_HOUR>
                        <START_MINUTE>0</START_MINUTE>
                        <NEXTLAUNCH_UTC>2019-11-
      19T22:00:00</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
                          <TIME_ZONE_DETAILS>(GMT-0800) United States:
      America/Los_Angeles</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
                        <DST_SELECTED>1</DST_SELECTED>
                    </SCHEDULE>
                    <NOTIFICATIONS />
                </SCAN>
            </COMPLIANCE_SCHEDULE_SCAN_LIST>
        </RESPONSE>
</COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/schedule/scan/compliance/compliance_schedule_scan_list_output.dtd "

Create a Compliance Scan Schedule

/api/2.0/fo/schedule/scan/compliance/?action=create

[POST]

Create a scan schedule in the user's account.

Input Parameters

The input parameters for creating a scan schedule are below. For complete details see Scan Parameters and Azure Internal Scan Parameters.

Type	Parameter List
Request	action=create (required),
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
Scan	scan_title (required), active=0|1 (required)
Compliance Profile	option_id or option_profile (one is required)
Scanner Appliance	iscanner_id or iscanner_name
Asset IPs/Groups	ip, asset_group_ids, asset_groups, exclude_ip_per_scan, default_scanner, scanners_in_ag
Asset Tags	target_from=tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags
Network	ip_network_id to filter IPs/ranges in "ip" parameter (valid when the networks feature is enabled)
Scheduling	start_date (current date by default) start_hour, start_minute, time_zone_code, occurrence (required) observe_dst, recurrence, end_after, pause_after_hours, resume_in_days
Daily Scan	occurrence=daily, frequency_days (required)
Weekly Scan	occurrence=weekly, frequency_weeks, weeks (required)

Type	Parameter List
Monthly Scan	occurrence=monthly, frequency_months (required) Nth day of month: day_of_month (required) Day in Nth week: day_of_week, week_of_month (required)
Notifications	before_notify, before_notify_unit, before_notify_time, before_notify_message, after_notify, after_notify_message, recipient_group_ids, delay_notify, delay_notify_message, skipped_notify, skipped_notify_message, deactivate_notify, deactivate_notify_message

Sample - Create compliance scan schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?action=create&scan_title=My+Scan+Schedule+api6&active=1&option_id
=76960&asset_groups=policyred7&iscanner_name=pyscandsp&occurrence=
daily&frequency_days=5&time_zone_code=US-
CA&observe_dst=yes&start_hour=14&start_minute=0"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-19T11:14:19Z</DATETIME>
        <TEXT>New compliance scan scheduled successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57368</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create compliance scan schedule and cancel after 45 minutes

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?action=create&scan_title=My_Weekly_Scan&option_title=nordea
windows&ip=10.10.10.10&active=1&occurrence=weekly&start_hour=13&st
art_minute=30&time_zone_code=IN&frequency_weeks=1&weekdays=Sunday&
end_after=0&end_after_mins=45&iscanner_name=pyscandsp&before_notif
y=1&before_notify_unit=hours&before_notify_time=20"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-21T08:06:49Z</DATETIME>
        <TEXT>New compliance scan scheduled successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57369</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create compliance scan schedule using all scanners in network

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?action=create&scan_title=API+Schedule+scan&option_title=nordea
windows&ip_network_id=52010&scanners_in_network=1&ip=10.10.10.10
,10.10.10.11&occurrence=monthly&frequency_months=12&day_of_month=2
0&start_minute=00&start_hour=22&time_zone_code=IN&observe_dst=no&p
ause_after_hours=3&resume_in_days=4&recurrence=5&start_date=08/20/
2020&active=1"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-21T08:26:00Z</DATETIME>
        <TEXT>New compliance scan scheduled successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57370</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create EC2 compliance scan schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?
action=create&scan_title=API_Schedule_EC2_PC&target_from=tags&tag_
set_by=name&tag_include_selector=any&tag_set_include=Auth&connecto
r_name=AWS+Connector&ec2_endpoint=us-east-
1&active=0&occurrence=daily&start_date=05/21/2020&start_hour=20&st
art_minute=30&time_zone_code=IN&option_title=Initial+PC+Options&fr
equency_days=364&end_after=1&observe_dst=no&iscanner_name=EC2_Scan
ner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-06-07T22:09:26Z</DATETIME>
    <TEXT>New compliance scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>279256</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update a Compliance Scan Schedule

/api/2.0/fo/schedule/scan/compliance/?action=update&id=<id>

[POST]

Update a scan schedule in the user's account.

Input Parameters

The input parameters for updating a scan schedule are below. For complete details see Scan Parameters and Azure Internal Scan Parameters.

Type	Parameter List
Request	action=update (required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
Scan Title	scan_title
id={value}	(Required)The ID of the scan schedule you want to update.
Status	active=0|1
Compliance Profile	option_id or option_title
Scanner Appliance	iscanner_id, iscanner_name, default_scanner, scanners_in_ag, scanners_in_network, scanners_in_tagset
Asset IPs/Groups	ip, asset_group_ids or asset_groups, exclude_ip_per_scan
Asset Tags	target_from=tags, use_ip_nt_range_tags_include, use_ip_nt_range_tags_exclude, use_ip_nt_range_tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include
Network	ip_network_id (when the Network Support feature is enabled)
Start Time	Must be specified together: set_start_time=1, start_date, start_hour, start_minute, time_zone_code, observe_dst
recurrence={value}	(Optional) The number of times the scan will be run before it is deactivated. For example, if you set recurrence=2, the scan schedule will be deactivated after it runs 2 times. By default no value is set. A valid value is an integer from 1 to 99.
Daily Scan	Must be specified together: occurrence=daily, frequency_days
Weekly Scan	Must be specified together: occurrence=weekly, frequency_weeks, weekdays

Type	Parameter List
Monthly Scan	Must be specified together: occurrence=monthly, frequency_months, Nth day of month: day_of_month, Day in Nth week: day_of_week, week_of_month
End	end_after, end_after_mins
Pause and Resume	pause_after_hours, pause_after_mins, resume_in_days, resume_in_hours
Notifications	before_notify, before_notify_unit, before_notify_time, before_notify_message, after_notify, after_notify_message, recipient_group_ids, delay_notify, delay_notify_message, skipped_notify, skipped_notify_message, deactivate_notify, deactivate_notify_message

Sample - Update compliance scan schedule.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/schedule/scan/compliance/?action=upda
te&id=57360&option_id=39594"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-19T12:04:44Z</DATETIME>
        <TEXT>Edit scheduled Scan Completed successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57360</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Delete a Compliance Scan Schedule

/api/2.0/fo/schedule/scan/compliance/?action=delete&id=<id>

[POST]

Delete a scan schedule in the user's account.

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the scan schedule you want to delete.
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.

Sample - Delete compliance scan schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/
?action=delete&id=57360"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-19T12:10:45Z</DATETIME>
        <TEXT>Schedule scan deleted successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57360</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Scan List Parameters

Request Type

Parameter	Description
action=list	(Required) A flag used to make a request for a scan list.
echo_request={0|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Filters

Several parameters allow you to set filters to restrict the scan list output. When no filters are specified, the service returns all scans launched by all users within the past 30 days.

Parameter	Description
scan_ref={value}	(Optional) Show only a scan with a certain scan reference code. When unspecified, the scan list is not restricted to a certain scan. For a vulnerability scan, the format is: scan/987659876.19876 For a compliance scan the format is: compliance/98765456.12345 For a SCAP scan the format is: qscap/987659999.22222
scan_id={value}	(Optional) Show only a scan with a certain compliance scan ID.
state={value}	(Optional) Show only one or more scan states. By default, the scan list is not restricted to certain states. A valid value is: Running, Paused, Canceled, Finished, Error, Queued (scan job is waiting to be distributed to scanner(s)), or Loading (scanner(s) are finished and scan results are being loaded onto the platform). Multiple values are comma separated.
processed={0|1}	(Optional) Specify 0 to show only scans that are not processed. Specify 1 to show only scans that have been processed. When not specified, the scan list output is not filtered based on the processed status.
type={value}	(Optional) Show only a certain scan type. By default, the scan list is not restricted to a certain scan type. A valid value is: On-Demand, Scheduled, or API.
target={value}	(Optional) Show only one or more target IP addresses. By default, the scan list includes all scans on all IP addresses. Multiple IP addresses and/or ranges may be entered. Multiple entries are comma separated. You may enter an IP address range using the hyphen (-) to separate the start and end IP address, as in: 10.10.10.1-10.10.10.2
user_login={value}	(Optional) Show only a certain user login. The user login identifies a user who launched scans. By default, the scan list is not restricted to scans launched by a particular user. Enter the login name for a valid Qualys user account.

Parameter	Description
launched_after_datetime={date}	(Optional) Show only scans launched after a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”. When launched_after_datetime and launched_before_datetime are unspecified, the service selects scans launched within the past 30 days. A date/time in the future returns an empty scans list.
launched_before_datetime={date}	(Optional) Show only scans launched before a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”. When launched_after_datetime and launched_before_datetime are unspecified, the service selects scans launched within the past 30 days. A date/time in the future returns a list of all scans (not limited to scans launched within the past 30 days).
scan_type=certview	(Optional) List CertView in VM scans only. This option will be supported when CertView GA is released and enabled for your account.
scan_type=ec2certview	(Optional) List EC2 CertView VM scans only.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.

Show/Hide

These parameters specify whether certain information will be shown in the XML output.

Parameter	Description
show_ags={**0**|1}	(Optional) Specify 1 to show asset group information for each scan in the XML output. By default, asset group information is not shown.
show_op={**0**|1}	(Optional) Specify 1 to show option profile information for each scan in the XML output. By default, option profile information is not shown.
show_status={0|**1**}	(Optional) Specify 0 to not show scan status for each scan in the XML output. By default, scan status is shown.
show_last={**0**|1}	(Optional) Specify 1 to show only the most recent scan (which meets all other search filters in the request) in the XML output. By default, all scans are shown in the XML output.

Parameter	Description
pci_only={**0**|1}	(Optional) Specify 1 to show only external PCI scans in the XML output. External PCI scans are vulnerability scans run with the option profile "Payment Card Industry (PCI) Options". When pci_only=1 is specified, the XML output will not include other types of scans run with other option profiles.
ignore_target={**0**|1}	(Optional) Specify 1 to hide target information from the scan list. Specify 0 to display the target information.

Scan Parameters

Input parameters used to launch a VM or PC scan are below.

Parameter	Description
action={launch}	(Required) Specify "launch" to launch a new scan.
echo_request={**0**|1}	(Optional) Specify 1 to list the input parameters in the XML output. When unspecified, parameters are not listed in the XML output.
scan_title={value}	(Optional) The scan title. This can be a maximum of 2000 characters (ascii).
target_from={**assets**|tags}	(Optional) Specify "assets" (the default) when your scan target will include IP addresses/ranges and/or asset groups. Specify "tags" when your scan target will include asset tags.
fqdn={value}	(Optional) The target FQDN for a vulnerability scan. You must specify at least one target i.e. IPs, asset groups or FQDNs. Multiple values are comma separated.
ip={value}	(Optional) The IP addresses to be scanned. You may enter individual IP addresses and/or ranges. Multiple entries are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	ip is valid only when target_from=assets is specified.
asset_groups={value}	(Optional) The titles of asset groups containing the hosts to be scanned. Multiple titles are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	asset_groups is valid only when target_from=assets is specified. These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.
asset_group_ids={value}	(Optional) The IDs of asset groups containing the hosts to be scanned. Multiple IDs are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	asset_group_ids is valid only when target_from=assets is specified. These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.

Parameter	Description
exclude_ip_per_scan={value}	(Optional) The IP addresses to be excluded from the scan when the scan target is specified as IP addresses (not asset tags). You may enter individual IP addresses and/or ranges. Multiple entries are comma separated.
	exclude_ip_per_scan is valid only when target_from=assets is specified.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
	tag_include_selector is valid only when target_from=tags is specified.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
	tag_exclude_selector is valid only when target_from=tags is specified.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
	tag_set_by is valid only when target_from=tags is specified.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	tag_set_include is valid only when target_from=tags is specified.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	tag_set_exclude is valid only when target_from=tags is specified.
use_ip_nt_range_tags_include={**0**|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to scan all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
	use_ip_nt_range_tags_include is valid only when target_from=tags is specified.
use_ip_nt_range_tags_exclude={**0**|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to exclude all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
	use_ip_nt_range_tags_exclude is valid only when target_from=tags is specified.

Parameter	Description
use_ip_nt_range_tags={**0**|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to scan all IP addresses defined in tags. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
	This parameter has been replaced by use_ip_nt_range_tags_include and use_ip_nt_range_tags_exclude parameters. The use_ip_nt_range_tag parameter is still supported.
	use_ip_nt_range_tags is valid only when target_from=tags is specified.
iscanner_id={value}	(Optional) The IDs of the scanner appliances to be used. Multiple entries are comma separated. For an Express Lite user, Internal Scanning must be enabled in the user's account.
	One of these parameters must be specified in a request: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. These parameters are mutually exclusive and cannot be specified in the same request: iscanner_id and iscanner_name.
iscanner_name={value}	(Optional) The friendly names of the scanner appliances to be used or "External" for external scanners. Multiple entries are comma separated. For an Express Lite user, Internal Scanning must be enabled in the user's account.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. These parameters are mutually exclusive and cannot be specified in the same request: iscanner_id and iscanner_name.
default_scanner={**0**|1}	(Optional) Specify 1 to use the default scanner in each target asset group. For an Express Lite user, Internal Scanning must be enabled in the user's account.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. default_scanner is valid when the scan target is specified using one of these parameters: asset_groups, asset_group_ids.

Parameter	Description
scanners_in_ag={**0**|1}	(Optional) Specify 1 to distribute the scan to the target asset groups' scanner appliances. Appliances in each asset group are tasked with scanning the IPs in the group. By default up to 5 appliances per group will be used and this can be configured for your account (please contact your Account Manager or Support). For an Express Lite user, Internal Scanning must be enabled in the user's account.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. scanners_in_ag is valid when the scan target is specified using one of these parameters: asset_groups, asset_group_ids.
scanners_in_tagset={**0**|1}	(Optional) Specify 1 to distribute the scan to scanner appliances that match the asset tags specified for the scan target.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. scanners_in_tagset is valid when the target_from=tags is specified.
scanners_in_network={value}	(Optional) Specify 1 to distribute the scan to all scanner appliances in the network.
option_title={value}	(Optional) The title of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
option_id={value}	(Optional) The ID of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
priority={value}	(Optional for VM scans only) Specify a value of 0 - 9 to set a processing priority level for the scan. When not specified, a value of 0 (no priority) is used. Valid values are: 0 = No Priority (the default) 1 = Emergency 2 = Ultimate 3 = Critical 4 = Major 5 = High 6 = Standard 7 = Medium 8 = Minor 9 = Low

Parameter	Description
connector_name={value}	(Required for an EC2 scan) (VM scan only) The name of the EC2 connector for the AWS integration you want to run the scan on.
ec2_endpoint={value}	(Required for an EC2 scan) The EC2 region code or the ID of the Virtual Private Cloud (VPC) zone. Need help finding the region code? See the following: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions-availability-zones
ec2_instance_ids={value}	(Optional) (VM scan only) The ID of the EC2 instance on which you want to launch the VM or compliance scan. Multiple ec2 instance ids are comma separated. You can add up to maximum 10 instance Ids. When you launch an EC2 scan and specify EC2 instance IDs as part of the scan target, we can identify and skip any invalid instances and continue the scan on the valid instances.
ip_network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) The ID of a network used to filter the IPs/ranges specified in the"ip" parameter. Set to a custom network ID (note this does not filter IPs/ranges specified in "asset_groups" or "asset_group_ids"). Or set to "0" (the default) for the Global Default Network - this is used to scan hosts outside of your custom networks.
runtime_http_header={value}	(Optional) Set a custom value in order to drop defenses (such as logging, IPs, etc) when an authorized scan is being run. The value you enter will be used in the "Qualys-Scan:" header that will be set for many CGI and web application fingerprinting checks. Some discovery and web server fingerprinting checks will not use this header.
scan_type=certview	(Optional) (VM scan only) Launch a CertView type scan. This option will be supported when CertView GA is released and enabled for your account.
fqdn={value}	(Optional) The target FQDN for a vulnerability scan. You must specify at least one target i.e. IPs, asset groups or FQDNs. Multiple values are comma separated. - DNS Tracking must be enabled for the subscription. A Manager user can enable this feature in the Qualys UI by going to Scans > Setup > DNS Tracking and checking the "Enable DNS Tracking for hosts" option. - You can specify FQDNs in combination with IPs and asset groups but not with asset tags.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).

Parameter	Description
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.
include_agent_targets={**0**|1}	(Optional) Specify 1 when your scan target includes agent hosts. This lets you scan private IPs where agents are installed when these IPs are not in your VM/PC license. Supported capabilities - This parameter is supported for internal scans using scanner appliance(s). This option is not supported for scans using External scanners. - This parameter is supported when launching on demand scans only. It is not supported for scheduled scans. Parameter iscanner_id or iscanner_name must be specified in the same request.

Cloud Perimeter Scan Parameters

The input parameters for creating or updating a Cloud Perimeter scan are below.

Parameter	Description
action={create|update}	(Required) Specify "create" to configure a new cloud perimeter scan job. Specify "update" to make changes to an existing scan job.
id={value}	(Required and only applicable for Update request) The ID of the scan schedule you want to update.
module={vm|pc}	(Required for Create request) Specify "vm" for a vulnerability scan and "pc" for a compliance scan.
cloud_provider={value}	(Optional) Specify "azure" for an Azure scan. Specify "aws" for an AWS EC2 scan. Specify "gcp" for a GCP scan.The cloud_provider value cannot be changed during an update request. When cloud_provider=azure, the following parameters cannot be specified in the same request: platform_type, region_code, vpc_id, include_micro_nano_instances, include_lb_from_connector. These parameters only apply when cloud_provider=aws is specified.
cloud_service={value}	(Optional) Specify "vm" (Azure virtual machine) for an Azure scan. Specify "ec2" for an AWS EC2 scan. Specify "compute_engine" for GCP scan.The cloud_service value cannot be changed during an update request.

Parameter	Description
connector_name={value}	(Optional) The name of the connector to be used. We will check if the specified connector_name exists for your Qualys subscription. If not, then API request returns an error message “Invalid connector_name provided”.
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
connector_uuid={value}	(Optional) The ID of the connector to be used. We will check if the specified connector_uuid exists for your Qualys subscription. If not, then API request returns an error message “Invalid connector_uuid provided”
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
scan_title={value}	(Optional) The scan title. When not specified the default scan title is "AWS EC2 Perimeter Scan <date>"
active={0|1}	(Required for Create request) Specify "1" to create an active schedule. Specify "0" to create an inactive schedule.
option_title={value}	(Optional) The title of the option profile to be used.
	One of these parameters must be specified in the request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
option_id={value}	(Optional) The ID of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
priority={value}	(Optional) Specify a value of 0 - 9 to set a processing priority level for the scan. When not specified, a value of 0 (no priority) is used. Valid values are: 0 = No Priority (the default) 1 = Emergency 2 = Ultimate 3 = Critical 4 = Major 5 = High 6 = Standard 7 = Medium 8 = Minor 9 = Low
iscanner_id={value}	(Optional, only valid when your account is configured to allow internal scanners) The IDs of the scanner appliances to be used. Specify "0" for external scanners. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.

Parameter	Description
iscanner_name={value}	(Optional, only valid when your account is configured to allow internal scanners) The friendly names of the scanner appliances to be used or "External" for external scanners. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.
platform_type={value}	(Optional) The platform type. Valid values are: classic, vpc_peered or selected_vpc.
region_code={value}	(Optional) The EC2 region code. Valid values are: ap-northeast-1, ap-southeast-1, ap-southeast-2, ap-east-1, eu-west-1, eu-north-1, asa-east-1, us-east-1, us-west-1, us-west-2, me-south-1, eu-south-1, and af-south-1, ap-northeast-1, ap-southeast-1, ap-southeast-2, ap-southeast-3, ap-southeast-4, ap-east-1, eu-west-1, eu-north-1, eu-central-2, asa-east-1, us-east-1, us-west-1, us-west-2, me-south-1, me-central-1, eu-south-1, eu-south-2, and af-south-1, ap-south-2, ca-west-1, il-central-1.
	One of these parameters must be specified in the request: region_code or vpc_id. These are mutually exclusive and cannot be specified in the same request.
vpc_id={value}	(Optional) The ID of the Virtual Private Cloud (VPC) zone. The ID value must start with vpc-*. We will check if the specified vpc_id exists for the selected connector
	One of these parameters must be specified in the request: region_code or vpc_id. These are mutually exclusive and cannot be specified in the same request.
include_micro_nano_instances={**0**|1}	(Optional) Specify 1 to include EC2 assets with instance types t2.nano, t3.nano, t1.micro and m1.small in the scan job. By default, this parameter value is set to 0. Note that these instance types must be activated for your account.
	Warning AWS EC2 assets with instance types t2.nano, t3.nano, t1.micro and m1.small have very limited CPU. When scanning these instance types we recommend you choose an option profile with Light port scanning and no authentication. Alternatively, use Qualys Cloud Agent to perform the equivalent of authenticated scanning for the least performance impact for these instance types.
tag_include_selector={all|**any**}	(Optional) Select “any” (the default) to include hosts that match at least one of the selected tags. Select “all” to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select “any” (the default) to exclude hosts that match at least one of the selected tags. Select “all” to exclude hosts that match all of the selected tags.

Parameter	Description
tag_set_by={**id**|name}	(Optional) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names. We will check if the tag ids or tag names are valid.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
include_lb_from_connector ={**0**|1}	(Optional) Specify 1 to include public load balancers from the selected connector in the scan job. By default, this parameter value is set to 0. When you set this parameter to 1, we fetch public load balancers from the AWS connector in CloudView that has the same configuration as that of the selected connector. If you select this option, ensure that you have the connector created in your CloudView account with a configuration similar to that of the selected connector. If the connector in CloudView is not found, then we can't fetch the public load balancers from the connector.
	Note To create the connector, your account must have CloudView subscription and your platform has access to CloudView base URL “qweb_cloud_view_base_url”
elb_dns={value}	(Optional) One or more load balancer DNS names to include in the scan job. Multiple values are comma-separated.
schedule={value}	(Required for Create request) Specify "now" to schedule the scan job for now. Specify "recurring" to schedule the scan job to start at a later time or on a recurring basis. See Scan Schedule - Occurrence.

Parameter	Description
remove_recurrence={0|1}	Specify 1 to reset after the recurrence value. For example, reset the recurrence after two scans. **Note:** This parameter cannot be passed with: - schedule=now parameter. - Any of these parameters (end_after, end_after_mins, pause_after_hours, pause_after_mins) - This parameter is applicable to only V4.0 version
remove_duration={0|1}	Specify 1 to reset the cancel/pause after the duration setting. **Note:** - This parameter cannot be passed with schedule=now - remove_recurrence and recurrence parameters cannot be passed together. - This parameter is applicable to only V4.0 version

Azure Internal Scan Parameters

The input parameters for creating or updating a Cloud Perimeter scan are below.

Parameter	Description
action={create|update}	(Required) Specify "create" to configure a new internal Azure scan job. Specify "update" to make changes to an existing scan job.
id={value}	(Required and only applicable for Update request) The ID of the scan schedule you want to update.
module={vm}	(Required for Create request) Specify "vm" for a vulnerability scan.
cloud_provider={azure}	(Required) Specify azure for an Azure internal scan. The cloud_provider value cannot be changed during an update request. Note: Currently supporting Azure only
cloud_service={vm}	(Required) SSpecify vm (Azure virtual machine) for an Azure internal scan. The cloud_service value cannot be changed during an update request.
connector_name={value}	(Required) The name of the connector to be used. We check if the specified connector_name exists for your Qualys subscription. If the specified connector name does not exists in your Qualys subscription, then the API request returns an error message - Invalid connector_name provided.
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.

Parameter	Description
connector_uuid={value}	(Required) The ID of the connector to be used. If the specified connector name does not exists in your Qualys subscription, then the API request returns an error message - Invalid connector_uuid provided.
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
scan_title={value}	(Required) The scan title to create.
active={0|1}	(Required for Create request) Specify "1" to create an active schedule. Specify "0" to create an inactive schedule.
option_title={value}	(Required) The title of the option profile to be used.
	One of these parameters must be specified in the request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
option_id={value}	(Optional) The ID of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
priority={value}	(Optional) Specify a value of 0 - 9 to set a processing priority level for the scan. When not specified, a value of 0 (no priority) is used. Valid values are: 0 = No Priority (the default) 1 = Emergency 2 = Ultimate 3 = Critical 4 = Major 5 = High 6 = Standard 7 = Medium 8 = Minor 9 = Low
iscanner_id={value}	(Required) The IDs of the scanner appliances to be used. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.
iscanner_name={value}	(Required) The friendly names of the scanner appliances to be used. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.
platform_type={location|virtual_network}	(Optional) Select the platform type as either location or virtual network.

Parameter	Description
region_code={value}	(Required) The Azure region code. Valid values are: ap-northeast-1, ap-southeast-1, ap-southeast-2, ap-east-1, eu-west-1, eu-north-1, asa-east-1, us-east-1, us-west-1, us-west-2, me-south-1, eu-south-1, and af-south-1 **Note:** This parameter is mandatory when the platform type is set to location
virtual_network_id={value}	(Required) Provide the Id of the Azure virtual network. **Note:** This parameter is mandatory when the platform type is set to virtual network.
tag_include_selector={all|**any**}	(Optional) Select any (the default) to include hosts that match at least one of the selected tags. Select all to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select any (the default) to exclude hosts that match at least one of the selected tags. Select all to exclude hosts that match all of the selected tags.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names. We will check if the tag ids or tag names are valid.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
cloud_resource_ids={remove|any VM ID}	(Optional) Only applicable for Update request. Specific VM IDs on which scan needs to be launched (VM IDs are comma separated). Specify remove to delete the existing VM-IDs. Specify any VM ID to replace the existing VM-IDs.
schedule={value}	(Required for Create request) Specify now to schedule the scan job for now. Specify recurring to schedule the scan job to start at a later time or on a recurring basis. See Azure and GCP Internal Scan Schedule Parameters.

Google Cloud Platform Internal Scan Parameters

The input parameters for creating or updating a Google Cloud Platform (GCP) internal scan are below.

Parameter	Description
action={create|update}	(Required) Specify "create" to configure a new internal GCP scan job. Specify "update" to make changes to an existing scan job.
id={value}	(Required and only applicable for Update request) The ID of the scan schedule you want to update.
module={vm/cm}	(Required for Create request) Specify "vm" for a vulnerability scan and “cm” for Policy Audit.
cloud_provider={gcp}	(Required) Specify GCP for an GCP internal scan. The cloud_provider value cannot be changed during an update request.
cloud_service={compute engine}	(Required) Specify compute engine for an GCP internal scan. The cloud_service value cannot be changed during an update request.
connector_name={value}	(Required) The name of the connector to be used. We check if the specified connector_name exists for your Qualys subscription. If the specified connector name does not exists in your Qualys subscription, then the API request returns an error message - Invalid connector_name provided.
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
connector_uuid={value}	(Required) The ID of the connector to be used. If the specified connector name does not exists in your Qualys subscription, then the API request returns an error message - Invalid connector_uuid provided.
	One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
scan_title={value}	(Required) The scan title to create.
active={0|1}	(Required for Create request) Specify "1" to create an active schedule. Specify "0" to create an inactive schedule.
option_title={value}	(Required) The title of the option profile to be used.
	One of these parameters must be specified in the request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
option_id={value}	(Optional) The ID of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.

Parameter	Description
priority={value}	(Optional) Specify a value of 0 - 9 to set a processing priority level for the scan. When not specified, a value of 0 (no priority) is used. Valid values are: 0 = No Priority (the default) 1 = Emergency 2 = Ultimate 3 = Critical 4 = Major 5 = High 6 = Standard 7 = Medium 8 = Minor 9 = Low
iscanner_id={value}	(Required) The IDs of the scanner appliances to be used. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.
iscanner_name={value}	(Required) The friendly names of the scanner appliances to be used. Multiple entries are comma separated.
	These parameters cannot be specified in the same request: iscanner_id and iscanner_name.
region_code={value}	(Required) The GCP region code. For example, values are: ap-northeast-1, ap-southeast-1, ap-southeast-2, ap-east-1, eu-west-1, eu-north-1, asa-east-1, us-east-1, us-west-1, us-west-2, me-south-1, eu-south-1, and af-south-1
virtual_network_id={value}	(Required) Provide the Id of the GCP virtual network.
tag_include_selector={all|**any**}	(Optional) Select any (the default) to include hosts that match at least one of the selected tags. Select all to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select any (the default) to exclude hosts that match at least one of the selected tags. Select all to exclude hosts that match all of the selected tags.
tag_set_by={**id**|name}	(Optional) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names. We will check if the tag ids or tag names are valid.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

Parameter	Description
cloud_resource_ids={remove|any VM ID}	(Optional) Specific VM IDs on which the scan needs to be launched (VM IDs are comma-separated). The following are only applicable for the Update request: • Specify remove to delete the existing VM-IDs. • Specify any VM ID to replace the existing VM-IDs.
schedule={value}	(Required for Create request) Specify now to schedule the scan job for now. Specify recurring to schedule the scan job to start at a later time or on a recurring basis. See Azure and GCP Internal Scan Schedule Parameters .

Scan Schedule Parameters

Scan Schedule - Occurrence

Parameter	Description
occurrence=daily	Required for a daily scan.
frequency_days={value}	Required for a daily scan. The scan will run every N number of days. Value is an integer from 1 to 365.
occurrence=weekly	Required for a weekly scan.
frequency_weeks={value}	Required for a weekly scan. The scan will run every N number of weeks. Value is an integer from 1 to 52.
weekdays={value}	Required for a weekly scan. The scan will run on the one or more weekdays. Value is one or more days: sunday, monday, tuesday, wednesday, thursday, friday, saturday. Multiple days are comma separated.
occurrence=monthly	Required for a monthly scan.
frequency_months={value}	Required for a monthly scan. The scan will run every N number of months. Value is an integer from 1 to 12.
day_of_month={value}	Required for monthly scan - Nth day of the month. The scan will run on the Nth day of the month. Value is an integer from 1 to 31.
day_of_week={value}	Required for monthly scan - day in Nth week. The scan will run on this day of the week. Value is and integer from 0 to 6, where 0 is Sunday and 2 is Tuesday.
week_of_month={value}	Required for monthly scan - day in Nth week. The scan will run on this week of the month. Value is one of: first, second, third, fourth, last.

Scan Schedule - Start Time

Parameter	Description
start_date={mm/dd/yyyy}	(Optional) By default the start date is the date when the schedule is created. You can define another start date in mm/dd/yyyy format.
start_hour={hour}	(Required) The hour when a scan will start. The hour is an integer from 0 to 23, where 0 represents 12 AM, 7 represents 7 AM, and 22 represents 10 PM.
start_minute={minute}	(Required) The minute when a scan will start. A valid value is an integer from 0 to 59.
time_zone_code={value}	(Required) The time zone code for starting a scan, in upper case. For example, the time zone code for US California is US-CA. Valid codes are returned by the Time Zone Code API (/msp/time_zone_code_list.php).
observe_dst={yes|**no**}	(Optional) Specify yes to observe Daylight Saving Time (DST). This parameter is valid when the time zone code specified in time_zone_code supports DST.

Parameter	Description
recurrence={value}	(Optional) The number of times the scan will be run before it is deactivated. For example, if you set recurrence=2, the scan schedule will be deactivated after it runs 2 times. By default no value is set. A valid value is an integer from 1 to 99.
end_after={value}	(Optional) End a scan after some number of hours. A valid value is from 0 to 119.
end_after_mins={value}	(Optional) End a scan after some number of minutes. A valid value is an integer from 0 to 59.
	Must be specified with end_after. For example, to end the scan after 2 hours and 30 minutes, you would specify end_after=2 and end_after_mins=30.
	When end_after is set to 0, the minimum value for end_after_mins is 15.
pause_after_hours={value}	(Optional) Pause a scan after some number of hours if the scan has not finished by then. A valid value is an integer from 0 to 119.
pause_after_mins={value}	(Optional) Pause a scan after some number of minutes if the scan has not finished by then. A valid value is an integer from 0-59.
	Must be specified with pause_after_hours. For example, to pause the scan after 2 hours and 30 minutes, you would specify pause_after_hours=2 and pause_after_mins=30.
	When pause_after_hours is set to 0, the minimum value for pause_after_mins is 15.
resume_in_days={value}	(Optional) Resume a paused scan in some number of days. A valid value is an integer from 0 to 9 or Manually.
resume_in_hours={value}	(Optional) Resume a paused scan in some number of hours. A valid value is an integer from 0-23.
	Must be specified with pause_after_hours and resume_in_days. For example, to resume your scan in 5 hours, specify resume_in_days=0 and resume_in_hours=5. To resume your scan in 1 day and 12 hours, specify resume_in_days=1 and resume_in_hours=12. Note - The value you set for pause will determine the minimum value for resume. For example, if you set the scan to pause after 1 hour then you can set it to resume in 2 or more hours. If you set the scan to pause between 1-2 hours (from 1hr, 1min to 1 hr, 59min) then you can set it to resume in 3 hours or more.
set_start_time={**0**|1}	(Optional for Update only) Specify set_start_time=1 to update any of the start time parameters.
	Must be specified with all start time parameters together: start_date, start_hour, start_minute, time_zone_code, observe_dst

Scan Schedule - Notifications

Parameter	Description
before_notify={0|1}	(Optional) Specify before_notify=1 to send a notification before the scan starts. When not specified during a create request no notification is sent. When not specified during an update request we keep the previous setting.
before_notify_unit={value}	(Optional) Specify the time unit for when to send the before scan notification. Possible values are: days, hours, minutes.
	This parameter is required when before_notify=1. Not valid when before_notify=0.
before_notify_time={value}	(Optional) Indicates the number of days, hours or minutes before the scan starts the notification will be sent. For days, enter a value of 1-31. For hours, enter a value of 1-24. For minutes, enter a value of 5-120.
	This parameter is required when before_notify=1. Not valid when before_notify=0.
before_notify_message={value}	(Optional) Specify a custom message to add to the before scan notification. The notification will always include certain details like the scan title, owner, option profile and start time. Include up to 4000 characters, no HTML tags. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the last saved message.
	This parameter is only valid when before_notify=1.
after_notify={0|1}	(Optional) Specify after_notify=1 to send a notification after the scan is finished. When not specified during a create request no notification is sent. When not specified during an update request we keep the previous setting.
after_notify_message={value}	(Optional) Specify a custom message to add to the after scan notification. When not specified during a create request, no notification message is saved. Include up to 4000 characters, no HTML tags. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the last saved message. - If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the after notify message.
	This parameter is only valid when after_notify=1.

Parameter	Description
recipient_group_ids={value}	(Optional) The notification recipients in the form of one or more valid distribution group IDs. When not specified during a create request, only the task owner will be notified. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the list of IDs. - If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the list of IDs.
	This parameter is only valid when before_notify=1 or after_notify=1 is specified in the same request.
delay_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is delayed.
delay_notify_message={value}	(Optional) Specify a message to send notification for a delayed scheduled scan. If a message is not specified or if the delay_notify=1, the following default message is shown: "The Qualys scan launch has been delayed and will be tried again."
	This parameter is only valid when delay_notify=1.
skipped_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is skipped.
skipped_notify_message={value}	(Optional) Specify a message to send notification for a skipped scheduled scan. If a message is not specified or if the skipped_notify=1, the following default message is shown: "The Qualys scan launch has been skipped."
	This parameter is only valid when skipped_notify=1.
deactivate_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is deactivated.
deactivate_notify_message={value}	(Optional) Specify a message to send notification for a deactivated scheduled scan. If a message is not specified or if the deactivate_notify=1, the following default message is shown: "The Qualys scan has been deactivated by the service."
	This parameter is only valid when deactivate_notify=1.

Scan Schedule - Consultant type subscriptions

Parameter	Description
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions).
	Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.

Azure and GCP Internal Scan Schedule Parameters

Scan Schedule - Occurrence

Parameter	Description
occurrence=daily	Required for a daily scan.
frequency_days={value}	Required for a daily scan. The scan will run every N number of days. Value is an integer from 1 to 365.
occurrence=weekly	Required for a weekly scan.
frequency_weeks={value}	Required for a weekly scan. The scan will run every N number of weeks. Value is an integer from 1 to 52.
weekdays={value}	Required for a weekly scan. The scan will run on the one or more weekdays. Value is one or more days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday. Multiple days are comma separated.
occurrence=monthly	Required for a monthly scan.
frequency_months={value}	Required for a monthly scan. The scan will run every N number of months. Value is an integer from 1 to 12.
day_of_month={value}	Required for monthly scan - N^{th} day of the month. The scan will run on the Nth day of the month. Value is an integer from 1 to 31.
day_of_week={value}	Required for monthly scan - day in N^{th} week. The scan will run on this day of the week. Value is and integer from 0 to 6, where 0 is Sunday and 2 is Tuesday.
week_of_month={value}	Required for monthly scan - day in N^{th} week. The scan will run on this week of the month. Value is one of: first, second, third, fourth, last.

Scan Schedule - Start Time

Parameter	Description
start_date={mm/dd/yyyy}	(Optional) By default the start date is the date when the schedule is created. You can define another start date in mm/dd/yyyy format.
start_hour={hour}	(Required) The hour when a scan will start. The hour is an integer from 0 to 23, where 0 represents 12 AM, 7 represents 7 AM, and 22 represents 10 PM.

Parameter	Description
start_minute={minute}	(Required) The minute when a scan will start. A valid value is an integer from 0 to 59.
time_zone_code={value}	(Required) The time zone code for starting a scan, in upper case. For example, the time zone code for US California is US-CA. Valid codes are returned by the Time Zone Code API (/msp/time_zone_code_list.php).
observe_dst={yes|**no**}	(Optional) Specify yes to observe Daylight Saving Time (DST). This parameter is valid when the time zone code specified in time_zone_code supports DST.
recurrence={value}	(Optional) The number of times the scan will be run before it is deactivated. For example, if you set recurrence=2, the scan schedule will be deactivated after it runs 2 times. By default no value is set. A valid value is an integer from 1 to 99.
end_after={value}	(Optional) End a scan after some number of hours. A valid value is from 0 to 119.
end_after_mins={value}	(Optional) End a scan after some number of minutes. A valid value is an integer from 0 to 59.
	Must be specified with end_after. For example, to end the scan after 2 hours and 30 minutes, you would specify end_after=2 and end_after_mins=30.
	When end_after is set to 0, the minimum value for end_after_mins is 15.
pause_after_hours={value}	(Optional) Pause a scan after some number of hours if the scan has not finished by then. A valid value is an integer from 0 to 119.
pause_after_mins={value}	(Optional) Pause a scan after some number of minutes if the scan has not finished by then. A valid value is an integer from 0-59.
	Must be specified with pause_after_hours. For example, to pause the scan after 2 hours and 30 minutes, you would specify pause_after_hours=2 and pause_after_mins=30.
	When pause_after_hours is set to 0, the minimum value for pause_after_mins is 15.
resume_in_days={value}	(Optional) Resume a paused scan in some number of days. A valid value is an integer from 0 to 9 or Manually.

Parameter	Description
resume_in_hours={value}	(Optional) Resume a paused scan in some number of hours. A valid value is an integer from 0-23.
	Must be specified with pause_after_hours and resume_in_days. For example, to resume your scan in 5 hours, specify resume_in_days=0 and resume_in_hours=5. To resume your scan in 1 day and 12 hours, specify resume_in_days=1 and resume_in_hours=12. Note - The value you set for pause will determine the minimum value for resume. For example, if you set the scan to pause after 1 hour then you can set it to resume in 2 or more hours. If you set the scan to pause between 1-2 hours (from 1hr, 1min to 1 hr, 59min) then you can set it to resume in 3 hours or more.
set_start_time={**0**|1}	(Optional for Update only) Specify set_start_time=1 to update any of the start time parameters.
	Must be specified with all start time parameters together: start_date, start_hour, start_minute, time_zone_code, observe_dst

Scan Schedule - Notifications

Parameter	Description
before_notify={0|1}	(Optional) Specify before_notify=1 to send a notification before the scan starts. When not specified during a create request no notification is sent. When not specified during an update request we keep the previous setting.
before_notify_unit={value}	(Optional) Specify the time unit for when to send the before scan notification. Possible values are: days, hours, minutes.
	This parameter is required when before_notify=1. Not valid when before_notify=0.
before_notify_time={value}	(Optional) Indicates the number of days, hours or minutes before the scan starts the notification will be sent. For days, enter a value of 1-31. For hours, enter a value of 1-24. For minutes, enter a value of 5-120.
	This parameter is required when before_notify=1. Not valid when before_notify=0.
before_notify_message={value}	(Optional) Specify a custom message to add to the before scan notification. The notification will always include certain details like the scan title, owner, option profile and start time. Include up to 4000 characters, no HTML tags. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the last saved message.
	This parameter is only valid when before_notify=1.
after_notify={0|1}	(Optional) Specify after_notify=1 to send a notification after the scan is finished. When not specified during a create request no notification is sent. When not specified during an update request we keep the previous setting.
after_notify_message={value}	(Optional) Specify a custom message to add to the after scan notification. When not specified during a create request, no notification message is saved. Include up to 4000 characters, no HTML tags. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the last saved message. - If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the after notify message.
	This parameter is only valid when after_notify=1.

Parameter	Description
recipient_group_ids={value}	(Optional) The notification recipients in the form of one or more valid distribution group IDs. When not specified during a create request, only the task owner will be notified. For update requests: - When not specified we keep the previous setting. - Specify an empty string to delete the list of IDs. - If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the list of IDs. This parameter is only valid when before_notify=1 or after_notify=1 is specified in the same request.

VM Scan Statistics

/api/2.0/fo/scan/stats/?action=list

[GET] [POST]

List details about vulnerability scans and assets that are waiting to be processed.

Permissions - Manager role is required.

You'll see these sections in the XML output:

UNPROCESSED SCANS - The total number of scans that are not processed, including scans that are queued, running, loading, finished, etc.

VM RECRYPT BACKLOG - The total number of assets across your finished scans that are waiting to be processed.

VM RECRYPT BACKLOG BY SCAN - Scan details for vulnerability scans that are waiting to be processed. For each scan, you'll see the scan ID, scan title, scan status, processing priority and number of hosts that the scan finished but not processed.

VM RECRYPT BACKLOG BY TASK - Processing task details for vulnerability scans that are waiting to be processed. For each task, you'll see the same scan details as VM RECRYPT BACKLOG BY SCAN plus additional information like the total hosts alive for the scan, the number of hosts from the scan that have been processed, the number of hosts waiting to be processed, the scan start date, the task type and task status.

Sample - List VM statistics

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"<qualy_base_url>/api/2.0/fo/scan/stats/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE TASK_PROCESSING SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/stats/vm_recrypt_res
```

```
ults.dtd">
      <TASK_PROCESSING>
        <UNPROCESSED_SCANS><![CDATA[366]]></UNPROCESSED_SCANS>
        <VM_RECRYPT_BACKLOG><![CDATA[116]]></VM_RECRYPT_BACKLOG>
        <VM_RECRYPT_BACKLOG_BY_SCAN>
          <SCAN>
            <ID><![CDATA[189275]]></ID>
            <TITLE><![CDATA[API_V2_IP_Scan_1511513769]]></TITLE>
            <STATUS><![CDATA[Loading]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <COUNT><![CDATA[2]]></COUNT>
          </SCAN>
          <SCAN>
            <ID><![CDATA[189281]]></ID>
            <TITLE><![CDATA[API_V2_AG_Scan_1511513846]]></TITLE>
            <STATUS><![CDATA[Loading]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <COUNT><![CDATA[2]]></COUNT>
          </SCAN>
          <SCAN>
            <ID><![CDATA[190773]]></ID>
            <TITLE><![CDATA[API_V2_IP_Scan_]]></TITLE>
            <STATUS><![CDATA[Finished]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <COUNT><![CDATA[2]]></COUNT>
          </SCAN>
          <SCAN>
            <ID><![CDATA[190775]]></ID>
            <TITLE><![CDATA[API_V2_IP_Scan_]]></TITLE>
            <STATUS><![CDATA[Finished]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <COUNT><![CDATA[2]]></COUNT>
          </SCAN>
          ...
        </VM_RECRYPT_BACKLOG_BY_SCAN>
        <VM_RECRYPT_BACKLOG_BY_TASK>
          <SCAN>
            <ID><![CDATA[210337]]></ID>
            <TITLE><![CDATA[API_V2_AG_Scan_1515055579]]></TITLE>
            <STATUS><![CDATA[Loading]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
```

```
            <NBHOST><![CDATA[]]></NBHOST>
            <TO_PROCESS><![CDATA[3]]></TO_PROCESS>
            <PROCESSED><![CDATA[0]]></PROCESSED>
           <SCAN_DATE><![CDATA[2018-01-04T08:46:13Z]]></SCAN_DATE>
            <SCAN_UPDATED_DATE><![CDATA[2018-01-
04T08:58:05Z]]></SCAN_UPDATED_DATE>
            <TASK_TYPE><![CDATA[VM Scan Processing]]></TASK_TYPE>
            <TASK_STATUS><![CDATA[Queued]]></TASK_STATUS>
            <TASK_UPDATED_DATE><![CDATA[2018-01-
12T08:17:09Z]]></TASK_UPDATED_DATE>
          </SCAN>
          <SCAN>
            <ID><![CDATA[215356]]></ID>
            <TITLE><![CDATA[API_V2_AG_Scan_1515742250]]></TITLE>
            <STATUS><![CDATA[Running]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <NBHOST><![CDATA[]]></NBHOST>
            <TO_PROCESS><![CDATA[0]]></TO_PROCESS>
            <PROCESSED><![CDATA[0]]></PROCESSED>
           <SCAN_DATE><![CDATA[2018-01-12T07:30:42Z]]></SCAN_DATE>
            <SCAN_UPDATED_DATE><![CDATA[2018-01-
12T08:01:10Z]]></SCAN_UPDATED_DATE>
            <TASK_TYPE><![CDATA[VM Scan Processing]]></TASK_TYPE>
            <TASK_STATUS><![CDATA[Queued]]></TASK_STATUS>
            <TASK_UPDATED_DATE><![CDATA[2018-01-
12T08:17:11Z]]></TASK_UPDATED_DATE>
          </SCAN>
          <SCAN>
            <ID><![CDATA[215357]]></ID>
            <TITLE><![CDATA[API_V2_AG_Scan_1515742265]]></TITLE>
            <STATUS><![CDATA[Loading]]></STATUS>

<PROCESSING_PRIORITY><![CDATA[None]]></PROCESSING_PRIORITY>
            <NBHOST><![CDATA[]]></NBHOST>
            <TO_PROCESS><![CDATA[0]]></TO_PROCESS>
            <PROCESSED><![CDATA[0]]></PROCESSED>
           <SCAN_DATE><![CDATA[2018-01-12T07:30:58Z]]></SCAN_DATE>
            <SCAN_UPDATED_DATE><![CDATA[2018-01-
12T08:14:45Z]]></SCAN_UPDATED_DATE>
            <TASK_TYPE><![CDATA[VM Scan Processing]]></TASK_TYPE>
            <TASK_STATUS><![CDATA[Queued]]></TASK_STATUS>
            <TASK_UPDATED_DATE><![CDATA[2018-01-
12T08:17:11Z]]></TASK_UPDATED_DATE>
          </SCAN>
          ...
```

```
    </VM_RECRYPT_BACKLOG_BY_TASK>
  </TASK_PROCESSING>
```

DTD

<platform API server>/api/2.0/fo/scan/stats/vm_recrypt_results.dtd

VM Scan Summary

/api/2.0/fo/scan/vm/summary/

[GET] [POST]

This API can be used as an alternative to the original Scan Summary API. It's easier to use, has more filter options and enhanced output content.

This API helps you to identify hosts that were scanned or not scanned and why. You can choose to get a scan summary for a particular scan by specifying the scan reference ID or for all scans launched since a certain date/time or within a date range.

This API will return details for all scans. Note, however, that the output will not include the <SCAN_RESULTS> block if the scan did not return results for some reason.

Permissions

Manager role is required.

Input Parameters

The following input parameters are supported.

Parameter	Description
action=list	(Required) The list action.
output_format=xml	(Optional) The only supported output format at this time is XML.
scan_reference={value}	(Optional) Specifies a unique scan reference ID. Use this option to include scan summary information for a single scan only. For VM scans, the scan reference has the format scan/987654321.98765.
	One of these parameters must be specified in the request: scan_datetime_since or scan_reference. You cannot specify scan_reference in the same request as scan_datetime_since and scan_datetime_until.
scan_datetime_since={value}	(Optional) Include scans started since a certain date. The date must be less than or equal to today's date. Specify the date in GMT timezone in RFC 3339 format: yyyy-mm-ddThh-mm-ssZ. Example: 2020-10-01T09:30:48Z
	One of these parameters must be specified in the request: scan_datetime_since or scan_reference. You cannot specify scan_datetime_since in the same request as scan_reference.
scan_datetime_until={value}	(Optional) Include scans started up to a certain date. The date must be more than or equal to scan_datetime_since, and less than or equal to today's date. Specify the date in GMT timezone in RFC 3339 format: yyyy-mm-ddThh-mm-ssZ. Example: 2020-10-01T09:30:48Z
	The parameter scan_datetime_until can only be specified when scan_datetime_since is also specified. You cannot specify scan_datetime_until in the same request as scan_reference.

Parameter	Description
include_scan_input={0|1}	(Optional) By default, scan input information is included in the XML output in the <SCAN_INPUT> block. Specify include_scan_input=0 if you don't want this entire block to appear in the output. Scan input information includes the scan title, user login (for user who launched the scan), whether or not the scan was scheduled, scan target, network, option profile, etc.
include_scan_details={0|1}	(Optional) By default, scan details are included in the XML output in the <SCAN_DETAILS> block. Specify include_scan_details=0 if you don't want this entire block to appear in the output. Scan details include the scan status, launch date/time, and scan duration.
include_hosts_summary={0|1}	(Optional) By default, hosts summary information is included in the XML output in the <HOSTS> block under <SCAN_RESULTS>. Specify include_hosts_summary=0 if you don't want the <HOSTS> block to appear in the output. The hosts summary shows the total number of hosts scanned, and lists the IP addresses, DNS hostnames and NetBIOS hostnames in the scan.
include_detections_summary={0|1}	(Optional) By default, detections summary information is included in the XML output in the <DETECTIONS> block under <SCAN_RESULTS>. Specify include_detections_summary=0 if you don't want the <DETECTIONS> block to appear in the output. The detections summary includes the total number of detections, and the number of detections by severity for confirmed, potential and information gathered. All detections, irrespective of their status, are included in the response. **Note:** You may notice a discrepancy when comparing the summary response with the Scan Results section. This is expected because the Scan Results section excludes vulnerabilities that have already been closed, whereas the summary response reflects the full count, including closed vulnerabilities.
include_hosts_summary_categories={value}	(Optional) When unspecified, all categories are included in the XML output. To filter the categories, provide a comma-separated list of the categories to include in the output. Possible values are: scanned, excluded, cancelled, unresolved, duplicate, not_vulnerable, dead, aborted, blocked, failed_slice, exceeded_scan_duration. See Host Summary Categories below for more information on each category. Each category appears a block inside <SCAN_RESULTS> <HOSTS>. If a category is filtered out, the respective category block does not appear in the output.

Host Summary Categories

The following host summary categories may be included in the scan summary output:

Scanned - The hosts were scanned successfully.

Excluded - The hosts were excluded. Hosts may be excluded on a per scan basis (by the user launching or scheduling the scan) or globally for all scans. Managers and Unit Managers have privileges to edit the global excluded hosts list for the subscription.

Cancelled - Hosts were not scanned because the scan was cancelled. Scans may be cancelled by a user, by an administrator or automatically by the service as specified in scheduled scan settings.

Unresolved - Hosts were scanned but they could not be reported because the NetBIOS or DNS hostname, whichever tracking method is specified for each host, could not be resolved.

Duplicate - The hosts were duplicated within a single segment/slice of the scan job. For example, two different hostnames resolving to the same IP with tracking by IP.

Not Vulnerable - Hosts were found to be not vulnerable during host discovery without having to run a full scan. This could happen for example if the list of QIDs to be scanned are limited to certain ports and those ports are found to be closed.

Dead - The hosts were not “alive” at the time of the scan, meaning that they did not respond to probes sent by the scanning engine, and the option to Scan Dead Hosts was not enabled.

Aborted - The scan was abruptly discontinued. This is a rare occurrence that may be caused for different reasons. For example, it's possible that a connection timed out or there were connection errors on a particular port or the scan time elapsed.

Blocked - Hosts were blocked from scanning for some reason. For example, user provided blacklisted IPs to scan and after the scan was launched it was blocked due to improper configuration.

Failed Slice Hosts - The scan failed for these hosts.

Exceeded Scan Duration - Applicable when the Maximum Scan Duration per Asset feature is enabled and a maximum scan duration is specified in the option profile used for the scan. This setting determines how long a scan can run on a single asset. The scan on these hosts exceeded the scan duration allowed so the scan on these hosts was aborted.

Sample 1 - Get scan summary by scan reference

In this sample, the scan reference ID is included as part of the request.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/scan/vm/summary/?action=list&include_scan_i
nput=1&include_hosts_summary=1&output_format=xml&include_detections_summa
ry=1&scan_reference=scan/9876543210.12345"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2020-09-15T09:09:36Z</DATETIME>
        <SCAN_SUMMARY_LIST>
            <SCAN_SUMMARY>
                <SCAN_REFERENCE>scan/9876543210.12345</SCAN_REFERENCE>
                <SCAN_INPUT>
                    <TITLE>CustomAgScan</TITLE>
                    <USER>
                        <USERNAME>qualys_joe</USERNAME>
                    </USER>
                    <SCHEDULED>0</SCHEDULED>
                    <SCAN_DATETIME>2020-04-01 06:55:55</SCAN_DATETIME>
                    <NETWORK>
                        <ID>63010</ID>
                        <NAME>Custom Network</NAME>
                    </NETWORK>
                    <OPTION_PROFILE>
                        <ID>86395</ID>
                        <NAME>Initial Options</NAME>
                    </OPTION_PROFILE>
                    <TARGETS>
                        <IP_LIST>
                            <COUNT>256</COUNT>
                            <IP_DATA>
                                <RANGES>
                                    <RANGE>11.1.1.0-11.1.1.255</RANGE>
                                </RANGES>
                            </IP_DATA>
                        </IP_LIST>
                        <DNS_LIST>
                            <COUNT>3</COUNT>
                            <DNS_DATA>

<DNS_CSV>sample2.com,sample3.com,sample1.com</DNS_CSV>
                            </DNS_DATA>
                        </DNS_LIST>
                        <NETBIOS_LIST>
                            <COUNT>3</COUNT>
                            <NETBIOS_DATA>

<NETBIOS_CSV>NB1.COM,NB3.COM,NB2.COM</NETBIOS_CSV>
                            </NETBIOS_DATA>
                        </NETBIOS_LIST>
                        <ASSET_GROUP_LIST>
                            <COUNT>1</COUNT>
                            <ASSET_GROUP_DATA>
                                <ASSET_GROUP>
                                    <ID>206216</ID>
                                   <NAME>Custom Network Asset Group</NAME>
                                </ASSET_GROUP>
                            </ASSET_GROUP_DATA>
                        </ASSET_GROUP_LIST>
                    </TARGETS>
                </SCAN_INPUT>
                <SCAN_DETAILS>
```

```
                    <STATUS>ERROR</STATUS>
                   <LAUNCH_DATETIME>2020-04-01 06:55:55</LAUNCH_DATETIME>
                    <DURATION>1261</DURATION>
                </SCAN_DETAILS>
                <SCAN_RESULTS>
                    <HOSTS>
                        <COUNT>262</COUNT>
                        <HOSTS_DATA>
                            <SCANNED>
                                 <IP_LIST>
                                    <COUNT>9</COUNT>
                                    <IP_DATA>
                                        <RANGES>
                                            <RANGE>43.56.78.111-
43.56.78.119</RANGE>
                                        </RANGES>
                                    </IP_DATA>
                                </IP_LIST>
                            </SCANNED>
                            <FAILED_SLICE_HOSTS>
                                <IPV4_LIST>
                                    <COUNT>8</COUNT>
                                    <IPV4_DATA>
                                        <IPV4_CSV>10.10.10.1,10.20.10.10-
10.20.10.13,10.10.10.3,10.20.10.7,10.10.10.8,10.20.10.11</IPV4_CSV>
                                    </IPV4_DATA>
                                </IPV4_LIST>
                                <IPV6_LIST>
                                    <COUNT>2</COUNT>
                                    <IPV6_DATA>

<IPV6_CSV>::ff01,::ff02,::ff02</IPV6_CSV>
                                    </IPV6_DATA>
                                </IPV6_LIST>
                                <DNS_LIST>
                                    <COUNT>4</COUNT>
                                    <DNS_DATA>
                                       <DNS_CSV>sample4.com, sample5.com,
sample6.com, sample7.com</DNS_CSV>
                                    </DNS_DATA>
                                </DNS_LIST>
                                <NETBIOS_LIST>
                                    <COUNT>4</COUNT>
                                    <NETBIOS_DATA>
                                        <NETBIOS_CSV>WIN2KB,
SATEELITE,WIN4KB, KRWSDG</NETBIOS_CSV>
                                    </NETBIOS_DATA>
                                </NETBIOS_LIST>
                            </FAILED_SLICE_HOSTS>
</HOSTS_DATA>
                    </HOSTS>
                    <DETECTIONS>
                        <IG>
                            <TOTAL_COUNT>7216</TOTAL_COUNT>
```

```
                        <COUNT_BY_SEVERITY>
                            <SEVERITY_1>4467</SEVERITY_1>
                            <SEVERITY_2>2232</SEVERITY_2>
                            <SEVERITY_3>517</SEVERITY_3>
                            <SEVERITY_4>0</SEVERITY_4>
                            <SEVERITY_5>0</SEVERITY_5>
                        </COUNT_BY_SEVERITY>
                    </IG>
                    <VULN>
                        <CONFIRMED>
                            <TOTAL_COUNT>8054</TOTAL_COUNT>
                            <COUNT_BY_SEVERITY>
                                <SEVERITY_1>238</SEVERITY_1>
                                <SEVERITY_2>985</SEVERITY_2>
                                <SEVERITY_3>2124</SEVERITY_3>
                                <SEVERITY_4>2546</SEVERITY_4>
                                <SEVERITY_5>2161</SEVERITY_5>
                            </COUNT_BY_SEVERITY>
                        </CONFIRMED>
                        <POTENTIAL>
                            <TOTAL_COUNT>1497</TOTAL_COUNT>
                            <COUNT_BY_SEVERITY>
                                <SEVERITY_1>17</SEVERITY_1>
                                <SEVERITY_2>420</SEVERITY_2>
                                <SEVERITY_3>579</SEVERITY_3>
                                <SEVERITY_4>304</SEVERITY_4>
                                <SEVERITY_5>177</SEVERITY_5>
                            </COUNT_BY_SEVERITY>
                        </POTENTIAL>
                    </VULN>
                </DETECTIONS>
            </SCAN_RESULTS>
        </SCAN_SUMMARY>
    </SCAN_SUMMARY_LIST>
</RESPONSE>
</SCAN_SUMMARY_OUTPUT>
```

Sample 2 - Get scan summary by scan date

In this sample, all scans within the date range will be returned.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/?action=list&out
put_format=xml&scan_datetime_since=2020-04-
06T02:30:00Z&scan_datetime_until=2020-04-06T02:30:00Z"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
```

```
<RESPONSE>
  <DATETIME>2020-09-22T05:02:40Z</DATETIME>
  <SCAN_SUMMARY_LIST>
    <SCAN_SUMMARY>
      <SCAN_REFERENCE>scan/1234567890.12345</SCAN_REFERENCE>
      <SCAN_INPUT>
        <TITLE>My-Scan</TITLE>
        <USER>
          <USERNAME>qualys_joe</USERNAME>
        </USER>
        <SCHEDULED>0</SCHEDULED>
        <SCAN_DATETIME>2020-04-06 07:17:45</SCAN_DATETIME>
        <NETWORK>
          <ID>0</ID>
          <NAME>Global Default Network</NAME>
        </NETWORK>
        <OPTION_PROFILE>
          <ID>2171</ID>
          <NAME>Initial Options</NAME>
        </OPTION_PROFILE>
        <TARGETS>
          <IP_LIST>
            <COUNT>3</COUNT>
            <IP_DATA>
              <RANGES>
                <RANGE>10.10.30.10-10.10.30.12</RANGE>
              </RANGES>
            </IP_DATA>
          </IP_LIST>
        </TARGETS>
      </SCAN_INPUT>
      <SCAN_DETAILS>
        <STATUS>FINISHED</STATUS>
        <LAUNCH_DATETIME>2020-04-06 07:17:45</LAUNCH_DATETIME>
        <DURATION>21656</DURATION>
      </SCAN_DETAILS>
      <SCAN_RESULTS>
        <HOSTS>
          <COUNT>3</COUNT>
          <HOSTS_DATA>
            <SCANNED>
              <IP_LIST>
                <COUNT>2</COUNT>
                <IP_DATA>
                  <RANGES>
                    <RANGE>10.10.30.10-10.10.30.11</RANGE>
                  </RANGES>
                </IP_DATA>
              </IP_LIST>
            </SCANNED>
            <DEAD>
              <IP_LIST>
                <COUNT>1</COUNT>
                <IP_DATA>
```

```
                    <IP_CSV>10.10.30.12</IP_CSV>
                  </IP_DATA>
                </IP_LIST>
              </DEAD>
              <FAILED_SLICE_HOSTS>
               <IPV4_LIST>
                 <COUNT>8</COUNT>
                 <IPV4_DATA>
                   <IPV4_CSV>10.10.10.1,10.20.10.10-
10.20.10.13,10.10.10.3,10.20.10.7,10.10.10.8,10.20.10.11</IPV4_CSV>
                 </IPV4_DATA>
              </IPV4_LIST>
              <IPV6_LIST>
                <COUNT>2</COUNT>
                <IPV6_DATA>
                <IPV6_CSV>::ff01,::ff02,::ff02</IPV6_CSV>
              </IPV6_DATA>
              </IPV6_LIST>
              <DNS_LIST>
                <COUNT>4</COUNT>
              <DNS_DATA>
                 <DNS_CSV>sample1.com, sample2.com, sample3.com,
sample4.com</DNS_CSV>
              </DNS_DATA>
              </DNS_LIST>
              <NETBIOS_LIST>
                <COUNT>4</COUNT>
              <NETBIOS_DATA>
             <NETBIOS_CSV>SAMPLE1, SAMPLE2, SAMPLE3, SAMPLE4</NETBIOS_CSV>
               </NETBIOS_DATA>
               </NETBIOS_LIST>
              </FAILED_SLICE_HOSTS>
            </HOSTS_DATA>
          </HOSTS>
          <DETECTIONS>
            <IG>
              <TOTAL_COUNT>77</TOTAL_COUNT>
              <COUNT_BY_SEVERITY>
                <SEVERITY_1>52</SEVERITY_1>
                <SEVERITY_2>12</SEVERITY_2>
                <SEVERITY_3>5</SEVERITY_3>
                <SEVERITY_4>2</SEVERITY_4>
                <SEVERITY_5>6</SEVERITY_5>
              </COUNT_BY_SEVERITY>
            </IG>
            <VULN>
              <CONFIRMED>
                <TOTAL_COUNT>17</TOTAL_COUNT>
                <COUNT_BY_SEVERITY>
                  <SEVERITY_1>0</SEVERITY_1>
                  <SEVERITY_2>3</SEVERITY_2>
                  <SEVERITY_3>10</SEVERITY_3>
                  <SEVERITY_4>0</SEVERITY_4>
                  <SEVERITY_5>4</SEVERITY_5>
```

```
                </COUNT_BY_SEVERITY>
              </CONFIRMED>
              <POTENTIAL>
                <TOTAL_COUNT>18</TOTAL_COUNT>
                <COUNT_BY_SEVERITY>
                  <SEVERITY_1>2</SEVERITY_1>
                  <SEVERITY_2>4</SEVERITY_2>
                  <SEVERITY_3>10</SEVERITY_3>
                  <SEVERITY_4>1</SEVERITY_4>
                  <SEVERITY_5>1</SEVERITY_5>
                </COUNT_BY_SEVERITY>
              </POTENTIAL>
            </VULN>
          </DETECTIONS>
        </SCAN_RESULTS>
      </SCAN_SUMMARY>
...
```

Sample 3 - Filter list of categories in output

In this sample, only the Cancelled category is included.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/?action=list&out
put_format=xml&scan_reference=scan/1234567890.12345&include_hosts_summary
_categories=cancelled"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-22T05:07:05Z</DATETIME>
    <SCAN_SUMMARY_LIST>
      <SCAN_SUMMARY>
        <SCAN_REFERENCE>scan/1234567890.12345</SCAN_REFERENCE>
        <SCAN_INPUT>
          <TITLE>My-Scan-2</TITLE>
          <USER>
            <USERNAME>qualys_joe</USERNAME>
          </USER>
          <SCHEDULED>0</SCHEDULED>
          <SCAN_DATETIME>2020-08-06 03:52:30</SCAN_DATETIME>
          <NETWORK>
            <ID>1000</ID>
            <NAME>My-Custom-Network</NAME>
          </NETWORK>
          <OPTION_PROFILE>
            <ID>2134</ID>
            <NAME>Initial Options</NAME>
```

```
  </OPTION_PROFILE>
  <TARGETS>
  </TARGETS>
</SCAN_INPUT>
<SCAN_DETAILS>
  <STATUS>CANCELED</STATUS>
  <LAUNCH_DATETIME>2020-08-06 03:52:30</LAUNCH_DATETIME>
  <DURATION>10</DURATION>
</SCAN_DETAILS>
<SCAN_RESULTS>
  <HOSTS>
    <COUNT>4</COUNT>
    <HOSTS_DATA>
      <CANCELLED>
        <IP_LIST>
          <COUNT>2</COUNT>
          <IP_DATA>
            <IP_CSV>10.10.25.232, 10.10.25.240</IP_CSV>
          </IP_DATA>
        </IP_LIST>
        <DNS_LIST>
          <COUNT>2</COUNT>
          <DNS_DATA>
            <DNS_CSV>dns1.qualys.com,dns2.qualys.com</DNS_CSV>
          </DNS_DATA>
        </DNS_LIST>
      </CANCELLED>
    </HOSTS_DATA>
  </HOSTS>
  <DETECTIONS>
    <IG>
      <TOTAL_COUNT>0</TOTAL_COUNT>
      <COUNT_BY_SEVERITY>
        <SEVERITY_1>0</SEVERITY_1>
        <SEVERITY_2>0</SEVERITY_2>
        <SEVERITY_3>0</SEVERITY_3>
        <SEVERITY_4>0</SEVERITY_4>
        <SEVERITY_5>0</SEVERITY_5>
      </COUNT_BY_SEVERITY>
    </IG>
    <VULN>
      <CONFIRMED>
        <TOTAL_COUNT>0</TOTAL_COUNT>
        <COUNT_BY_SEVERITY>
          <SEVERITY_1>0</SEVERITY_1>
          <SEVERITY_2>0</SEVERITY_2>
          <SEVERITY_3>0</SEVERITY_3>
          <SEVERITY_4>0</SEVERITY_4>
          <SEVERITY_5>0</SEVERITY_5>
        </COUNT_BY_SEVERITY>
      </CONFIRMED>
      <POTENTIAL>
        <TOTAL_COUNT>0</TOTAL_COUNT>
        <COUNT_BY_SEVERITY>
```

```
                    <SEVERITY_1>0</SEVERITY_1>
                    <SEVERITY_2>0</SEVERITY_2>
                    <SEVERITY_3>0</SEVERITY_3>
                    <SEVERITY_4>0</SEVERITY_4>
                    <SEVERITY_5>0</SEVERITY_5>
                  </COUNT_BY_SEVERITY>
                </POTENTIAL>
              </VULN>
            </DETECTIONS>
          </SCAN_RESULTS>
        </SCAN_SUMMARY>
      </SCAN_SUMMARY_LIST>
    </RESPONSE>
  </SCAN_SUMMARY_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/scan/vm/summary/output.dtd

Scan Summary

/api/2.0/fo/scan/summary/

[GET] [POST]

This is the original VM Scan Summary API for identifying hosts that were not scanned and why. We recommend you try the new improved VM Scan Summary API which has more filter options and enhanced output content. See VM Scan Summary.

Permissions

Manager role is required.

How it works

First we'll find all the scans launched since the date (or within the date range) that you specify. Then we'll identify hosts that were included in the scan target but not scanned for some reason. For each host you'll see the category/reason it was not scanned and the host's tracking method.

Categories for hosts not scanned:

Excluded - The hosts were excluded. Hosts may be excluded on a per scan basis (by the user launching or scheduling the scan) or globally for all scans. Managers and Unit Managers have privileges to edit the global excluded hosts list for the subscription.

Cancelled - Hosts were not scanned because the scan was cancelled. Scans may be cancelled by a user, by an administrator or automatically by the service as specified in scheduled scan settings.

Dead - The hosts were not "alive" at the time of the scan, meaning that they did not respond to probes sent by the scanning engine, and the option to Scan Dead Hosts was not enabled.

Unresolved - Hosts were scanned but they could not be reported because the NetBIOS or DNS hostname, whichever tracking method is specified for each host, could not be resolved.

Duplicate - The hosts were duplicated within a single segment/slice of the scan job. For example, two different hostnames resolving to the same IP with tracking by IP.

Not Vulnerable - Hosts were found to be not vulnerable during host discovery without having to run a full scan. This could happen for example if the list of QIDs to be scanned are limited to certain ports and those ports are found to be closed.

Aborted - The scan was abruptly discontinued. This is a rare occurrence that may be caused for different reasons. For example, it's possible that a connection timed out or there were connection errors on a particular port or the scan time elapsed.

Blocked - Hosts were blocked from scanning for some reason. For example, user provided blacklisted IPs to scan and after the scan was launched it was blocked due to improper configuration.

Input Parameters

Parameter	Description
action=list	(Required)
scan_date_since={value}	(Required) Include scans started since a certain date. Specify the date in YYYY-MM-DD format. The date must be less than or equal to today's date.
scan_date_to={value}	(Optional) Include scans started up to a certain date. Specify the date in YYYY-MM-DD format. The date must be more than or equal to scan_date_since, and less than or equal to today's date.
output_format={value}	(Optional) The output format: XML (the default), CSV or JSON.
tracking_method={value}	(Optional) By default hosts with any tracking method will be returned in the output. Use this option to only include hosts with a certain tracking method. Valid values are: IP, DNS, NETBIOS.
include_dead={0|**1**}	(Optional) Set to 0 if you do not want to include dead hosts in the output. Dead hosts are included by default.
include_excluded={**0**|1}	(Optional) Set to 1 to include hosts that were excluded from a scan in the output. Excluded hosts are not included by default.
include_unresolved={**0**|1}	(Optional) Set to 1 to include unresolved hosts in the output. Unresolved hosts are not included by default.
include_cancelled={**0**|1}	(Optional) Set to 1 to include cancelled hosts in the output. Cancelled hosts are not included by default.
include_notvuln={**0**|1}	(Optional) Set to 1 to include hosts that are not vulnerable in the output. Not vulnerable hosts are not included by default.
include_blocked={**0**|1}	(Optional) Set to 1 to include blocked hosts in the output. Blocked hosts are not included by default.
include_duplicate={**0**|1}	(Optional) Set to 1 to include duplicate hosts in the output. Duplicate hosts are not included by default.
include_aborted={**0**|1}	(Optional) Set to 1 to include aborted hosts in the output. Aborted hosts are not included by default.

Sample - VM scan summary

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/summary/?action=list
&scan_date_since=2018-04-
27&include_excluded=1&include_unresolved=1
&include_cancelled=1&include_notvuln=1&include_duplicate=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/summary/scan_summary
```

```
_output.dtd">
<SCAN_SUMMARY_OUTPUT>
 <RESPONSE>
   <DATETIME>2018-05-02T10:45:40Z</DATETIME>
   <SCAN_SUMMARY_LIST>
     <SCAN_SUMMARY>
       <SCAN_REF>scan/1525251885.92469</SCAN_REF>
       <SCAN_DATE>2018-05-02T09:04:34Z</SCAN_DATE>
       <HOST_SUMMARY category="notvuln" tracking="IP">10.10.10.10-
10.10.10.15,10.10.10.17</HOST_SUMMARY>
       <HOST_SUMMARY category="notvuln" tracking="DNS">gfi-31-
1.caac125.qualys.com,gfi-31-2.caac125.qualys.com</HOST_SUMMARY>
       <HOST_SUMMARY category="notvuln" tracking="NETBIOS">gfi-31-
3,gfi-31-4</HOST_SUMMARY>
       <HOST_SUMMARY category="cancelled"
tracking="IP">10.10.10.20,10.10.10.22</HOST_SUMMARY>
       <HOST_SUMMARY category="cancelled" tracking="DNS">gfi-31-
5.caac125.qualys.com,gfi-31-6.caac125.qualys.com</HOST_SUMMARY>
       <HOST_SUMMARY category="dead"
tracking="IP">10.10.10.25</HOST_SUMMARY>
       <HOST_SUMMARY category="dead" tracking="NETBIOS">gfi-31-
10,gfi-31-11</HOST_SUMMARY>
       <HOST_SUMMARY category="excluded"
tracking="IP">10.10.10.26</HOST_SUMMARY>
       <HOST_SUMMARY category="unresolved" tracking="NETBIOS">gfi-
31-13</HOST_SUMMARY>
       <HOST_SUMMARY category="duplicate"
tracking="IP">10.10.10.27</HOST_SUMMARY>
       <HOST_SUMMARY category="duplicate" tracking="DNS">gfi-31-
14.caac125.qualys.com</HOST_SUMMARY>
     </SCAN_SUMMARY>
   </SCAN_SUMMARY_LIST>
 </RESPONSE>
</SCAN_SUMMARY_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/scan/summary/scan_summary_output.dtd

Scanner Details

/api/2.0/fo/scan/scanner

[GET] [POST]

Identify the scanner used to scan a particular IP address at a given time.

Permissions - Manager role is required.

This is supported for vulnerability scans only. This API is especially useful when you're scanning a large number of IPs using a pool of scanners and you're not sure which scanner was used to scan a particular host.

The XML output will show the IP address scanned with the scan reference number, scan date, the scanner identifier (external scanner or scanner appliance name), scanner type (extranet or appliance) and scanner software versions.

Input Parameters

Parameter	Description
action=list	(Required)
scan_date_since={value}	(Required) Include scans started since a certain date. Specify the date in YYYY-MM-DD format. The date must be less than or equal to today's date.
scan_date_to={value}	(Optional) Include scans started up to a certain date. Specify the date in YYYY-MM-DD format. The date must be later than or equal to scan_date_since, and less than or equal to today's date.
ips={value}	(Required) The IP addresses you want scanner details for. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
output_format=XML	(Optional) The output format: XML (the default).

Sample - List scanner details for certain IPs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ips=10.10.10.2-10.10.10.7,10.10.10.10
&scan_date_since=2018-05-24&scan_date_to=2018-09-28"
"https://qualysapi.qualys.com/api/2.0/fo/scan/scanner/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_SCANNERS_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scanner/scanner_list
_output.dtd">
```

```
<IP_SCANNERS_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-11-08T21:49:51Z</DATETIME>
    <IP_SCANNERS_OUTPUT>
      <IP_SCANNED>
        <IP>10.10.10.7</IP>
        <SCAN_REF>scan/1527197914.13102</SCAN_REF>
        <SCAN_DATE>2018-05-24T21:39:08Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>external scanner</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>extranet</SCANNER_TYPE>
        <ML_VERSION>ML-9.7.20-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.182-2</VULNSIGS_VERSION>
      </IP_SCANNED>
      <IP_SCANNED>
        <IP>10.10.10.7</IP>
        <SCAN_REF>scan/1538093810.64913</SCAN_REF>
        <SCAN_DATE>2018-09-28T00:19:25Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>Esxi_4_Network</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>appliance</SCANNER_TYPE>
        <ML_VERSION>ML-9.10.21-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.284-2</VULNSIGS_VERSION>
      </IP_SCANNED>
      <IP_SCANNED>
        <IP>10.10.10.10</IP>
        <SCAN_REF>scan/1538093810.64913</SCAN_REF>
        <SCAN_DATE>2018-09-28T00:19:25Z</SCAN_DATE>
        <SCANNER_IDENTIFIER>Esxi_4_Network</SCANNER_IDENTIFIER>
        <SCANNER_TYPE>appliance</SCANNER_TYPE>
        <ML_VERSION>ML-9.10.21-1</ML_VERSION>
        <VULNSIGS_VERSION>VULNSIGS-2.4.284-2</VULNSIGS_VERSION>
      </IP_SCANNED>
    </IP_SCANNERS_OUTPUT>
  </RESPONSE>
</IP_SCANNERS_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/scan/scanner/scanner_list_output.dtd

Share PCI Scan

The Share PCI Scan API (/api/2.0/fo/scan/pci/) povides an automated way to share (export) finished PCI scans to PCI Merchant accounts and check the export status. A PCI scan is a vulnerability scan that was run with the option profile “Payment Card Industry (PCI) Options”.

Express Lite: This API is available to Express Lite users.

In advance of sharing a PCI scan using the share PCI scan API, the target PCI Merchant account must be already defined as a PCI account link within the API user’s Qualys account. Account links can be defined using the Qualys user interface only.

Permissions - Any user with scan permissions (Manager, Unit Manager or Scanner) can share a PCI scan with one of their own PCI Merchant accounts and obtain share status. The user’s Qualys account must allow access to the PCI scan and must have a link to the target PCI Merchant account.

Share Restriction - The following share restriction applies to all users. One PCI scan can be shared (exported) to one PCI Merchant subscription one time only, assuming the share request is successful. (Note: If a particular scan has been exported to any PCI account in the same PCI Merchant subscription as your PCI account, the scan can’t be exported.) If a share request fails for some reason, it's possible to submit another share request for the same PCI scan and PCI Merchant account.

Share a PCI Scan

/api/2.0/fo/scan/pci/ with action=share

[POST]

Export a finished PCI scan to a selected PCI Merchant account. It’s possible to export a PCI scan one time per PCI Merchant account, and the same PCI scan can be exported to multiple PCI Merchant accounts.

Input Parameters

Parameter	Description
action=share	(Required) Specify “share” to share a PCI scan.
echo_request={**0**|1}	(Optional) Specify 1 to view parameters in the XML output. When unspecified, parameters are not included in the XML output.
scan_ref={value}	(Required) The scan reference of a finished PCI scan. The scan status of this scan must be “Finished”.
merchant_username={value}	(Required) The user name of the PCI Merchant account that the PCI scan will be exported to. The API user’s Qualys account must have a PCI account link already defined for this target PCI Merchant account.

Sample - Share PCI scan

API request:

```
curl -s -H "X-Requested-With: curl demo 2" -D headers.15 -b
"QualysSession=38255848108d68a2feaf9ee664ca78a7; path=/api;
secure" -d
"action=share&merchant_username=manager1@qualys&scan_ref=scan/1281
646610.5720"
"https://qualysapi.qualys.com/api/2.0/fo/scan/pci/"
```

XML output Successful Share:

The XML output uses the simple return DTD and the message is “Requested share of scan to PCI”.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-17T00:50:39Z</DATETIME>
    <TEXT>Requested share of scan to PCI</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>scan_ref</KEY>
        <VALUE>scan/1281646610.5720</VALUE>
      </ITEM>
      <ITEM>
        <KEY>merchant_username</KEY>
        <VALUE>manager1@qualys</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

XML output Share Already in Progress or Completed:

When the request to share a PCI scan fails, the XML output uses the simple return DTD with the error. If the failure is because sharing is in progress for the PCI Merchant account or the scan has already been shared to the PCI account, the output includes the message “This scan has already been shared with the Merchant account”.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualy_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-04T14:54:01Z</DATETIME>
    <CODE>999</CODE>
```

```
    <TEXT>This scan has already been shared with the Merchant
account.</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Get PCI Share Status

/api/2.0/fo/scan/pci/ with action=status

[GET] [POST]

Get the share status of a PCI scan that has already been shared with a PCI merchant account.

Input Parameters

Parameter	Description
action=status	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view parameters in the XML output. When unspecified, parameters are not included in the XML output.
scan_ref={value}	(Required) The scan reference of the shared scan that you want to check the export status for.
merchant_username={value}	(Required) The username of the PCI account which the scan was shared with.

Sample - PCI Share status

API request:

```
curl -s -H "X-Requested-With: curl demo 2" -u "USERNAME:PASSWD" -d
"action=status&scan_ref=scan/1531755831.21639&merchant_username=as
mith@hq" "https://qualysapi.qualys.com/api/2.0/fo/scan/pci/"
```

XML output:

The XML response for a status requests identifies the share status: Queued (request was received and not started yet), In Progress, Finished (scan was exported to PCI account successfully), or Error.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PCI_SCAN_SHARE_STATUS SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/pci/pci_scan_share_s
tatus.dtd">
<PCI_SCAN_SHARE_STATUS>
 <RESPONSE>
   <SCAN>
     <MERCHANT_USERNAME>asmith@hq</MERCHANT_USERNAME>
     <SCAN_REF>scan/1531755831.21639</SCAN_REF>
```

```
      <STATUS>In Progress</STATUS>
      <LAST_SHARED>2018-07-19T05:05:58Z</LAST_SHARED>
    </SCAN>
  </RESPONSE>
</PCI_SCAN_SHARE_STATUS>
```

DTD

<platform API server>/api/2.0/fo/scan/pci/pci_scan_share_status.dtd

Discovery Scans (maps)

Launch discovery scans, also called maps, to launch network discovery of your domains and/or IP addresses in asset groups. This returns an inventory of your network devices.

Launch Map | Map Report List | Cancel Running Map | Download Saved Map Report | Delete Saved Map Report | Scheduled Scans and Maps | Domain List | Add/Edit Domain

Launch Map

/msp/map-2.php

[GET] [POST]

Launch a Qualys network map for one or more domains, initiating network discovery. The map target may include asset groups and the default scanner option may be enabled for distributed mapping across multiple scanner appliances.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

A map request for multiple domains issued using the map-2.php API, runs one map at a time, one domain at a time. If you cancel a running map for a domain using the scan_cancel.php function and there are multiple domains in the map target, the service cancels the maps for any remaining, undiscovered domains in the same map target.

For a map request with multiple domains, the XML map report returned by the map-2.php function includes all domains that were successfully discovered. When you view the map results for this request using the map_report.php function or the Qualys user interface, each map report includes map results for one domain. Also, if the map summary notification is enabled in your account, there is a separate notification for each target domain.

Permissions - Managers can map all domains in the subscription. Unit Managers can map domains in the user's same business unit. Scanners can map domains in their own account.

Input Parameters

Parameter	Description
map_title={title}	(Optional) Specifies a title for the map. The map title can have a maximum of 2,000 characters. When specified, the map title appears in the header section of the map results. When unspecified, the API returns a standard, descriptive title in the header section.
domain={target}	(Optional) Specifies one or more domain names for the map target. Multiple entries are comma separated. (Target may include domain names and/or asset groups) For each domain, include the domain name only; do not enter "www." at the start of the domain name. Netblocks may be specified with each domain name to extend the scope of the map. Multiple domains must be comma separated. This parameter and/or asset_groups must be specified.
asset_groups={title1,title2...}	(Optional) Specifies the titles of asset groups for the map target. Multiple asset groups must be comma separated. (Target may include domain names and/or asset groups) This parameter and/or the domain parameter must be specified.
iscanner_name={name}	(Optional) Specifies the name of the Scanner Appliance for the map, when the map target has private use internal IPs. Using Express Lite, Internal Scanning must be enabled in your account.
	One of these parameters may be specified in the map request: iscanner_name or default scanner.
default_scanner=1	(Optional) Enables the default scanner feature, which is only valid when the map target consists of asset groups. A valid value is 1 to enable the default scanner, or 0 (the default) to disable it. Using Express Lite, Internal Scanning must be enabled in your account.
	One of these parameters may be specified in the same map request: iscanner_name or default scanner.
option={title}	(Optional) Specifies the title of an option profile to be applied to the map. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied.

Parameter	Description
network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network by specifying the network ID. When unspecified, we default to "0" for Global Default Network.
save_report=yes	(Optional) Saves a map report for each target domain on the Qualys server for later use. A valid value is "yes" to save a map report for each target domain, or "no" (the default) to not save the report. If set to "yes", you can close the HTTP connection when the map is in progress, without cancelling the map. When the map completes the resulting map report is saved on the Qualys platform, and a map summary email notification is sent (if this option is enabled in your user account). Saved map reports can be retrieved using map_report_list.php and map_report.php.

Samples - Launch map

Request a map of the domain "www.mycompany.com" using the external scanners and to receive a map report:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com
```

Request a map of the domain "www.mycompany.com" using the external scanners, save map report on the Qualys platform:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com
&save_report=yes
```

Request a map for the following domain/netblock pair using the scanner appliance "Hong Kong" and custom domain mycompany:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mycompany.com:19
2.168.0.1-192.168.0.254&iscanner_name=Hong+Kong
```

Request a map for this domain/netblock pair using the scanner appliance "San Francisco" and none domain:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=none:192.168.0.1
-192.168.0.254&iscanner_name=San+Franscisco
```

Request a map for the domain "mydomain.com" using a network ID and to receive a map report:

```
https://qualysapi.qualys.com/msp/map-2.php?domain=mydomain.com:
10.10.10.10-10.10.10.20&iscanner_name=my_scanner&network_id=
4234545&save_report=yes
```

DTD

<platform API server>/map-2.dtd

<platform API server>/map-2.dtd

Map Report List

/msp/map_report_list.php

[GET] [POST]

List saved map reports in the user's account. Each entry in the map report list identifies a saved map report for a specific domain. There is a separate saved map report for each domain in the map target.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Managers can view all saved map reports in the subscription. Unit Managers can view saved map reports for domains in user's business unit. Scanners and Readers can view saved map reports for domains in user's account.

Input Parameters

Parameter	Description
last=yes	(Optional) Used to retrieve information only about the last saved map report. A valid value is "yes" to retrieve the last saved map report, or "no" (the default) to retrieve all map reports.
domain={target}	(Optional) Used to receive a list of all saved map reports for the specified target domain. If both parameters domain={target} and last=yes are specified, you will receive information about the last saved map for the target domain.

Sample

Receive information about the last saved map for the domain "www.companyabc.com":

```
https://qualysapi.qualys.com/msp/map_report_list.php?
  domain=www.companyabc.com&last=yes
```

DTD

<platform API server>/map_report_list.dtd

Running Map Report List

/msp/scan_running_list.php

[GET] [POST]

List maps and scans that are currently running in the user's account. If you're interested in listing scans only (not maps), we recommend using VM Scan List (/api/2.0/fo/scan/) instead.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Managers can view all running maps/scans in the subscription. Unit Managers can view running maps/scans on assets in the user's business unit. Scanners and Readers can view running maps/scans on assets their account.

Sample - Running map/scan list

```
https://qualysapi.qualys.com/msp/scan_running_list.php?
```

DTD

<platform API server>/scan_running_list.dtd

Cancel Running Map

/msp/scan_cancel.php

[GET] [POST]

Cancel a map in progress. It's not possible to cancel a map when it has the scan status "Loading".

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Managers can cancel all running maps in the subscription. Unit Managers can cancel running maps launched by users in their same business unit. Scanners can cancel running maps they have launched.

Input Parameter

Parameter	Description
ref={value}	(Required) Specifies the map reference for the map to be cancelled (or a scan reference for the scan to be cancelled). A map reference starts with "map/".

Sample - Cancel a map in progress

```
https://qualysapi.qualys.com/msp/scan_cancel.php?ref=map/987659876
.19876
```

DTD

<platform API server>/generic_return.dtd

Download Saved Map Report

/msp/map_report.php

[GET] [POST]

Download a saved map in the user's account, when the map has the scan status "Finished". Each saved map report identifies map results for a specific domain. If you issue a map request for multiple domains using the map-2.php API, there is a separate saved map report for each domain in the map target.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Managers can download all saved map reports in subscription. Unit Managers can download saved map report for domain in user's business unit. Scanners and Readers can download saved map report for domain in user's account.

Input Parameter

Parameter	Description
ref={value}	(Required) Specifies the map reference for the scan you want to download. A map reference starts with "map/".

Sample - Download saved map report

```
https://qualysapi.qualys.com/msp/map_report.php?
  ref=map/987659876.19876
```

DTD

<platform API server>/map.dtd

Delete Saved Map Report

/msp/scan_report_delete.php

[GET] [POST]

Delete a previously saved network map or scan report, when the scan status is “Finished”.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Managers can delete saved map reports in the subscription. Unit Managers can delete saved map reports for domains in the user’s business unit, including the user’s own maps and maps run by other users in the same business unit. Scanners can delete saved map reports in user’s account.

Input Parameter

Parameter	Description
ref={value}	(Required) Specifies the map reference for the map to be deleted. A map reference starts with “map/”.

Sample - Delete saved map report

```
https://qualysapi.qualys.com/msp/scan_report_delete.php?
  ref=map/999666888.12345
```

DTD

<platform API server>/generic_return.dtd

Scheduled Scans and Maps

/msp/scheduled_scans.php

[POST]

Functional Overview

The Scheduled Scans API (/msp/scheduled_scans.php) is used to add, list, and remove scheduled scan and map tasks on the Qualys server. Scheduled tasks can be defined to run daily, weekly, and monthly. The Qualys service automatically starts the scheduled tasks according to their specifications.

Express Lite: This API is available to Express Lite users.

The scheduled_scans.php function applies the default option profile in the user account to a scheduled task, unless another profile is specified for the task using the option={name} parameter.

Each scheduled task runs in the local time defined for the task. You have the option to specify the local time as a time zone code or as a GMT shift value. When a time zone code that supports Daylight Saving Time (DST) is specified in the time_zone_code parameter with observe_dst=yes, the task observes DST by automatically adjusting the task's run time to reflect local time.

The Qualys service assigns a task ID to each scheduled task when the scheduled task is added. This task ID can be used to delete the scheduled task as described below in "Remove Task."

Each time a scheduled task successfully completes, the API user receives an email notification with scan or map results, unless this notification option is disabled in the user account. This email includes summary information plus a link to the detailed scan or map report. These results may also be returned using the scan_report_list.php and scan_report.php functions.

The reports produced by scheduled scans and maps are saved on the Qualys server. A scan report can be retrieved using the scan_report.php function. A map report can be retrieved using the map_report.php function. A report for a scheduled scan or map can be removed using the scan_report_delete.php function. The scan_report_list.php function lists reports for scheduled scans and maps.

Important: The scheduled_scans.php function does not check for validity of IP addresses and other task settings until run time — the first time the scheduled task is initiated. For example, in a case where you submit a request to add a new scheduled scan with an invalid IP address, the scheduled_scans.php function will create the new task without error or warning. Then, at run time the Qualys service will send an email notification stating "This scheduled task has been deactivated," with a reason for the deactivation. This email is sent to the registered Qualys user of the account.

Task Type selection

The type parameter specifies the scheduled task type. When this parameter is not set, the default is type=scan for a scheduled scan.

Use the type=map parameter to add a scheduled map or request a list of scheduled

maps. For example, to request a list of scheduled maps, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=map.

Use the type=all parameter to request a list of scheduled scans and maps together.

Task Target

The task target is defined using the scan_target and asset_groups parameters. For a scan task, you may specify a combination of IP addresses, IP address ranges, and asset groups. For a map task, you may specify a combination of domain names and asset groups.

The scan_target parameter is used to specify the target for a new scheduled scan or map. To add a scan task on IP addresses using the external scanner, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php?
add_task=yes&type=scan&scan_target={addresses}

To add a map task on two domains using a scanner appliance, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&type=map&scan_target={domain1,domain2}&iscanner_name=name.

Use the asset_groups={title1,title2...} parameter to specify asset groups for a task target.

Scanner Selection

For each scan a scanner is applied to the task. External scanning at the network perimeter is supported by the Qualys external scanners, and internal scanning of private use internal IPs is supported using Qualys Scanner Appliances. Private use internal IPs must be scanned using scanner appliances, which are installed inside the corporate network. When a scanner is unspecified for a scan task, the Qualys External Scanners are used.

User permissions

User permissions for the scheduled_scans.php function are described below.

User Role	Permissions
Manager	Add tasks for all assets in the subscription. Remove all tasks. View all tasks in the subscription.
Unit manager	Add tasks for assets in user's business unit. Remove tasks in user's business unit. View tasks in the subscription* (see below).
Scanner	Add tasks for assets in user's account. Remove user's scheduled tasks. View tasks in the subscription* (see below).
Reader	No permission to add and remove tasks. View tasks in the subscription* (see below).

* Qualys includes an account permission setting that restricts Unit Managers, Scanners, and Readers from viewing scheduled tasks on unassigned assets. For more details on this and user role-based permissions, see the Qualys online help.

Parameters

General Information

The parameters below apply to all scheduled tasks, both scans and maps. There are four required parameters to add a scheduled scan, and five required parameters for a scheduled map. The iscanner_name parameter is required when a Scanner Appliance is used.

Parameter	Description
add_task=yes	(Required to add a task) Used to add a scheduled task.
scan_title={title}	(Required to add a task) Specifies a title for the scheduled task.
type=scan | map | all	(Optional) Specifies the scheduled task type: **scan** for a scan task or **map** for a map task. If unspecified, the type is set to **type=scan**. For a scheduled map, this parameter must be set to **type=map**. The **all** type applies only when retrieving a list of scheduled tasks. For example, to receive a list of scheduled scans and maps, specify **type=all**.
active=yes | no	(Required to add a task) Specifies whether the scheduled task is active. When active, the scheduled task runs at the specified time. When inactive, the scheduled task does not run at its specified time.
scan_target={target}	(Optional) Specifies the task target. For a scheduled scan, specify IPs and/or IP ranges. For a scheduled map, specify one or more domain names. Multiple domain names must be comma separated. This parameter and/or **asset_groups** must be specified when adding a scheduled task.
scan_target={target}	(Optional) Specifies the task target. For a scheduled scan, specify IPs and/or IP ranges. For a scheduled map, specify one or more domain names. Multiple domain names must be comma separated. This parameter and/or asset_groups must be specified when adding a scheduled task.
asset_groups={title1,title2...}	(Optional) Specifies the titles of asset groups to be included in the scheduled task target. Multiple asset groups must be comma separated. This parameter and/or scan_target must be specified when adding a scheduled task.
exclude_ip_per_scan={value}	(Optional) Used to exclude certain IP addresses/ranges for the scheduled scan. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20).
iscanner_name={name}	(Optional) Specifies the name of the Scanner Appliance to be used for the scheduled task, when the task target has private use internal IPs. Using Express Lite, Internal Scanning must be enabled in your account. Note: One of these parameters may be specified in the same request: iscanner_name, default_scanner, or scanners_in_ag (for scheduled scan only).

Parameter	Description
runtime_http_header={value}	Set a custom value in order to drop defenses (such as logging, IPs, etc) when an authorized scan is being run. The value you enter will be used in the "Qualys-Scan:" header that will be set for many CGI and web application fingerprinting checks. Some discovery and web server fingerprinting checks will not use this header.
default_scanner=1	(Optional) Enables the default scanner feature, which is only valid when the task target consists of asset groups. A valid value is 1 to enable the default scanner, or 0 (the default) to disable it. Using Express Lite, Internal Scanning must be enabled in your account. **Note:** One of these parameters may be specified in the same request: iscanner_name, default_scanner, or scanners_in_ag (for scheduled scan only).
scanners_in_ag=1	(Optional) et to 1 to use the scanners in asset group features. This lets you scan an asset group using the appliances defined for the group. If you want to scan multiple asset groups, each asset group will be scanned using the appliances in its own group. This features is not available for a scheduled map. Using Express Lite, Internal Scanning must be enabled in your account. **Note:** One of these parameters may be specified in the same request: iscanner_name, default_scanner, or scanners_in_ag (for scheduled scan only).
option={title}	(Optional) Specifies the title of an option profile to be applied to the task, used when adding a task. The profile title must be defined in the user account, and it can have a maximum of 64 characters. If unspecified, the default option profile in the user account is applied. Note that custom option profiles can be defined only using the Qualys user interface. A selective vulnerability scan that includes a subset vulnerabilities (QIDs) in the KnowledgeBase may be specified. It's recommended that you include certain QIDs to ensure host information is available in your scan results and other reports.

Add Daily Task

The parameters listed below are required for daily tasks. See **Recurrences** for an optional parameters.

Parameter	Description
occurrence=daily	(Required) Specifies that the task will occur daily.
frequency_days={value}	(Required) Specifies that the task will run every N days, where N is the number of days. A valid value is an integer from 1 to 365.
{start time parameters}	(Required) Specifies when the task will start. See “Start Time” for a complete list of parameters.

Add Weekly Task

The parameters listed below are required for daily tasks. See Recurrences for an optional parameter.

Parameter	Description
occurrence=weekly	(Required) Specifies that the task will occur weekly.
frequency_weeks={value}	(Required) Specifies that the task will run every N weeks, where N is a number of weeks. A valid value is an integer from 1 to 52.
weekdays={value}	(Required) Specifies on which weekdays the task will run. One or more days may be specified. A valid value is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday. Multiple days are comma separated.
{start time parameters}	(Required) Specifies when the task will start. See “Start Time” for a complete list of parameters.

Add Monthly Task -Nth Day of Month

The parameters listed below are required for a monthly task to be run on the Nth day of the month where N is a day of the month that you specify. For example, you can setup a monthly task to run on the 15th day of each month. See **Recurrence** for an optional parameter.

Parameter	Description
occurrence=monthly	(Required) Specifies that the scheduled task will occur monthly.
frequency_months={value}	(Required) Specifies that the task will run, as in every N months, where N is a number of months. A valid value is an integer from 1 to 12.
day_of_month={value}	(Required) Specifies the day of the month to run. A valid value is an integer from 1 to 31.
{start time parameters}	(Required) Specifies when the task will start. See “Start Time” for a complete list of parameters.

Add Monthly Task - Weekday in Nth Week of Month

The parameters listed below are required for a monthly task to be run on a day of the week (for example Monday, Tuesday) in a particular week of the month. For example, you can setup a monthly task to run on the second Tuesday of the month. See **Recurrence** for an optional parameter.

Parameter	Description
occurrence=monthly	(Required) Specifies that the scheduled task will occur monthly.
frequency_months={value}	(Required) Specifies that the task will run every N months, where N is a number of months. A valid value is an integer from 1 to 12.
day_of_week={value}	(Required) Specifies the day of the week when the task will run. A valid value is an integer from 0 to 6, where 0 is Sunday and 6 is Saturday.
week_of_month={value}	(Required) Specifies the Nth week of the month, when the task will run. A valid value is: first, second, third, fourth, or last.
{start time parameters}	(Required) Specifies when the task will See Start Time for a complete list of parameters.

Start Time

The parameters listed below specify start time settings used to launch the scheduled task. Some start time parameters are required for all scheduled tasks as indicated.

Parameter	Description
time_zone_code={value}	(Optional) Specifies the time zone for the task as a pre-defined code. For example, the time zone code for US California is US-CA. Time zone codes must be specified in upper case. Valid time zone codes are provided in the "Time Zone Code List" returned by the time_zone_code_list.php function. For a time zone code that supports Daylight Saving Time, you can specify observe_dst=yes so that the task is updated automatically to reflect local time. This parameter or time_zone must be specified. See "Time Zone Selection" below for further details.
observe_dst={yes}	(Optional) Enables the observe Daylight Saving Time (DST) feature for the task. This feature can be enabled when the time zone code specified in time_zone_code supports DST. When enabled, the service automatically adjusts the start time for the task to reflect local time. To enable this feature, specify observe_dst=yes. Some locales do not support DST, like Arizona and Hawaii. For these locales, if you specify a time zone code with observe_dst=yes, the function returns an error. This parameter may be specified with time_zone_code. (This parameter is invalid when specified with time_zone.)

Parameter	Description
time_zone={value}	(Optional) Specifies the time zone for the task as a GMT shift value. This is the difference, in hours, between GMT and the local time zone. A valid value is an integer from -12 to 12. For example, the GMT shift for Pacific Standard Time (PST) in California is -8. This parameter cannot be used when the timezone has a 30 or 15 minute offset (for example GMT-930 or GMT+1245). This parameter or time_zone_code must be specified. See "Time Zone Selection" below for further details. Note: This parameter is available for backward compatibility and may not be supported in future releases.
start_date={mm/dd/yyyy}	(Optional) Specifies the start date in mm/dd/yyyy format. By default, the start date is the date when the task is created.
start_hour={hour}	(Required) Specifies the hour when the task will start. The hour variable is an integer from 0 to 23, where 0 represents 12 AM, 7 represents 7 AM, and 22 represents 10 PM.
start_minute={minute}	(Optional) Specifies the minute when the task will start. A valid value is an integer from 0 to 59.
end_after={value}	(Optional) Specifies the number of hours to wait for a map or scan to complete before deactivating the task. By default the service does not deactivate tasks until they complete. A valid value is an integer from 1 to 48.

Recurrence

The recurrence parameter listed below is optional. By default the task does not end unless it is deactivated or deleted.

Parameter	Description
orecurrence={value}	(Optional) Specifies the number of times the task will be run before it is deactivated. A valid value is an integer from 1 to 99. For example, if you set recurrence=2, the scheduled task will be deactivated after it runs 2 times.

Remove Task

The following parameters are required to remove a scheduled task. Both parameters must be specified. When these parameters are set, the function removes the specified scheduled task and returns an XML success message.

If you remove a scheduled task, any saved reports for the scheduled task remain on the Qualys server.

Parameter	Description
drop_task=yes	(Required) Used to delete a scheduled task. A valid value is "yes" to delete the task or "no" (the default) to not delete the task.
task_id={taskID}	(Required) Specifies the task ID of the task to be deleted. The Qualys service assigns a task ID to each scheduled task when the task is added.

Time Zone Selection

When adding a task, you must identify local time by specifying either a time zone code or a GMT shift value using the parameters described below. These are mutually exclusive parameters which cannot be used together.

Time Zone Parameters

For the time_zone_code parameter, you specify a time zone code that corresponds to local time. Refer to the "Time Zone Code List" below to select an appropriate code. For example if the task will run in New York, then you specify the code "US-NY". Many time zones, like New York, observe DST. If you specify a code for a time zone that supports DST, you have the option to enable the observe Daylight Saving Time (DST) feature so the task is updated automatically to reflect local time. To enable this feature. specify observe_dst=yes.

For the time_zone parameter, you specify a GMT shift, like -8 for Pacific Standard Time in California, that corresponds to local time. When the timezone has a 30 or 15 minute offset, then the time_zone parameter cannot be used. When specified, the service automatically determines the appropriate time zone code for the task and includes this in scheduled scans reports. Note this parameter has been available in previous releases and is supported for backward compatibility.

Time Zone Code List

The time_zone_code_list.php function provides a list of all available time zone codes that can be specified with the time_zone_code parameter.

To retrieve a list of time zone codes, use this URL:

<qualys_base_url>/msp/time_zone_code_list.php

The DTD for the XML document returned from time_zone_code_list.php can be found at the following URL:

https://qualysapi.qualys.com/time_zone_code_list.dtd

Sample - Time zone code list output

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULEDSCANS SYSTEM
"https://qualysapi.qualys.com/time_zone_code_list.dtd">
<TIME_ZONES>
    <TIME_ZONE>
        <TIME_ZONE_CODE>AS</TIME_ZONE_CODE>
        <TIME_ZONE_DETALS>
            <![CDATA[(GMT-1100) American Samoa: Pago
Pago]]>
        </TIME_ZONE_DETALS>
        <DST_SUPPORTED>0</DST_SUPPORTED>
```

```
    </TIME_ZONE>
    <TIME_ZONE>
        <TIME_ZONE_CODE>UM2</TIME_ZONE_CODE>
        <TIME_ZONE_DETALS>
            <![CDATA[(GMT-1100) Midway Islands
(U.S.)]]>
        </TIME_ZONE_DETALS>
        <DST_SUPPORTED>0</DST_SUPPORTED>
    </TIME_ZONE>
    <TIME_ZONE>
        <TIME_ZONE_CODE>NU</TIME_ZONE_CODE>
        <TIME_ZONE_DETALS>
            <![CDATA[(GMT-1100) Niue: Alofi]]>
        </TIME_ZONE_DETALS>
        <DST_SUPPORTED>0</DST_SUPPORTED>
    </TIME_ZONE>
    <TIME_ZONES>
```

Each <TIME_ZONE> element identifies a time zone properties, including the code, in the sub-elements described below.

Elements	Description
<TIME_ZONE_CODE>	A time zone code. These are pre-defined codes.
<TIME_ZONE_DETAILS>	Text describing the time zone.
<DST_SUPPORTED>	A value (0 or 1) indicating whether the time zone supports Daylight Saving Time (DST). 1 is reported when DST is supported, and 0 is reported when DST is not supported.

Examples

Scheduled Tasks Lists

To receive an XML document including a list of all scheduled scans, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php

To receive an XML document with a list of all scheduled scans and maps, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=all

To receive an XML document including a list of all scheduled maps, use this URL:
https://qualysapi.qualys.com/msp/scheduled_scans.php?type=map

Scheduled Scans

The URL below adds a daily scan called “Scan1” that is defined to scan IP address “10.20.30.3”. “Scan1” is scheduled to start at 2 PM every day in Los Angeles, California where DST is observed. The URL below includes all parameters required to add “Scan1” as an active scan:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan1&active=yes&scan_target=10.20.30.3&iscanner_
name=scanner1&occurrence=daily&frequency_days=1&time_zone_code=
US-CA&observe_dst=yes&start_hour=14&start_minute=0
```

To add a daily scan called “My Daily Scan” that is defined to scan IP address “10.10.10.3”, specify the URL below. This daily scan is scheduled to start at 4 PM every day in the California time zone. The URL below includes all required parameters:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=My+Daily+Scan&active=yes&scan_target=10.10.10.3&i
scanner_name=scanner1&occurrence=daily&frequency_days=1&time_zo
ne_code=US-CA&observe_dst=yes&start_hour=14&start_minute=0
```

The URL below adds a weekly scan called “Scan2” that is defined to scan the asset groups “Finance” and “Operations”. “Scan2” is scheduled to start at 10 AM every 2nd Tuesday in Paris, France where DST is observed. The URL below includes all required parameters:

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan2&active=yes&asset_groups=Finance,Operations&
iscanner_name=scanner2&option=RV10+Options&occurrence=weekly&fr
equency_weeks=2&weekdays=Tuesday&time_zone_code=FR&observe_dst=
yes&start_hour=10&start_minute=0&recurrence=90
```

The URL below adds a monthly scan called “Scan3” that is defined to scan 3 asset groups with the default scanner enabled. “Scan3” starts every 2 months on the 2nd Friday of the month at 6 PM in New York City where DST is observed.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=Scan3&active=yes&asset_groups=Critical+Group+4,Cr
itical+Group+5,Critical+Group+6&default_scanner=1&occurrence=mo
nthly&frequency_months=2&day_of_week=5&week_of_month=2&time_zon
e_code=US-NY&observe_dst=yes&start_hour=18&start_minute=0
```

The URL below adds a monthly scan called “My Scheduled Scan” that uses the scanners in asset group feature.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?
add_task=yes&scan_title=My+Scheduled+Scan&active=yes&
asset_groups=Group+A,Group+B,Group+C&scanners_in_ag=1&
occurrence=monthly&frequency_months=2&day_of_week=5&
week_of_month=2& time_zone_code=US-NY&
observe_dst=yes&start_hour=18& start_minute=0
```

The URL below removes a scheduled scan with the task ID “6703”. Two parameters are required as shown.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?drop_task=
yes&task_id=6703
```

Scheduled Maps

To add a weekly map called “My Weekly Map” to perform discovery on “mydomain.com”, specify the URL below. This weekly map runs every 8 weeks and starts on Sunday at 2 AM in Tokyo, Japan.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?add_task=y
es&scan_title=My+Weekly+Map&active=yes&type=map&scan_target=myd
omain.com&iscanner_name=scanner5&occurrence=weekly&frequency_we
eks=8&weekdays=Sunday&time_zone_code=JP&start_hour=2&start_minu
te=0
```

The URL below removes a scheduled map with the task ID “11155”. Note that two parameters are required as shown.

```
https://qualysapi.qualys.com/msp/scheduled_scans.php?
drop_task=yes&task_id=11155
```

XML Reports

The DTD for the XML results returned by the scheduled_scans.php function can be found at the following URL:

https://qualysapi.qualys.com/scheduled_scans.dtd

This XML document supports reporting on scheduled scans and maps.

Sample - Scheduled scans and maps

API Request

```
curl --location --request POST
'<qualys_base_url>/msp/scheduled_scans.php?add_task=yes&scan_title=Scan1&
active=yes&scan_target=10.10.10.1&iscanner_name=shreya_test_scanner1&occu
rrence=daily&frequency_days=1&time_zone_code=US-
CA&observe_dst=yes&start_hour=14&start_minute=0' \
--header 'X-Requested-With: test' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULEDSCANS SYSTEM "<qualys_base_url>/scheduled_scans.dtd">
<SCHEDULEDSCANS>
    <SCAN active="yes" ref="6197007">
        <TITLE>
            <![CDATA[Scan1]]>
        </TITLE>
        <TARGETS>
            <![CDATA[11.11.11.1]]>
        </TARGETS>
        <SCHEDULE>
            <DAILY frequency_days="1"/>
            <START_DATE_UTC>2025-03-17T22:00:00</START_DATE_UTC>
            <START_HOUR>14</START_HOUR>
            <START_MINUTE>0</START_MINUTE>
            <TIME_ZONE>
                <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
                <TIME_ZONE_DETAILS>
                    <![CDATA[(GMT -08:00) United States, California
(Pacific Standard Time)]]>
                </TIME_ZONE_DETAILS>
            </TIME_ZONE>
            <DST_SELECTED>1</DST_SELECTED>
        </SCHEDULE>
        <NEXTLAUNCH_UTC>2025-03-17T21:00:00</NEXTLAUNCH_UTC>
        <DEFAULT_SCANNER></DEFAULT_SCANNER>
        <ISCANNER_NAME>xxx_test_scanner1</ISCANNER_NAME>
        <OPTION>Initial Options</OPTION>
        <TYPE>SCAN</TYPE>
        <USER_ENTERED_IPS network_id="0">
```

```
            <RANGE>
                <START>11.11.11.1</START>
                <END>11.11.11.1</END>
            </RANGE>
        </USER_ENTERED_IPS>
        <OPTION_PROFILE>
            <OPTION_PROFILE_TITLE option_profile_default="1">
                <![CDATA[Initial Options]]>
            </OPTION_PROFILE_TITLE>
        </OPTION_PROFILE>
    </SCAN>
</SCHEDULEDSCANS>
```

Domain List

/msp/asset_domain_list.php

[GET] [POST]

List asset domains in the user account.

Basic HTTP authentication is required. Session based authentication is not supporte using this API.

Permissions - Managers can view all domains in subscription. Unit Managers can view domains in user's business unit. Scanners, Readers can view domains in their own account.

Sample - List all domains in account

```
https://qualysapi.qualys.com/msp/asset_domain_list.php
```

DTD

<platform API server>/domain_list.dtd

Add/Edit Domain

/msp/asset_domain.php

[GET] [POST]

Add and edit domains and related netblocks in the subscription. The domains defined may be used as targets for network scans (maps).

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Permissions - Manager user role is required.

Input Parameter

Parameter	Description
action={add | edit}	(Required)

Parameter	Description
domain={domain}	(Required) Specifies the domain name to add or edit. Include the domain name only; do not enter "www." at the start of the domain name.
netblock={ranges}	(Optional for add request, and Required for an edit request) Specifies the netblock(s) associated with the domain name. Multiple netblocks are comma separated. Looking for more help? Search for "none domain" or "netblock" in online help (log in to your account and go to Help > Online Help). For an edit request, it's not possible to add or remove netblocks for a domain. To clear associated netblocks for an existing domain, specify netblock=

Sample - Add domain

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=add&domai
n=mydomain.com
```

Sample - Edit domain

```
https://qualysapi.qualys.com/msp/asset_domain.php?action=edit&doma
in=acme.com&netblock=10.10.10.0/24,10.1.1.0-10.1.1.100
```

DTD

<platform API server>/generic_return.dtd

Domain V2 API-List Domain

/api/2.0/fo/asset/domain/

[GET]

List asset domains in the user account. Basic HTTP authentication is required. Session based authentication is not supported using this API. Permissions - Managers can view all domains in subscription. Unit Managers can view domains in user's business unit. Scanners, Readers can view domains in their own account.

Input Parameters

Parameter	Description
action={list}	(Required) Specify the list action to make domain list request.

Sample- List Domain

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/domain/?action=list' \
--header 'X-Requested-With: curl' \
--header 'Authorization: XXXXXXXXXXXX' \
--data ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DOMAIN_LIST SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/domain/domain_list_output.dtd">
<DOMAIN_LIST>
<DOMAIN>
        <DOMAIN_NAME>qualysguard.com</DOMAIN_NAME>
        <DOMAIN_ID>47943018</DOMAIN_ID>
        <NETWORK>
            <NETWORK_NAME>Global Default Network</NETWORK_NAME>
            <NETWORK_ID>0</NETWORK_ID>
        </NETWORK>
        <NETBLOCK>
            <RANGE>
                <START>10.10.10.10</START>
                <END>20.20.20.20</END>
            </RANGE>
        </NETBLOCK>
    </DOMAIN>
    <DOMAIN>
        <DOMAIN_NAME>quays.test.com</DOMAIN_NAME>
        <DOMAIN_ID>47916505</DOMAIN_ID>
        <NETWORK>
            <NETWORK_NAME>Global Default Network</NETWORK_NAME>
            <NETWORK_ID>0</NETWORK_ID>
        </NETWORK>
        <NETBLOCK>
            <RANGE>
                <START>30.330.30.30</START>
                <END>40.440.40.40</END>
            </RANGE>
        </NETBLOCK>
    </DOMAIN>
    <DOMAIN>
        <DOMAIN_NAME>sj.com</DOMAIN_NAME>
        <DOMAIN_ID>47916506</DOMAIN_ID>
        <NETWORK>
            <NETWORK_NAME>Global Default Network</NETWORK_NAME>
            <NETWORK_ID>0</NETWORK_ID>
        </NETWORK>
        <NETBLOCK>
            <RANGE>
                <START>50.550.50.50</START>
                <END>60.660.60.60</END>
```

```
            </RANGE>
        </NETBLOCK>
    </DOMAIN>
</DOMAIN_LIST>
```

Domain V2 API-Create a Domain

Add domains and related netblocks in the subscription. The domains defined may be used as targets for network scans (maps). Basic HTTP authentication is required. Session based authentication is not supported using this API. Permissions - Manager user role is required.

/api/2.0/fo/asset/domain/

[POST]

Input Parameters

Parameter	Description
action={create}	(Required) Specify the create action to create a domain.
domain	(Required) Specify domain that you want to add.
netblock	(Optional) Specify netblocks of domain
network_id	(Optional) By default, the network ID for adding domains is set to GDN(0). Specify the network ID if you wish to add a domain to a different network.

Sample- Create a Domain

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/asset/domain/?action=create&domain=Vulndash
board.com' \
--header 'X-Requested-With: curl' \
--header 'Authorization: XXXXXXXXXXX' \
--data ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-10-25T09:38:13Z</DATETIME>
        <TEXT>Domain successfully created.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Domain V2 API-Update a Domain

Update existing domains and related netblocks in the subscription. The domains defined may be used as targets for network scans (maps). Basic HTTP authentication is required. Session based authentication is not supported using this API. Permissions - Manager user role is required.

/api/2.0/fo/asset/domain/

[POST]

Input Parameters

Parameter	Description
action={update}	(Required) Specify the update action to update/edit an existing domain.
domain/id	(Required) Specify either the name or the id of the domain that you want to update.
netblock	(Required) Specify netblocks of domain. If you specify the value, it gets updated. If you don't specify any value, then the Qualys system clears the associated netblocks of domains.
network_id	(Optional) If the network feature is enabled for your subscription, then specify the network ID for updating a domain.

Sample- Update a Domain

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/asset/domain/?action=update&domain=Vulndash
board.com&netblock=12.12.12.12' \
--header 'X-Requested-With: curl' \
--header 'Authorization: XXXXXXXXXXX' \
--data ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-10-25T09:40:18Z</DATETIME>
        <TEXT>Domain successfully updated.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Domain V2 API-Delete a Domain

Delete existing domains and related netblocks in the subscription. The domains defined may be used as targets for network scans (maps). Basic HTTP authentication is required. Session based authentication is not supported using this API. Permissions - Manager user role is required.

/api/2.0/fo/asset/domain/

[POST]

Input Parameters

Parameter	Description
action={delete}	(Required) Specify the delete action to delete an existing domain.
ids	(Required) Specify the id of the domain that you want to delete. Pass comma separated ids for bulk delete.

Sample- Delete a Domain

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/2.0/fo/asset/domain/?action=delete&ids=48793501' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic XXXXXXXXXX' \
--data ''
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-10-25T09:43:22Z</DATETIME>
        <TEXT>Domain(s) successfully deleted.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Scan Configuration

Manage scan configurations in your account - scanner appliances, KnowledgeBase, search lists and option profiles.

Scanner Appliance List

Manage Virtual Scanner Appliances

Update Physical Scanner Appliance

Replace Scanner Appliance

Scanner Appliance VLANs and Static Routes

Option Profile Export | Option Profile Import

Option Profiles for VM | PCI | PC

KnowledgeBase | Editing VulnerabilitiesKnowledgeBase QVS Download in JSON Format

Static Search Lists

Dynamic Search Lists | Vendor IDs and References

Manage Containerized Scanner Appliance

Scanner Appliance List

/api/2.0/fo/appliance/?action=list

[GET] [POST]

List scanner appliances in your account with their configurations. The list output is shown in "brief" mode by default. Specify output_mode=full to include full output (the same information available within the Qualys user interface).

Permissions - Managers can view all scanner appliances in the subscription. Unit Managers can view appliances in the user's own business unit. Scanners and Readers can view appliances in their own account.

Express Lite - This API is available to Express Lite users when Internal Scanning is enabled in the user's account.

Input Parameters

Parameter	Description
action=list	(Required) A flag used to make a request for a list of scanner appliances. The GET or POST method may be used for a list request.
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
output_mode={**brief|**full}	(Optional) The amount of detail provided for each scanner appliance in the output: brief (default) or full. The "brief" output includes this information for each appliance: appliance ID, friendly name, software version, the number of running scans, and heartbeat check status (online or offline). The "full" output includes the full appliance information, including the same details available in the Qualys user interface.
scan_detail={**0**|1}	(Optional) Set to 1 to include scan details for scans currently running on the scanner appliance. Set to 0 (default) to not include scan details. Scan detail includes scan ID, title, scan reference, scan type and scan date.
show_tags={0|**1**}	(Optional. When specified, output_mode=full is required.) Set to 1 (default) to include asset tag information for each scanner appliance in the output. Set to 0 to not include asset tag information in the output.
include_cloud_info={**0**|1}	(Optional. When specified, output_mode=full is required.) Set to 1 to include cloud information in the output for virtual scanner appliances deployed on cloud platforms e.g. Amazon EC2, Microsoft Azure Cloud Platform and Google Cloud Platform. Set to 0 (default) to not include cloud info.

Parameter	Description
busy={0|1}	(Optional) By default all scanner appliances in the user account are shown. Set to 0 to show only appliances which are not currently running scans. Set to 1 (default) to show only appliances which are currently running scans.
scan_ref={value}	(Optional) Specify a scan reference code to show only the scanner appliances running a particular scan.You may enter a valid scan reference code for a currently running scan. The scan reference code starts with a string that identifies the scan type: “scan/” for a vulnerability scan, “compliance/” for a compliance scan, “was/” for a web application scan, “qscap/” for an FDCC scan, or “map/” for a network map.
name={string}	(Optional) List only scanner appliances (physical and virtual) that have names matching the string provided. Tip - Substring match is supported. For example, if you have 2 appliances named “myscanner” and “anotherscanner” and you supply the string “name=scan” both appliance both appliances will be returned in the XML output.
ids={id1,id2,..}	(Optional) List only scanner appliances (physical and virtual) that have certain IDs. Multiple IDs are comma separated.
include_license_info={**0**|1}	(Optional) Set to 1 to return virtual scanner license information in the XML output. This tells you the number of licenses you have and the number used. This information is not returned by default. When specified the XML output will include the LICENSE_INFO element.
type={physical | virtual | containerized | offline}	(Optional) Type of scanner appliances: physical, virtual, containerized, or offline. Appears when output_mode=full is specified in API request.
platform_provider	(Optional) Specify a platform to show scanners deployed on that platform. The valid values are: ec2, ec2_compat, gce, azure, vCenter. ec2 - Amazon EC2, ec2_compat - OpenStack, gce - Google Cloud Platform, azure - Microsoft Azure Cloud Platform, vCenter - VMware vCenter

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&echo_request=1&ids=777,1127,1131&include_license_info=1"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_list_output.
dtd">
<APPLIANCE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2014-01-02T09:26:01Z</DATETIME>
        <APPLIANCE_LIST>
            <APPLIANCE>
                <ID>777</ID>
                <NAME>scanner1</NAME>
                <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
                <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
                <STATUS>Online</STATUS>
            </APPLIANCE>
            <APPLIANCE>
                <ID>1127</ID>
                <NAME>scanner2</NAME>
                <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
                <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
                <STATUS>Online</STATUS>
            </APPLIANCE>
            <APPLIANCE>
                <ID>1131</ID>
                <NAME>scanner3</NAME>
                <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
                <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
                <STATUS>Offline</STATUS>
            </APPLIANCE>
        </APPLIANCE_LIST>
        <LICENSE_INFO>
            <QVSA_LICENSES_COUNT>10</QVSA_LICENSES_COUNT>
            <QVSA_LICENSES_USED>3</QVSA_LICENSES_USED>
        </LICENSE_INFO>
    </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&type=virtual&platform_provider=ec2&include_cloud_info=1&outp
ut_mode=full"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

Sample shows Cloud Info for Amazon EC2.

```
...
        <IS_CLOUD_DEPLOYED>1</IS_CLOUD_DEPLOYED>
        <CLOUD_INFO>
          <PLATFORM_PROVIDER>ec2</PLATFORM_PROVIDER>
          <EC2_INFO>
            <INSTANCE_ID>i-02441120f4e14e32c</INSTANCE_ID>
            <INSTANCE_TYPE>m3.medium</INSTANCE_TYPE>
            <AMI_ID>ami-2d4ed53a</AMI_ID>
            <ACCOUNT_ID>205767712438</ACCOUNT_ID>
            <INSTANCE_REGION>US East (N. Virginia)</INSTANCE_REGION>
            <INSTANCE_AVAILABILITY_ZONE>us-east-
1c</INSTANCE_AVAILABILITY_ZONE>
            <INSTANCE_ZONE_TYPE>Classic</INSTANCE_ZONE_TYPE>
            <IP_ADDRESS_PRIVATE>10.181.43.219</IP_ADDRESS_PRIVATE>
            <HOSTNAME_PRIVATE>ip-10-181-43-
219.ec2.internal</HOSTNAME_PRIVATE>
            <API_PROXY_SETTINGS>
              <SETTING>Enabled</SETTING>
              <PROXY>
                <PROTOCOL>http</PROTOCOL>
                <IP_ADDRESS>1.1.1.1</IP_ADDRESS>
                <HOSTNAME>test_hostname.com</HOSTNAME>
                <PORT>234</PORT>
                <USER>*****</USER>
              </PROXY>
            </API_PROXY_SETTINGS>
          </EC2_INFO>
...
```

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&output_mode=full"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

Sample shows the type of scanner appliance and the other information:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_list_output.
dtd">
<APPLIANCE_LIST_OUTPUT>
```

```
<RESPONSE>
    <DATETIME>2017-08-31T09:14:49Z</DATETIME>
    <APPLIANCE_LIST>
        <APPLIANCE>
            <ID>132455</ID>
            <UUID>6ae4efce-0c5e-e227-82e0-1b7f55f1b98b</UUID>
            <NAME>VS_ND_1</NAME>
            <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
            <RUNNING_SLICES_COUNT>0</RUNNING_SLICES_COUNT>
            <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
            <STATUS>Offline</STATUS>
            <MODEL_NUMBER>cvscanner</MODEL_NUMBER>
            <TYPE>Virtual</TYPE>
            <SERIAL_NUMBER>0</SERIAL_NUMBER>
            <ACTIVATION_CODE>15440265032293</ACTIVATION_CODE>
            <INTERFACE_SETTINGS>
                <INTERFACE>lan</INTERFACE>
                <IP_ADDRESS>1.1.1.1</IP_ADDRESS>
                <NETMASK>128.0.0.0</NETMASK>
                <GATEWAY>128.0.0.0</GATEWAY>
                <LEASE>Static</LEASE>
                <IPV6_ADDRESS></IPV6_ADDRESS>
                <SPEED></SPEED>
                <DUPLEX>Unknown</DUPLEX>
                <DNS>
                    <DOMAIN></DOMAIN>
                    <PRIMARY>128.0.0.0</PRIMARY>
                    <SECONDARY>128.0.0.0</SECONDARY>
                </DNS>
            </INTERFACE_SETTINGS>
...
            <MAX_CAPACITY_UNITS></MAX_CAPACITY_UNITS>
            <CPU_INFO>Intel(R) Xeon(R) CPU E5-2699 v3
@2.30GHz</CPU_INFO>
            <MEMORY_INFO>2,070,484 MB</MEMORY_INFO>
            <REGION_INFO></REGION_INFO>
...
```

DTD:

<platform API server>/api/2.0/fo/appliance/appliance_list_output.dtd

Manage Virtual Scanner Appliances

Use the Scanner Appliance API (**/api/2.0/fo/appliance/**) to create, update and delete virtual scanner appliances.

Tell me about permissions. Managers can perform all actions (create, update, delete). Unit Managers and Scanners must have the “Manage virtual scanner appliances” permission to create, update and delete virtual scanners. This permission is only available to Scanner users when your subscription is configured to allow it.

Add New Virtual Scanner Appliance

/api/2.0/fo/appliance/ with action=create

[POST]

Create a new virtual scanner appliance in your account.

Permissions - Managers can create new virtual scanner appliance. Unit Managers and Scanners must have the "Manage virtual scanner appliances" permission. This permission is only available to Scanner users when your subscription is configured to allow it.

Input Parameters

Parameter	Description
action=create	(Required)
name={string}	(Required) The friendly name. This name can't already be assigned to an appliance in your account. It can be a maximum of 15 characters, spaces are not allowed.
polling_interval={value}	(Optional) The polling interval, in seconds. A valid value is 60 to 3600 (we recommend 180 which is the default). This is the frequency that the virtual scanner will attempt to connect to our Cloud Security Platform. The appliance calls home to provide health updates/heartbeats to the platform, to get software updates from the platform, to learn if new scan jobs have been requested by users, and to upload scan results data to the platform, if applicable.
asset_group_id={value}	(Required for Unit Managers and Scanners for Create request) The ID of an asset group the virtual scanner will be assigned to.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=create&echo_request=1&name=scanner1"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_create_outpu
t.dtd">
<APPLIANCE_CREATE_OUTPUT>
    <RESPONSE>
        <DATETIME>2014-01-02T09:26:01Z</DATETIME>
        <ID>777</ID>
        <NAME>scanner1</NAME>
        <ACTIVATION CODE>ACTIVATION-CODE</ACTIVATION CODE>
        <REMAINING_QVSA_LICENSES>4</REMAINING_QVSA_LICENSES>
    </RESPONSE>
```

```
</APPLIANCE_CREATE_OUTPUT>
```

DTD:

<platform API server>/api/2.0/fo/appliance/appliance_create_output.dtd

Update Virtual Scanner Appliance

/api/2.0/fo/appliance/ with action=update

[POST]

Update a virtual scanner appliance in your account. You can add tags, remove and reset tags for your scanner appliances.

Permissions - Managers can update a virtual scanner appliance. Unit Managers and Scanners must have the "Manage virtual scanner appliances" permission. This permission is only available to Scanner users when your subscription is configured to allow it.

Input Parameters

Parameter	Description
action=update	(Required)
id={id}	(Required) A valid ID of a virtual scanner.
name={string}	(Optional) The friendly name. This name can't already be assigned to an appliance in your account. It can be a maximum of 15 characters, spaces are not allowed.
polling_interval={value}	(Optional) The polling interval, in seconds. A valid value is 60 to 3600 (we recommend 180 which is the default). This is the frequency that the virtual scanner will attempt to connect to our Cloud Security Platform. The appliance calls home to provide health updates/heartbeats to the platform, to get software updates from the platform, to learn if new scan jobs have been requested by users, and to upload scan results data to the platform, if applicable.
comment={value}	(Optional) User-defined comments.
set_tags={value}	(Optional) Specify tag to be assigned to the scanner appliance. Both virtual and physical scanners can be tagged.
	These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
add_tags={value}	(Optional) Specify tag to be added to the existing list of tags assigned to the scanner. Multiple entries are comma separated.
	These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.

Parameter	Description
remove_tags={value}	(Optional) Specify tag to be removed from the existing list of tags assigned to scanner. Multiple tags are comma separated. These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
tag_set_by={id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
enable_ipv6=0	Enable or disable IPv6 on LAN. Specify 1 to enable IPv6 and 0 to disable it.

Sample - Update virtual scanner appliance name

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=update&echo_request=1&id=12345&name=scanner15"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2014-04-03T12:12:45Z</DATETIME>
        <TEXT>Virtual scanner updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>17110</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Add tags for windows agent, remove tags for linux agents

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X POST -d
"action=update&id=3105&tag_set_by=name&add_tags=windows_agent&remove_tags
=linux_agents"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2016-09-15T19:44:35Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3105</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Assign tags to virtual scanner appliance

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X POST -d
"action=update&id=3112&tag_set_by=name&set_tags=local_host,local_IP"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2016-09-15T19:47:37Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3112</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
```

Delete Virtual Scanner Appliance

/api/2.0/fo/appliance/ with action=delete

[POST]

Delete a virtual scanner appliance in your account.

Permissions - Managers can delete new virtual scanner appliance. Unit Managers and Scanners must have the “Manage virtual scanner appliances” permission. This permission is only available to Scanner users when your subscription is configured to allow it.

Deleting a virtual scanner results in these actions: 1) The scanner will be removed from associated Asset Groups, and 2) Scheduled Scans using this scanner will be deactivated.

Is your virtual scanner running scans? If yes it’s not possible to delete it. We recommend you check to be sure the virtual scanner you want to delete is not running scans.

Input Parameters

Parameter	Description
action=delete	(Required)
id={id}	(Required) A valid ID of a virtual scanner.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=delete&echo_request=1&id=12345"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

The XML output uses the simple return (/api/2.0/simple_return.dtd).

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2014-01-02T09:26:01Z</DATETIME>
        <TEXT>Virtual scanner deleted successfully</ID>
        <ITEM_LIST>
             <ITEM>
                  <KEY>ID<KEY>
                  <VALUE>115<VALUE>
             </ITEM>
             <ITEM>
                  <KEY>DEACTIVATED_SCHEDULED_SCANS<KEY>
                  <VALUE>None<VALUE>
             </ITEM>
             <ITEM>
                  <KEY>AFFECTED_ASSET_GROUPS<KEY>
                  <VALUE>None<VALUE>
             </ITEM>
        <ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Update Physical Scanner Appliance

/api/2.0/fo/appliance/physical/ with action=update

[POST]

Using the Physical Scanner Appliance API (/api/2.0/fo/appliance/physical/), Managers and Unit Managers can update physical scanner appliances.

Input Parameters

Parameter	Description
action=update	(Required)
id={id}	(Required) A valid ID of a physical scanner.
name={string}	(Optional) The friendly name. This name can't already be assigned to an appliance in your account. It can be a maximum of 15 characters, spaces are not allowed.
polling_interval={value}	(Optional) The polling interval, in seconds. A valid value is 60 to 3600 (we recommend 180 which is the default). This is the frequency that the physical scanner will attempt to connect to our Cloud Security Platform. The appliance calls home to provide health updates/heartbeats to the platform, to get software updates from the platform, to learn if new scan jobs have been requested by users, and to upload scan results data to the platform, if applicable.
set_vlans={value}	Use this parameter to specify one or more VLANs for scanner. See Manage Virtual Scanner Appliances.
set_tags= {value}	(Optional) Specify tag to be assigned to the scanner appliance. Both virtual and physical scanners can be tagged.
	These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
add_tags= {value}	(Optional) Specify tag to be added to the existing list of tags assigned to the scanner. Multiple entries are comma separated.
	These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
remove_tags= {value}	(Optional) Specify tag to be removed from the existing list of tags assigned to scanner. Multiple entries are comma separated.
	These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
tag_set_by= {id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
set_routes={value}	Use this parameter to specify one or more routes for scanner. See Manage Virtual Scanner Appliances
comment={value}	(Optional) User-defined comments.

Sample 1

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
```

```
-d "action=update&id=5115&comment=Hello"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/physical/"
```

Sample 2

Add VLAN and routes with Name, Polling interval and comments to Physical scanner:

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"action=update&id=5115&name=physcanner&polling_interval=360&set_routes=10
.10.10.10|255.255.255.0|10.10.10.10|routes1&set_vlans=1|10.2.0.2|255.255.
255.0|Testvlan1&comment=Update_scanner"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/physical/"
```

Sample 3

Update physical scanner using tag_set_by and add_tags parameters:

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=5115&tag_set_by=id&add_tags=7691422"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/physical/"
```

Sample 4

Update physical scanner using tag_set_by and set_tags parameters:

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=5115&tag_set_by=id&set_tags=7691422"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/physical/"
```

Sample 5

Update physical scanner using tag_set_by and remove_tags parameters:

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=5115&tag_set_by=id&remove_tags=7691422"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/physical/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2017-10-01T00:12:29Z</DATETIME>
        <TEXT>Physical scanner updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>5115</VALUE>
            </ITEM>
```

```
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Replace Scanner Appliance

Using the Replace Scanner Appliance API (/api/2.0/fo/appliance/replace_iscanner), Managers and Unit Managers can replace a scanner appliance with a new one. Tell us the name of the appliance you want to replace and the one you want to use.

Good to Know
- You can replace one scanner appliance at a time.
- Do not replace a scanner appliance while scans (using the appliance) are in progress.
- The old scanner and the new scanner must be in the same network, if applicable.
- You can only replace an EC2 scanner with another EC2 scanner.

Input Parameters

Parameter	Description
action=replace	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
old_scanner_name={value}	(Required) The name of the scanner you want to replace.
new_scanner_name={value}	(Required) The name of the scanner you want to use.
do_not_copy_settings={**0**|1}	(Optional) When not specified, we will transfer settings from the old scanner to the new scanner for you. Specify 1 if you do not want us to transfer appliance settings. Settings include the polling interval, heartbeat checks, scanning options, VLANs and static routes, associated asset groups, schedules and network, if applicable.
do_not_remove_new_scanner_from_objects={**0**|1}	(Optional) When not specified, we will remove the new appliance from business objects (asset groups and schedules) that it's already associated with. Specify 1 if you do not want us to remove the new appliance from business objects. This parameter cannot be set for EC2 scanners.

Sample - Replace scanner with new one

Replace "scanner1" with "scanner2" and copy scanner appliance settings but do not remove the new scanner from business objects.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/replace_iscanner/?acti
on=replace&echo_request=1&old_scanner_name=scanner1&new_scanner_name=scan
ner2&do_not_copy_settings=0&do_not_remove_new_scanner_from_objects=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCANNER_REPLACE_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/appliance/replace_iscanner/repla
ce_iscanner_output.dtd">
<SCANNER_REPLACE_OUTPUT>
  <REQUEST>
    <DATETIME>2018-01-16T06:52:53Z</DATETIME>
    <USER_LOGIN>abcd</USER_LOGIN>

<RESOURCE><qualys_base_url>/api/2.0/fo/appliance/replace_iscanner/</RESOU
RCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>old_scanner_name</KEY>
        <VALUE>scanner1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>new_scanner_name</KEY>
        <VALUE>scanner2</VALUE>
      </PARAM>
      <PARAM>
        <KEY>do_not_copy_settings</KEY>
        <VALUE>0</VALUE>
      </PARAM>
      <PARAM>
        <KEY>do_not_remove_new_scanner_from_objects</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>replace</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2018-01-16T06:52:53Z</DATETIME>
    <NEW_SETTINGS>POLLING_INTERVAL: 180, HEARTBEAT: 1</NEW_SETTINGS>
    <SCHEDULED_SCANS>Scheduled-Scan1, Scheduled-Scan2</SCHEDULED_SCANS>
    <ASSET_GROUPS>AG123, AG456</ASSET_GROUPS>
    <SUCCESS>Scanner Appliance replaced successfully.</SUCCESS>
  </RESPONSE>
</SCANNER_REPLACE_OUTPUT>
```

DTD

A replace scanner appliance API request uses this DTD:

<platform API server>/api/2.0/fo/appliance/replace_iscanner/replace_iscanner_output.dtd

Scanner Appliance VLANs and Static Routes

/api/2.0/fo/appliance/?action=update (virtual appliance)

/api/2.0/fo/appliance/physical/?action=update (physical appliance)

Manage your VLANs and static routes for virtual and physical scanner appliances using the Virtual Scanner Appliance API () or Physical Scanner Appliance API (/api/2.0/fo/appliance/physical/?action=update). Use the parameters “set_vlans” and “set_routes” to add, update and remove these settings.

What do I need? Your Qualys account must have the VLANs and Static Routes feature enabled. Please contact our Support Team or your Qualys TAM if you would like us to enable this feature for you.

Permissions - Managers can add/remove VLANs and static routes for all scanner appliances in the subscription. Unit Managers can add/remove VLANs and static routes in the user’s same business unit.

Set VLANs on Scanner Appliance

Use the “set_vlans” parameter to specify one or more VLANs.

The format for a single VLAN is ID|IPv4_ADDRESS|NETMASK|NAME|ipv6_static or ipv6_auto|IPv6_ADDRESS, with pipe (|) used as a delimiter. All attributes are required. Multiple VLANs can be assigned using a comma separated list.

Good to know - An API call with the parameter “set_vlans” set to ” (empty string) will replace (i.e. remove) *all* of the VLANs that are assigned to the scanner appliance.

Attribute	Description
ID	Customer-defined ID (not assigned by Qualys). Must be in the range 0 to 4096, inclusive.
IPv4_ADDRESS	A valid IPv4 IP address (dotted quad), such as 10.10.10.1. Leave empty when specifying an IPv6 address.
NETMASK	A valid network mask (dotted quad), such as 255.255.255.0. Leave empty when specifying an IPv6 address.
NAME	A valid name (can be empty). The name can be a maximum of 256 ASCII characters. The character : (colon) is permitted. These characters are not permitted: , (comma), < (less than), > (greater than), " (double quote), & (ampersand), |(pipe), = (equals).
ipv6_static or ipv6_auto	Specify ipv6_static to provide a static IPv6 address. Specify ipv6_auto to auto-configure IPv6 using SLAAC on the VLAN.
IPv6_ADDRESS	A valid IPv6 address is required when ipv6_static is specified, such as fdd1:0:1:107::500. Leave empty when ipv6_auto is specified.

API request (1 IPv4 VLAN):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
```

```
"id=43463&set_vlans=0|10.10.10.1|255.255.255.0|vlan1"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

API request (mix of IPv6 and IPv4 VLANs):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"id=43463&set_vlans=1234|||Name1234|ipv6_static|fdd1:0:1:108::500,5678|12
3.123.123.123|255.255.255.255|Name5678,9012|244.244.244.244|255.255.255.0
|Name9012|ipv6_auto,3456|12.12.12.12|255.255.255.0|Name3456|ipv6_static|f
dd1:0:1:107::500"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-07-09T08:46:54Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>43463</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Set Static Routes on Scanner Appliance

Use the “set_routes” parameter to specify one or more static routes.

The format for a single static route is IPv4_ADDRESS|NETMASK|IPv4_GATEWAY|NAME|IPv6_ADDRESS|IPv6_GATEWAY, with pipe (|) used as the delimiter. All attributes are required. Multiple static routes can be assigned using a comma separated list.

Good to know - An API call with the parameter “set_routes” set to ” (empty string) will replace (i.e. remove) *all* of the static routes that are assigned to the scanner appliance.

Attribute	Description
IPv4_ADDRESS	A valid IPv4 IP address (dotted quad), such as 10.10.26.0. Leave empty when specifying an IPv6 address.
NETMASK	A valid network mask (dotted quad), such as 255.255.255.0. Leave empty when specifying an IPv6 address.
IPv4_GATEWAY	A valid IPv4 address (dotted quad), such as 10.10.25.255. Leave empty when specifying an IPv6 address.
NAME	A valid name (can be empty). The name can be a maximum of 256 ASCII characters. The character : (colon) is permitted. These characters are not permitted: , (comma), < (less than), > (greater than), " (double quote), & (ampersand), |(pipe), = (equals).
IPv6_ADDRESS	A valid IPv6 address (with or without the prefix), such as fdd1:0:1:107::500.
IPv6_GATEWAY	A valid IPv6 gateway address, such as 2001:470:8418:280d::1.

API request (1 IPv4 static route):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"id=43463&set_routes=10.10.25.0|255.255.255.0|10.10.25.255|Route1"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

API request (mix of IPv4 and IPv6 static routes):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"id=43463&set_routes=192.0.0.0|255.255.255.0|10.100.11.157|Name2,192.168.
0.0|255.255.0.0|10.100.11.157|Name3,192.168.10.0||10.100.11.157|Name4,192
.167.0.0|255.255.0.0|10.100.11.157|Name5|fdd1:0:1:107::500|2001:470:8418:
280d::1,|||Name1|fdd1:0:1:107::500/64|2001:470:8418:280d::1"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-07-09T08:49:18Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
    <ITEM_LIST>
```

```
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>43463</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

View Scanner Appliances with VLANs, Static Routes

Use the parameters “action=list” and “output_mode=full”.

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "GET"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=list&ids=43463
&output_mode=full"
```

XML output:

```
...
   <VLANS>
      <SETTING>Enabled</SETTING>
      <VLAN>
         <ID>0</ID>
         <NAME>vlan1</NAME>
         <IP_ADDRESS>10.10.10.1</IP_ADDRESS>
         <NETMASK>255.255.255.0</NETMASK>
      </VLAN>
   </VLANS>
   <STATIC_ROUTES>
      <ROUTE>
         <NAME>Route1</NAME>
         <IP_ADDRESS>10.10.25.0</IP_ADDRESS>
         <NETMASK>255.255.255.0</NETMASK>
         <GATEWAY>10.10.25.255</GATEWAY>
      </ROUTE>
      <ROUTE>
         <NAME>Route2</NAME>
         <IP_ADDRESS>10.10.26.0</IP_ADDRESS>
         <NETMASK>255.255.255.0</NETMASK>
         <GATEWAY>10.10.26.255</GATEWAY>
      </ROUTE>
   </STATIC_ROUTES>
...
```

Delete All VLAN Records

Use the “set_vlans” parameters and set it to “ (empty string).

API request (deletes all VLAN records):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: -d "id=43463&set_vlans="
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-07-09T08:49:18Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
...
```

Delete All Static Route Records

Use the "set_routes" parameters and set it to " (empty string).

API request (deletes all static route records):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: -d "id=43463&set_routes="
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-07-09T08:49:18Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
...
```

Option Profile Export

For API version information, refer to the API Version History section.

V2.0| V3.0|V4.0|V5.0|V6.0 | V7.0

V2.0

/api/2.0/fo/subscription/option_profile/?action=export

[GET]

Export one option profile or all option profiles in the subscription to an XML file. Manager user role is required.

Permissions - The API user must have the Manager role.

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.

DTD

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

All the option profiles in the user's account get exported in XML format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=export"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>111186</ID>
            <GROUP_NAME>
                <![CDATA[OP-SCAN]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Doe(john_doe)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>44</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>N/A</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>full</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>1</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                    <UDP_PORTS_ADDITIONAL>
                        <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                        <ADDITIONAL_PORTS>1-
1024,8080,8181</ADDITIONAL_PORTS>
                    </UDP_PORTS_ADDITIONAL>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
            <CLOSE_VULNERABILITIES>

<HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
                <HOST_NOT_FOUND_ALIVE>7</HOST_NOT_FOUND_ALIVE>
            </CLOSE_VULNERABILITIES>
```

```
<PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>30</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>48</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>18</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>18</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Minimum</PACKET_DELAY>
                <PORT_SCANNING_AND_HOST_DISCOVERY>Minimum
                </PORT_SCANNING_AND_HOST_ DISCOVERY>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
            <PASSWORD_BRUTE_FORCING>
                <SYSTEM>
                    <HAS_SYSTEM>1</HAS_SYSTEM>
                    <SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
                </SYSTEM>
                <CUSTOM_LIST>
                    <CUSTOM>
                        <ID>3001</ID>
                        <TITLE>
                            <![CDATA[123]]>
                        </TITLE>
                        <TYPE>FTP</TYPE>
                        <LOGIN_PASSWORD>
                            <![CDATA[L:temp,P:123123123]]>
                        </LOGIN_PASSWORD>
                    </CUSTOM>
                </CUSTOM_LIST>
            </PASSWORD_BRUTE_FORCING>
            <VULNERABILITY_DETECTION>
                <CUSTOM_LIST>
                    <CUSTOM>
                        <ID>2094</ID>
                        <TITLE>
                           <![CDATA[Option Profile: Qualys Top 20
Options]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
```

```
                        <ID>2095</ID>
                        <TITLE>
                            <![CDATA[Option Profile: 2008 SANS20
Options]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>2096</ID>
                        <TITLE>
                            <![CDATA[Scan Report Template: High
Severity Report]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>5230</ID>
                        <TITLE>
                            <![CDATA[118960]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>87936</ID>
                        <TITLE>
                            <![CDATA[Bash Shellshock Detection]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>87937</ID>
                        <TITLE>
                            <![CDATA[Heartbleed Detection]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>87938</ID>
                        <TITLE>
                          <![CDATA[Windows Authentication Results
v.1]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>87939</ID>
                        <TITLE>
                            <![CDATA[Unix Authentication Results
v.1]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
```

```
                        <ID>87940</ID>
                        <TITLE>
                            <![CDATA[Inventory Results v.1]]>
                        </TITLE>
                    </CUSTOM>
                    <CUSTOM>
                        <ID>87941</ID>
                        <TITLE>
                            <![CDATA[SSL Certificates]]>
                        </TITLE>
                    </CUSTOM>
                </CUSTOM_LIST>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>1</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>1</OVAL_CHECKS>
                </DETECTION_INCLUDE>
                <DETECTION_EXCLUDE>
                    <CUSTOM_LIST>
                        <CUSTOM>
                            <ID>2099</ID>
                            <TITLE>
                                <![CDATA[DL]]>
                            </TITLE>
                        </CUSTOM>
                    </CUSTOM_LIST>
                </DETECTION_EXCLUDE>
            </VULNERABILITY_DETECTION>
            <AUTHENTICATION>
                <![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,Sybase]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_L EAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
            <DISSOLVABLE_AGENT>

<DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>
                <WINDOWS_SHARE_ENUMERATION_ENABLE>1
                </WINDOWS_SHARE_ENUMERATION_ENA BLE>
            </DISSOLVABLE_AGENT>
            <LITE_OS_SCAN>1</LITE_OS_SCAN>
            <CUSTOM_HTTP_HEADER>
                <VALUE>AFCD</VALUE>
            </CUSTOM_HTTP_HEADER>
```

```
            <FILE_INTEGRITY_MONITORING>

<AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
            </FILE_INTEGRITY_MONITORING>
            <DO_NOT_OVERWRITE_OS>1</DO_NOT_OVERWRITE_OS>
            <SYSTEM_AUTH_RECORD>
                <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
                </INCLUDE_SYSTEM_AUTH>
            </SYSTEM_AUTH_RECORD>
        </SCAN>
        <MAP>

<BASIC_INFO_GATHERING_ON>netblockonly</BASIC_INFO_GATHERING_ON>
            <TCP_PORTS>

<TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                <TCP_PORTS_ADDITIONAL>
                    <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                    <ADDITIONAL_PORTS>1,2,3,80</ADDITIONAL_PORTS>
                </TCP_PORTS_ADDITIONAL>
            </TCP_PORTS>
            <UDP_PORTS>

<UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
                <UDP_PORTS_ADDITIONAL>
                    <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                   <ADDITIONAL_PORTS>4,5,6,8181</ADDITIONAL_PORTS>
                </UDP_PORTS_ADDITIONAL>
            </UDP_PORTS>
            <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>16</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>14</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>64</NETBLOCK_SIZE>
                </MAP_PARALLEL>
                <PACKET_DELAY>Maximum</PACKET_DELAY>
            </MAP_PERFORMANCE>
            <MAP_AUTHENTICATION>VMware</MAP_AUTHENTICATION>
```

```
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                        <TCP_ADDITIONAL>
                            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                            <ADDITIONAL_PORTS>1-
6,1024</ADDITIONAL_PORTS>
                        </TCP_ADDITIONAL>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <BLOCK_RESOURCES>
                    <WATCHGUARD_DEFAULT_BLOCKED_PORTS>1
                    </WATCHGUARD_DEFAULT_BLOCKED_PO RTS>
                    <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
                </BLOCK_RESOURCES>
                <PACKET_OPTIONS>
                    <IGNORE_FIREWALL_GENERATED_TCP_RST>1
                    </IGNORE_FIREWALL_GENERATED_TC P_RST>
                    <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>
                    <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1
                    </IGNORE_FIREWALL_GENERATE D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1
                    </NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Option Profile with specific title and ID

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
-X GET "action=export&option_profile_title=OP-
COMP&option_profile_id=111235"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>111235</ID>
            <GROUP_NAME>
                <![CDATA[OP-COMP]]>
            </GROUP_NAME>
            <GROUP_TYPE>compliance</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Doe (john_doe)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>44</SUBSCRIPTION_ID>
            <IS_GLOBAL>0</IS_GLOBAL>
            <UPDATE_DATE>N/A</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TARGETED_SCAN>1</TARGETED_SCAN>
            </PORTS>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>5</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Short</PACKET_DELAY>
                <PORT_SCANNING_AND_HOST_DISCOVERY>Minimum
                </PORT_SCANNING_AND_HOST_ DISCOVERY>
            </PERFORMANCE>
            <DISSOLVABLE_AGENT>

<DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>
                <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>1</HAS_PASSWORD_AUDITING_ENABLE>
```

```
<CUSTOM_PASSWORD_DICTIONARY>asdf</CUSTOM_PASSWORD_DICTIONARY>
                </PASSWORD_AUDITING_ENABLE>
                <WINDOWS_SHARE_ENUMERATION_ENABLE>1
                </WINDOWS_SHARE_ENUMERATION_ENA BLE>
                <WINDOWS_DIRECTORY_SEARCH_ENABLE>1
                </WINDOWS_DIRECTORY_SEARCH_ENABL E>
            </DISSOLVABLE_AGENT>
            <CONTROL_TYPES>
                <FIM_CONTROLS_ENABLED>1</FIM_CONTROLS_ENABLED>

<CUSTOM_WMI_QUERY_CHECKS>1</CUSTOM_WMI_QUERY_CHECKS>
            </CONTROL_TYPES>
            <TEST_AUTHENTICATION>1</TEST_AUTHENTICATION>
            <SYSTEM_AUTH_RECORD>
                <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
                </INCLUDE_SYSTEM_AUTH>
            </SYSTEM_AUTH_RECORD>
        </SCAN>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </UDP_PORTS>
                <ICMP>1</ICMP>
            </HOST_DISCOVERY>
            <BLOCK_RESOURCES>
                <WATCHGUARD_DEFAULT_BLOCKED_PORTS>1
                </WATCHGUARD_DEFAULT_BLOCKED_PO RTS>
                <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
            </BLOCK_RESOURCES>
            <PACKET_OPTIONS>
                <IGNORE_FIREWALL_GENERATED_TCP_RST>1
                </IGNORE_FIREWALL_GENERATED_TC P_RST>
                <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1
                </IGNORE_FIREWALL_GENERATE D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1
                </NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
```

```
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Option Profile with the specific title

API request:

```
curl --location
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=
export&option_profile_title=VM_API_Option_profile_01" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Bearer< JWT Token>"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2445050</ID>
            <GROUP_NAME>
                <![CDATA[VM_API_Option_profile_01]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Automation Test (scan_at)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>590924</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2023-08-31T09:34:28Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
```

```
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
                <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>

<PERFORM_PARTIAL_SSL_TLS_AUDITING>1</PERFORM_PARTIAL_SSL_TLS_AUDIT
ING>
        </SCAN>
        <MAP>
```

```
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
             <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                 <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
             </MAP_OPTIONS>
             <MAP_PERFORMANCE>
                 <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                 <MAP_PARALLEL>
                     <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                     <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                     <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                 </MAP_PARALLEL>
                 <PACKET_DELAY>Minimum</PACKET_DELAY>
             </MAP_PERFORMANCE>
             <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
         </MAP>
         <ADDITIONAL>
             <HOST_DISCOVERY>
                 <TCP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </TCP_PORTS>
                 <UDP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </UDP_PORTS>
                 <ICMP>1</ICMP>
             </HOST_DISCOVERY>
             <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
             </PACKET_OPTIONS>
         </ADDITIONAL>
     </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Option Profile of type PCI

The option profile with PCI type in the user's account get exported in XML format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
-X GET "action=export&option_profile_type=pci"
"https://<qualys_base_url>/api/2.0/fo/subscription/option_profile/
"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://<qualys_base_url>/api/2.0/fo/subscription/option_profile/
option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>111223</ID>
      <GROUP_NAME><![CDATA[PCI-Example]]></GROUP_NAME>
      <GROUP_TYPE>pci</GROUP_TYPE>
      <USER_ID><![CDATA[John Doe (john_doe)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>44</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>N/A</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
      <CLOSE_VULNERABILITIES>
        <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
        <HOST_NOT_FOUND_ALIVE>4</HOST_NOT_FOUND_ALIVE>
      </CLOSE_VULNERABILITIES>
      <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Low</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>5</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>10</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>4</TOTAL_PROCESSES>
          <HTTP_PROCESSES>2</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
```

```
        <PACKET_DELAY>Long</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_
DISCOVERY>
      </PERFORMANCE>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1-6,1024</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
      </HOST_DISCOVERY>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Options Profile for Database UDC

Export the Option Profile for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, and IBM DB2 with database preference key setting and its corresponding value defined.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X -d
"action=export&option_profile_id=1710150"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <...
         </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <DATABASE_PREFERENCE_KEY>
        <MSSQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>250</DB_UDC_LIMIT>
        </MSSQL>
        <ORACLE>
```

```
            <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
            <DB_UDC_LIMIT>10</DB_UDC_LIMIT>
          </ORACLE>
          <SYBASE>
            <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
            <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
          </SYBASE>
          <POSTGRESQL>
            <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
            <DB_UDC_LIMIT>2500</DB_UDC_LIMIT>
          </POSTGRESQL>
          <DB2>
            <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
            <DB_UDC_LIMIT>350</DB_UDC_LIMIT>
          </DB2>
        </DATABASE_PREFERENCE_KEY>
        <FILE_INTEGRITY_MONITORING>
          <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
        </FILE_INTEGRITY_MONITORING>
      ...
    </OPTION_PROFILE>
  </OPTION_PROFILES>
```

V3.0

/api/3.0/fo/subscription/option_profile/?action=export

[GET]

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD

<platform API server>/api/3.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=export"
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/?action=
export&option_profile_title=Option_profile_vCenter_scan_disconnect
ed_esxi"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
```

```
                <ID>2633919</ID>
                <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[John Manager (agms_nb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2024-07-01T09:55:01Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                      <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                       <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>
                    <PORT_SCANNING_AND_HOST_DISCOVERY>Normal
                    </PORT_SCANNING_AND_HOST_DISCOVER
Y>
```

```
                </PERFORMANCE>

<LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
            <MAP>

<BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
```

```
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
                    <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0
                    </IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0

</NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

Sample - Export Option Profile with Specific ID

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/?action=
export&option_profile_id=2639622"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639622</ID>
            <GROUP_NAME>
                <![CDATA[mob1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-09T06:41:00Z</UPDATE_DATE>
```

```
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
```

```
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
             <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                 <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
             </MAP_OPTIONS>
             <MAP_PERFORMANCE>
                 <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                 <MAP_PARALLEL>
                     <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                     <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                     <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                 </MAP_PARALLEL>
                 <PACKET_DELAY>Minimum</PACKET_DELAY>
             </MAP_PERFORMANCE>
             <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
             <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
         </MAP>
         <ADDITIONAL>
             <HOST_DISCOVERY>
                 <TCP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </TCP_PORTS>
                 <UDP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </UDP_PORTS>
                 <ICMP>1</ICMP>
             </HOST_DISCOVERY>
             <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                 <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
             </PACKET_OPTIONS>
         </ADDITIONAL>
     </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Option Profile with Specific Title

API request:

```
curl --location
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/?action=
export&option_profile_title=mob1"
\--header "Content-Type: application/x-www-form-urlencoded"
\--header "X-Requested-With: curl demo2"
\--header "Accept: */*"
\--header "Content-Length: 0"
\--header "Authorization: Basic encoded username:password string"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639622</ID>
            <GROUP_NAME>
                <![CDATA[mob1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-09T06:41:00Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
```

```
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
           <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
```

```
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

V4.0

/api/4.0/fo/subscription/option_profile/?action=export

[GET]

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD

<platform API server>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=export"
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action=
export&option_profile_title=Option_profile_vCenter_scan_disconnect
ed_esxi"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
```

```
                <ID>2633919</ID>
                <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[John Manager (agms_nb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2024-07-01T09:55:01Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                      <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                       <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>
                    <PORT_SCANNING_AND_HOST_DISCOVERY>Normal
                    </PORT_SCANNING_AND_HOST_DISCOVER
Y>
```

```
                </PERFORMANCE>

<LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
            <MAP>

<BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
```

```
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
                    <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0
                    </IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0

</NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

Sample - Export Option Profile with Specific ID

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action=
export&option_profile_id=2639622"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639622</ID>
            <GROUP_NAME>
                <![CDATA[mob1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-09T06:41:00Z</UPDATE_DATE>
```

```
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
```

```
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
             <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                 <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
             </MAP_OPTIONS>
             <MAP_PERFORMANCE>
                 <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                 <MAP_PARALLEL>
                     <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                     <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                     <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                 </MAP_PARALLEL>
                 <PACKET_DELAY>Minimum</PACKET_DELAY>
             </MAP_PERFORMANCE>
             <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
             <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
         </MAP>
         <ADDITIONAL>
             <HOST_DISCOVERY>
                 <TCP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </TCP_PORTS>
                 <UDP_PORTS>
                     <STANDARD_SCAN>1</STANDARD_SCAN>
                 </UDP_PORTS>
                 <ICMP>1</ICMP>
             </HOST_DISCOVERY>
             <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                 <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
             </PACKET_OPTIONS>
         </ADDITIONAL>
     </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export Option Profile with Specific Title

API request:

```
curl --location
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action=
export&option_profile_title=mob1"
\--header "Content-Type: application/x-www-form-urlencoded"
\--header "X-Requested-With: curl demo2"
\--header "Accept: */*"
\--header "Content-Length: 0"
\--header "Authorization: Bearer< JWT Token>"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639622</ID>
            <GROUP_NAME>
                <![CDATA[mob1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-09T06:41:00Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
```

```
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
           <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
```

```
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

V5.0

/api/5.0/fo/subscription/option_profile/?action=export

[GET]

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD

<platform API server>/api/5.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "<username>:<password>"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/?action=export&
&output_format=xml&option_profile_type=compliance&option_profile_id=77544
47"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>7754447</ID>
      <GROUP_NAME><![CDATA[agent correlation enabled OP]]></GROUP_NAME>
```

```
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Doe (<username>)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>4027198</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2025-09-25T08:53:52Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>
          <HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
      </DISSOLVABLE_AGENT>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>0</ICMP>
```

```
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
        <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
      <AGENT_CORRELATION_IDENTIFIER>

<IS_AGENT_CORRELATION_ID_ENABLED>1</IS_AGENT_CORRELATION_ID_ENABLED>

<AGENT_CORRELATION_ID_PORTS>10001,10002,10003,10004,10005</AGENT_CORRELAT
ION_ID_PORTS>
      </AGENT_CORRELATION_IDENTIFIER>
    </ADDITIONAL>
    <INSTANCE_DATA_COLLECTION />
    <OS_BASED_INSTANCE_DISC_COLLECTION />
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

V6.0

/api/6.0/fo/subscription/option_profile/?action=export

[GET]

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD

<platform API server>/api/6.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/subscription/option_profile/?action=export&
option_profile_id=3494139' \
--header 'Content-Type: application/xml' \
--header 'Accept: */*' \
--header 'x-requested-with: curl demo2' \
--header 'Authorization: Bearer <JWT Token>
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/6.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>3494139</ID>
```

```
            <GROUP_NAME>
                <![CDATA[Abhishek OP Full Enabled Do not use]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Aditya Gangadharan (vmsp_ag1)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>970969</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>1</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2026-01-19T06:54:38Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                    <UDP_PORTS_ADDITIONAL>
                        <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                        <ADDITIONAL_PORTS>8080</ADDITIONAL_PORTS>
                    </UDP_PORTS_ADDITIONAL>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
            <CLOSE_VULNERABILITIES>
                <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
                <HOST_NOT_FOUND_ALIVE>2</HOST_NOT_FOUND_ALIVE>
            </CLOSE_VULNERABILITIES>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>20</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
            <PASSWORD_BRUTE_FORCING>
                <SYSTEM>
```

```
                    <HAS_SYSTEM>1</HAS_SYSTEM>
                    <SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
                </SYSTEM>
            </PASSWORD_BRUTE_FORCING>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>1</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <AUTHENTICATION>
                <![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,MongoDB,Tomcat Server,Oracle Weblogic
Server,Palo Alto Networks Firewall,Jboss Server,Sybase,Nutanix,NSX]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_LEAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
            <SYSTEM_AUTH_RECORD>
                <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
                </INCLUDE_SYSTEM_AUTH>
            </SYSTEM_AUTH_RECORD>
            <LITE_OS_SCAN>1</LITE_OS_SCAN>
            <HOST_ALIVE_TESTING>1</HOST_ALIVE_TESTING>

<MAX_SCAN_DURATION_PER_ASSET>2500</MAX_SCAN_DURATION_PER_ASSET>
            <DO_NOT_OVERWRITE_OS>1</DO_NOT_OVERWRITE_OS>
            <TEST_AUTHENTICATION>1</TEST_AUTHENTICATION>

<PERFORM_PARTIAL_SSL_TLS_AUDITING>1</PERFORM_PARTIAL_SSL_TLS_AUDITING>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
            <TCP_PORTS>
                <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
            </TCP_PORTS>
            <UDP_PORTS>
                <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
            </UDP_PORTS>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>8</EXTERNAL_SCANNERS>
```

```
                        <SCANNER_APPLIANCES>10</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>4096 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

V7.0

/api/7.0/fo/subscription/option_profile/?action=export

[GET]

Input Parameters

Parameter	Description
action=export	(Required)
output_format={XML}	(Optional) XML format is supported. When unspecified, output format is XML.
option_profile_id={value}	(Optional) By default all option profiles will be exported. Specify an option profile ID and we'll export the option profile matching this ID only.
option_profile_title={value}	(Optional) By default all option profiles will be exported. Specify a title and we'll export the option profile matching this title only - exact match is required.
option_profile_type={value}	(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: "option_profile_type" parameter can be specified with "option_profile_id" or "option_profile_title".
include_system_option_profiles ={**0**|1}	(Optional) When unspecified or set to 0, system option profiles are not included in the output. Specify 1 to include system option profiles in the output.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD

<platform API server>/api/6.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - Export Option Profiles

API request:

```
curl --location '

/api/7.0/fo/subscription/option_profile/?action=export&output_format=XML&
option_profile_id=4084375' \
--header 'X-Requested-With: Test' \
--header 'Cookie: QualysSession=xxxxxxxxxxxxxxxxxxxxxxxx'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/7.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>4084375</ID>
```

```
            <GROUP_NAME>
                <![CDATA[HOST_SCRIPT_EXECUTION_CREATE_SM]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[username (xxxx_yy)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>970969</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2026-06-23T09:18:42Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>

<ALLOW_ON_HOST_SCRIPT_EXECUTION>1</ALLOW_ON_HOST_SCRIPT_EXECUTION>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
```

```
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <AUTHENTICATION>
                <![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,MongoDB,Tomcat Server,Oracle Weblogic
Server,Palo Alto Networks Firewall,Jboss Server,Sybase,NSX]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_LEAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                </MAP_PARALLEL>
                <PACKET_DELAY>Minimum</PACKET_DELAY>
            </MAP_PERFORMANCE>
            <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </UDP_PORTS>
                <ICMP>0</ICMP>
            </HOST_DISCOVERY>
            <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/7.0/fo/subscription/option_profile/?action=export	Active	Active
/api/6.0/fo/subscription/option_profile/?action=export	January 2027	July 2027
/api/5.0/fo/subscription/option_profile/?action=export	July 2026	January 2027
/api/4.0/fo/subscription/option_profile/?action=export	December 2025	December 2026
/api/3.0/fo/subscription/option_profile/?action=export	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=export	December 2025	December 2026

Option Profile Import

For API version information, refer to the API Version History section.

V2.0| V3.0| V4.0|V5.0|V6.0 | V7.0

V2.0

/api/2.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required) Specify action to import option profile.
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.

DTD (Request POST Data)

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/2.0/simple_return.dtd

Sample - Import option profiles in the input file into the users account

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H "content-type:
text/xml" -X POST --data-binary @Export_OP.xml
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=import"
```

Note: "Export_OP.xml" contains the request POST data.

Request POST data:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>11123</ID>
      <GROUP_NAME><![CDATA[OP-SCAN]]></GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID><![CDATA[John Doe (john_doe)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>76084</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>1</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
```

```
      <UPDATE_DATE>N/A</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TCP_PORTS>
          <TCP_PORTS_TYPE>full</TCP_PORTS_TYPE>
          <THREE_WAY_HANDSHAKE>1</THREE_WAY_HANDSHAKE>
        </TCP_PORTS>
        <UDP_PORTS>
          <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
          <UDP_PORTS_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1-1024,8080,8181</ADDITIONAL_PORTS>
          </UDP_PORTS_ADDITIONAL>
        </UDP_PORTS>
        <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
      </PORTS>
      <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
      <CLOSE_VULNERABILITIES>
        <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
        <HOST_NOT_FOUND_ALIVE>7</HOST_NOT_FOUND_ALIVE>
      </CLOSE_VULNERABILITIES>
      <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>30</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>48</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>18</TOTAL_PROCESSES>
          <HTTP_PROCESSES>18</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Maximum</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_DISCOVE
RY>
      </PERFORMANCE>
      <LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
      <PASSWORD_BRUTE_FORCING>
        <SYSTEM>
          <HAS_SYSTEM>1</HAS_SYSTEM>
          <SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
        </SYSTEM>
        <CUSTOM_LIST>
          <CUSTOM>
            <ID>3001</ID>
            <TITLE><![CDATA[123]]></TITLE>
            <TYPE>FTP</TYPE>
<LOGIN_PASSWORD><![CDATA[L:temp,P:123123123]]></LOGIN_PASSWORD>
          </CUSTOM>
        </CUSTOM_LIST>
      </PASSWORD_BRUTE_FORCING>
      <VULNERABILITY_DETECTION>
```

```
        <CUSTOM_LIST>
          <CUSTOM>
            <ID>2094</ID>
            <TITLE><![CDATA[Option Profile: Qualys Top 20
Options]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>2095</ID>
           <TITLE><![CDATA[Option Profile: 2008 SANS20 Options]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>2096</ID>
            <TITLE><![CDATA[Scan Report Template: High Severity
Report]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>5230</ID>
            <TITLE><![CDATA[118960]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87936</ID>
            <TITLE><![CDATA[Bash Shellshock Detection]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87937</ID>
            <TITLE><![CDATA[Heartbleed Detection]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87938</ID>
            <TITLE><![CDATA[Windows Authentication Results v.1]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87939</ID>
            <TITLE><![CDATA[Unix Authentication Results v.1]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87940</ID>
            <TITLE><![CDATA[Inventory Results v.1]]></TITLE>
          </CUSTOM>
          <CUSTOM>
            <ID>87941</ID>
            <TITLE><![CDATA[SSL Certificates]]></TITLE>
          </CUSTOM>
        </CUSTOM_LIST>
        <DETECTION_INCLUDE>
          <BASIC_HOST_INFO_CHECKS>1</BASIC_HOST_INFO_CHECKS>
          <OVAL_CHECKS>1</OVAL_CHECKS>
        </DETECTION_INCLUDE>
        <DETECTION_EXCLUDE>
          <CUSTOM_LIST>
            <CUSTOM>
              <ID>2099</ID>
              <TITLE><![CDATA[DL]]></TITLE>
            </CUSTOM>
```

```
          </CUSTOM_LIST>
        </DETECTION_EXCLUDE>
      </VULNERABILITY_DETECTION>
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL]]></AUTHENTICATION>

<AUTHENTICATION_LEAST_PRIVILEGE><![CDATA[Unix]]></AUTHENTICATION_LEAST_PR
IVILEGE>
      <ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>
<WINDOWS_SHARE_ENUMERATION_ENABLE>1</WINDOWS_SHARE_ENUMERATION_ENABLE>
      </DISSOLVABLE_AGENT>
      <LITE_OS_SCAN>1</LITE_OS_SCAN>
      <CUSTOM_HTTP_HEADER>
        <VALUE>AFCD</VALUE>
      </CUSTOM_HTTP_HEADER>
      <FILE_INTEGRITY_MONITORING>
       <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <DO_NOT_OVERWRITE_OS>1</DO_NOT_OVERWRITE_OS>
      <SYSTEM_AUTH_RECORD>
          <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_SYSTEM_AUTH>1</ON_DUPLICATE_USE_SYSTEM_AUTH>
          </INCLUDE_SYSTEM_AUTH>
      </SYSTEM_AUTH_RECORD>
    </SCAN>
    <MAP>
      <BASIC_INFO_GATHERING_ON>netblockonly</BASIC_INFO_GATHERING_ON>
      <TCP_PORTS>
        <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
        <TCP_PORTS_ADDITIONAL>
          <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
          <ADDITIONAL_PORTS>1,2,3,80</ADDITIONAL_PORTS>
        </TCP_PORTS_ADDITIONAL>
      </TCP_PORTS>
      <UDP_PORTS>
        <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
        <UDP_PORTS_ADDITIONAL>
          <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
          <ADDITIONAL_PORTS>4,5,6,8181</ADDITIONAL_PORTS>
        </UDP_PORTS_ADDITIONAL>
      </UDP_PORTS>
      <MAP_OPTIONS>
        <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
        <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
      </MAP_OPTIONS>
      <MAP_PERFORMANCE>
        <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
        <MAP_PARALLEL>
          <EXTERNAL_SCANNERS>16</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>14</SCANNER_APPLIANCES>
          <NETBLOCK_SIZE>64</NETBLOCK_SIZE>
```

```
        </MAP_PARALLEL>
        <PACKET_DELAY>Medium</PACKET_DELAY>
      </MAP_PERFORMANCE>
      <MAP_AUTHENTICATION>VMware</MAP_AUTHENTICATION>
    </MAP>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1-6,1024</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PORTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
        <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
 <RESPONSE>
   <DATETIME>2017-04-03T11:17:43Z</DATETIME>
   <TEXT>Successfully imported Option profile for the subscription Id
76084</TEXT>
   <ITEM_LIST>
     <ITEM>
       <KEY>111234</KEY>
       <VALUE>PCI-John</VALUE>
     </ITEM>
   </ITEM_LIST>
 </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Import option profiles

API request:

```
curl --location
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=import"
\--header "X-Requested-With: curl demo2"
\--header "Accept: */*"
\--header "Content-Type: text/xml"
\--header "Authorization: Bearer< JWT Token>"
\--data "
```

Request Post data:

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_
info.dtd">
    <OPTION_PROFILES>
      <OPTION_PROFILE>
        <BASIC_INFO>
          <ID>1599154</ID>
          <GROUP_NAME><![CDATA[API_IMPORT_OP_1647433780]]></GROUP_NAME>
          <GROUP_TYPE>user</GROUP_TYPE>
          <USER_ID><![CDATA[Network Disabled (pv_nd)]]></USER_ID>
          <UNIT_ID>0</UNIT_ID>
          <SUBSCRIPTION_ID>915185</SUBSCRIPTION_ID>
          <IS_DEFAULT>0</IS_DEFAULT>
          <IS_GLOBAL>0</IS_GLOBAL>
          <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
          <UPDATE_DATE>2019-03-19T09:13:26Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
          <PORTS>
            <TCP_PORTS>
              <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
              <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
            </TCP_PORTS>
            <UDP_PORTS>
              <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
            </UDP_PORTS>
            <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
          </PORTS>
          <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
          <PERFORMANCE>
            <PARALLEL_SCALING>0</PARALLEL_SCALING>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <HOSTS_TO_SCAN>
              <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
            </HOSTS_TO_SCAN>
            <PROCESSES_TO_RUN>
              <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
              <HTTP_PROCESSES>10</HTTP_PROCESSES>
            </PROCESSES_TO_RUN>
            <PACKET_DELAY>Medium</PACKET_DELAY>
```

```
        <PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_
DISCOVERY>
          </PERFORMANCE>
          <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
          <VULNERABILITY_DETECTION>
            <COMPLETE><![CDATA[complete]]></COMPLETE>
            <DETECTION_INCLUDE>
              <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
              <OVAL_CHECKS>0</OVAL_CHECKS>
            </DETECTION_INCLUDE>
          </VULNERABILITY_DETECTION>
          <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,MongoDB,Tomcat Server,Oracle Weblogic
Server,Palo Alto Networks Firewall,Jboss Server]]></AUTHENTICATION>
          <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
          <TEST_AUTHENTICATION>1</TEST_AUTHENTICATION>

   <PERFORM_PARTIAL_SSL_TLS_AUDITING>1</PERFORM_PARTIAL_SSL_TLS_AUDITING>
        </SCAN>
        <MAP>
          <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
          <TCP_PORTS>
            <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
          </TCP_PORTS>
          <MAP_OPTIONS>
            <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
          </MAP_OPTIONS>
          <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
              <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
              <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Minimum</PACKET_DELAY>
          </MAP_PERFORMANCE>
          <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
          <HOST_DISCOVERY>
            <TCP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </TCP_PORTS>
            <UDP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </UDP_PORTS>
            <ICMP>1</ICMP>
          </HOST_DISCOVERY>
          <PACKET_OPTIONS>

 <IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
            <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
```

```
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
          </PACKET_OPTIONS>
        </ADDITIONAL>
      </OPTION_PROFILE>
    </OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-08-31T10:08:47Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
590924</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2445059</KEY>
                <VALUE>API_IMPORT_OP_1647433780</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Import Option Profile

API Request

```
curl --location
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/?action=import'
\
--header 'X-Requested-With: curl' \
--header 'Content-Type: application/xml' \
--header 'Authorization: Bearer <JWT Token> ' \
--data '
```

Request Post data

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>26210000</ID>
            <GROUP_NAME>
                <![CDATA[OP import API]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
```

```
            <USER_ID>
                <![CDATA[John Doe (john_doe)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>1309337</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-09-02T10:25:44Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>full</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>full</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <CUSTOM_LIST>
                    <CUSTOM>
                        <ID>1616684</ID>
                        <TITLE>
                            <![CDATA[VM-22616 - Search Lists - CRM]]>
                        </TITLE>
                    </CUSTOM>
                </CUSTOM_LIST>
```

```
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>1</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            <DISSOLVABLE_AGENT>
                <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
            </DISSOLVABLE_AGENT>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
            <TCP_PORTS>
                <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
            </TCP_PORTS>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                </MAP_PARALLEL>
                <PACKET_DELAY>Minimum</PACKET_DELAY>
            </MAP_PERFORMANCE>
            <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </UDP_PORTS>
                <ICMP>0</ICMP>
            </HOST_DISCOVERY>
            <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
```

```
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>'
```

XML Output

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-08-12T11:27:42Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
75299</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>70018</KEY>
                <VALUE>
                 OptionProfile-Import6
                </VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD (Request POST Data)

<platform API server>/api/3.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/3.0/simple_return.dtd

Sample - Import Option Profiles

Note: “Export_OP.xml” contains the request POST data.

API request:

```
curl --location
“https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/?action
=import”\
--header “X-Requested-With: postman” \
--header “Content-Type: application/xml” \
--header “Authorization: Bearer <JWT Token>” \
--data “
```

Request POST data:

```
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639142</ID>
            <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi_mobimport]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
```

```
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-08T13:16:26Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
```

```
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:04:17Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
194334</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2639624</KEY>
                <VALUE>
        Option_profile_vCenter_scan_disconnected_esxi_import_file
```

```
                </VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Import Option Profile

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/?action
=import'
\
--header 'X-Requested-With: postman' \
--header 'Content-Type: application/xml' \
--header 'Authorization: BBearer <JWT Token>' \
--data '
```

Request POST data:

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639142</ID>
            <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi_mobimport]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-08T13:16:26Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
```

```
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                </MAP_PARALLEL>
                <PACKET_DELAY>Minimum</PACKET_DELAY>
            </MAP_PERFORMANCE>
            <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
            <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
        </MAP>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
```

```
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T06:53:47Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
194334</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2639623</KEY>
                <VALUE>

Option_profile_vCenter_scan_disconnected_esxi_mobimport
</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

V4.0

/api/4.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD (Request POST Data)

<platform API server>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/4.0/simple_return.dtd

Sample - Import Option Profiles

Note: "Export_OP.xml" contains the request POST data.

API request:

```
curl --location
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action
=import"\
```

```
--header "X-Requested-With: postman" \
--header "Content-Type: application/xml" \
--header "Authorization: Bearer <JWT Token>" \
--data "
```

Request POST data:

```
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639142</ID>
            <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi_mobimport]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-08T13:16:26Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
```

```
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
            </MAP_OPTIONS>
            <MAP_PERFORMANCE>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <MAP_PARALLEL>
                    <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                    <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                </MAP_PARALLEL>
                <PACKET_DELAY>Minimum</PACKET_DELAY>
            </MAP_PERFORMANCE>
            <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
            <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
        </MAP>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </UDP_PORTS>
                <ICMP>1</ICMP>
            </HOST_DISCOVERY>
            <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
```

```
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:04:17Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
194334</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2639624</KEY>
                <VALUE>
        Option_profile_vCenter_scan_disconnected_esxi_import_file
                </VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Import Option Profile

API request:

```
curl --location
'https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action
=import'
\
--header 'X-Requested-With: postman' \
--header 'Content-Type: application/xml' \
--header 'Authorization: Bearer <JWT Token>' \
--data '
```

Request POST data:

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>2639142</ID>
            <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi_mobimport]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Manager (agms_jb)]]>
            </USER_ID>
```

```
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2024-07-08T13:16:26Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>0</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
        <MAP>
            <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
            <MAP_OPTIONS>
                <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
```

```
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
https://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T06:53:47Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
194334</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>2639623</KEY>
                <VALUE>

Option_profile_vCenter_scan_disconnected_esxi_mobimport
```

```
</VALUE>
            </ITEM>
         </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

V5.0

/api/5.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD (Request POST Data)

<platform API server>/api/5.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/5.0/simple_return.dtd

Sample - Import Option Profiles

Note: “Export_OP.xml” contains the request POST data.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "<username>:<password>" -H
"content-type: text/xml" -H "X-Requested-With:curl" -X "POST" --data-
binary @/home/<username>/John/Export_Op_agent_corr_enbaled.xml
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/?action=import"
```

Request POST data:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-09-26T10:28:48Z</DATETIME>
    <TEXT>Successfully imported Option profile for the subscription Id
4027198</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>7779470</KEY>
        <VALUE>agent correlation enabled OP</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V6.0

/api/6.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD (Request POST Data)

<platform API server>/api/6.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/6.0/simple_return.dtd

Sample - Import Option Profiles

Note: "Export_OP.xml" contains the request POST data.

API request:

```
curl --location --request POST
'<qualys_base_url>/api/6.0/fo/subscription/option_profile/?action=import'
\
--header 'Content-Type: application/xml' \
--header 'Accept: */*' \
--header 'x-requested-with: curl demo2' \
--header 'Authorization: Bearer <JWT Token \
--data '<?xml version="1.0" encoding="UTF-8" ?>
```

Request POST data:

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/6.0/fo/subscription/option_profile/option_profile_
info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>3494139</ID>
            <GROUP_NAME>
                <![CDATA[Import Option Profile 1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Aditya Gangadharan (vmsp_ag1)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>970969</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>1</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2026-01-19T06:54:38Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                    <UDP_PORTS_ADDITIONAL>
                        <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                        <ADDITIONAL_PORTS>8080</ADDITIONAL_PORTS>
                    </UDP_PORTS_ADDITIONAL>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
            <CLOSE_VULNERABILITIES>
                <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
                <HOST_NOT_FOUND_ALIVE>2</HOST_NOT_FOUND_ALIVE>
            </CLOSE_VULNERABILITIES>
```

```
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>20</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
            <PASSWORD_BRUTE_FORCING>
                <SYSTEM>
                    <HAS_SYSTEM>1</HAS_SYSTEM>
                    <SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
                </SYSTEM>
            </PASSWORD_BRUTE_FORCING>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                    <QRDI_CHECKS>1</QRDI_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <AUTHENTICATION>
                <![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,MongoDB,Tomcat Server,Oracle Weblogic
Server,Palo Alto Networks Firewall,Jboss Server,Sybase,Nutanix,NSX]]>
            </AUTHENTICATION>
            <AUTHENTICATION_LEAST_PRIVILEGE>
                <![CDATA[Unix]]>
            </AUTHENTICATION_LEAST_PRIVILEGE>
            <ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
            <SYSTEM_AUTH_RECORD>
                <INCLUDE_SYSTEM_AUTH>

<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
                </INCLUDE_SYSTEM_AUTH>
            </SYSTEM_AUTH_RECORD>
            <LITE_OS_SCAN>1</LITE_OS_SCAN>
            <HOST_ALIVE_TESTING>1</HOST_ALIVE_TESTING>

<MAX_SCAN_DURATION_PER_ASSET>2500</MAX_SCAN_DURATION_PER_ASSET>
        </SCAN>
```

```
            <MAP>
                <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
                <TCP_PORTS>
                    <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
                </UDP_PORTS>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>8</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>10</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>4096 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

Request POST data:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/6.0/simple_return.dtd">
<SIMPLE_RETURN>
```

```
    <RESPONSE>
        <DATETIME>2026-01-19T09:48:09Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
970969</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>3494173</KEY>
                <VALUE>

                            Import Option Profile 1

        </VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

V7.0

/api/7.0/fo/subscription/option_profile/?action=import

[POST]

Import all option profiles defined in input XML file.

Permissions - The API user must have the Manager role.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user's subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user's subscription before making an Import Option Profile call. At import time we try to match the Search List "title" to a search list title in the user's subscription. If a match is found the search list is used, otherwise "Complete" Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Input Parameter

Parameter	Description
action=import	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

DTD (Request POST Data)

<platform API server>/api/7.0/fo/subscription/option_profile/option_profile_info.dtd

DTD (XML Output)

<platform API server>/api/7.0/simple_return.dtd

Sample - Import Option Profiles

Note: “Export_OP.xml” contains the request POST data.

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/subscription/option_profile/?action=import'
\
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Type: text/xml' \
--header 'Authorization: Bearer
    <JWT Token>' \
--header 'Cookie: DWRSESSIONID=xxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
--data '
```

Request POST data:

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.p01.eng.sjc01.qualys.com/api/7.0/fo/subscription/optio
n_profile/option_profile_info.dtd">
        <OPTION_PROFILES>
            <OPTION_PROFILE>
                <BASIC_INFO>
                    <ID>76474</ID>
                    <GROUP_NAME>
                        <![CDATA[IMPORT-With-
ALLOW_ON_HOST_SCRIPT_EXECUTION-7.0 New]]>
                    </GROUP_NAME>
                    <GROUP_TYPE>user</GROUP_TYPE>
                    <USER_ID>
```

```
                        <![CDATA[Aditya Gangadharan (vmsp_ag1)]]>
                    </USER_ID>
                    <UNIT_ID>0</UNIT_ID>
                    <SUBSCRIPTION_ID>970969</SUBSCRIPTION_ID>
                    <IS_DEFAULT>0</IS_DEFAULT>
                    <IS_GLOBAL>1</IS_GLOBAL>
                    <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                    <UPDATE_DATE>2024-11-28T10:26:59Z</UPDATE_DATE>
                </BASIC_INFO>
                <SCAN>
                    <PORTS>
                        <TCP_PORTS>
                            <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                            <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                        </TCP_PORTS>
                        <UDP_PORTS>
                            <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                        </UDP_PORTS>
                        <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                    </PORTS>
                    <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                    <PERFORMANCE>
                        <PARALLEL_SCALING>1</PARALLEL_SCALING>
                        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                        <HOSTS_TO_SCAN>
                            <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                            <SCANNER_APPLIANCES>200</SCANNER_APPLIANCES>
                        </HOSTS_TO_SCAN>
                        <PROCESSES_TO_RUN>
                            <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                            <HTTP_PROCESSES>20</HTTP_PROCESSES>
                        </PROCESSES_TO_RUN>
                        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                        <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                        <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                        <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
                    </PERFORMANCE>

<ALLOW_ON_HOST_SCRIPT_EXECUTION>1</ALLOW_ON_HOST_SCRIPT_EXECUTION>
                    <VULNERABILITY_DETECTION>
                        <COMPLETE>
                            <![CDATA[complete]]>
                        </COMPLETE>
                        <DETECTION_INCLUDE>
```

```
<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                            <OVAL_CHECKS>0</OVAL_CHECKS>
                        </DETECTION_INCLUDE>
                    </VULNERABILITY_DETECTION>
                    <AUTHENTICATION>
                        <![CDATA[Windows,Unix]]>
                    </AUTHENTICATION>
                    <AUTHENTICATION_LEAST_PRIVILEGE>
                        <![CDATA[Unix]]>
                    </AUTHENTICATION_LEAST_PRIVILEGE>
                    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                </SCAN>
                <MAP>
                   <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
                    <TCP_PORTS>

<TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>

<UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
                    </UDP_PORTS>
                    <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                        <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                    </MAP_OPTIONS>
                    <MAP_PERFORMANCE>
                        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                        <MAP_PARALLEL>
                            <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                            <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                            <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                        </MAP_PARALLEL>
                        <PACKET_DELAY>Minimum</PACKET_DELAY>
                    </MAP_PERFORMANCE>
                    <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
                </MAP>
                <ADDITIONAL>
                    <HOST_DISCOVERY>
                        <TCP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </TCP_PORTS>
                        <UDP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </UDP_PORTS>
                        <ICMP>0</ICMP>
                    </HOST_DISCOVERY>
                    <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                        <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
```

```
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                    </PACKET_OPTIONS>
                </ADDITIONAL>
            </OPTION_PROFILE>
        </OPTION_PROFILES>
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/7.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2026-06-24T08:52:44Z</DATETIME>
          <TEXT>Successfully imported Option profile for the subscription
Id 970969</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>4121328</KEY>
                    <VALUE>
IMPORT-With-ALLOW_ON_HOST_SCRIPT_EXECUTION-7.0 New </VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/7.0/fo/subscription/option_profile/?action=import	Active	Active
/api/6.0/fo/subscription/option_profile/?action=import	January 2027	July 2027
/api/5.0/fo/subscription/option_profile/?action=import	July 2026	January 2027
/api/4.0/fo/subscription/option_profile/?action=import	December 2025	December 2026
/api/3.0/fo/subscription/option_profile/?action=import	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=import	December 2025	December 2026

Option Profiles for VM

/api/2.0/fo/subscription/option_profile/vm/

Create, update, list and delete option profiles for VM scans.

Permissions - All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create VM Option Profile

For API version information, refer to the API Version History section.

V2.0| V3.0 | V4.0 | V5.0

V2.0

/api/2.0/fo/subscription/option_profile/vm/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required) Specify action to create VM option profile.
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
title={value}	(Required) The title of the option profile.
id=value	(Required) An option profile ID.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
default={**0**|1}	(Optional) Make this profile the default for all scans and maps. Specify 1 to make default. There can only be one default profile for the subscription.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
offline_scanner={**0**|1}	(Optional) Specify to 1 to download this profile to your offline scanners during the next sync.

Parameter	Description
scan_tcp_ports={none|full|standard|light}	(Required) We use ports to send packets to the host in order to determine whether the host is alive and also to do fingerprinting for the discovery of services. Specify "full" to scan all ports, "standard" to scan standard ports or "light" to scan fewer ports. See Appendix B - Ports used for scanning for a list of ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
scan_tcp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 12500 ports).
3_way_handshake={**0**|1}	(Optional) Specify 1 to let the scanning engine perform a 3-way handshake with target hosts. After a connection between the service and the target host is established, the connection will be closed. This option should be enabled only if you have a configuration that does not allow an SYN packet to be followed by an RST packet. Also, when this is enabled, TCP based OS detection is not performed on target hosts. Without TCP based OS detection, the service may not be able to identify the operating system installed on target hosts and perform OS-specific vulnerability checks
Scan	
scan_udp_ports={none|full|**standard**|light}	(Required) Specify "full" to scan all ports, "standard" to scan standard ports or "light" to scan fewer ports. See Appendix B - Ports used for scanning for a list of UDP ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
vulnerability_detection={**complete**|custom|runtime}	(Required) With a "complete" scan we'll scan for all vulnerabilities (QIDs) in the KnowledgeBase applicable to each host being scanned. Specify "custom" to limit the scan to specified QIDs only. Then add the QIDs you want to scan. **Note:** The runtime option profile is not supported using this API. If you perform a VM scan using this API with an option profile configured as Select at Runtime, the response returns an error.
scan_udp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 20500 ports).
authoritative_option={**0**|1}	(Optional) Specify 1 to enable Authoritative Scan Option. By enabling the authoritative scan option your light scan will work like a full or standard scan. We will update the vulnerability status for all vulnerabilities found, regardless of which ports they were detected on.
scan_dead_hosts={**0**|1}	(Optional) Specify 1 to enable scanning dead hosts. A dead host is a host that is unreachable - it didn't respond to any pings. Your scan may run longer if you choose to scan dead hosts.
close_vuln_on_dead_hosts={**0**|1}	(Optional) Specify 1 to quickly close vulnerabilities for hosts that are not found alive after a set number of scans. When enabled, we'll mark existing tickets associated with dead hosts as Closed/Fixed and update the vulnerability status to Fixed.

Parameter	Description
not_found_alive_times={value}	(Optional) Specify the number of times the host is not found alive after which the vulnerability should be closed. This setting is available only when close_vuln_on_dead_hosts=1.
purge_host_data={0|**1**}	(Optional) Specify 1 to purge host data. This option is especially useful if you have systems that are regularly decommissioned or replaced. By specifying this option you'are telling us you want to purge the host if we detect a change in the host's Operating System (OS) vendor at scan time, for example the OS changed from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.
external_scanners_use={value}	(Optional) Specify the maximum number of external scanners to use for scanning perimeter assets. (This option is available when your subscription is configured with multiple external scanners).
scan_parallel_scaling={0|**1**}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
scan_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.

Parameter	Description
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_multiple_slices_per_scanner={0|1}	(Optional) TWhen unspecified or set to 0, scan using multiple slices are not used. Specify 1 to scan multiple slices in a single scan.
load_balancer={**0**|1}	(Optional) Specify 1 to check each target host to determine if it's a load balancer. When a load balancer is detected, we determine the number of Web servers behind it and report QID 86189 "Presence of a Load-Balancing Device Detected" in your results.
password_brute_forcing_system={**minimal**|limited|standard|exhaustive}	(Optional) How vulnerable are your hosts to password-cracking techniques? we'll attempt to guess the password for each detected login ID on each target host scanned. Specify the level of brute forcing you prefer (“minimal” to “exhaustive”).
password_brute_forcing_custom={value1,value2}	(Optional) Specify titles of the login/password pairs you create for password brute forcing on the Qualys Cloud Platform UI.
custom_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to use in your scan.
custom_search_list_title={value1, value2}	(Optional) Specify titles of search lists you want to use in your scan.
basic_host_information_checks={0|**1**}	(Optional) Adds basic host information checks (hostname, OS, etc) to your Custom scans. These are already included in Complete scans. This setting is enabled by default.
oval_checks={**0**|1}	(Optional) Specify 1 to add a search list with QID 105186 (a diagnostic check for OVAL).
all_qrdi_checks={**0**|1}	(Optional) Specify 1 to scan target assets for all QRDI vulnerabilities in your subscription, i.e. all custom vulnerability checks defined with QRDI (Qualys Remote Detection Interface).
exclude_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to exclude from your scan.

Parameter	Description
authentication={value1, value2}	(Optional) Want to run authenticated scans? When you use authentication we'll perform a more in-depth assessment and get you the most accurate results with fewer false positives. Specify one or more technologies for the hosts you want to scan. Be sure you've configured authentication records (under Scans > Authentication) before running your scan. The following options are available: - Windows - Unix - Oracle - Oracle Listener - SNMP - VMware - DB2 - HTTP - MySQL - MongoDB - Tomcat Server - Palo Alto Networks Firewall - Sybase
authentication_least_privilege=Unix	(Optional) Specify authentication_least_privilege=Unix (this value is case sensitive) to use the least privileges required for Unix authentication. When specified, the scanner will not pass root delegation information specified in the Unix record to the scanner for vulnerability scans. When not specified (the default), root delegation will be used if specified in the Unix record. Note: Unix authentication must be enabled in the same option profile (authentication=Unix).
enable_additional_certificate_detection={**0**|1}	(Optional) Want to detect additional certificates beyond ports? You need to enable authentication and then run new vulnerability scans. Specify 1 to enable this option before scanning and see additional certificate records (under Assets > Certificates).
enable_dissolvable_agent={0|**1**}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_windows_share_enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_lite_os_scan={**0**|1}	(Optional) Only interested in OS detection? Specify 1 to include QID 45017 in the scan (under Vulnerability Detection).
custom_http_header={value}	(Optional) Specify a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Parameter	Description
custom_http_definition_key={value}	(Optional) Specify a custom HTTP header definition key
custom_http_definition_header={value}	(Optional) Specify a value for the custom HTTP header definition key defined in custom_http_definition_key.
host_alive_testing={**0**|1}	(Optional) Specify 1 to run a quick scan to determine which of your target hosts are alive without also performing other scan tests. The Appendix section of your Scan Results report will list the hosts that are alive and hosts that are not alive. You may see some Information Gathered QIDs in the results for hosts found alive.
not_overwrite_os={**0**|1}	(Optional) Specify 1 if you're running a light or custom scan and you don't want to overwrite the OS detected by a previous scan.
test_authentication={**0**|1}	(Optional) Specify 1 to test authentication to target hosts.
enable_max_scan_duration_per_asset={0|1}	If flag value is 1 then scan duration is enabled for option profile, else it is disabled. This parameter should be used along with max_scan_duration_per_asset_minutes.
max_scan_duration_per_asset_minutes=maximum	Maximum duration in minutes for scan to be performed on each asset. The parameters enable_max_scan_duration_per_asset and max_scan_duration_per_asset are mutually exclusive, and can only be specified if enable_max_scan_duration_per_asset is 1.
System Authentication	
include_system_auth={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify include_system_auth=1 to include system created authentication records in scans along with user created records. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. This identifies which record to use if you have a system created record and a user created record for the same instance configuration. When include_system_auth=0, the user created record will be selected for scans by default.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_system_auth_on_duplicate=1 to use the system created authentication record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if “include_system_auth=1”.

Parameter	Description
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_user_auth_on_duplicate=1 to use the user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if "include_system_auth=1".
Map	
basic_information_gathering=[`all`|**register**|netblockonly|none]	(Required) Perform basic information gathering on: All: All Hosts (hosts detected by the map), Register: Registered Hosts (hosts in your account), Netblockonly: Netblock Hosts (hosts added by a user to the netblock for the target domain) or None.
map_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445.
map_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
map_udp_ports_standard_scan={**0**|1}	(Optional) Specify 1 to enable standard scan of UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500.
map_udp_ports_additional={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
perform_live_host_sweep={0|**1**}	(Optional) Default setting is 1. Specify 0 to only discover devices using DNS discovery methods (DNS, Reverse DNS and DNS Zone Transfer.) Active probes will not be sent. As a result, we may not be able to detect all hosts in the netblock, and undetected hosts will not be analyzed.
disable_dns_traffic={**0**|1}	(Optional) Specify 1 if you want to disable DNS traffic for maps. This is valid only when the target domain name includes one or more netblocks, e.g. none:[10.10.10.2-10.10.10.100]. We'll perform network discovery only for the IP addresses in the netblocks. No forward or reverse DNS lookups, DNS zone transfers or DNS guessing/bruteforcing will be made, and DNS information will not be included in map results.
map_overall_performance={high|**`normal`**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for map_external_scanners, map_scanner_appliances, map_netblock_size, and map_packet_delay change as per the specified profile. Normal - Well balanced between intensity and speed. High - Optimized for speed. May be faster to complete but may overload firewalls and other networking devices. Low - Optimized for low bandwidth network connections. May take longer to complete.

Parameter	Description
map_external_scanners={value}	(Optional) Specify the number of external scanners for netblocks to map at the same time per scanner. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
map_scanner_appliances={value}	(Optional) Specify the number of scanner appliances for netblocks to map at the same time per scanner. Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
map_netblock_size={1024 IPs|4096 IPs|8192 IPs|**16384 IPs**|32768 IPs|65536 IPs}	(Optional) Specify the max number of IPs per netblock being mapped. The netblock specified for the domain is broken into smaller netblocks for processing. Each of these smaller netblocks equals a single map process. Use this setting to define how many IPs should be included in each process.
map_packet_delay={**minimum**|short|medium|long|maximum}	(Optional) This is the delay between groups of packets sent to the netblocks being mapped. With a short delay, packets are sent more frequently, resulting in more bandwidth utilization and a shorter mapping time. With a long delay, packets are sent less frequently, resulting in less bandwidth utilization and a longer mapping time.
map_authentication={VMware}	(Optional) Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type={**standard**|custom}	(Optional) Specify “standard” to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is “standard”. Specify “custom” to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={**0**|1}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.

Parameter	Description
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify "custom" to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_firewall_generated_tcp_rst_packets={0|**1**}	(Optional) Specify 1 to identify firewall-generated TCP RESET packets and ignore them.
ignore_all_tcp_rst_packets={0|**1**}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_tcp_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_tcp_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

DTD

<platform API server>/api/2.0/simple_return.dtd

Sample - Create VM Option Profile

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
POST"action=create&title=99&global=1&scan_tcp_ports=full&scan_udp_
ports=standard&&scan_overall_performance=normal&vulnerability_dete
ction=complete&basic_information_gathering=all"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T06:40:03Z</DATETIME>
    <TEXT>Option profile successfully added.</TEXT>
```

```
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>32112</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile with SSL/TLS auditing enabled.

API Request:

```
curl --location --request POST
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/?%20a
ction=create&title=VM_API_Option_profile_696969&scan_tcp_ports=non
e&scan_udp_ports=none&vulnerability_detection=complete&basic_infor
mation_gathering=none &enable_partial_ssl_tls_auditing=1"
\--header "Content-Type: application/x-www-form-urlencoded"
\--header "X-Requested-With: curl demo2"
\--header "Accept: */*"
\--header "Content-Length: 0"
\--header "Authorization: Bearer <JWT Token>"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-08-31T10:05:16Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2445054</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
POST"?action=create&purge_host_data=1&scan_parallel_scaling=1&scan_scanne
r
_appliances=50&scan_total_process=20&scan
```

```
_http_process=20&authentication_
least_privilege=Unix&enable_dissolvable_agent=1&icmp=0&ignore_
firewall_generated_tcp_rst_packets=1&ignore_firewall_generated_
tcp_syn_ack_packets=1&title=VM_API_Option_profile&scan_tcp_
ports=none&scan_udp_ports=none&vulnerability_detection=
complete&basic_information_gathering=none&scan_overall_
performance=custom&authentication=Unix"
'<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
       <DATETIME>2024-08-23T07:45:54Z</DATETIME>
       <TEXT>Option profile successfully added.</TEXT>
           <ITEM_LIST>
              <ITEM>
                 <KEY>ID</KEY>
                <VALUE>2665297</VALUE>
              </ITEM>
           </ITEM_LIST>
    </RESPONSE>
 </SIMPLE_RETURN>
```

Sample- Create VM Option Profile with VMware NSX enabled

API Request:

```
curl --location --request POST '
/api/2.0/fo/subscription/option_profile/vm/?action=create&title=nsxtest1&
scan_tcp_ports=none&scan_udp_ports=full&vulnerability_detection=complete&
basic_information_gathering=none&authoritative_option=1&authentication=NS
X%27 \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/2.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-15T06:41:38Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8153637</VALUE>
```

```
            </ITEM>
          </ITEM_LIST>
        </RESPONSE>
      </SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/subscription/option_profile/vm/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) A title for easy identification.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
default={**0**|1}	(Optional) Make this profile the default for all scans and maps. Specify 1 to make default. There can only be one default profile for the subscription.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
offline_scanner={**0**|1}	(Optional) Specify to 1 to download this profile to your offline scanners during the next sync.
scan_tcp_ports={none|full|**standard**|light}	(Required) We use ports to send packets to the host in order to determine whether the host is alive and also to do fingerprinting for the discovery of services. Specify “full” to scan all ports, “standard” to scan standard ports or “light” to scan fewer ports. See Appendix B - Ports used for scanning for a list of ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
scan_tcp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 20,500 ports).

Parameter	Description
3_way_handshake={**0**|1}	(Optional) Specify 1 to let the scanning engine perform a 3-way handshake with target hosts. After a connection between the service and the target host is established, the connection will be closed. This option should be enabled only if you have a configuration that does not allow an SYN packet to be followed by an RST packet. Also, when this is enabled, TCP based OS detection is not performed on target hosts. Without TCP based OS detection, the service may not be able to identify the operating system installed on target hosts and perform OS-specific vulnerability checks.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.
Scan	
scan_udp_ports={none|full|**standard**|light}	(Required) Specify “full” to scan all ports, “standard” to scan standard ports or “light” to scan fewer ports. See Appendix B - Ports used for scanning for a list of UDP ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
vulnerability_detection={**complete**|custom|runtime}	(Required) With a "complete" scan we'll scan for all vulnerabilities (QIDs) in the KnowledgeBase applicable to each host being scanned. Specify "custom" to limit the scan to specified QIDs only. Then add the QIDs you want to scan. **Note:** The runtime option profile is not supported using this API. If you perform a VM scan using this API with an option profile configured as Select at Runtime, the response returns an error.
scan_udp_ports_additional ={port1,port2}	(Optional) Specify additional ports to scan (up to 20500 ports).
authoritative_option={**0**|1}	(Optional) Specify 1 to enable Authoritative Scan Option. By enabling the authoritative scan option your light scan will work like a full or standard scan. We will update the vulnerability status for all vulnerabilities found, regardless of which ports they were detected on.
scan_dead_hosts={**0**|1}	(Optional) Specify 1 to enable scanning dead hosts. A dead host is a host that is unreachable - it didn't respond to any pings. Your scan may run longer if you choose to scan dead hosts.
close_vuln_on_dead_hosts={**0**|1}	(Optional) Specify 1 to quickly close vulnerabilities for hosts that are not found alive after a set number of scans. When enabled, we'll mark existing tickets associated with dead hosts as Closed/Fixed and update the vulnerability status to Fixed.
not_found_alive_times={value}	(Optional) Specify the number of times the host is not found alive after which the vulnerability should be closed. This setting is available only when close_vuln_on_dead_hosts=1.

Parameter	Description
purge_host_data={**0**|1}	(Optional) Specify 1 to purge host data. This option is especially useful if you have systems that are regularly decommissioned or replaced. By specifying this option you're telling us you want to purge the host if we detect a change in the host's Operating System (OS) vendor at scan time, for example the OS changed from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.
external_scanners_use={value}	(Optional) Specify the maximum number of external scanners to use for scanning perimeter assets. (This option is available when your subscription is configured with multiple external scanners).
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
scan_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.

Parameter	Description
scan_packet_delay={minimum|short|medium|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={normal|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_multiple_slices_per_scanner={0|1}	(Optional) When unspecified or set to 0, scan using multiple slices are not used. Specify 1 to scan multiple slices in a single scan.
load_balancer={0|1}	(Optional) Specify 1 to check each target host to determine if it's a load balancer. When a load balancer is detected, we determine the number of Web servers behind it and report QID 86189 "Presence of a Load-Balancing Device Detected" in your results.
password_brute_forcing_system={minimal|limited|standard|exhaustive}	(Optional) How vulnerable are your hosts to password-cracking techniques? we'll attempt to guess the password for each detected login ID on each target host scanned. Specify the level of brute forcing you prefer (“minimal” to “exhaustive”).
password_brute_forcing_custom={value1,value2}	(Optional) Specify titles of the login/password pairs you create for password brute forcing on the Qualys Cloud Platform UI.
custom_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to use in your scan.
custom_search_list_title={value1, value2}	(Optional) Specify titles of search lists you want to use in your scan.
basic_host_information_checks={0|**1**}	(Optional) Adds basic host information checks (hostname, OS, etc) to your Custom scans. These are already included in Complete scans. This setting is enabled by default.
oval_checks={**0**|1}	(Optional) Specify 1 to add a search list with QID 105186 (a diagnostic check for OVAL).
all_qrdi_checks={**0**|1}	(Optional) Specify 1 to scan target assets for all QRDI vulnerabilities in your subscription, i.e. all custom vulnerability checks defined with QRDI (Qualys Remote Detection Interface).
exclude_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to exclude from your scan.

Parameter	Description
authentication={value1, value2}	(Optional) Want to run authenticated scans? When you use authentication we'll perform a more in-depth assessment and get you the most accurate results with fewer false positives. Specify one or more technologies for the hosts you want to scan. Be sure you've configured authentication records (under Scans > Authentication) before running your scan. The following options are available: - Windows - Unix - Oracle - Oracle Listener - SNMP - VMware - DB2 - HTTP - MySQL - MongoDB - Tomcat Server - Palo Alto Networks Firewall - Sybase
authentication_least_privilege=Unix	(Optional) Specify authentication_least_privilege=Unix (this value is case sensitive) to use the least privileges required for Unix authentication. When specified, the scanner will not pass root delegation information specified in the Unix record to the scanner for vulnerability scans. When not specified (the default), root delegation will be used if specified in the Unix record. Note: Unix authentication must be enabled in the same option profile (authentication=Unix).
enable_additional_certificate_detection={**0**|1}	(Optional) Want to detect additional certificates beyond ports? You need to enable authentication and then run new vulnerability scans. Specify 1 to enable this option before scanning and see additional certificate records (under Assets > Certificates).
enable_dissolvable_agent={**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_windows_share_enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_lite_os_scan={**0**|1}	(Optional) Only interested in OS detection? Specify 1 to include QID 45017 in the scan (under Vulnerability Detection).
custom_http_header={value}	(Optional) Specify a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Parameter	Description
custom_http_definition_key={value}	(Optional) Specify a custom HTTP header definition key
custom_http_definition_header={value}	(Optional) Specify a value for the custom HTTP header definition key defined in custom_http_definition_key.
host_alive_testing={**0**|1}	(Optional) Specify 1 to run a quick scan to determine which of your target hosts are alive without also performing other scan tests. The Appendix section of your Scan Results report will list the hosts that are alive and hosts that are not alive. You may see some Information Gathered QIDs in the results for hosts found alive.
not_overwrite_os={**0**|1}	(Optional) Specify 1 if you're running a light or custom scan and you don't want to overwrite the OS detected by a previous scan.
test_authentication={**0**|1}	(Optional) Specify 1 to test authentication to target hosts.
enable_max_scan_duration_per_asset={0|1}	If flag value is 1 then scan duration is enabled for option profile, else it is disabled. This parameter should be used along with max_scan_duration_per_asset_minutes.
max_scan_duration_per_asset_minutes=maximum	Maximum duration in minutes for scan to be performed on each asset. The parameters enable_max_scan_duration_per_asset and max_scan_duration_per_asset are mutually exclusive, and can only be specified if enable_max_scan_duration_per_asset is 1.
System Authentication	
include_system_auth={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify include_system_auth=1 to include system created authentication records in scans along with user created records. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. This identifies which record to use if you have a system created record and a user created record for the same instance configuration. When include_system_auth=0, the user created record will be selected for scans by default.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_system_auth_on_duplicate=1 to use the system created authentication record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if “include_system_auth=1”.

Parameter	Description
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_user_auth_on_duplicate=1 to use the user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if "include_system_auth=1".
Map	
basic_information_gathering=[**all**|register|netblockonly|none]	(Required) Perform basic information gathering on: All: All Hosts (hosts detected by the map), Register: Registered Hosts (hosts in your account), Netblockonly: Netblock Hosts (hosts added by a user to the netblock for the target domain) or None.
map_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445.
map_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
map_udp_ports_standard_scan={**0**|1}	(Optional) Specify 1 to enable standard scan of UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500.
map_udp_ports_additional={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
perform_live_host_sweep={0|**1**}	(Optional) Default setting is 1. Specify 0 to only discover devices using DNS discovery methods (DNS, Reverse DNS and DNS Zone Transfer.) Active probes will not be sent. As a result, we may not be able to detect all hosts in the netblock, and undetected hosts will not be analyzed.
disable_dns_traffic={**0**|1}	(Optional) Specify 1 if you want to disable DNS traffic for maps. This is valid only when the target domain name includes one or more netblocks, e.g. none:[10.10.10.2-10.10.10.100]. We'll perform network discovery only for the IP addresses in the netblocks. No forward or reverse DNS lookups, DNS zone transfers or DNS guessing/bruteforcing will be made, and DNS information will not be included in map results.
map_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for map_external_scanners, map_scanner_appliances, map_netblock_size, and map_packet_delay change as per the specified profile. Normal - Well balanced between intensity and speed. High - Optimized for speed. May be faster to complete but may overload firewalls and other networking devices. Low - Optimized for low bandwidth network connections. May take longer to complete.

Parameter	Description
map_external_scanners={value}	(Optional) Specify the number of external scanners for netblocks to map at the same time per scanner. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
map_scanner_appliances={value}	(Optional) Specify the number of scanner appliances for netblocks to map at the same time per scanner. Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
map_netblock_size={1024 IPs|4096 IPs|8192 IPs|**16384 IPs**|32768 IPs|65536 IPs}	(Optional) Specify the max number of IPs per netblock being mapped. The netblock specified for the domain is broken into smaller netblocks for processing. Each of these smaller netblocks equals a single map process. Use this setting to define how many IPs should be included in each process.
map_packet_delay={**minimum**|short|medium|long|maximum}	(Optional) This is the delay between groups of packets sent to the netblocks being mapped. With a short delay, packets are sent more frequently, resulting in more bandwidth utilization and a shorter mapping time. With a long delay, packets are sent less frequently, resulting in less bandwidth utilization and a longer mapping time.
map_authentication={VMware}	(Optional) Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type={**standard**|custom}	(Optional) Specify “standard” to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is “standard”. Specify “custom” to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.

Parameter	Description
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify "custom" to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_firewall_generated_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to identify firewall-generated TCP RESET packets and ignore them.
ignore_all_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_tcp_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_tcp_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

DTD

<platform API server>/api/3.0/simple_return.dtd

Sample- Create VM Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X
POST"action=create&title=Option_profile_vCenter_scan_disconnected_
esxi&scan_tcp_ports=none&scan_udp_ports=none&vulnerability_detecti
on=complete&basic_information_gathering=none&map_authentication=vC
enter&scan_disconnected_esxi=1"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://
<qualys_base_url>/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
```

```
        <RESPONSE>
            <DATETIME>2024-07-01T09:55:47Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2633919</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample- Create VM Option Profile with SSL/TLS auditing enabled

API Request:

```
curl --location --request POST
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
vm/?action=create&title=VM_API_Option_profile_696969_mob&scan_tcp_
ports=none&scan_udp_ports=none&vulnerability_detection=complete&ba
sic_information_gathering=none%20&enable_partial_ssl_tls_auditing=
1" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Basic YWdtc19uYjpRYXRlbXAxMjMj"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:16:57Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile with VMware NSX enabled

API Request:

```
curl --location --request POST '
/api/3.0/fo/subscription/option_profile/vm/?action=create&title=nsxtest1&
scan_tcp_ports=none&scan_udp_ports=full&vulnerability_detection=complete&
basic_information_gathering=none&authoritative_option=1&authentication=NS
X%27 \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-15T06:41:38Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8153637</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V4.0

/api/4.0/fo/subscription/option_profile/vm/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) A title for easy identification.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
default={**0**|1}	(Optional) Make this profile the default for all scans and maps. Specify 1 to make default. There can only be one default profile for the subscription.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.

Parameter	Description
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
offline_scanner={**0**|1}	(Optional) Specify to 1 to download this profile to your offline scanners during the next sync.
scan_tcp_ports={none|full|**standard**|light}	(Required) We use ports to send packets to the host in order to determine whether the host is alive and also to do fingerprinting for the discovery of services. Specify "full" to scan all ports, "standard" to scan standard ports or "light" to scan fewer ports. See Appendix B - Ports used for scanning for a list of ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
scan_tcp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 20,500 ports).
3_way_handshake={**0**|1}	(Optional) Specify 1 to let the scanning engine perform a 3-way handshake with target hosts. After a connection between the service and the target host is established, the connection will be closed. This option should be enabled only if you have a configuration that does not allow an SYN packet to be followed by an RST packet. Also, when this is enabled, TCP based OS detection is not performed on target hosts. Without TCP based OS detection, the service may not be able to identify the operating system installed on target hosts and perform OS-specific vulnerability checks.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.
Scan	
scan_udp_ports={none|full|**standard**|light}	(Required) Specify "full" to scan all ports, "standard" to scan standard ports or "light" to scan fewer ports. See Appendix B - Ports used for scanning for a list of UDP ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
vulnerability_detection={**complete**|custom|runtime}	(Required) With a "complete" scan we'll scan for all vulnerabilities (QIDs) in the KnowledgeBase applicable to each host being scanned. Specify "custom" to limit the scan to specified QIDs only. Then add the QIDs you want to scan. **Note:** The runtime option profile is not supported using this API. If you perform a VM scan using this API with an option profile configured as Select at Runtime, the response returns an error.
scan_udp_ports_additional ={port1,port2}	(Optional) Specify additional ports to scan (up to 20500 ports).

Parameter	Description
authoritative_option={**0**|1}	(Optional) Specify 1 to enable Authoritative Scan Option. By enabling the authoritative scan option your light scan will work like a full or standard scan. We will update the vulnerability status for all vulnerabilities found, regardless of which ports they were detected on.
scan_dead_hosts={**0**|1}	(Optional) Specify 1 to enable scanning dead hosts. A dead host is a host that is unreachable - it didn't respond to any pings. Your scan may run longer if you choose to scan dead hosts.
close_vuln_on_dead_hosts={**0**|1}	(Optional) Specify 1 to quickly close vulnerabilities for hosts that are not found alive after a set number of scans. When enabled, we'll mark existing tickets associated with dead hosts as Closed/Fixed and update the vulnerability status to Fixed.
not_found_alive_times={value}	(Optional) Specify the number of times the host is not found alive after which the vulnerability should be closed. This setting is available only when close_vuln_on_dead_hosts=1.
purge_host_data={**0**|1}	(Optional) Specify 1 to purge host data. This option is especially useful if you have systems that are regularly decommissioned or replaced. By specifying this option you're telling us you want to purge the host if we detect a change in the host's Operating System (OS) vendor at scan time, for example the OS changed from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.
external_scanners_use={value}	(Optional) Specify the maximum number of external scanners to use for scanning perimeter assets. (This option is available when your subscription is configured with multiple external scanners).
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
scan_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.

Parameter	Description
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|medium|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={normal|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_multiple_slices_per_scanner={0|1}	(Optional) When unspecified or set to 0, scan using multiple slices are not used. Specify 1 to scan multiple slices in a single scan.
load_balancer={0|1}	(Optional) Specify 1 to check each target host to determine if it's a load balancer. When a load balancer is detected, we determine the number of Web servers behind it and report QID 86189 "Presence of a Load-Balancing Device Detected" in your results.
password_brute_forcing_system={minimal|limited|standard|exhaustive}	(Optional) How vulnerable are your hosts to password-cracking techniques? we'll attempt to guess the password for each detected login ID on each target host scanned. Specify the level of brute forcing you prefer (“minimal” to “exhaustive”).
password_brute_forcing_custom={value1,value2}	(Optional) Specify titles of the login/password pairs you create for password brute forcing on the Qualys Cloud Platform UI.
custom_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to use in your scan.
custom_search_list_title={value1, value2}	(Optional) Specify titles of search lists you want to use in your scan.

Parameter	Description
basic_host_information_checks={0|**1**}	(Optional) Adds basic host information checks (hostname, OS, etc) to your Custom scans. These are already included in Complete scans. This setting is enabled by default.
oval_checks={**0**|1}	(Optional) Specify 1 to add a search list with QID 105186 (a diagnostic check for OVAL).
all_qrdi_checks={**0**|1}	(Optional) Specify 1 to scan target assets for all QRDI vulnerabilities in your subscription, i.e. all custom vulnerability checks defined with QRDI (Qualys Remote Detection Interface).
exclude_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to exclude from your scan.
authentication={value1, value2}	(Optional) Want to run authenticated scans? When you use authentication we'll perform a more in-depth assessment and get you the most accurate results with fewer false positives. Specify one or more technologies for the hosts you want to scan. Be sure you've configured authentication records (under Scans > Authentication) before running your scan. The following options are available: - Windows - Unix - Oracle - Oracle Listener - SNMP - VMware - DB2 - HTTP - MySQL - MongoDB - Tomcat Server - Palo Alto Networks Firewall - Sybase
authentication_least_privilege=Unix	(Optional) Specify authentication_least_privilege=Unix (this value is case sensitive) to use the least privileges required for Unix authentication. When specified, the scanner will not pass root delegation information specified in the Unix record to the scanner for vulnerability scans. When not specified (the default), root delegation will be used if specified in the Unix record. Note: Unix authentication must be enabled in the same option profile (authentication=Unix).
enable_additional_certificate_detection={**0**|1}	(Optional) Want to detect additional certificates beyond ports? You need to enable authentication and then run new vulnerability scans. Specify 1 to enable this option before scanning and see additional certificate records (under Assets > Certificates).
enable_dissolvable_agent={**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.

Parameter	Description
enable_windows_share_enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_lite_os_scan={**0**|1}	(Optional) Only interested in OS detection? Specify 1 to include QID 45017 in the scan (under Vulnerability Detection).
custom_http_header={value}	(Optional) Specify a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.
custom_http_definition_key={value}	(Optional) Specify a custom HTTP header definition key
custom_http_definition_header={value}	(Optional) Specify a value for the custom HTTP header definition key defined in custom_http_definition_key.
host_alive_testing={**0**|1}	(Optional) Specify 1 to run a quick scan to determine which of your target hosts are alive without also performing other scan tests. The Appendix section of your Scan Results report will list the hosts that are alive and hosts that are not alive. You may see some Information Gathered QIDs in the results for hosts found alive.
not_overwrite_os={**0**|1}	(Optional) Specify 1 if you're running a light or custom scan and you don't want to overwrite the OS detected by a previous scan.
test_authentication={**0**|1}	(Optional) Specify 1 to test authentication to target hosts.
enable_max_scan_duration_per_asset={0|1}	If flag value is 1 then scan duration is enabled for option profile, else it is disabled. This parameter should be used along with max_scan_duration_per_asset_minutes.
max_scan_duration_per_asset_minutes=maximum	Maximum duration in minutes for scan to be performed on each asset. The parameters enable_max_scan_duration_per_asset and max_scan_duration_per_asset are mutually exclusive, and can only be specified if enable_max_scan_duration_per_asset is 1.
System Authentication	
include_system_auth={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify include_system_auth=1 to include system created authentication records in scans along with user created records. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. This identifies which record to use if you have a system created record and a user created record for the same instance configuration. When include_system_auth=0, the user created record will be selected for scans by default.

Parameter	Description
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_system_auth_on_duplicate=1 to use the system created authentication record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if "include_system_auth=1".
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_user_auth_on_duplicate=1 to use the user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if "include_system_auth=1".
Map	
basic_information_gathering=[**all**|register|netblockonly|none]	(Required) Perform basic information gathering on: All: All Hosts (hosts detected by the map), Register: Registered Hosts (hosts in your account), Netblockonly: Netblock Hosts (hosts added by a user to the netblock for the target domain) or None.
map_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445.
map_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
map_udp_ports_standard_scan={**0**|1}	(Optional) Specify 1 to enable standard scan of UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500.
map_udp_ports_additional={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
perform_live_host_sweep={0|**1**}	(Optional) Default setting is 1. Specify 0 to only discover devices using DNS discovery methods (DNS, Reverse DNS and DNS Zone Transfer.) Active probes will not be sent. As a result, we may not be able to detect all hosts in the netblock, and undetected hosts will not be analyzed.
disable_dns_traffic={**0**|1}	(Optional) Specify 1 if you want to disable DNS traffic for maps. This is valid only when the target domain name includes one or more netblocks, e.g. none:[10.10.10.2-10.10.10.100]. We'll perform network discovery only for the IP addresses in the netblocks. No forward or reverse DNS lookups, DNS zone transfers or DNS guessing/bruteforcing will be made, and DNS information will not be included in map results.

Parameter	Description
map_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for map_external_scanners, map_scanner_appliances, map_netblock_size, and map_packet_delay change as per the specified profile. Normal - Well balanced between intensity and speed. High - Optimized for speed. May be faster to complete but may overload firewalls and other networking devices. Low - Optimized for low bandwidth network connections. May take longer to complete.
map_external_scanners={value}	(Optional) Specify the number of external scanners for netblocks to map at the same time per scanner. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
map_scanner_appliances={value}	(Optional) Specify the number of scanner appliances for netblocks to map at the same time per scanner. Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
map_netblock_size={1024 IPs|4096 IPs|8192 IPs|**16384 IPs**|32768 IPs|65536 IPs}	(Optional) Specify the max number of IPs per netblock being mapped. The netblock specified for the domain is broken into smaller netblocks for processing. Each of these smaller netblocks equals a single map process. Use this setting to define how many IPs should be included in each process.
map_packet_delay={**minimum**|short|medium|long|maximum}	(Optional) This is the delay between groups of packets sent to the netblocks being mapped. With a short delay, packets are sent more frequently, resulting in more bandwidth utilization and a shorter mapping time. With a long delay, packets are sent less frequently, resulting in less bandwidth utilization and a longer mapping time.
map_authentication={VMware}	(Optional) Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.

Parameter	Description
additional_udp_ports_type={**standard**|custom}	(Optional) Specify "standard" to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is "standard". Specify "custom" to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify "custom" to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_firewall_generated_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to identify firewall-generated TCP RESET packets and ignore them.
ignore_all_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_tcp_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_tcp_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

DTD

<platform API server>/api/3.0/simple_return.dtd

Sample- Create VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
POST"action=create&title=Option_profile_vCenter_scan_disconnected_esxi&sc
an_tcp_ports=none&scan_udp_ports=none&vulnerability_detection=complete&ba
sic_information_gathering=none&map_authentication=vCenter&scan_disconnect
ed_esxi=1"
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-01T09:55:47Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2633919</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample- Create VM Option Profile with SSL/TLS auditing enabled

API Request:

```
curl --location --request POST
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?action=crea
te&title=VM_API_Option_profile_696969_mob&scan_tcp_ports=none&scan_udp_po
rts=none&vulnerability_detection=complete&basic_information_gathering=non
e%20&enable_partial_ssl_tls_auditing=1" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Basic YWdtc19uYjpRYXRlbXAxMjMj"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:16:57Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile

API Request:

```
curl --location --request POST '
```

```
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?action=creat
e&title=Option%20profile%20V4%20API1&scan_tcp_ports=standard&scan_udp_por
ts=standard&vulnerability_detection=complete&basic_information_gathering=
all&map_tcp_ports_standard_scan=1&map_tcp_ports_additional=1' \
--header 'X-Requested-With: xxx' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-18T05:44:15Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>7723450</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile with VMware NSX enabled

API Request:

```
curl --location --request POST '
/api/4.0/fo/subscription/option_profile/vm/?action=create&title=nsxtest1&
scan_tcp_ports=none&scan_udp_ports=full&vulnerability_detection=complete&
basic_information_gathering=none&authoritative_option=1&authentication=NS
X%27 \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer  '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-15T06:41:38Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8153637</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V5.0

/api/5.0/fo/subscription/option_profile/vm/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) A title for easy identification.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
default={**0**|1}	(Optional) Make this profile the default for all scans and maps. Specify 1 to make default. There can only be one default profile for the subscription.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
offline_scanner={**0**|1}	(Optional) Specify to 1 to download this profile to your offline scanners during the next sync.
scan_tcp_ports={none|full|**standard**|light}	(Required) We use ports to send packets to the host in order to determine whether the host is alive and also to do fingerprinting for the discovery of services. Specify “full” to scan all ports, “standard” to scan standard ports or “light” to scan fewer ports. See Appendix B - Ports used for scanning for a list of ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
scan_tcp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 20,500 ports).
3_way_handshake={**0**|1}	(Optional) Specify 1 to let the scanning engine perform a 3-way handshake with target hosts. After a connection between the service and the target host is established, the connection will be closed. This option should be enabled only if you have a configuration that does not allow an SYN packet to be followed by an RST packet. Also, when this is enabled, TCP based OS detection is not performed on target hosts. Without TCP based OS detection, the service may not be able to identify the operating system installed on target hosts and perform OS-specific vulnerability checks.

Parameter	Description
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.
Scan	
allow_on_host_script_execution={0|1}	(Optional) Specify 1 to allow the scanner to execute local scripts on the target host during the authentication scans.
scan_udp_ports={none|full|**standard**|light}	(Required) Specify “full” to scan all ports, “standard” to scan standard ports or “light” to scan fewer ports. See Appendix B - Ports used for scanning for a list of UDP ports used for standard or light scan. We will scan the standard list of ports unless you choose a different option in the profile.
vulnerability_detection={**complete**|custom|runtime}	(Required) With a "complete" scan we'll scan for all vulnerabilities (QIDs) in the KnowledgeBase applicable to each host being scanned. Specify "custom" to limit the scan to specified QIDs only. Then add the QIDs you want to scan. **Note:** The runtime option profile is not supported using this API. If you perform a VM scan using this API with an option profile configured as Select at Runtime, the response returns an error.
scan_udp_ports_additional={port1,port2}	(Optional) Specify additional ports to scan (up to 20500 ports).
authoritative_option={**0**|1}	(Optional) Specify 1 to enable Authoritative Scan Option. By enabling the authoritative scan option your light scan will work like a full or standard scan. We will update the vulnerability status for all vulnerabilities found, regardless of which ports they were detected on.
scan_dead_hosts={**0**|1}	(Optional) Specify 1 to enable scanning dead hosts. A dead host is a host that is unreachable - it didn't respond to any pings. Your scan may run longer if you choose to scan dead hosts.
close_vuln_on_dead_hosts={**0**|1}	(Optional) Specify 1 to quickly close vulnerabilities for hosts that are not found alive after a set number of scans. When enabled, we'll mark existing tickets associated with dead hosts as Closed/Fixed and update the vulnerability status to Fixed.
not_found_alive_times={value}	(Optional) Specify the number of times the host is not found alive after which the vulnerability should be closed. This setting is available only when close_vuln_on_dead_hosts=1.
purge_host_data={**0**|1}	(Optional) Specify 1 to purge host data. This option is especially useful if you have systems that are regularly decommissioned or replaced. By specifying this option you’re telling us you want to purge the host if we detect a change in the host's Operating System (OS) vendor at scan time, for example the OS changed from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.

Parameter	Description
external_scanners_use={value}	(Optional) Specify the maximum number of external scanners to use for scanning perimeter assets. (This option is available when your subscription is configured with multiple external scanners).
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
scan_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|`medium`|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.

Parameter	Description
scan_intensity={normal|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_multiple_slices_per_scanner={0|1}	(Optional) When unspecified or set to 0, scan using multiple slices are not used. Specify 1 to scan multiple slices in a single scan.
load_balancer={0|1}	(Optional) Specify 1 to check each target host to determine if it's a load balancer. When a load balancer is detected, we determine the number of Web servers behind it and report QID 86189 "Presence of a Load-Balancing Device Detected" in your results.
password_brute_forcing_system={minimal|limited|standard|exhaustive}	(Optional) How vulnerable are your hosts to password-cracking techniques? we'll attempt to guess the password for each detected login ID on each target host scanned. Specify the level of brute forcing you prefer ("minimal" to "exhaustive").
password_brute_forcing_custom={value1,value2}	(Optional) Specify titles of the login/password pairs you create for password brute forcing on the Qualys Cloud Platform UI.
custom_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to use in your scan.
custom_search_list_title={value1, value2}	(Optional) Specify titles of search lists you want to use in your scan.
basic_host_information_checks={0|**1**}	(Optional) Adds basic host information checks (hostname, OS, etc) to your Custom scans. These are already included in Complete scans. This setting is enabled by default.
oval_checks={**0**|1}	(Optional) Specify 1 to add a search list with QID 105186 (a diagnostic check for OVAL).
all_qrdi_checks={**0**|1}	(Optional) Specify 1 to scan target assets for all QRDI vulnerabilities in your subscription, i.e. all custom vulnerability checks defined with QRDI (Qualys Remote Detection Interface).
exclude_search_list_ids={value1, value2}	(Optional) Specify ids of search lists you want to exclude from your scan.

Parameter	Description
authentication={value1, value2}	(Optional) Want to run authenticated scans? When you use authentication we'll perform a more in-depth assessment and get you the most accurate results with fewer false positives. Specify one or more technologies for the hosts you want to scan. Be sure you've configured authentication records (under Scans > Authentication) before running your scan. The following options are available: - Windows - Unix - Oracle - Oracle Listener - SNMP - VMware - DB2 - HTTP - MySQL - MongoDB - Tomcat Server - Palo Alto Networks Firewall - Sybase
authentication_least_privilege=Unix	(Optional) Specify authentication_least_privilege=Unix (this value is case sensitive) to use the least privileges required for Unix authentication. When specified, the scanner will not pass root delegation information specified in the Unix record to the scanner for vulnerability scans. When not specified (the default), root delegation will be used if specified in the Unix record. Note: Unix authentication must be enabled in the same option profile (authentication=Unix).
enable_additional_certificate_detection={**0**|1}	(Optional) Want to detect additional certificates beyond ports? You need to enable authentication and then run new vulnerability scans. Specify 1 to enable this option before scanning and see additional certificate records (under Assets > Certificates).
enable_dissolvable_agent={**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_windows_share_enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_lite_os_scan={**0**|1}	(Optional) Only interested in OS detection? Specify 1 to include QID 45017 in the scan (under Vulnerability Detection).
custom_http_header={value}	(Optional) Specify a custom value in order to drop defenses (such as logging, IPs, etc) when authorized scans are being run.

Parameter	Description
custom_http_definition_key={value}	(Optional) Specify a custom HTTP header definition key
custom_http_definition_header={value}	(Optional) Specify a value for the custom HTTP header definition key defined in custom_http_definition_key.
host_alive_testing={**0**|1}	(Optional) Specify 1 to run a quick scan to determine which of your target hosts are alive without also performing other scan tests. The Appendix section of your Scan Results report will list the hosts that are alive and hosts that are not alive. You may see some Information Gathered QIDs in the results for hosts found alive.
not_overwrite_os={**0**|1}	(Optional) Specify 1 if you're running a light or custom scan and you don't want to overwrite the OS detected by a previous scan.
test_authentication={**0**|1}	(Optional) Specify 1 to test authentication to target hosts.
enable_max_scan_duration_per_asset={0|1}	If flag value is 1 then scan duration is enabled for option profile, else it is disabled. This parameter should be used along with max_scan_duration_per_asset_minutes.
max_scan_duration_per_asset_minutes=maximum	Maximum duration in minutes for scan to be performed on each asset. The parameters enable_max_scan_duration_per_asset and max_scan_duration_per_asset are mutually exclusive, and can only be specified if enable_max_scan_duration_per_asset is 1.
System Authentication	
include_system_auth={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify include_system_auth=1 to include system created authentication records in scans along with user created records. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. This identifies which record to use if you have a system created record and a user created record for the same instance configuration. When include_system_auth=0, the user created record will be selected for scans by default.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_system_auth_on_duplicate=1 to use the system created authentication record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if “include_system_auth=1”.

Parameter	Description
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record, applicable for subscriptions with both PC and VM/VMDR) Specify use_user_auth_on_duplicate=1 to use the user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive, and can only be specified if "include_system_auth=1".
Map	
basic_information_gathering=[**all**|register|netblockonly|none]	(Required) Perform basic information gathering on: All: All Hosts (hosts detected by the map), Register: Registered Hosts (hosts in your account), Netblockonly: Netblock Hosts (hosts added by a user to the netblock for the target domain) or None.
map_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445.
map_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
map_udp_ports_standard_scan={**0**|1}	(Optional) Specify 1 to enable standard scan of UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500.
map_udp_ports_additional={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
perform_live_host_sweep={0|**1**}	(Optional) Default setting is 1. Specify 0 to only discover devices using DNS discovery methods (DNS, Reverse DNS and DNS Zone Transfer.) Active probes will not be sent. As a result, we may not be able to detect all hosts in the netblock, and undetected hosts will not be analyzed.
disable_dns_traffic={**0**|1}	(Optional) Specify 1 if you want to disable DNS traffic for maps. This is valid only when the target domain name includes one or more netblocks, e.g. none:[10.10.10.2-10.10.10.100]. We'll perform network discovery only for the IP addresses in the netblocks. No forward or reverse DNS lookups, DNS zone transfers or DNS guessing/bruteforcing will be made, and DNS information will not be included in map results.
map_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for map_external_scanners, map_scanner_appliances, map_netblock_size, and map_packet_delay change as per the specified profile. Normal - Well balanced between intensity and speed. High - Optimized for speed. May be faster to complete but may overload firewalls and other networking devices. Low - Optimized for low bandwidth network connections. May take longer to complete.

Parameter	Description
map_external_scanners={value}	(Optional) Specify the number of external scanners for netblocks to map at the same time per scanner. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
map_scanner_appliances={value}	(Optional) Specify the number of scanner appliances for netblocks to map at the same time per scanner. Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
map_netblock_size={1024 IPs|4096 IPs|8192 IPs|**16384 IPs**|32768 IPs|65536 IPs}	(Optional) Specify the max number of IPs per netblock being mapped. The netblock specified for the domain is broken into smaller netblocks for processing. Each of these smaller netblocks equals a single map process. Use this setting to define how many IPs should be included in each process.
map_packet_delay={**minimum**|short|medium|long|maximum}	(Optional) This is the delay between groups of packets sent to the netblocks being mapped. With a short delay, packets are sent more frequently, resulting in more bandwidth utilization and a shorter mapping time. With a long delay, packets are sent less frequently, resulting in less bandwidth utilization and a longer mapping time.
map_authentication={VMware}	(Optional) Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type={**standard**|custom}	(Optional) Specify “standard” to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is “standard”. Specify “custom” to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.

Parameter	Description
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify "custom" to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_firewall_generated_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to identify firewall-generated TCP RESET packets and ignore them.
ignore_all_tcp_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_tcp_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_tcp_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

DTD

<platform API server>/api/5.0/simple_return.dtd

Sample- Create VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
POST"action=create&title=Option_profile_vCenter_scan_disconnected_esxi&sc
an_tcp_ports=none&scan_udp_ports=none&vulnerability_detection=complete&ba
sic_information_gathering=none&map_authentication=vCenter&scan_disconnect
ed_esxi=1"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-01T09:55:47Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
```

```
                    <ITEM>
                        <KEY>ID</KEY>
                        <VALUE>2633919</VALUE>
                    </ITEM>
                </ITEM_LIST>
            </RESPONSE>
        </SIMPLE_RETURN>
```

Sample- Create VM Option Profile with SSL/TLS auditing enabled

API Request:

```
curl --location --request POST
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?action=crea
te&title=VM_API_Option_profile_696969_mob&scan_tcp_ports=none&scan_udp_po
rts=none&vulnerability_detection=complete&basic_information_gathering=non
e%20&enable_partial_ssl_tls_auditing=1" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Basic YWdtc19uYjpRYXRlbXAxMjMj"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:16:57Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?action=creat
e&title=Option%20profile%20V4%20API1&scan_tcp_ports=standard&scan_udp_por
ts=standard&vulnerability_detection=complete&basic_information_gathering=
all&map_tcp_ports_standard_scan=1&map_tcp_ports_additional=1' \
--header 'X-Requested-With: xxx' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
```

```
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-18T05:44:15Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>7723450</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile with VMware NSX enabled

API Request:

```
curl --location --request POST '
/api/5.0/fo/subscription/option_profile/vm/?action=create&title=nsxtest1&
scan_tcp_ports=none&scan_udp_ports=full&vulnerability_detection=complete&
basic_information_gathering=none&authoritative_option=1&authentication=NS
X%27 \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer  '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/5.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-15T06:41:38Z</DATETIME>
            <TEXT>Option profile successfully added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8153637</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
</SIMPLE_RETURN>
```

Sample- Create VM Option Profile with VMware NSX enabled

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?action=creat
e&title=HOST_SCRIPT_EXECUTION_CREATE_SM007&global=1&scan_overall_performa
nce=custom&scan_tcp_ports=none&scan_udp_ports=none&vulnerability_detectio
n=complete&basic_information_gathering=none&allow_on_host_script_executio
n=1' \
--header 'X-Requested-With: Test' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-06-24T08:41:25Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4121321</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/?action=create	Active	Active
/api/4.0/fo/subscription/option_profile/?action=create	January 2027	July 2027
/api/3.0/fo/subscription/option_profile/?action=create	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=create	December 2025	December 2026

Update VM Option Profile

For API version information, refer to the API Version History section.

V2.0| V3.0 | V4.0 | V5.0

V2.0

/api/2.0/fo/subscription/option_profile/vm/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.

For a list of optional parameters, see the Input Parameters for V2.0 under Create VM Option Profile.

DTD

<platform API server>/api/2.0/simple_return.dtd

Sample - Update VM Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=33jj&id=25121"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T09:51:15Z</DATETIME>
    <TEXT>Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>25121</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM option profile with SSL/TLS auditing disabled

API Request:

```
ccurl --location --request POST
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/?enable_part
ial_ssl_tls_auditing=0&%20action=update&id=2437618&scan_tcp_ports=standar
d&scan_udp_ports=standard&vulnerability_detection=runtime" \

--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Bearer <JWT Token>"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-08-31T10:04:24Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2437618</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile with VMware NSX enabled

API request:

```
curl --location --request POST '
/api/2.0/fo/subscription/option_profile/vm/?scan_tcp_ports=none&scan_udp_
ports=full&vulnerability_detection=complete&basic_information_gathering=n
one&authoritative_option=1&authentication=NSX&action=update&id=8154392%27
\
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JEWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/2.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-17T05:40:35Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
```

```
                    <KEY>ID</KEY>
                    <VALUE>8154392</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/subscription/option_profile/vm/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

For a list of optional parameters, see the Input Parameters for V3.0 under Create VM Option Profile.

DTD

<platform API server>/api/3.0/simple_return.dtd

Sample - Update VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X
POST"action=update&id=2633932&scan_tcp_ports=full&scan_udp_ports=full&vul
nerability_detection=runtime&map_authentication=vCenter&scan_disconnected
_esxi=1"
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/vm/
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
```

```
            <DATETIME>2024-07-01T10:05:48Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2633932</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Update VM Option Profile With SSL/TSL Auditing Disabled

API request:

```
curl --location --request POST
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/vm/?enable_part
ial_ssl_tls_auditing=0&action=update&id=2639625&scan_tcp_ports=standard&s
can_udp_ports=standard&vulnerability_detection=runtime"\
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Bearer <JWT Token>"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:19:13Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile with VMware NSX enabled

API request:

```
curl --location --request POST '
/api/3.0/fo/subscription/option_profile/vm/?scan_tcp_ports=none&scan_udp_
ports=full&vulnerability_detection=complete&basic_information_gathering=n
one&authoritative_option=1&authentication=NSX&action=update&id=8154392%27
\
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JEWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-17T05:40:35Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8154392</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V4.0

/api/4.0/fo/subscription/option_profile/vm/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.

For a list of optional parameters, see the Input Parameters for V3.0 under Create VM Option Profile.

DTD

<platform API server>/api/4.0/simple_return.dtd

Sample - Update VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X
POST"action=update&id=2633932&scan_tcp_ports=full&scan_udp_ports=full&vul
nerability_detection=runtime&map_authentication=vCenter&scan_disconnected
```

```
_esxi=1"
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-01T10:05:48Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2633932</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Update VM Option Profile with SSL/TSL Auditing Disabled

API request:

```
curl --location --request POST
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?enable_part
ial_ssl_tls_auditing=0&action=update&id=2639625&scan_tcp_ports=standard&s
can_udp_ports=standard&vulnerability_detection=runtime"\
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Bearer <JWT Token>"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:19:13Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile

API request:

```
curl --location --request POST '
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?action=updat
e&title=Option%20profile%20V4%20API%20updated&id=7721450' \
--header 'X-Requested-With: test' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-18T05:50:54Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>7721450</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile with VMware NSX enabled

API request:

```
curl --location --request POST '
/api/4.0/fo/subscription/option_profile/vm/?scan_tcp_ports=none&scan_udp_
ports=full&vulnerability_detection=complete&basic_information_gathering=n
one&authoritative_option=1&authentication=NSX&action=update&id=8154392%27
\
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JEWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-17T05:40:35Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8154392</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V5.0

api/5.0/fo/subscription/option_profile/vm/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
enable_partial_ssl_tls_auditing = {**0**|1}	(Optional) Use to enable or disable the partial SSL/TLS auditing during scan execution. Specify 1 to enable partial SSL/TLS checks while executing the scan.
scan_disconnected_esxi={0|1}	(Optional) Launch the authenticated scan on ESXi hosts without creating VMware authorization records and VMware, vCenter mapping. 1 - If set to 1, the Disconnected ESXi checkbox is selected. 0 - If set to 0, the Disconnected ESXi checkbox is not selected.
allow_on_host_script_execution={0|1}	(Optional) Specify 1 to allow the scanner to execute local scripts on the target host during the authentication scans.

For a list of optional parameters, see the Input Parameters for V3.0 under Create VM Option Profile.

DTD

<platform API server>/api/5.0/simple_return.dtd

Sample - Update VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X
POST"action=update&id=2633932&scan_tcp_ports=full&scan_udp_ports=full&vul
nerability_detection=runtime&map_authentication=vCenter&scan_disconnected
_esxi=1"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-01T10:05:48Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
```

```
                        <VALUE>2633932</VALUE>
                    </ITEM>
                </ITEM_LIST>
            </RESPONSE>
        </SIMPLE_RETURN>
```

Sample - Update VM Option Profile with SSL/TSL Auditing Disabled

API request:

```
curl --location --request POST
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?enable_part
ial_ssl_tls_auditing=0&action=update&id=2639625&scan_tcp_ports=standard&s
can_udp_ports=standard&vulnerability_detection=runtime"\
--header "Content-Type: application/x-www-form-urlencoded" \
--header "X-Requested-With: curl demo2" \
--header "Accept: */*" \
--header "Content-Length: 0" \
--header "Authorization: Bearer <JWT Token>"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:19:13Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639625</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile

API request:

```
curl --location --request POST '
<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?action=updat
e&title=Option%20profile%20V4%20API%20updated&id=7721450' \
--header 'X-Requested-With: test' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-18T05:50:54Z</DATETIME>
```

```
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>7721450</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Update VM Option Profile with VMware NSX enabled

API request:

```
curl --location --request POST '
/api/5.0/fo/subscription/option_profile/vm/?scan_tcp_ports=none&scan_udp_
ports=full&vulnerability_detection=complete&basic_information_gathering=n
one&authoritative_option=1&authentication=NSX&action=update&id=8154392%27
\
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JEWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/5.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-17T05:40:35Z</DATETIME>
            <TEXT>Option profile successfully updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8154392</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update VM Option Profile with On-Host Script Execution enabled

API request:

```
ccurl --location --request POST
'<qualys_base_url>/api/5.0/fo/subscription/option_profile/vm/?action=upda
te&id=4121321&allow_on_host_script_execution=0' \
--header 'X-Requested-With: Test' \
--header 'Authorization: Bearer <JWt Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
```

```
    <RESPONSE>
        <DATETIME>2026-06-24T08:45:57Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4121321</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/?action=update	Active	Active
/api/4.0/fo/subscription/option_profile/?action=update	January 2027	July 2027
/api/3.0/fo/subscription/option_profile/?action=update	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=update	December 2025	December 2026

VM Option Profile List

For API version information, refer to the API Version History section.

V2.0| V3.0 | V4.0

V2.0

/api/2.0/fo/subscription/option_profile/vm/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for V2.0 under Create VM Option Profile.

DTD

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - List VM Option Profile

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X GET
"action=list"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
<OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51451401</ID>
      <GROUP_NAME><![CDATA[user op - 1]]></GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID><![CDATA[John smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>1</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>1</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2018-04-10T13:39:41Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
```

```
        <TCP_PORTS>
          <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
          <TCP_PORTS_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1024</ADDITIONAL_PORTS>
          </TCP_PORTS_ADDITIONAL>
          <THREE_WAY_HANDSHAKE>1</THREE_WAY_HANDSHAKE>
        </TCP_PORTS>
        <UDP_PORTS>
          <UDP_PORTS_TYPE>light</UDP_PORTS_TYPE>
          <UDP_PORTS_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>8080</ADDITIONAL_PORTS>
          </UDP_PORTS_ADDITIONAL>
        </UDP_PORTS>
        <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
      </PORTS>
      <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
      <CLOSE_VULNERABILITIES>
        <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
        <HOST_NOT_FOUND_ALIVE>10</HOST_NOT_FOUND_ALIVE>
      </CLOSE_VULNERABILITIES>
      <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
      <PASSWORD_BRUTE_FORCING>
        <SYSTEM>
          <HAS_SYSTEM>1</HAS_SYSTEM>
          <SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
        </SYSTEM>
        <CUSTOM_LIST>
```

```
          <CUSTOM>
            <ID>1001</ID>
            <TITLE><![CDATA[ftp - 1]]></TITLE>
            <TYPE>FTP</TYPE>

<LOGIN_PASSWORD><![CDATA[L:Guest,P:temp]]></LOGIN_PASSWORD>
          </CUSTOM>
          <CUSTOM>
            <ID>1002</ID>
            <TITLE><![CDATA[ssh - 1]]></TITLE>
            <TYPE>SSH</TYPE>

<LOGIN_PASSWORD><![CDATA[L:Guest,P:temp]]></LOGIN_PASSWORD>
          </CUSTOM>
          <CUSTOM>
            <ID>1003</ID>
            <TITLE><![CDATA[window - 1]]></TITLE>
            <TYPE>Windows</TYPE>

<LOGIN_PASSWORD><![CDATA[L:Guest,P:temp]]></LOGIN_PASSWORD>
          </CUSTOM>
        </CUSTOM_LIST>
      </PASSWORD_BRUTE_FORCING>
      <VULNERABILITY_DETECTION>
        <COMPLETE><![CDATA[complete]]></COMPLETE>
        <DETECTION_INCLUDE>
          <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
          <OVAL_CHECKS>1</OVAL_CHECKS>
        </DETECTION_INCLUDE>
      </VULNERABILITY_DETECTION>
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,Sybase]]></AUTHENTICATION>
<AUTHENTICATION_LEAST_PRIVILEGE><![CDATA[Unix]]></AUTHENTICATION_L
EAST_PRIVILEGE>
      <ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>1</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
      </DISSOLVABLE_AGENT>
      <LITE_OS_SCAN>1</LITE_OS_SCAN>
      <CUSTOM_HTTP_HEADER>
        <VALUE>sdfdsf</VALUE>
        <DEFINITION_KEY>abc</DEFINITION_KEY>
        <DEFINITION_VALUE>xyz</DEFINITION_VALUE>
```

```
      </CUSTOM_HTTP_HEADER>
      <SYSTEM_AUTH_RECORD>
          <INCLUDE_SYSTEM_AUTH>
<ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
          </INCLUDE_SYSTEM_AUTH>
      </SYSTEM_AUTH_RECORD>
    </SCAN>
    <MAP>
      <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
      <TCP_PORTS>
        <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
        <TCP_PORTS_ADDITIONAL>
          <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
          <ADDITIONAL_PORTS>2</ADDITIONAL_PORTS>
        </TCP_PORTS_ADDITIONAL>
      </TCP_PORTS>
      <UDP_PORTS>
        <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
        <UDP_PORTS_ADDITIONAL>
          <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
          <ADDITIONAL_PORTS>9</ADDITIONAL_PORTS>
        </UDP_PORTS_ADDITIONAL>
      </UDP_PORTS>
      <MAP_OPTIONS>
        <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
        <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
      </MAP_OPTIONS>
      <MAP_PERFORMANCE>
        <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
        <MAP_PARALLEL>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>12</SCANNER_APPLIANCES>
          <NETBLOCK_SIZE>8192 IPs</NETBLOCK_SIZE>
        </MAP_PARALLEL>
        <PACKET_DELAY>Medium</PACKET_DELAY>
      </MAP_PERFORMANCE>
      <MAP_AUTHENTICATION>VMware</MAP_AUTHENTICATION>
    </MAP>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1024</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
```

```
        </TCP_PORTS>
        <UDP_PORTS>
          <CUSTOM_PORT><![CDATA[69,111]]></CUSTOM_PORT>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>

<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
        <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - List the VM Option profile with VMware NSX

API request:

```
curl --location --request POST '
/api/2.0/fo/subscription/option_profile/vm/?action=list&id=8148496
' \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Tokens> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_profile_i
nfo.dtd%22>
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>8153637</ID>
                <GROUP_NAME>
                    <![CDATA[nsxtest1]]>
```

```
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[t b (vmspxtb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2025-12-15T06:41:03Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>full</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>1</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>20</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                    <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                    <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                    <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
```

```
                        <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                         <OVAL_CHECKS>0</OVAL_CHECKS>
                         <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <AUTHENTICATION>
                    <![CDATA[NSX]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                <DISSOLVABLE_AGENT>
                   <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
                </DISSOLVABLE_AGENT>
            </SCAN>
            <MAP>
                <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>0</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
```

```
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

V3.0

/api/3.0/fo/subscription/option_profile/vm/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for V3.0 under Create VM Option Profile.

DTD

<platform API server>/api/3.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - List VM Option Profile

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
GET"action=list"
"action=list&title=Option_profile_vCenter_scan_disconnected_esxi"
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/vm/""
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_
profile_info.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>2633919</ID>
                <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[John Manager (agms_nb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
```

```
                <UPDATE_DATE>2024-07-01T09:55:01Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                      <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>

<PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                       <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>
                    <PORT_SCANNING_AND_HOST_DISCOVERY>Normal
                    </PORT_SCANNING_AND_HOST_DISCOVER
Y>
                </PERFORMANCE>

<LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>

<BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
```

```
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
            <MAP>

<BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>

<PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
                    <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0
                    </IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0
                    </NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
```

```
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

Sample - List the VM Option profile with VMware NSX

API request:

```
curl --location --request POST '
/api/3.0/fo/subscription/option_profile/vm/?action=list&id=8148496
' \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Tokens> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_profile_i
nfo.dtd%22>
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>8153637</ID>
                <GROUP_NAME>
                    <![CDATA[nsxtest1]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[t b (vmspxtb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2025-12-15T06:41:03Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>full</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>1</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
```

```
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>20</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                    <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                    <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                    <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                       <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <AUTHENTICATION>
                    <![CDATA[NSX]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                <DISSOLVABLE_AGENT>
                   <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
                </DISSOLVABLE_AGENT>
            </SCAN>
            <MAP>
                <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
```

```
                    </MAP_PERFORMANCE>
                    <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
                </MAP>
                <ADDITIONAL>
                    <HOST_DISCOVERY>
                        <TCP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </TCP_PORTS>
                        <UDP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </UDP_PORTS>
                        <ICMP>0</ICMP>
                    </HOST_DISCOVERY>
                    <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                        <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                    </PACKET_OPTIONS>
                </ADDITIONAL>
            </OPTION_PROFILE>
        </OPTION_PROFILES>
```

V4.0

/api/4.0/fo/subscription/option_profile/vm/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the “id” or “title” parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for V3.0 under Create VM Option Profile.

DTD

<platform API server>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd

Sample - List VM Option Profile with vCenter and Scan disconnected ESXi

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X
GET"action=list"
"action=list&title=Option_profile_vCenter_scan_disconnected_esxi"
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_
profile_info.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>2633919</ID>
                <GROUP_NAME>

<![CDATA[Option_profile_vCenter_scan_disconnected_esxi]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[John Manager (agms_nb)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>194334</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2024-07-01T09:55:01Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>
                    <PORT_SCANNING_AND_HOST_DISCOVERY>Normal
                    </PORT_SCANNING_AND_HOST_DISCOVER
Y>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
```

```
                        <COMPLETE>
                            <![CDATA[complete]]>
                        </COMPLETE>
                        <DETECTION_INCLUDE>
                            <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                            <OVAL_CHECKS>0</OVAL_CHECKS>
                            <QRDI_CHECKS>0</QRDI_CHECKS>
                        </DETECTION_INCLUDE>
                    </VULNERABILITY_DETECTION>
                    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                </SCAN>
                <MAP>
                    <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                    <MAP_OPTIONS>
                        <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                        <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                    </MAP_OPTIONS>
                    <MAP_PERFORMANCE>
                        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                        <MAP_PARALLEL>
                            <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                            <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                            <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                        </MAP_PARALLEL>
                        <PACKET_DELAY>Minimum</PACKET_DELAY>
                    </MAP_PERFORMANCE>
                    <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
                    <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
                </MAP>
                <ADDITIONAL>
                    <HOST_DISCOVERY>
                        <TCP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </TCP_PORTS>
                        <UDP_PORTS>
                            <STANDARD_SCAN>1</STANDARD_SCAN>
                        </UDP_PORTS>
                        <ICMP>1</ICMP>
                    </HOST_DISCOVERY>
                    <PACKET_OPTIONS>

   <IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                        <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>
                        <IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0
                        </IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>
                        <NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0
                        </NOT_SEND_TCP_ACK_OR
   _SYN_ACK_DURING_HOST_DISCOVERY>
                    </PACKET_OPTIONS>
                </ADDITIONAL>
            </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - List VM Option Profile

API request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?action=list&
id=7723450' \
--header 'X-Requested-With: curl' \
--header 'Content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_i
nfo.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>7723450</ID>
                <GROUP_NAME>
                    <![CDATA[Option profile V4 API1]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[name (username)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>4073130</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2025-09-18T05:43:45Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>1</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>49</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
```

```
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>20</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                       <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <AUTHENTICATION>
                    <![CDATA[Windows,Unix]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
            <MAP>
                <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
                <TCP_PORTS>
                    <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                    <TCP_PORTS_ADDITIONAL>
                        <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                        <ADDITIONAL_PORTS>1</ADDITIONAL_PORTS>
                    </TCP_PORTS_ADDITIONAL>
                </TCP_PORTS>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
```

```
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>0</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

Sample - List all the VM Option profile

API request:

```
curl --location '
<qulays_base_url>/api/4.0/fo/subscription/option_profile/vm/?actio
n=list' \
--header 'X-Requested-With: test' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_i
nfo.dtd">
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>7319681</ID>
                <GROUP_NAME>
                    <![CDATA[Vmware and Vcenter]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[Shreya Joshi (quays_xs70)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>4073130</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2024-10-21T15:59:47Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
```

```
                    <PORTS>
                        <TCP_PORTS>
                            <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                            <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                        </TCP_PORTS>
                        <UDP_PORTS>
                            <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                        </UDP_PORTS>
                        <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                    </PORTS>
                    <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                    <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                    <PERFORMANCE>
                        <PARALLEL_SCALING>1</PARALLEL_SCALING>
                        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                        <HOSTS_TO_SCAN>
                            <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                            <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                        </HOSTS_TO_SCAN>
                        <PROCESSES_TO_RUN>
                            <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                            <HTTP_PROCESSES>10</HTTP_PROCESSES>
                        </PROCESSES_TO_RUN>
                        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                    </PERFORMANCE>
                    <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                    <VULNERABILITY_DETECTION>
                        <COMPLETE>
                            <![CDATA[complete]]>
                        </COMPLETE>
                        <DETECTION_INCLUDE>
                           <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                            <OVAL_CHECKS>0</OVAL_CHECKS>
                        </DETECTION_INCLUDE>
                    </VULNERABILITY_DETECTION>
                    <AUTHENTICATION>
                        <![CDATA[Windows,Unix,VMware]]>
                    </AUTHENTICATION>
                    <AUTHENTICATION_LEAST_PRIVILEGE>
                        <![CDATA[Unix]]>
                    </AUTHENTICATION_LEAST_PRIVILEGE>
                    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                </SCAN>
                <MAP>
                   <BASIC_INFO_GATHERING_ON>register</BASIC_INFO_GATHERING_ON>
                    <TCP_PORTS>
                        <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                    </TCP_PORTS>
                    <MAP_OPTIONS>
                        <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                        <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
```

```
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>0</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>7349173</ID>
                <GROUP_NAME>
                    <![CDATA[option profile parallel scanning]]>
                </GROUP_NAME>
                <GROUP_TYPE>user</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[Shreya Joshi (quays_xs70)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>4073130</SUBSCRIPTION_ID>
                <IS_DEFAULT>0</IS_DEFAULT>
                <IS_GLOBAL>0</IS_GLOBAL>
                <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
                <UPDATE_DATE>2025-02-17T13:40:37Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
```

```
                    <TCP_PORTS>
                        <TCP_PORTS_TYPE>standard</TCP_PORTS_TYPE>
                        <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <UDP_PORTS_TYPE>standard</UDP_PORTS_TYPE>
                    </UDP_PORTS>
                    <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
                </PORTS>
                <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
                <PERFORMANCE>
                    <PARALLEL_SCALING>1</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>61</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>20</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                       <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <AUTHENTICATION>
                    <![CDATA[Windows,Unix]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
            <MAP>
              <BASIC_INFO_GATHERING_ON>register</BASIC_INFO_GATHERING_ON>
                <TCP_PORTS>
                    <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
                </TCP_PORTS>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
```

```
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>0</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
...
    </OPTION_PROFILES>
```

Sample - List the VM Option profile with VMware NSX

API request:

```
curl --location --request POST '
/api/4.0/fo/subscription/option_profile/vm/?action=list&id=8148496
' \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Tokens> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_i
nfo.dtd%22>
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
```

```
            <ID>8153637</ID>
            <GROUP_NAME>
                <![CDATA[nsxtest1]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[t b (vmspxtb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2025-12-15T06:41:03Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS>
                    <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                    <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                </TCP_PORTS>
                <UDP_PORTS>
                    <UDP_PORTS_TYPE>full</UDP_PORTS_TYPE>
                </UDP_PORTS>
                <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>1</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>20</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
```

```
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                        <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                        <QRDI_CHECKS>0</QRDI_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <AUTHENTICATION>
                    <![CDATA[NSX]]>
                </AUTHENTICATION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
                <DISSOLVABLE_AGENT>
                    <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
                </DISSOLVABLE_AGENT>
            </SCAN>
            <MAP>
                <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
                <MAP_OPTIONS>
                    <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
                    <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
                </MAP_OPTIONS>
                <MAP_PERFORMANCE>
                    <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <MAP_PARALLEL>
                        <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
                        <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
                    </MAP_PARALLEL>
                    <PACKET_DELAY>Minimum</PACKET_DELAY>
                </MAP_PERFORMANCE>
                <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
            </MAP>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>0</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
                    <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
```

```
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/subscription/option_profile/?action=list	Active	Active
/api/3.0/fo/subscription/option_profile/?action=list	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=list	December 2025	December 2026

Delete VM Option Profile

For API version information, refer to the API Version History section.

V2.0| V3.0 | V4.0

V2.0

/api/2.0/fo/subscription/option_profile/vm/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

DTD

<platform API server>/api/2.0/simple_return.dtd

Sample - Delete VM Option Profile

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X POST
"action=delete&id=25121"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
```

```
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T10:58:06Z</DATETIME>
    <TEXT>Option Profile Deleted Successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>25121</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/subscription/option_profile/vm/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

DTD

<platform API server>/api/3.0/simple_return.dtd

Sample - Delete VM Option Profile

API request:

```
curl --location --request POST
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/vm/?action=dele
te&id=2639142"
\
--header 'X-Requested-With: postman' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2024-07-09T07:07:10Z</DATETIME>
        <TEXT>An option profile does not exist.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>2639142</VALUE>
            </ITEM>
```

```
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V4.0

/api/4.0/fo/subscription/option_profile/vm/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

DTD

<platform API server>/api/4.0/simple_return.dtd

Sample - Delete VM Option Profile

API request:

```
curl --location --request POST 'curl --location --request POST '
/api/4.0/fo/subscription/option_profile/vm/?id=8154392&action=delete' \
--header 'X-Requested-With: hfds' \
--header 'Authorization: Bearer <JWT Token> '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-12-17T05:41:04Z</DATETIME>
            <TEXT>Option Profile Deleted Successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>8154392</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/subscription/option_profile/?action=delete	Active	Active
/api/3.0/fo/subscription/option_profile/?action=delete	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/?action=delete	December 2025	December 2026

Option Profiles for PCI

/api/2.0/fo/subscription/option_profile/pci/

Create, update, list and delete option profiles for PCI.

Permissions - All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create PCI Option Profile

/api/2.0/fo/subscription/option_profile/pci/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) A title for easy identification.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
offline_scanner={**0**|1}	(Optional) Specify to 1 to download this profile to your offline scanners during the next sync.

Parameter	Description
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
Scan	
scan_overall_performance={high|**normal**|low|custom}	(Optional) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.

Parameter	Description
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_dead_hosts={**0**|1}	(Optional) Specify 1 to enable scanning dead hosts. A dead host is a host that is unreachable - it didn't respond to any pings. Your scan may run longer if you choose to scan dead hosts.
close_vuln_on_dead_hosts={**0**|1}	(Optional) Specify 1 to quickly close vulnerabilities for hosts that are not found alive after a set number of scans. When enabled, we'll mark existing tickets associated with dead hosts as Closed/Fixed and update the vulnerability status to Fixed.
not_found_alive_times={value}	(Optional) Specify the number of times the host is not found alive after which the vulnerability should be closed. This setting is available only when close_vuln_on_dead_hosts=1.
purge_host_data={**0**|1}	(Optional) Specify 1 to purge host data. This option is especially useful if you have systems that are regularly decommissioned or replaced. By specifying this option you're telling us you want to purge the host if we detect a change in the host's Operating System (OS) vendor at scan time, for example the OS changed from Linux to Windows or Debian to Ubuntu. We will not purge the host for an OS version change like Linux 2.8.13 to Linux 2.9.4.
Additional	
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 7 additional ports apart from the 13 standard scan ports used by default: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X POST
"action=create&title=pci&global=1&offline_scanner=1&external_scann
ers_use=3&scan_parallel_scaling=1&scan_overall_performance=high&ad
ditional_tcp_ports_additional=80,35"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pci/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T13:04:21Z</DATETIME>
```

```
    <TEXT>Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>32113</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update PCI Option Profile

/api/2.0/fo/subscription/option_profile/pci/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.

For a list of optional parameters, see Input Parameters for Create PCI Option Profile.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X POST
"action=update&id=31102&title=pci2"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pci/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T10:32:50Z</DATETIME>
    <TEXT>Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>31102</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

PCI Option Profile List

/api/2.0/fo/subscription/option_profile/pci/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for Create PCI Option Profile.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X GET
"action=list"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pci/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<username>:<password/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>31102</ID>
      <GROUP_NAME><![CDATA[jp pci 11]]></GROUP_NAME>
      <GROUP_TYPE>pci</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2018-04-10T10:32:50Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
      <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>high</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
```

```
        <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
        <HTTP_PROCESSES>15</HTTP_PROCESSES>
      </PROCESSES_TO_RUN>
      <PACKET_DELAY>Short</PACKET_DELAY>
    </PERFORMANCE>
  </SCAN>
  <ADDITIONAL>
    <HOST_DISCOVERY>
      <TCP_PORTS>
        <STANDARD_SCAN>1</STANDARD_SCAN>
        <TCP_ADDITIONAL>
          <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
          <ADDITIONAL_PORTS>80,35</ADDITIONAL_PORTS>
        </TCP_ADDITIONAL>
      </TCP_PORTS>
    </HOST_DISCOVERY>
  </ADDITIONAL>
</OPTION_PROFILE>
<OPTION_PROFILE>
  <BASIC_INFO>
    <ID>32113</ID>
    <GROUP_NAME><![CDATA[jp pci 333]]></GROUP_NAME>
    <GROUP_TYPE>pci</GROUP_TYPE>
    <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
    <UNIT_ID>0</UNIT_ID>
    <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
    <IS_GLOBAL>1</IS_GLOBAL>
    <IS_OFFLINE_SYNCABLE>1</IS_OFFLINE_SYNCABLE>
    <UPDATE_DATE>2018-04-10T10:32:50Z</UPDATE_DATE>
  </BASIC_INFO>
  <SCAN>
    <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
    <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
    <PERFORMANCE>
      <PARALLEL_SCALING>1</PARALLEL_SCALING>
      <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
      <HOSTS_TO_SCAN>
        <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
        <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
      </HOSTS_TO_SCAN>
      <PROCESSES_TO_RUN>
        <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
        <HTTP_PROCESSES>15</HTTP_PROCESSES>
      </PROCESSES_TO_RUN>
      <PACKET_DELAY>Short</PACKET_DELAY>
```

```
      </PERFORMANCE>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>80,35</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
      </HOST_DISCOVERY>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51471401</ID>
      <GROUP_NAME><![CDATA[pci op - 1]]></GROUP_NAME>
      <GROUP_TYPE>pci</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>2018-04-10T10:32:50Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
      <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
    </SCAN>
```

```
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1024</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
      </HOST_DISCOVERY>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

DTD

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

Delete PCI Option Profile

/api/2.0/fo/subscription/option_profile/pci/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X POST
"action=delete&id=51471401"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pci/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T10:32:50Z</DATETIME>
    <TEXT>Option Profile Deleted Successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
```

```
        <KEY>ID</KEY>
        <VALUE>51471401</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Option Profiles for Compliance

For API version information, refer to API Version History section.

V2.0|V 3.0|V 4.0|V 5.0

V2.0

/api/2.0/fo/subscription/option_profile/pc/

Create, update, list and delete option profiles for compliance scans.

Permissions

Note: The list PC option profiles API is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create PC Option Profile

/api/2.0/fo/subscription/option_profile/pc/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) The title for the option profile.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.

Parameter	Description
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
Scan	
scan_overall_performance={high|**normal**|low|custom}	(Required) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.

Parameter	Description
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_by_policy={**0**|1}	(Optional) Specify 1 to enable scan by policy. The Scan by Policy option allows you to restrict your scans to the controls in specified policies. You can choose up to 20 policies, one policy at a time. Once you've specified a policy, all controls in that policy will be scanned including any special control types in the policy. This is regardless of the Control Types settings in the profile.
policy_names={value1, value2}	(Optional) Specify policy names to scan by policy.
policy_ids={value1,value2}	(Optional) Specify policy IDs to scan by policy.
auto_update_expected_value ={**0**|1}	(Optional) Specify 1 to update the control expected value used for posture evaluation with the actual value returned by the scan.
fim_controls_enabled={**0**|1}	(Optional) Specify 1 to perform file integrity monitoring based on user defined file integrity checks. A file integrity check is a user defined control that checks for changes to a specific file. You should set auto_update_expected_value=1 in order to use this parameter.
custom_wmi_query_checks={ **0**|1}	(Optional) Specify 1 to run Windows WMI query checks. When enabled, WMI query checks will be performed for user defined WMI Query Check controls.
enable_dissolvable_agent= {**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_password_auditing= {**0**|1}	(Optional) Specify 1 to check for service provided password auditing controls (control IDs 3893, 3894 and 3895). These controls are used to identify 1) user accounts with empty passwords, 2) user accounts with the password equal to the user name, and 3) user accounts with passwords equal to an entry in a user-defined password dictionary. This setting is available only if enable_dissolvable_agent=1.
custom_password_dictionary ={value1,value2}	(Optional) Specify passwords in order to create a password dictionary. This is used when evaluating control ID 3895, which identifies user accounts where the password is equal to an entry in the password dictionary.

Parameter	Description
enable_windows_share_enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_windows_directory_search={**0**|1}	(Optional) Specify 1 if you've set up Windows Directory Search controls and want to include them in the scan. This custom control allows you to search for files/directories based on various criteria like file name and user access permissions.
scan_ports={standard|**targeted**}	(Required) Specify "standard" to enable standard scan of TCP ports. See Appendix B - Ports used for scanning for a list of ports used for standard scan. Specify "targeted" to perform a targeted scan. Which ports are included in a targeted scan? For Unix hosts, these well known ports are scanned: 22 (SSH), 23 (telnet) and 513 (rlogin). Any one of these services is sufficient for authentication. If services (SSH, telnet, rlogin) are not running on these well known ports for the hosts you will be scanning, specify this option and define a custom ports list in the Unix authentication record. Note: The actual ports scanned also depends on the Ports setting in the Unix authentication record. For Windows hosts, the service scans a fixed set of required Windows ports (a service defined, internal list).
mssql_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom MS SQL Database checks.
mssql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256).
oracle_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Oracle Database checks.
oracle_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 5000).
sybase_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Sybase Database checks.
sybase_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for Sybase is 2500 rows.
postgresql_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks.
postgresql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for PostgreSQL/Pivotal Greenplum is 5000 rows.

Parameter	Description
sapiq_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom SAP IQ Database checks.
sapiq_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for SAP IQ is 10000 rows.
db2_db_udc_restriction= {**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks.
db2_db_udc_limit= {value}	(Optional) The default value is 256 and maximum allowed limit is 5000 rows.
enable_auth_instance_discovery={**0**|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances. The parameters enable_auth_instance_discovery, scan_by_policy and include_system_auth are mutually exclusive and cannot be specified together in the same request. In UI, this parameter is a check box and referred to "Allow instance discovery..." in the System Authentication Records section on the New/Edit Compliance Profile page.
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. The valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle and MongoDB. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.
ibm_was_discovery_mode={value}	(Optional to create or update option profile record) Specify ibm_was_discovery_mode=server_dir to auto discover instances at the server directory level. Specify ibm_was_discovery_mode=installation_dir to auto discover instances at the installation directory level. When unspecified and auto_auth_types=IBM WebSphere App Server, we will auto discover instances at the installation directory level. This parameter can only be specified if auto_auth_types includes IBM WebSphere App Server.
oracle_template_id={value}	(Optional) The Template ID for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.

Parameter	Description
oracle_template_name={value}	(Optional) The Template Name for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
mongodb_template_id={value}	(Optional) The Template ID for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
mongodb_template_name={val ue}	((Optional) The Template Name for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
include_system_auth={**0**|1}	(Optional to create or update option profile record) Specify include_system_auth=1 if you have a system created auth record and user created auth record for the same instance configuration and choose which one to include for scans. When unspecified (include_system_auth=0), user record will be selected for scan by default. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. In UI, this parameter is a check box and referred to "Use System Authentication Records" in the System Authentication Records section in the Scan tab on the New/Edit Compliance Profile page.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to include system created auth record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to include user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
Instance Data Collection	
enable_instance_data_collection={0|1}	(Optional) Specify 1 to enable database instance data collection by using underlying OS authentication record. By default, this option is disabled.

Parameter	Description
instance_data_collection_auth_types	(Optional) Specify the database technologies for which you want to enable OS authentication-based data collection. The valid values are: IBM DB2, InformixDB, MongoDB, MSSQL, MySQL, Oracle, Pivotal Greenplum, PostgreSQL, Sybase. You can use this parameter only if you set the value of the enable_instance_data_collection parameter to 1.
enable_os_based_instance_discovery={0|1}	(Optional) Set the value to 1 to enable technology instance data collection by using underlying OS authentication record. By default, this option is disabled.
os_based_instance_disc_technologies	(Optional) Specify a comma-separated list of technologies to enable OS authentication-based data collection. Currently we support Oracle JRE and IBM WebSphere Liberty. Hence, the valid values are: Oracle JRE and IBM WebSphere Liberty. You can use this parameter only if you set the value of the enable_os_based_instance_discovery parameter to 1.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type={**standard**|custom}	(Optional) Specify "standard" to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is "standard". Specify "custom" to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify custom to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.

Parameter	Description
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X POST
"action=create&title=pcjp&global=1&scan_parallel_scaling=1&scan_ov
erall_performance=high&scan_by_policy=1&policy_names=jp2&auto_upda
te_expected_value=1&scan_ports=standard&additional_tcp_ports=1&not
_send_ack_or_syn_ack_packets_during_host_discovery=1"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>39044</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for Oracle instance discovery

In this sample we are creating an option profile with instance discovery and system record creation enabled for Oracle and we're using template ID 2237327.

API request:

```
curl -u "<username>:<password" -H "X-Requested-With:curl" -X POST
-d
"action=create&title=Profile-Auth-Ins-
Oracle&enable_auth_instance_discovery=1&auto_auth_types=Oracle&sca
n_ports=targeted&oracle_template_id=2237327"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T19:12:10Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3305478</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for MongoDB instance discovery

In this sample we are creating an option profile with the option to enable instance discovery and system record creation for MongoDB and we're using template ID 6731346. .

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -X POST
"action=create&title=Profile-Auth-
InsMongodtestapi2&enable_auth_instance_discovery=1&auto_auth_types
=MongoD B&scan_ports=targeted&mongodb_template_id=6731346"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
     <RESPONSE>
          <DATETIME>2022-12-19T07:48:27Z</DATETIME>
          <TEXT>Compliance Option profile successfully
added.</TEXT>
          <ITEM_LIST>
               <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>6863066</VALUE>
               </ITEM>
          </ITEM_LIST>
     </RESPONSE>
</SIMPLE_RETURN>
```

Database UDCs for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2

We have added the following parameters to the Options Profile API to help you set a limit on the number of rows returned per scan for the MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2 UDCs.

- DATABASE_PREFERENCE_KEY

- mssql_db_udc_restriction

- mssql_db_udc_limit

- oracle_db_udc_restriction

- oracle_db_udc_limit

- sybase_db_udc_restriction

- sybase_db_udc_limit

- postgreSQL_db_udc_restriction

- postgreSQL_db_udc_limit

- sapiq_db_udc_restriction

- sapiq_db_udc_limit

- db2_db_udc_restriction

- db2_db_udc_limit

Maximum allowed limit for MS SQL is 256 rows, for Oracle, PostgreSQL/Pivotal Greenplum, and IBM DB2, it's 5000 rows, for Sybase it's 2500 rows, and for SAP IQ, it's 10000 rows.

Sample - Create for Database UDC

Create with Database Preference Key and custom Limit set for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d "action=create&title=API-PC-
OP&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_l
imit=10&mssql_db_udc_restriction=1&mssql_db_udc_limit=250&sybase_d
b_udc_restriction=1&sybase_db_udc_limit=50&postgreSQL_db_udc_restr
iction=1&postgreSQL_db_udc_limit=50&db2_db_udc_restriction=1&db2_d
b_udc_limit=300"
"<qualys_base_url>api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T19:16:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1710286</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V 3.0

/api/3.0/fo/subscription/option_profile/pc/

Create, update, list and delete option profiles for compliance scans.

Permissions

Note: The list PC option profiles API is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create PC Option Profile

/api/3.0/fo/subscription/option_profile/pc/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) The title for the option profile.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.

Parameter	Description
Scan	
scan_overall_performance={high|**normal**|low|custom}	(Required) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.

Parameter	Description
scan_by_policy={**0**|1}	(Optional) Specify 1 to enable scan by policy. The Scan by Policy option allows you to restrict your scans to the controls in specified policies. You can choose up to 20 policies, one policy at a time. Once you've specified a policy, all controls in that policy will be scanned including any special control types in the policy. This is regardless of the Control Types settings in the profile.
policy_names={value1, value2}	(Optional) Specify policy names to scan by policy.
policy_ids={value1,value2}	(Optional) Specify policy IDs to scan by policy.
auto_update_expected_value ={**0**|1}	(Optional) Specify 1 to update the control expected value used for posture evaluation with the actual value returned by the scan.
fim_controls_enabled={**0**|1}	(Optional) Specify 1 to perform file integrity monitoring based on user defined file integrity checks. A file integrity check is a user defined control that checks for changes to a specific file. You should set auto_update_expected_value=1 in order to use this parameter.
custom_wmi_query_checks={ **0**|1}	(Optional) Specify 1 to run Windows WMI query checks. When enabled, WMI query checks will be performed for user defined WMI Query Check controls.
enable_dissolvable_agent= {**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_password_auditing= {**0**|1}	(Optional) Specify 1 to check for service provided password auditing controls (control IDs 3893, 3894 and 3895). These controls are used to identify 1) user accounts with empty passwords, 2) user accounts with the password equal to the user name, and 3) user accounts with passwords equal to an entry in a user-defined password dictionary. This setting is available only if enable_dissolvable_agent=1.
custom_password_dictionary ={value1,value2}	(Optional) Specify passwords in order to create a password dictionary. This is used when evaluating control ID 3895, which identifies user accounts where the password is equal to an entry in the password dictionary.
enable_windows_share_ enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_windows_directory_ search={**0**|1}	(Optional) Specify 1 if you've set up Windows Directory Search controls and want to include them in the scan. This custom control allows you to search for files/directories based on various criteria like file name and user access permissions.

Parameter	Description
scan_ports={standard|**targeted**}	(Required) Specify "standard" to enable standard scan of TCP ports. See Appendix B - Ports used for scanning for a list of ports used for standard scan. Specify "targeted" to perform a targeted scan. Which ports are included in a targeted scan? For Unix hosts, these well known ports are scanned: 22 (SSH), 23 (telnet) and 513 (rlogin). Any one of these services is sufficient for authentication. If services (SSH, telnet, rlogin) are not running on these well known ports for the hosts you will be scanning, specify this option and define a custom ports list in the Unix authentication record. Note: The actual ports scanned also depends on the Ports setting in the Unix authentication record. For Windows hosts, the service scans a fixed set of required Windows ports (a service defined, internal list).
mssql_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom MS SQL Database checks.
mssql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256).
oracle_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Oracle Database checks.
oracle_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 5000).
sybase_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Sybase Database checks.
sybase_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for Sybase is 2500 rows.
postgresql_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks.
postgresql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for PostgreSQL/Pivotal Greenplum is 5000 rows.
sapiq_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom SAP IQ Database checks.
sapiq_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for SAP IQ is 10000 rows.
db2_db_udc_restriction= {**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks.

Parameter	Description
db2_db_udc_limit= {value}	(Optional) The default value is 256 and maximum allowed limit is 5000 rows.
enable_auth_instance_discovery={**0**|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances. The parameters enable_auth_instance_discovery, scan_by_policy and include_system_auth are mutually exclusive and cannot be specified together in the same request. In UI, this parameter is a check box and referred to "Allow instance discovery..." in the System Authentication Records section on the New/Edit Compliance Profile page.
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. The valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle, MongoDB and MySQL. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.
ibm_was_discovery_mode={value}	(Optional to create or update option profile record) Specify ibm_was_discovery_mode=server_dir to auto discover instances at the server directory level. Specify ibm_was_discovery_mode=installation_dir to auto discover instances at the installation directory level. When unspecified and auto_auth_types=IBM WebSphere App Server, we will auto discover instances at the installation directory level. This parameter can only be specified if auto_auth_types includes IBM WebSphere App Server.
oracle_template_id={value}	(Optional) The Template ID for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
oracle_template_name={value}	(Optional) The Template Name for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.

Parameter	Description
mongodb_template_id={value}	(Optional) The Template ID for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
mongodb_template_name={val ue}	((Optional) The Template Name for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
include_system_auth={**0**|1}	(Optional to create or update option profile record) Specify include_system_auth=1 if you have a system created auth record and user created auth record for the same instance configuration and choose which one to include for scans. When unspecified (include_system_auth=0), user record will be selected for scan by default. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. In UI, this parameter is a check box and referred to "Use System Authentication Records" in the System Authentication Records section in the Scan tab on the New/Edit Compliance Profile page.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to include system created auth record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to include user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
mysql_template_id={value}	(Optional) The Template ID for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.

Parameter	Description
mysql_template_name={value}	(Optional) The Template Name for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.
Instance Data Collection	
enable_instance_data_collection={0|1}	(Optional) Specify 1 to enable database instance data collection by using underlying OS authentication record. By default, this option is disabled.
instance_data_collection_auth_types	(Optional) Specify the database technologies for which you want to enable OS authentication-based data collection. The valid values are: IBM DB2, InformixDB, MongoDB, MSSQL, MySQL, Oracle, Pivotal Greenplum, PostgreSQL, Sybase. You can use this parameter only if you set the value of the enable_instance_data_collection parameter to 1.
enable_os_based_instance_discovery={0|1}	(Optional) Set the value to 1 to enable technology instance data collection by using underlying OS authentication record. By default, this option is disabled.
os_based_instance_disc_technologies	(Optional) Specify a comma-separated list of technologies to enable OS authentication-based data collection. Currently we support Oracle JRE and IBM WebSphere Liberty. Hence, the valid values are: Oracle JRE and IBM WebSphere Liberty. You can use this parameter only if you set the value of the enable_os_based_instance_discovery parameter to 1.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type={**standard**|custom}	(Optional) Specify “standard” to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is “standard”. Specify “custom” to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.

Parameter	Description
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**|custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify custom to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom={value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom={value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_ack_or_syn_ack_packets_during_host_discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=pcjp&global=1&scan_parallel_scaling=1&scan_ov
erall_performance=high&scan_by_policy=1&policy_names=jp2&auto_upda
te_expected_value=1&scan_ports=standard&additional_tcp_ports=1&not
_send_ack_or_syn_ack_packets_during_host_discovery=1"
"http://<qualys_base_url>/api/3.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>39044</VALUE>
      </ITEM>
```

```
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for Oracle instance discovery

In this sample we are creating an option profile with instance discovery and system record creation enabled for Oracle and we're using template ID 2237327.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=Profile-Auth-Ins-
Oracle&enable_auth_instance_discovery=1&auto_auth_types=Oracle&sca
n_ports=targeted&oracle_template_id=2237327"
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T19:12:10Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3305478</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for MongoDB instance discovery

In this sample we are creating an option profile with the option to enable instance discovery and system record creation for MongoDB and we're using template ID 6731346. .

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=Profile-Auth-
InsMongodtestapi2&enable_auth_instance_discovery=1&auto_auth_types
=MongoD B&scan_ports=targeted&mongodb_template_id=6731346"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
     <RESPONSE>
          <DATETIME>2022-12-19T07:48:27Z</DATETIME>
          <TEXT>Compliance Option profile successfully
added.</TEXT>
          <ITEM_LIST>
               <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>6863066</VALUE>
               </ITEM>
          </ITEM_LIST>
     </RESPONSE>
</SIMPLE_RETURN>
```

Database UDCs for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2

We have added the following parameters to the Options Profile API to help you set a limit on the number of rows returned per scan for the MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2 UDCs.

- DATABASE_PREFERENCE_KEY

- mssql_db_udc_restriction

- mssql_db_udc_limit

- oracle_db_udc_restriction

- oracle_db_udc_limit

- sybase_db_udc_restriction

- sybase_db_udc_limit

- postgreSQL_db_udc_restriction

- postgreSQL_db_udc_limit

- sapiq_db_udc_restriction

- sapiq_db_udc_limit

- db2_db_udc_restriction

- db2_db_udc_limit

Maximum allowed limit for MS SQL is 256 rows, for Oracle, PostgreSQL/Pivotal Greenplum, and IBM DB2, it's 5000 rows, for Sybase it's 2500 rows, and for SAP IQ, it's 10000 rows.

Sample - Create for Database UDC

Create with Database Preference Key and custom Limit set for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d "action=create&title=API-PC-
OP&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_l
imit=10&mssql_db_udc_restriction=1&mssql_db_udc_limit=250&sybase_d
b_udc_restriction=1&sybase_db_udc_limit=50&postgreSQL_db_udc_restr
iction=1&postgreSQL_db_udc_limit=50&db2_db_udc_restriction=1&db2_d
b_udc_limit=300"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T19:16:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1710286</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - create option profile for MySQL instance discovery using template ID

In this sample, we are creating an option profile with the option to enable the MySQL instance discovery and system record creation using the template ID 5129495.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u Username:Password"
-d
"action=create&title=mysql_auth_op_api&enable_auth_instance_discov
ery=1&scan_ports=targeted&auto_auth_types=MySQL&mysql_template_id=
5129495"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://

<qualys_base_url>/api/3.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T05:59:41Z</DATETIME>
            <TEXT>Compliance Option profile successfully
added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642120</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
</SIMPLE_RETURN>
```

Sample - create option profile for MySQL instance discovery using template Name

Creating option profile with MySQL record template using template name.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=create&title=mysql_auth_op_api1&enable_auth_instance_disco
very=1&scan_ports=targeted&auto_auth_types=MySQL&mysql_template_na
me=Mysql_template_api"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
```

```
<qualys_base_url>/api/3.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T12:14:53Z</DATETIME>
            <TEXT>Compliance Option profile successfully
added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 4.0

/api/4.0/fo/subscription/option_profile/pc/

Create, update, list and delete option profiles for compliance scans.

Permissions

Note: The list PC option profiles API is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create PC Option Profile

/api/4.0/fo/subscription/option_profile/pc/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) The title for the option profile.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.
clean_scan_data_on_dead_hosts{0|1}	(Optional) Use this parameter to indicate whether you would like to remove compliance scan data associated with dead hosts. Enter 1 if you wish to remove the compliance data or 0 if you do not wish to remove it.

Parameter	Description
host_not_found_alive_times{value}	(Optional) Enter the number of compliance scans to wait before removing compliance data associated with dead hosts. The valid range to set a number of compliance scans to wait before removing data is 1 to 99.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
Scan	
scan_overall_performance={high|**normal**|low|custom}	(Required) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.

Parameter	Description
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_by_policy={**0**|1}	(Optional) Specify 1 to enable scan by policy. The Scan by Policy option allows you to restrict your scans to the controls in specified policies. You can choose up to 20 policies, one policy at a time. Once you've specified a policy, all controls in that policy will be scanned including any special control types in the policy. This is regardless of the Control Types settings in the profile.
policy_names={value1, value2}	(Optional) Specify policy names to scan by policy.
policy_ids={value1,value2}	(Optional) Specify policy IDs to scan by policy.
auto_update_expected_value ={**0**|1}	(Optional) Specify 1 to update the control expected value used for posture evaluation with the actual value returned by the scan.
fim_controls_enabled={**0**|1}	(Optional) Specify 1 to perform file integrity monitoring based on user defined file integrity checks. A file integrity check is a user defined control that checks for changes to a specific file. You should set auto_update_expected_value=1 in order to use this parameter.
custom_wmi_query_checks={ **0**|1}	(Optional) Specify 1 to run Windows WMI query checks. When enabled, WMI query checks will be performed for user defined WMI Query Check controls.
enable_dissolvable_agent= {**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_password_auditing= {**0**|1}	(Optional) Specify 1 to check for service provided password auditing controls (control IDs 3893, 3894 and 3895). These controls are used to identify 1) user accounts with empty passwords, 2) user accounts with the password equal to the user name, and 3) user accounts with passwords equal to an entry in a user-defined password dictionary. This setting is available only if enable_dissolvable_agent=1.

Parameter	Description
custom_password_dictionary ={value1,value2}	(Optional) Specify passwords in order to create a password dictionary. This is used when evaluating control ID 3895, which identifies user accounts where the password is equal to an entry in the password dictionary.
enable_windows_share_ enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_windows_directory_ search={**0**|1}	(Optional) Specify 1 if you've set up Windows Directory Search controls and want to include them in the scan. This custom control allows you to search for files/directories based on various criteria like file name and user access permissions.
scan_ports={standard| **targeted**}	(Required) Specify “standard” to enable standard scan of TCP ports. See Appendix B - Ports used for scanning for a list of ports used for standard scan. Specify “targeted” to perform a targeted scan. Which ports are included in a targeted scan? For Unix hosts, these well known ports are scanned: 22 (SSH), 23 (telnet) and 513 (rlogin). Any one of these services is sufficient for authentication. If services (SSH, telnet, rlogin) are not running on these well known ports for the hosts you will be scanning, specify this option and define a custom ports list in the Unix authentication record. Note: The actual ports scanned also depends on the Ports setting in the Unix authentication record. For Windows hosts, the service scans a fixed set of required Windows ports (a service defined, internal list).
mssql_db_udc_restriction={**0**| 1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom MS SQL Database checks.
mssql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256).
oracle_db_udc_restriction={**0**| 1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Oracle Database checks.
oracle_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 5000).
sybase_db_udc_restriction={**0** |1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Sybase Database checks.
sybase_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for Sybase is 2500 rows.
postgresql_db_udc_restrictio n={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks.

Parameter	Description
postgresql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for PostgreSQL/Pivotal Greenplum is 5000 rows.
sapiq_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom SAP IQ Database checks.
sapiq_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for SAP IQ is 10000 rows.
db2_db_udc_restriction= {**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks.
db2_db_udc_limit= {value}	(Optional) The default value is 256 and maximum allowed limit is 5000 rows.
enable_auth_instance_discovery={**0**|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances. The parameters enable_auth_instance_discovery, scan_by_policy and include_system_auth are mutually exclusive and cannot be specified together in the same request. In UI, this parameter is a check box and referred to "Allow instance discovery..." in the System Authentication Records section on the New/Edit Compliance Profile page.
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. The valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle, MongoDB and MySQL. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.
ibm_was_discovery_mode={value}	(Optional to create or update option profile record) Specify ibm_was_discovery_mode=server_dir to auto discover instances at the server directory level. Specify ibm_was_discovery_mode=installation_dir to auto discover instances at the installation directory level. When unspecified and auto_auth_types=IBM WebSphere App Server, we will auto discover instances at the installation directory level. This parameter can only be specified if auto_auth_types includes IBM WebSphere App Server.

Parameter	Description
oracle_template_id={value}	(Optional) The Template ID for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
oracle_template_name={value}	(Optional) The Template Name for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
mongodb_template_id={value}	(Optional) The Template ID for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
mongodb_template_name={val ue}	((Optional) The Template Name for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
include_system_auth={**0**|1}	(Optional to create or update option profile record) Specify include_system_auth=1 if you have a system created auth record and user created auth record for the same instance configuration and choose which one to include for scans. When unspecified (include_system_auth=0), user record will be selected for scan by default. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. In UI, this parameter is a check box and referred to "Use System Authentication Records" in the System Authentication Records section in the Scan tab on the New/Edit Compliance Profile page.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to include system created auth record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".

Parameter	Description
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to include user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
mysql_template_id={value}	(Optional) The Template ID for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.
mysql_template_name={value}	(Optional) The Template Name for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.
Instance Data Collection	
enable_instance_data_collection={0|1}	(Optional) Specify 1 to enable database instance data collection by using underlying OS authentication record. By default, this option is disabled.
instance_data_collection_auth_types	(Optional) Specify the database technologies for which you want to enable OS authentication-based data collection. The valid values are: IBM DB2, InformixDB, MongoDB, MSSQL, MySQL, Oracle, Pivotal Greenplum, PostgreSQL, Sybase. You can use this parameter only if you set the value of the enable_instance_data_collection parameter to 1.
enable_os_based_instance_discovery={0|1}	(Optional) Set the value to 1 to enable technology instance data collection by using underlying OS authentication record. By default, this option is disabled.
os_based_instance_disc_technologies	(Optional) Specify a comma-separated list of technologies to enable OS authentication-based data collection. Currently we support Oracle JRE and IBM WebSphere Liberty. Hence, the valid values are: Oracle JRE and IBM WebSphere Liberty. You can use this parameter only if you set the value of the enable_os_based_instance_discovery parameter to 1.
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.

Parameter	Description
additional_tcp_ports_ additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type= {**standard**|custom}	(Optional) Specify "standard" to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is "standard". Specify "custom" to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_ custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**| custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify custom to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom= {value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom= {value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_ syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_ack_or_syn_ack_ packets_during_host_ discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=pcjp&global=1&scan_parallel_scaling=1&scan_ov
erall_performance=high&scan_by_policy=1&policy_names=jp2&auto_upda
te_expected_value=1&scan_ports=standard&additional_tcp_ports=1&not
_send_ack_or_syn_ack_packets_during_host_discovery=1"
"http://<qualys_base_url>/api/4.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>39044</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for Oracle instance discovery

In this sample we are creating an option profile with instance discovery and system record creation enabled for Oracle and we're using template ID 2237327.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=Profile-Auth-Ins-
Oracle&enable_auth_instance_discovery=1&auto_auth_types=Oracle&sca
n_ports=targeted&oracle_template_id=2237327"
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T19:12:10Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3305478</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile for MongoDB instance discovery

In this sample we are creating an option profile with the option to enable instance discovery and system record creation for MongoDB and we're using template ID 6731346. .

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=Profile-Auth-
InsMongodtestapi2&enable_auth_instance_discovery=1&auto_auth_types
=MongoD B&scan_ports=targeted&mongodb_template_id=6731346"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
     <RESPONSE>
          <DATETIME>2022-12-19T07:48:27Z</DATETIME>
          <TEXT>Compliance Option profile successfully
added.</TEXT>
          <ITEM_LIST>
               <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>6863066</VALUE>
               </ITEM>
          </ITEM_LIST>
     </RESPONSE>
</SIMPLE_RETURN>
```

Database UDCs for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2

We have added the following parameters to the Options Profile API to help you set a limit on the number of rows returned per scan for the MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2 UDCs.

- DATABASE_PREFERENCE_KEY

- mssql_db_udc_restriction

- mssql_db_udc_limit

- oracle_db_udc_restriction

- oracle_db_udc_limit

- sybase_db_udc_restriction

- sybase_db_udc_limit

- postgreSQL_db_udc_restriction

- postgreSQL_db_udc_limit

- sapiq_db_udc_restriction

- sapiq_db_udc_limit

- db2_db_udc_restriction

- db2_db_udc_limit

Maximum allowed limit for MS SQL is 256 rows, for Oracle, PostgreSQL/Pivotal Greenplum, and IBM DB2, it's 5000 rows, for Sybase it's 2500 rows, and for SAP IQ, it's 10000 rows.

Sample - Create for Database UDC

Create with Database Preference Key and custom Limit set for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d "action=create&title=API-PC-
OP&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_l
imit=10&mssql_db_udc_restriction=1&mssql_db_udc_limit=250&sybase_d
b_udc_restriction=1&sybase_db_udc_limit=50&postgreSQL_db_udc_restr
iction=1&postgreSQL_db_udc_limit=50&db2_db_udc_restriction=1&db2_d
b_udc_limit=300"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T19:16:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1710286</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - create option profile for MySQL instance discovery using template ID

In this sample, we are creating an option profile with the option to enable the MySQL instance discovery and system record creation using the template ID 5129495.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u Username:Password"
-d
"action=create&title=mysql_auth_op_api&enable_auth_instance_discov
ery=1&scan_ports=targeted&auto_auth_types=MySQL&mysql_template_id=
5129495"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://

<qualys_base_url>/api/4.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T05:59:41Z</DATETIME>
            <TEXT>Compliance Option profile successfully
added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642120</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
</SIMPLE_RETURN>
```

Sample - create option profile for MySQL instance discovery using template Name

Creating option profile with MySQL record template using template name.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=create&title=mysql_auth_op_api1&enable_auth_instance_disco
very=1&scan_ports=targeted&auto_auth_types=MySQL&mysql_template_na
me=Mysql_template_api"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
```

```
<qualys_base_url>/api/4.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T12:14:53Z</DATETIME>
            <TEXT>Compliance Option profile successfully
added.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 5.0

/api/5.0/fo/subscription/option_profile/pc/

Create, update, list and delete option profiles for compliance scans.

Permissions

Note: The list PC option profiles API is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

All users will be able to list option profiles. A Manager will be able to create, update, and delete option profiles in the subscription, and a Unit Manager will be able to create, update, and delete option profiles for users in their business unit.

Create PC Option Profile

/api/5.0/fo/subscription/option_profile/pc/?action=create

[POST]

Input Parameters

Parameter	Description
action=create	(Required)
title={value}	(Required) The title for the option profile.
owner={value}	(Optional) The owner of the option profile(s), or the user who created the option profile.

Parameter	Description
clean_scan_data_on_dead_hosts{0|1}	(Optional) Use this parameter to indicate whether you would like to remove compliance scan data associated with dead hosts. Enter 1 if you wish to remove the compliance data or 0 if you do not wish to remove it.
host_not_found_alive_times{value}	(Optional) Enter the number of compliance scans to wait before removing compliance data associated with dead hosts. The valid range to set a number of compliance scans to wait before removing data is 1 to 99.
global={**0**|1}	(Optional) Share this profile with other users by making it global. Are you a Manager? This profile will be available to all users. Are you a Unit Manager? This profile will be available to all users in your business unit. Specify 1 to make global.
scan_parallel_scaling={**0**|1}	(Optional) Specify 1 to enable parallel scaling. This setting can be useful in subscriptions which have physical and virtual scanner appliances with different performance characteristics (e.g., CPU, RAM). Specify this option to dynamically scale up the number of hosts to scan in parallel (at scan time) to a calculated value which is based upon the computing resources available on each appliance. Note that the number of hosts to scan in parallel value determines how many hosts each appliance will target concurrently, not how many appliances will be used for the scan.
enable_agent_correlation_identifier={1,0}	(Optional) Specify 1 to enable the Agent Correlation Identifier, else 0.
agent_correlation_ports={value}	(Optional) Enter the ports for the Agent Correlation identifier. You can enter a maximum of 5 ports.
Scan	
scan_overall_performance={high|**normal**|low|custom}	(Required) The profile "normal" is recommended in most cases. The settings for scan_external_scanners, scan_scanner_appliances, scan_total_process, scan_http_process, scan_packet_delay, and scan_intensity change as per the specified profile. Normal - Well balanced between intensity and speed. High - Recommended only when scanning a single IP or a small number of IPs. Optimized for speed and shorter scan times. Low - Recommended if responsiveness for individual hosts and services is low. Optimized for low bandwidth network connections and highly utilized networks. May take longer to complete.
scan_external_scanners={value}	(Optional) Specify the number of external scanners to be used for associated scans. This setting is available only if you have multiple external scanners in your subscription. For example, if you have 10 external scanners in your subscription, you can configure this setting to any number between 1 to 10.

Parameter	Description
scan_scanner_appliances={value}	(Optional) Specify the number of scanner appliances to scan at the same time (per scan task). Launching several concurrent scans on the same scanner appliance has a multiplying effect on bandwidth usage and may exceed available scanner resources. Don't have scanner appliances? Disregard the Scanner Appliance setting.
scan_total_process={value}	(Optional) Specify the maximum number of processes to run at the same time per host. Note that the total number of processes includes the HTTP processes.
scan_http_process={value}	(Optional) Specify the maximum number of HTTP processes to run at the same time.
scan_packet_delay={minimum|short|**medium**|long|maximum}	(Optional) Specify the delay between groups of packets sent to each host during a scan. With a short delay, packets are sent more frequently. With a long delay, packets are sent less frequently.
scan_intensity={**normal**|medium|low|minimum}	(Optional) This setting determines the aggressiveness (parallelism) of port scanning and host discovery at the port level. Lowering the intensity level has the effect of serializing port scanning and host discovery. This is useful for certain network conditions like cascading firewalls and lower scan prioritization on the network. Tip - If you are scanning through a firewall we recommended you reduce the intensity level. Unauthenticated scans see more of a performance difference using this option.
scan_by_policy={**0**|1}	(Optional) Specify 1 to enable scan by policy. The Scan by Policy option allows you to restrict your scans to the controls in specified policies. You can choose up to 20 policies, one policy at a time. Once you've specified a policy, all controls in that policy will be scanned including any special control types in the policy. This is regardless of the Control Types settings in the profile.
policy_names={value1, value2}	(Optional) Specify policy names to scan by policy.
policy_ids={value1,value2}	(Optional) Specify policy IDs to scan by policy.
auto_update_expected_value ={**0**|1}	(Optional) Specify 1 to update the control expected value used for posture evaluation with the actual value returned by the scan.
fim_controls_enabled={**0**|1}	(Optional) Specify 1 to perform file integrity monitoring based on user defined file integrity checks. A file integrity check is a user defined control that checks for changes to a specific file. You should set auto_update_expected_value=1 in order to use this parameter.
custom_wmi_query_checks={**0**|1}	(Optional) Specify 1 to run Windows WMI query checks. When enabled, WMI query checks will be performed for user defined WMI Query Check controls.

Parameter	Description
enable_dissolvable_agent={**0**|1}	(Optional) Specify 1 to enable dissolvable agent. This is required for certain scan features like Windows Share Enumeration. How does it work? At scan time the Agent is installed on Windows devices to collect data, and once the scan is complete it removes itself completely from target systems.
enable_password_auditing={**0**|1}	(Optional) Specify 1 to check for service provided password auditing controls (control IDs 3893, 3894 and 3895). These controls are used to identify 1) user accounts with empty passwords, 2) user accounts with the password equal to the user name, and 3) user accounts with passwords equal to an entry in a user-defined password dictionary. This setting is available only if enable_dissolvable_agent=1.
custom_password_dictionary ={value1,value2}	(Optional) Specify passwords in order to create a password dictionary. This is used when evaluating control ID 3895, which identifies user accounts where the password is equal to an entry in the password dictionary.
enable_windows_share_ enumeration={**0**|1}	(Optional) Specify 1 to use Windows Share Enumeration to find and report details about Windows shares that are readable by everyone. This test is performed using QID 90635. Make sure 1) the Dissolvable Agent is enabled, 2) QID 90635 is included in the Vulnerability Detection section, and 3) a Windows authentication record is defined.
enable_windows_directory_ search={**0**|1}	(Optional) Specify 1 if you've set up Windows Directory Search controls and want to include them in the scan. This custom control allows you to search for files/directories based on various criteria like file name and user access permissions.
scan_ports={standard| **targeted**}	(Required) Specify “standard” to enable standard scan of TCP ports. See Appendix B - Ports used for scanning for a list of ports used for standard scan. Specify “targeted” to perform a targeted scan. Which ports are included in a targeted scan? For Unix hosts, these well known ports are scanned: 22 (SSH), 23 (telnet) and 513 (rlogin). Any one of these services is sufficient for authentication. If services (SSH, telnet, rlogin) are not running on these well known ports for the hosts you will be scanning, specify this option and define a custom ports list in the Unix authentication record. Note: The actual ports scanned also depends on the Ports setting in the Unix authentication record. For Windows hosts, the service scans a fixed set of required Windows ports (a service defined, internal list).
mssql_db_udc_restriction={**0**| 1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom MS SQL Database checks.
mssql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256).
oracle_db_udc_restriction={**0**| 1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Oracle Database checks.

Parameter	Description
oracle_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 5000).
sybase_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Sybase Database checks.
sybase_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for Sybase is 2500 rows.
postgresql_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom PostgreSQL/Pivotal Greenplum Database checks.
postgresql_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for PostgreSQL/Pivotal Greenplum is 5000 rows.
sapiq_db_udc_restriction={**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom SAP IQ Database checks.
sapiq_db_udc_limit={value}	(Optional) Provide a value to define the number of rows to be returned per scan (default is 256). Maximum allowed limit for SAP IQ is 10000 rows.
db2_db_udc_restriction= {**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks.
db2_db_udc_limit= {value}	(Optional) The default value is 256 and maximum allowed limit is 5000 rows.
enable_auth_instance_discovery={**0**|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances. The parameters enable_auth_instance_discovery, scan_by_policy and include_system_auth are mutually exclusive and cannot be specified together in the same request. In UI, this parameter is a check box and referred to "Allow instance discovery..." in the System Authentication Records section on the New/Edit Compliance Profile page.
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. The valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle, MongoDB and MySQL. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.

Parameter	Description
ibm_was_discovery_mode={value}	(Optional to create or update option profile record) Specify ibm_was_discovery_mode=server_dir to auto discover instances at the server directory level. Specify ibm_was_discovery_mode=installation_dir to auto discover instances at the installation directory level. When unspecified and auto_auth_types=IBM WebSphere App Server, we will auto discover instances at the installation directory level. This parameter can only be specified if auto_auth_types includes IBM WebSphere App Server.
oracle_template_id={value}	(Optional) The Template ID for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
oracle_template_name={value}	(Optional) The Template Name for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.
mongodb_template_id={value}	(Optional) The Template ID for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
mongodb_template_name={val ue}	((Optional) The Template Name for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.
include_system_auth={**0**|1}	(Optional to create or update option profile record) Specify include_system_auth=1 if you have a system created auth record and user created auth record for the same instance configuration and choose which one to include for scans. When unspecified (include_system_auth=0), user record will be selected for scan by default. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. In UI, this parameter is a check box and referred to "Use System Authentication Records" in the System Authentication Records section in the Scan tab on the New/Edit Compliance Profile page.

Parameter	Description
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to include system created auth record if you have a system record and user record for the same instance configuration. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to include user created authentication record if you have a system record and user record for the same instance. The parameters use_system_auth_on_duplicate and use_user_auth_on_duplicate are mutually exclusive and can only be specified if "include_system_auth=1".
mysql_template_id={value}	(Optional) The Template ID for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.
mysql_template_name={value}	(Optional) The Template Name for the MySQL system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MySQL is specified, then mysql_template_id or mysql_template_name must also be specified.
Instance Data Collection	
enable_instance_data_collection={0|1}	(Optional) Specify 1 to enable database instance data collection by using underlying OS authentication record. By default, this option is disabled.
instance_data_collection_auth_types	(Optional) Specify the database technologies for which you want to enable OS authentication-based data collection. The valid values are: IBM DB2, InformixDB, MongoDB, MSSQL, MySQL, Oracle, Pivotal Greenplum, PostgreSQL, Sybase. You can use this parameter only if you set the value of the enable_instance_data_collection parameter to 1.
enable_os_based_instance_discovery={0|1}	(Optional) Set the value to 1 to enable technology instance data collection by using underlying OS authentication record. By default, this option is disabled.
os_based_instance_disc_technologies	(Optional) Specify a comma-separated list of technologies to enable OS authentication-based data collection. Currently we support Oracle JRE and IBM WebSphere Liberty. Hence, the valid values are: Oracle JRE and IBM WebSphere Liberty. You can use this parameter only if you set the value of the enable_os_based_instance_discovery parameter to 1.

Parameter	Description
Additional	
additional_tcp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional TCP ports. Default setting is 1.
additional_tcp_ports_ standard_scan={0|**1**}	(Optional) Specify 1 to enable standard scan of additional TCP ports. Standard Scan includes 13 ports: 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445. Default setting is 1.
additional_tcp_ports_ additional={value1,value2}	(Optional) Specify additional TCP ports to scan. You can specify up to 20 ports including the standard scan ports.
additional_udp_ports={0|**1**}	(Optional) Specify 1 to enable host discovery on additional UDP ports. Default setting is 1.
additional_udp_ports_type= {**standard**|custom}	(Optional) Specify "standard" to enable standard scan of additional UDP ports. Standard Scan includes 6 ports: 53, 111, 135, 137, 161, 500. Default is "standard". Specify "custom" to provide a custom list of ports using additional_udp_ports_custom.
additional_udp_ports_ custom={value1,value2}	(Optional) Specify additional UDP ports to scan. You can specify up to 10 ports including the standard scan ports.
icmp={0|**1**}	(Optional) Specify 1 to only discover live hosts that respond to an ICMP ping. Default setting is 1.
blocked_resources={**0**|1}	(Optional) Specify 1 in order to add ports protected by your firewall/IDS to prevent them from being scanned.
protected_ports={**default**| custom}	(Optional) Ports protected by your firewall/IDS. Specify "default" to provide a list of default blocked ports: 0-1, 111, 513-514, 2049, 4100, 6000-6005, 7100, 8000. Default setting is "default". Specify custom to provide a custom list of protected ports using protected_ports_custom.
protected_ports_custom= {value1,value2}	(Optional) Specify a custom list of protected ports.
protected_ips={**all**|custom}	(Optional) IP addresses and ranges protected by your firewall/IDS. Default is "all".
protected_ips_custom= {value1,value2}	(Optional) Specify a custom list of IP addresses and ranges protected by your firewall/IDS.
ignore_rst_packets={**0**|1}	(Optional) Specify 1 to ignore all TCP RESET packets - firewall-generated and live-host-generated.
ignore_firewall_generated_ syn_ack_packets={**0**|1}	(Optional) Specify 1 to determine if TCP SYN-ACK packets are generated by a filtering device and ignore packets that appear to originate from such devices.
not_send_ack_or_syn_ack_ packets_during_host_ discovery={**0**|1}	(Optional) Specify 1 if you do not want to send TCP ACK or SYN-ACK packets. Out of state TCP packets are not SYN packets and do not belong to an existing TCP session.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
```

```
"<username>:<password>" -d
"action=create&title=OP_agent_correlation_checked_API&global=1&sca
n_ports=targeted&enable_agent_correlation_identifier=1&agent_corre
lation_ports=10001,10002"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-09-29T13:21:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>7815368</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/pc/?action=create	Active	Active
/api/4.0/fo/subscription/option_profile/pc/?action=create	December 2025	December 2026
/api/3.0/fo/subscription/option_profile/pc/?action=create	December 2025	December 2026
/api/2.0/fo/subscription/option_profile/pc/?action=create	December 2025	December 2026

Update Compliance Option Profile

/api/2.0/fo/subscription/option_profile/pc/?action=update

For API version information, refer to API Version History section.

V 2.0|V 3.0|V 4.0| V 5.0

V 2.0

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.

For a list of optional parameters, see Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=pc-jp&id=51491401"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>51491401</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update for Database UDC

Update Option Profile with Oracle Database Preference Key

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d
"action=update&id=1709710&title=API-PC-OP-Oracle-custom-limit
&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_lim
it=100"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T06:45:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1709710</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V 3.0

/api/3.0/fo/subscription/option_profile/pc/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.

For a list of optional parameters, see Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=pc-jp&id=51491401"
"http://<qualys_base_url>/api/3.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>51491401</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update for Database UDC

Update Option Profile with Oracle Database Preference Key

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d
"action=update&id=1709710&title=API-PC-OP-Oracle-custom-limit
&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_lim
it=100"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://<qualys-
base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T06:45:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1709710</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Update Option Profile for MySQL using template name

Updating option profile with MySQL record template using template name.

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=update&title=mysql_auth_op_apiupdatqe&scan_ports=targeted&
id=2642191&mysql_template_name=Mysql_template_api&enable_auth_inst
ance_discovery=1&auto_auth_types=MySQL"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
<qualys_base_url>/api/3.0/simple_return.dtd>
```

```
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T12:19:05Z</DATETIME>
            <TEXT>Compliance Option profile successfully
updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 4.0

/api/4.0/fo/subscription/option_profile/pc/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
clean_scan_data_on_dead_hosts{0|1}	(Optional) Use this parameter to indicate whether you would like to remove compliance scan data associated with dead hosts. Enter 1 if you wish to remove the compliance data or 0 if you do not wish to remove it.
host_not_found_alive_times{value}	(Optional) Enter the number of compliance scans to wait before removing compliance data associated with dead hosts. The valid range to set a number of compliance scans to wait before removing data is 1 to 99.

For a list of optional parameters, see Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=pc-jp&id=51491401"
"http://<qualys_base_url>/api/4.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://<qualys_base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>51491401</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update for Database UDC

Update Option Profile with Oracle Database Preference Key

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X POST -d
"action=update&id=1709710&title=API-PC-OP-Oracle-custom-limit
&scan_ports=targeted&oracle_db_udc_restriction=1&oracle_db_udc_lim
it=100"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://<qualys-
base_url>/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T06:45:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1709710</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Update Option Profile for MySQL using template name

Updating option profile with MySQL record template using template name.

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=update&title=mysql_auth_op_apiupdatqe&scan_ports=targeted&
id=2642191&mysql_template_name=Mysql_template_api&enable_auth_inst
ance_discovery=1&auto_auth_types=MySQL"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
<qualys_base_url>/api/4.0/simple_return.dtd>
```

```
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T12:19:05Z</DATETIME>
            <TEXT>Compliance Option profile successfully
updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 5.0

/api/5.0/fo/subscription/option_profile/pc/?action=update

[POST]

Input Parameters

Parameter	Description
action=update	(Required)
id={value}	(Required) The ID of the option profile.
clean_scan_data_on_dead_hosts{0|1}	(Optional) Use this parameter to indicate whether you would like to remove compliance scan data associated with dead hosts. Enter 1 if you wish to remove the compliance data or 0 if you do not wish to remove it.
host_not_found_alive_times{value}	(Optional) Enter the number of compliance scans to wait before removing compliance data associated with dead hosts. The valid range to set a number of compliance scans to wait before removing data is 1 to 99.
enable_agent_correlation_identifier={1,0}	(Optional) Specify 1 to enable the Agent Correlation Identifier, else 0.
agent_correlation_ports={value}	(Optional) Enter the ports for the Agent Correlation identifier. You can enter a maximum of 5 ports.

For a list of optional parameters, see Input Parameters for Create PC Option Profile.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"<username>:<password>" -d
"action=update&title=OP_agent_correlation_unchecked_update_API&id=
7815368&enable_agent_correlation_identifier=0"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/5.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-09-29T13:23:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>7815368</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/pc/?action=update	Active	Active
/api/4.0/fo/subscription/option_profile/pc/?action=update	December 2025	June 2026
/api/3.0/fo/subscription/option_profile/pc/?action=update	December 2025	June 2026
/api/2.0/fo/subscription/option_profile/pc/?action=update	December 2025	June 2026

Compliance Option Profile List

For API version information, refer to the API Version History section.

V 2.0|V 3.0| V 4.0| V 5.0

V 2.0

/api/2.0/fo/subscription/option_profile/pc/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=list"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>19026</ID>
      <GROUP_NAME><![CDATA[Initial PC Options 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
```

```
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
      </DISSOLVABLE_AGENT>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
```

```
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>31118</ID>
      <GROUP_NAME><![CDATA[pc 55]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>10472</ID>
            <TITLE><![CDATA[jp]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
```

```
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>80,35</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>

<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51481401</ID>
      <GROUP_NAME><![CDATA[pc op - 1]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
```

```
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>14487</ID>
            <TITLE><![CDATA[jp2]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
```

```
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>

<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51491401</ID>
      <GROUP_NAME><![CDATA[pc op - 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <STANDARD_SCAN>1</STANDARD_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
```

```
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>14661401</ID>
            <TITLE><![CDATA[policy - 2]]></TITLE>
          </POLICY>
          <POLICY>
            <ID>14651401</ID>
            <TITLE><![CDATA[policy - 1]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <CUSTOM_PORT><![CDATA[37,53,68,69,111]]></CUSTOM_PORT>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
        <CUSTOM_PORT_LIST><![CDATA[111]]></CUSTOM_PORT_LIST>
        <CUSTOM_IP_LIST><![CDATA[10.10.10.6]]></CUSTOM_IP_LIST>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - List Option Profile for Database UDCs

List the database preference key setting and it's corresponding value in Option Profile for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X -d "action=list&id=1710150"
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/2.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>1710150</ID>
      ...
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <DATABASE_PREFERENCE_KEY>
        <MSSQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>250</DB_UDC_LIMIT>
        </MSSQL>
        <ORACLE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>10</DB_UDC_LIMIT>
        </ORACLE>
        <SYBASE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
        </SYBASE>
        <POSTGRESQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>2500</DB_UDC_LIMIT>
        </POSTGRESQL>
        <DB2>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>300</DB_UDC_LIMIT>
        </DB2>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
```

```
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    ...
</OPTION_PROFILES>
```

DTD

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

V 3.0

/api/3.0/fo/subscription/option_profile/pc/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=list"
"http://<qualys_base_url>/api/3.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://<qualys_base_url>/api/3.0/fo/subscription/option_profile/o
ption_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>19026</ID>
      <GROUP_NAME><![CDATA[Initial PC Options 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
```

```
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
      </DISSOLVABLE_AGENT>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>
```

```
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>31118</ID>
      <GROUP_NAME><![CDATA[pc 55]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>10472</ID>
            <TITLE><![CDATA[jp]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
```

```
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>80,35</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51481401</ID>
      <GROUP_NAME><![CDATA[pc op - 1]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
```

```
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>14487</ID>
            <TITLE><![CDATA[jp2]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
```

```
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51491401</ID>
      <GROUP_NAME><![CDATA[pc op - 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <STANDARD_SCAN>1</STANDARD_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>14661401</ID>
```

```
            <TITLE><![CDATA[policy - 2]]></TITLE>
          </POLICY>
          <POLICY>
            <ID>14651401</ID>
            <TITLE><![CDATA[policy - 1]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <CUSTOM_PORT><![CDATA[37,53,68,69,111]]></CUSTOM_PORT>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
        <CUSTOM_PORT_LIST><![CDATA[111]]></CUSTOM_PORT_LIST>
        <CUSTOM_IP_LIST><![CDATA[10.10.10.6]]></CUSTOM_IP_LIST>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - List Option Profile for Database UDCs

List the database preference key setting and it's corresponding value in Option Profile for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X -d "action=list&id=1710150"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>1710150</ID>
      ...
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <DATABASE_PREFERENCE_KEY>
        <MSSQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>250</DB_UDC_LIMIT>
        </MSSQL>
        <ORACLE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>10</DB_UDC_LIMIT>
        </ORACLE>
        <SYBASE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
        </SYBASE>
        <POSTGRESQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>2500</DB_UDC_LIMIT>
        </POSTGRESQL>
        <DB2>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>300</DB_UDC_LIMIT>
        </DB2>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    ...
</OPTION_PROFILES>
```

Sample: List Option Profile for MySQL template

List the option profile with MySQL record template using template name.

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&id=2642191"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM https://
<qualys_base_url>/api/3.0/fo/subscription/option_profile/option_pr
ofile_info.dtd>
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>2642191</ID>
                <GROUP_NAME>
                    <![CDATA[mysql_auth_op_apiupdatqe]]>
                </GROUP_NAME>
                <GROUP_TYPE>compliance</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[s m (username)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>316805</SUBSCRIPTION_ID>
                <IS_GLOBAL>0</IS_GLOBAL>
                <UPDATE_DATE>2024-07-15T12:19:03Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TARGETED_SCAN>1</TARGETED_SCAN>
                </PORTS>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                       <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
```

```
ISCOVERY>                </PERFORMANCE>
                <DISSOLVABLE_AGENT>

<DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
                  <PASSWORD_AUDITING_ENABLE>
<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
                  </PASSWORD_AUDITING_ENABLE>
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
                </DISSOLVABLE_AGENT>
                <SYSTEM_AUTH_RECORD>
                    <ALLOW_AUTH_CREATION>
                        <AUTHENTICATION_TYPE_LIST>

<AUTHENTICATION_TYPE>MySQL</AUTHENTICATION_TYPE>
                        </AUTHENTICATION_TYPE_LIST>
                        <MYSQL_AUTHENTICATION_TEMPLATE>
                            <ID>5144731</ID>
                            <TITLE>Mysql_template_api</TITLE>
                        </MYSQL_AUTHENTICATION_TEMPLATE>
                    </ALLOW_AUTH_CREATION>
                </SYSTEM_AUTH_RECORD>
                <FILE_INTEGRITY_MONITORING>
<AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
                </FILE_INTEGRITY_MONITORING>
                <CONTROL_TYPES>
                    <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>

<CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
                </CONTROL_TYPES>
            </SCAN>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
```

```
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
            <INSTANCE_DATA_COLLECTION />
            <OS_BASED_INSTANCE_DISC_COLLECTION />
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

DTD

<platform API server>/api/3.0/fo/subscription/option_profile/option_profile_info.dtd

V 4.0

/api/4.0/fo/subscription/option_profile/pc/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for Create PC Option Profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=list"
"http://<qualys_base_url>/api/4.0/fo/subscription/option_profile/p
c/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://<qualys_base_url>/api/4.0/fo/subscription/option_profile/o
ption_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>19026</ID>
      <GROUP_NAME><![CDATA[Initial PC Options 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
```

```
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
      </DISSOLVABLE_AGENT>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
```

```
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>31118</ID>
      <GROUP_NAME><![CDATA[pc 55]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>10472</ID>
            <TITLE><![CDATA[jp]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
```

```
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>1</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>80,35</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51481401</ID>
      <GROUP_NAME><![CDATA[pc op - 1]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
```

```
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>1</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
          <HTTP_PROCESSES>15</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Short</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
          <POLICY>
            <ID>14487</ID>
            <TITLE><![CDATA[jp2]]></TITLE>
          </POLICY>
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
          <TCP_ADDITIONAL>
            <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
            <ADDITIONAL_PORTS>1</ADDITIONAL_PORTS>
          </TCP_ADDITIONAL>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <BLOCK_RESOURCES>
<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PO
```

```
RTS>
        <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
      </BLOCK_RESOURCES>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>51491401</ID>
      <GROUP_NAME><![CDATA[pc op - 2]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Smith (jsmith_ap)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>10421401</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-04-10T11:10:36Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <STANDARD_SCAN>1</STANDARD_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>10</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <SCAN_RESTRICTION>
        <SCAN_BY_POLICY>
```

```
            <POLICY>
              <ID>14661401</ID>
              <TITLE><![CDATA[policy - 2]]></TITLE>
            </POLICY>
            <POLICY>
              <ID>14651401</ID>
              <TITLE><![CDATA[policy - 1]]></TITLE>
            </POLICY>
          </SCAN_BY_POLICY>
        </SCAN_RESTRICTION>
        <FILE_INTEGRITY_MONITORING>
          <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
        </FILE_INTEGRITY_MONITORING>
      </SCAN>
      <ADDITIONAL>
        <HOST_DISCOVERY>
          <TCP_PORTS>
            <STANDARD_SCAN>1</STANDARD_SCAN>
          </TCP_PORTS>
          <UDP_PORTS>
            <CUSTOM_PORT><![CDATA[37,53,68,69,111]]></CUSTOM_PORT>
          </UDP_PORTS>
          <ICMP>1</ICMP>
        </HOST_DISCOVERY>
        <BLOCK_RESOURCES>
          <CUSTOM_PORT_LIST><![CDATA[111]]></CUSTOM_PORT_LIST>
          <CUSTOM_IP_LIST><![CDATA[10.10.10.6]]></CUSTOM_IP_LIST>
        </BLOCK_RESOURCES>
        <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
        </PACKET_OPTIONS>
      </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - List Option Profile for Database UDCs

List the database preference key setting and it's corresponding value in Option Profile for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

API request:

```
curl -u "username:password" -H "X-Requested-With:curl" -H
"Content-type: text/xml" -X -d "action=list&id=1710150"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>1710150</ID>
      ...
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION>
      <DATABASE_PREFERENCE_KEY>
        <MSSQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>250</DB_UDC_LIMIT>
        </MSSQL>
        <ORACLE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>10</DB_UDC_LIMIT>
        </ORACLE>
        <SYBASE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
        </SYBASE>
        <POSTGRESQL>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>2500</DB_UDC_LIMIT>
        </POSTGRESQL>
        <DB2>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>300</DB_UDC_LIMIT>
        </DB2>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    ...
```

```
</OPTION_PROFILES>
```

Sample: List Option Profile for MySQL template

List the option profile with MySQL record template using template name.

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&id=2642191"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM https://
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_pr
ofile_info.dtd>
    <OPTION_PROFILES>
        <OPTION_PROFILE>
            <BASIC_INFO>
                <ID>2642191</ID>
                <GROUP_NAME>
                    <![CDATA[mysql_auth_op_apiupdatqe]]>
                </GROUP_NAME>
                <GROUP_TYPE>compliance</GROUP_TYPE>
                <USER_ID>
                    <![CDATA[s m (username)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>316805</SUBSCRIPTION_ID>
                <IS_GLOBAL>0</IS_GLOBAL>
                <UPDATE_DATE>2024-07-15T12:19:03Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <TARGETED_SCAN>1</TARGETED_SCAN>
                </PORTS>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>

<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                       <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>10</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
```

```
                <PACKET_DELAY>Medium</PACKET_DELAY>
<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>                </PERFORMANCE>
                <DISSOLVABLE_AGENT>

<DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
                    <PASSWORD_AUDITING_ENABLE>
<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
                    </PASSWORD_AUDITING_ENABLE>
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
                </DISSOLVABLE_AGENT>
                <SYSTEM_AUTH_RECORD>
                    <ALLOW_AUTH_CREATION>
                        <AUTHENTICATION_TYPE_LIST>

<AUTHENTICATION_TYPE>MySQL</AUTHENTICATION_TYPE>
                        </AUTHENTICATION_TYPE_LIST>
                        <MYSQL_AUTHENTICATION_TEMPLATE>
                            <ID>5144731</ID>
                            <TITLE>Mysql_template_api</TITLE>
                        </MYSQL_AUTHENTICATION_TEMPLATE>
                    </ALLOW_AUTH_CREATION>
                </SYSTEM_AUTH_RECORD>
                <FILE_INTEGRITY_MONITORING>
<AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
                </FILE_INTEGRITY_MONITORING>
                <CONTROL_TYPES>
                    <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>

<CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
                </CONTROL_TYPES>
            </SCAN>
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
```

```
D_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
            <INSTANCE_DATA_COLLECTION />
            <OS_BASED_INSTANCE_DISC_COLLECTION />
        </OPTION_PROFILE>
    </OPTION_PROFILES>
```

DTD

<platform API server>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd

V 5.0

/api/5.0/fo/subscription/option_profile/pc/?action=list

[GET] [POST]

Input Parameters

All option profiles are fetched if no parameters are given. To fetch a specific option profile, provide the "id" or "title" parameter with the option profile id or title of interest. Optionally, you can filter the results by using optional parameters listed under Input Parameters for Create PC Option Profile.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"<username>:<password> -d "action=list&id=7816368"
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"<qualys_base_url>/api/5.0/fo/subscription/option_profile/option_p
rofile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>7816368</ID>

<GROUP_NAME><![CDATA[OP_agent_correlation_checked_update_API]]></G
ROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[John Doe (<username>)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>4027198</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
```

```
      <UPDATE_DATE>2025-09-29T14:27:53Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_D
ISCOVERY>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABL
E>
      </DISSOLVABLE_AGENT>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
```

```
            <STANDARD_SCAN>1</STANDARD_SCAN>
          </TCP_PORTS>
          <UDP_PORTS>
            <STANDARD_SCAN>1</STANDARD_SCAN>
          </UDP_PORTS>
          <ICMP>1</ICMP>
        </HOST_DISCOVERY>
        <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>
          <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
        </PACKET_OPTIONS>
        <AGENT_CORRELATION_IDENTIFIER>

<IS_AGENT_CORRELATION_ID_ENABLED>1</IS_AGENT_CORRELATION_ID_ENABLE
D>

<AGENT_CORRELATION_ID_PORTS>10001</AGENT_CORRELATION_ID_PORTS>
        </AGENT_CORRELATION_IDENTIFIER>
      </ADDITIONAL>
      <INSTANCE_DATA_COLLECTION />
      <OS_BASED_INSTANCE_DISC_COLLECTION />
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

DTD

<platform API server>/api/5.0/fo/subscription/option_profile/option_profile_info.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/pc/?action=list	Active	Active
/api/4.0/fo/subscription/option_profile/pc/?action=list	December 2025	June 2026

API Version	EOS	EOL
/api/3.0/fo/subscription/option_profile/pc/?action=list	December 2025	June 2026
/api/2.0/fo/subscription/option_profile/pc/?action=list	December 2025	June 2026

Delete Compliance Option Profile

For API version information, refer to the API Version History section.

V 2.0|V 3.0| V 4.0|V 5.0

V 2.0

/api/2.0/fo/subscription/option_profile/pc/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=delete&id=51491401"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T11:10:36Z</DATETIME>
    <TEXT>Option Profile Deleted Successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>51491401</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
```

```
</SIMPLE_RETURN>
```

V 3.0

/api/3.0/fo/subscription/option_profile/pc/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"quay_sm:Qatemp123#" -d "action=delete&id=2642191"
"https://<qualys_base_url>/api/3.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
<qualys_base_url>/api/3.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-23T07:39:39Z</DATETIME>
            <TEXT>Option Profile Deleted Successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 4.0

/api/4.0/fo/subscription/option_profile/pc/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"quay_sm:Qatemp123#" -d "action=delete&id=2642191"
"https://<qualys_base_url>/api/4.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
<qualys_base_url>/api/4.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-23T07:39:39Z</DATETIME>
            <TEXT>Option Profile Deleted Successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

V 5.0

/api/5.0/fo/subscription/option_profile/pc/?action=delete

[GET] [POST]

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) The ID of the option profile.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"<username>:<password>" -d "action=delete&id=2642191"
"https://<qualys_base_url>/api/5.0/fo/subscription/option_profile/
pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM https://
<qualys_base_url>/api/5.0/simple_return.dtd>
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-23T07:39:39Z</DATETIME>
            <TEXT>Option Profile Deleted Successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>2642191</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/5.0/fo/subscription/option_profile/pc/?action=delete	Active	Active
/api/4.0/fo/subscription/option_profile/pc/?action=delete	December 2025	June 2026
/api/3.0/fo/subscription/option_profile/pc/?action=delete	December 2025	June 2026
/api/2.0/fo/subscription/option_profile/pc/?action=delete	December 2025	June 2026

KnowledgeBase

For API version information, refer to the API Version History section.

V2.0 |V3.0 | V4.0

V2.0

/api/2.0/fo/knowledge_base/vuln/?action=list

[GET] [POST]

Download a list of vulnerabilities from Qualys' KnowledgeBase. Several input parameters grant users control over which vulnerabilities to download and the amount of detail to download, and the XML output provides a rich information source for each vulnerability.

Qualys' Sofware-as-a-Service (SaaS) technology includes its KnowledgeBase, with the industry's largest number of vulnerability signatures, that is continuously updated by Qualys' Research and Development team. Qualys is fully dedicated to providing the most accurate security audits in the industry. Each day new and updated signatures are tested in Qualys' own vulnerability labs and then published, making them available to Qualys customers. When Threat Protection is enabled for your subscription, the output will include Samples - Lists the QIDs that exactly matches the given CVE. associated with vulnerabilities.

Authorized Qualys users have the ability to download vulnerability data using the KnowledgeBase API. Please contact Qualys Support or your sales representative if you would like to obtain authorization for your subscription.

Permissions - Your subscription must be granted permission to run this API function. Please contact Qualys Support or your sales representative to receive this authorization.

Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.
Auditor	No permission to download vulnerability data from the KnowledgeBase.

Input Parameters

Several optional input parameters may be specified. When unspecified, the XML output includes all vulnerabilities in the KnowledgeBase, showing basic details for each vulnerability. Several optional parameters allow you specify filters. When filter parameters are specified, these parameters are ANDed by the service to filter the data from the output.

Parameter	Description
action=list	(Required)
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).

Parameter	Description
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each vulnerability in the XML output. A valid value is: Basic (default), All, or None. Basic includes basic elements plus CVSS Base and Temporal scores. All includes all vulnerability details, including the Basic details.
ids={value}	(Optional) Used to filter the XML output to include only vulnerabilities that have QID numbers matching the QID numbers you specify. **Notes**: - If the QID numbers and number range specified are too large, it is recommended to use `id_min={value}` and `id_max={value}` parameters. - The query string length ranges from 8000 to 10,000 QIDs (Characters). If the length exceeds 10,000, the API may not return a response.
id_min={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number greater than or equal to a QID number you specify.
id_max={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number less than or equal to a QID number you specify.
is_patchable={**0**|1}	(Optional) Used to filter the XML output to show only vulnerabilities that are patchable or not patchable. A vulnerability is considered patchable when a patch exists for it. When 1 is specified, only vulnerabilities that are patchable will be included in the output. When 0 is specified, only vulnerabilities that are not patchable will be included in the output. When unspecified, patchable and unpatchable vulnerabilities will be included in the output.
last_modified_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified after a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified before a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).

Parameter	Description
last_modified_by_user_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_user_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
published_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities published after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
published_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities published before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
discovery_method={value}	(Optional) Used to filter the XML output to show only vulnerabilities assigned a certain discovery method. A valid value is: Remote, Authenticated, RemoteOnly, AuthenticatedOnly, or RemoteAndAuthenticated. When "Authenticated" is specified, the service shows vulnerabilities that have at least one associated authentication type. Vulnerabilities that have at least one authentication type can be detected in two ways: 1) remotely without using authentication, and 2) using authentication.
discovery_auth_types={value}	(Optional) Used to filter the XML output to show only vulnerabilities having one or more authentication types. A valid value is: Windows, Oracle, Unix, SNMP, DB2, HTTP, PANOS, TOMCAT, MARIADB, MongoDB, WEBLOGIC, MySQL, VMware. Multiple values should be comma-separated.

Parameter	Description
show_pci_reasons={**0**|1}	(Optional) Used to filter the XML output to show reasons for passing or failing PCI compliance (when the CVSS Scoring feature is turned on in the user's subscription). Specify 1 to view the reasons in the XML output. When unspecified, the reasons are not included in the XML output.
show_supported_modules_info={**0**|1}	(Optional) Used to filter the XML output to show Qualys modules that can be used to detect each vulnerability. Specify 1 to view supported modules in the XML output. When unspecified, supported modules are not included in the XML output.
show_disabled_flag={**0**|1}	(Optional) Specify 1 to include the disabled flag for each vulnerability in the XML output.
show_qid_change_log={**0**|1}	(Optional) Specify 1 to include QID changes for each vulnerability in the XML output.
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).

Samples - Lists the QIDs that exactly matches the given CVE.

API Request

```
curl --location --request POST
'qualys_base_url/api/2.0/fo/knowledge_base/vuln/index.php?action=
list&cve=CVE-1999-0527' \--header 'X-Requested-With: curl demo2' \--
header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"qualys_base_url/api/2.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_
output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-11-24T06:37:11Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>27002</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Writeable Root Directory on FTP Server]]>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2009-07-
```

```
08T17:28:46Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-0527]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <!CDATA>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <!CDATA>
                </CONSEQUENCE>
                <SOLUTION>
                    <!CDATA>
                </SOLUTION>
                <CVSS>
                    <BASE>10.0</BASE>
                    <TEMPORAL>8.6</TEMPORAL>
                                </VULN>
            <VULN>
                <QID>27005</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>
                    <!CDATA>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2020-11-
23T18:43:15Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]> .......

      </VULN_LIST>
</RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - List all the QIDs for the code modified before and after specific date.

API Request:

```
curl --location
```

```
'qualys_base_url/api/2.0/fo/knowledge_base/vuln/?ids=12136&code_modified_
before=2000-01-02&action=list&code_modified_after=2023-08-26' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"https://qualys_base_url/api/2.0/fo/knowledge_base/vuln/knowledge_base_vu
ln_list_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-11-29T07:27:37Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>994430</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                  <![CDATA[Python (Pip) Security Update for cobbler (GHSA-
96hw-v598-jvgh)]]>
                </TITLE>
                <CATEGORY>SCA</CATEGORY>
                <TECHNOLOGY>
                    <![CDATA[JAVA 8,Python 3.11]]>
                </TECHNOLOGY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2023-10-
27T05:33:30Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2023-07-
27T13:31:29Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2023-07-
27T13:31:29Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[pip]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[pip]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[GHSA-96hw-v598-jvgh]]>
                        </ID>
                        <URL>
                            <![CDATA[https://github.com/advisories/GHSA-
96hw-v598-jvgh]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
```

```
                    <CVE_LIST>
                        <CVE>
                            <ID>
                                <![CDATA[CVE-2017-1000469]]>
                            </ID>
                            <URL>
                                <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2017-1000469]]>
                            </URL>
                        </CVE>
                    </CVE_LIST>
</VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Real-Time Threat Indicators (RTIs)

The KnowledgeBase list output includes Real-Time Threat Indicators (RTIs) associated with each vulnerability. RTIs appear as part of vulnerability details under THREAT_INTELLIGENCE. Please note that RTIs are only visible when Threat Protection is enabled for the subscription.

Real-Time Threat Indicators are described below.

RTI (ID)	Description
Zero_Day (1)	Active attack has been observed in the wild and there is no patch from the vendor. An active attack is a prerequisite for this RTI in addition to no patch from the vendor. If a vulnerability is not actively attacked this RTI will not be set (even if there is no patch from the vendor). If a patch becomes available Qualys will remove the Zero Day RTI attribute which helps users to focus only on vulnerabilities that are actively exploited and there is no official patch.
Exploit_Public (2)	Exploit knowledge is well known and a working exploitation code is publicly available. Potential of active attacks is very high. This attribute is set for example when PoC exploit code is available from Exploit-DB, Metasploit, Core, Immunity or other exploit vendors. This RTI does not necessarily indicate that active attacks have been observed in the wild.
Active_Attacks (3)	Active attacks have been observed in the wild. This information is derived from Malware, Exploit Kits, acknowledgment from vendors, US-CERT and similar trusted sources. If there are no patches, Qualys will mark it as Zero Day, in addition, to actively attacked.
High_Lateral_Movement (4)	After a successful compromise, the attacker has high potential to compromise other machines in the network.
Easy_Exploit (5)	The attack can be carried out easily and requires little skills or does not require additional information.
High_Data_Loss (6)	Successful exploitation will result in massive data loss on the host.

RTI (ID)	Description
Denial_of_Service (7)	Successful exploitation will result in denial of service.
No_Patch (8)	The vendor has not provided an official fix.
Malware (9)	Malware has been associated with the vulnerability.
Exploit_Kit (10)	Exploit Kit has been associated with this vulnerability. Exploit Kits are usually cloud based toolkits that help malware writers in identifying vulnerable browsers/plugins and install malware. Users can also search on Exploit Kit name like Angler, Nuclear, Rig and others.
Wormable (11)	Wormable has been associated with this vulnerability. The vulnerability can be used in “worms” - malware that spreads itself without user interaction.
Predicted_High_Risk (12)	Predicted High Risk has been associated with this vulnerability. Qualys Machine Learning Model predicted this vulnerability as a High Risk based on various data sources including NVD, Social network, Dark web, Security Blogs, Code repository, Exploits, etc.
Privilege_Escalation (13)	Successful exploitation allows an attacker to gain elevated privileges.
Unauthenticated_Exploitation (14)	Exploitation of this vulnerability does not require authentication.
Remote_Code_Execution (15)	Successful exploitation allows an attacker to execute arbitrary commands or code on a targeted system or in a target process.
Ransomware (16)	This vulnerability has been exploited in attack vectors where ransomware has been deployed. In other words, this vulnerability is associated with known ransomware.
Solorigate_Sunburst (17)	Solorigate Sunburst has been associated with all the CVEs, used by FireEye's Red Team tools to test the security of their client environments and compromised versions of SolarWinds Orion.
CISA Known Exploited Vulnerabilities (18)	CISA maintains a catalog of the top publicly known vulnerabilities being exploited in the wild and organizations (referred as CISA Known Exploitable Vulnerabilities) are advised to patch affected systems on priority. This RTI indicates that the vulnerability is associated with the CISA catalog and with CVE mappings to respective QIDs. We will add the CISA Known Exploited Vulnerabilities to QIDs within 24hrs of CISA catalog updates with new CVEs. This CISA Directive recommends urgent and prioritized remediation of the vulnerabilities that adversaries are actively exploiting. The timelines are available in CISA's Catalog for each of the CVEs.

Samples

Sample 1 - Request all vulnerabilities in the KnowledgeBase showing basic details:

```
curl -u "<username>:<password>" -H "X-Requested-With: Curl" -X "POST"
-d "action=list" "<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/" >
output.txt
```

Sample 2 - Request patchable vulnerabilities that have QIDs 1-200 showing all details:

```
curl -u "<username>:<password>" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&ids=1-200&is_patchable=1&details=All"
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/" > output.txt
```

Sample 3 - Request vulnerabilities that were last modified by the service after July 20, 2011 and that have the “remote and authenticated” discovery method:

```
curl -u "<username>:<password>" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&last_modified_by_service_after=2011-07-20
&discovery_method=RemoteAndAuthenticated"
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/" > output.txt
```

DTD

<platform API server>/api/2.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd

V3.0

/api/3.0/fo/knowledge_base/vuln/?action=list

[GET] [POST]

Download a list of vulnerabilities from Qualys’ KnowledgeBase. Several input parameters grant users control over which vulnerabilities to download and the amount of detail to download, and the XML output provides a rich information source for each vulnerability.

Qualys’ Sofware-as-a-Service (SaaS) technology includes its KnowledgeBase, with the industry’s largest number of vulnerability signatures, that is continuously updated by Qualys’ Research and Development team. Qualys is fully dedicated to providing the most accurate security audits in the industry. Each day new and updated signatures are tested in Qualys’ own vulnerability labs and then published, making them available to Qualys customers. When Threat Protection is enabled for your subscription, the output will include Samples - Lists the QIDs that exactly matches the given CVE. associated with vulnerabilities.

Authorized Qualys users have the ability to download vulnerability data using the KnowledgeBase API. Please contact Qualys Support or your sales representative if you would like to obtain authorization for your subscription.

Permissions - Your subscription must be granted permission to run this API function. Please contact Qualys Support or your sales representative to receive this authorization.

Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.
Auditor	No permission to download vulnerability data from the KnowledgeBase.

Input Parameters

Several optional input parameters may be specified. When unspecified, the XML output includes all vulnerabilities in the KnowledgeBase, showing basic details for each vulnerability. Several optional parameters allow you specify filters. When filter parameters are specified, these parameters are ANDed by the service to filter the data from the output.

Parameter	Description
action=list	(Required)
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each vulnerability in the XML output. A valid value is: Basic (default), All, or None. Basic includes basic elements plus CVSS Base and Temporal scores. All includes all vulnerability details, including the Basic details.
ids={value}	(Optional) Used to filter the XML output to include only vulnerabilities that have QID numbers matching the QID numbers you specify. **Notes**: - If the QID numbers and number range specified are too large, it is recommended to use `id_min={value}` and `id_max={value}` parameters. - The query string length ranges from 8000 to 10,000 QIDs (Characters). If the length exceeds 10,000, the API may not return a response.
id_min={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number greater than or equal to a QID number you specify.

Parameter	Description
id_max={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number less than or equal to a QID number you specify.
is_patchable={**0**|1}	(Optional) Used to filter the XML output to show only vulnerabilities that are patchable or not patchable. A vulnerability is considered patchable when a patch exists for it. When 1 is specified, only vulnerabilities that are patchable will be included in the output. When 0 is specified, only vulnerabilities that are not patchable will be included in the output. When unspecified, patchable and unpatchable vulnerabilities will be included in the output.
last_modified_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified after a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified before a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_user_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_user_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
published_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities published after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).

Parameter	Description
published_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities published before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
discovery_method={value}	(Optional) Used to filter the XML output to show only vulnerabilities assigned a certain discovery method. A valid value is: Remote, Authenticated, RemoteOnly, AuthenticatedOnly, or RemoteAndAuthenticated. When "Authenticated" is specified, the service shows vulnerabilities that have at least one associated authentication type. Vulnerabilities that have at least one authentication type can be detected in two ways: 1) remotely without using authentication, and 2) using authentication.
discovery_auth_types={value}	(Optional) Used to filter the XML output to show only vulnerabilities having one or more authentication types. A valid value is: Windows, Oracle, Unix, SNMP, DB2, HTTP, PANOS, TOMCAT, MARIADB, MongoDB, WEBLOGIC, MySQL, VMware. Multiple values should be comma-separated.
show_pci_reasons={**0**|1}	(Optional) Used to filter the XML output to show reasons for passing or failing PCI compliance (when the CVSS Scoring feature is turned on in the user's subscription). Specify 1 to view the reasons in the XML output. When unspecified, the reasons are not included in the XML output.
show_supported_modules_info={**0**|1}	(Optional) Used to filter the XML output to show Qualys modules that can be used to detect each vulnerability. Specify 1 to view supported modules in the XML output. When unspecified, supported modules are not included in the XML output.
show_disabled_flag={**0**|1}	(Optional) Specify 1 to include the disabled flag for each vulnerability in the XML output.
show_qid_change_log={**0**|1}	(Optional) Specify 1 to include QID changes for each vulnerability in the XML output.
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).

Sample - Lists the QIDs that exactly matches the given CVE.

API Request

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/index.php?action=list&c
ve=CVE-1999-0527' \
--header 'X-Requested-With: curl demo2' \
```

```
--header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-10-28T07:21:55Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>27002</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Writeable Root Directory on FTP Server]]>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2009-07-
08T17:28:46Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-0527]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[The FTP server has a world writeable root
directory.  The root directory of your FTP server can therefore be
written-to by any user.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Writeable FTP servers are commonly abused by
unauthorized users to upload movies, pornography, pirated software and
other &amp;quot;warez&amp;quot;. Sometimes the secondary storage is completely
filled up resulting in performance degradation or even complete failure.
<P>For some FTP servers, the FTP root directory contains configuration
files. Allowing write permissions may allow an anonymous user to overwrite
these configuration files.
<P>In addition for UNIX, unauthorized users could place a
&amp;quot;.forward&amp;quot; or an &amp;quot;.rhosts&amp;quot; file in this directory.
&amp;quot;.forward&amp;quot; files may contain commands to be executed each time
the anonymous user receives an e-mail message.  &amp;quot;.rhosts&amp;quot; files
contain hostnames from which any user will be able to connect to this host
```

without a password. Thus, the unauthorized user can add the .rhosts file using their own hostname. They can then log in with rsh, rlogin or rexec service. These two files are commonly used to compromise servers.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Disable write access for unauthorized users in the root directory of the FTP server.
<P>For UNIX:
$ chmod o-w path/to/ftp/root/directory
<P>For Microsoft IIS 6:
1. Click Start, point to Administrative Tools, and then click Internet Information Services (IIS).
2. In IIS Manager, expand the local computer, expand the FTP Sites folder, right-click the FTP site in question, and click Properties.
3. Click the Home Directory tab and deselect the Write checkbox; click OK.
4. For advanced permissions, refer to step 2 and click Permissions instead of Properties; then click Advanced Permissions.
<P> For other versions of IIS, please refer to the Microsoft website.
]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="6">
                        <![CDATA[High_Data_Loss]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="7">
                        <![CDATA[Denial_of_Service]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="14">
                        <![CDATA[Unauthenticated_Exploitation]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>27005</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>

```
                    <![CDATA[World Readable and Writable Directory on
Anonymous FTP]]>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2020-11-
23T18:43:15Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-0527]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Your FTP server contains a directory with
dangerous permissions. This directory is world writable and world
readable.  If this is an incoming directory, users should not be able to
list the it's contents.
]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[Unauthorized users can write to your FTP
server. This FTP directory can be used as a pirate software repository or
for adult picture exchanges. You also run the risk of receiving virus or
Trojan programs. Do not run unknown files from this area. ]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Unless they are required, remove the
directories. Otherwise, make sure that no hidden directories are used for
illegal purposes.  These hidden directories may be named with control
characters or begin with a dot (.), making it harder to detect and remove
them.
<P>
Frequently monitor your FTP server directories. You can schedule a
repetitive task with the cron command under Unix, which will execute the
following command every week:
<P><DL><DD>find ~ftp/ -print</DD></DL><P>
This will regularly inform you of all files in this area, and advise you
whether or not they are writeable and readable.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
```

```
                    </THREAT_INTEL>
                    <THREAT_INTEL id="6">
                        <![CDATA[High_Data_Loss]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="7">
                        <![CDATA[Denial_of_Service]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="14">
                        <![CDATA[Unauthenticated_Exploitation]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
...
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - List all the QIDs for the code modified before and after specific date.

API Request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?null=null&code_modifie
d_before=2024-10-28&action=list&code_modified_after=2024-10-27' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-10-28T07:32:48Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>152263</QID>
                <VULN_TYPE>Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[WordPress Unseen Blog Theme: PHP Object
Injection Vulnerability (CVE-2024-7432)]]>
```

```
                </TITLE>
                <CATEGORY>Web Application</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-10-
27T18:12:51Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-10-
27T15:03:21Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-10-
27T15:03:21Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[None]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[wordpress]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Unseen Blog Changelog]]>
                        </ID>
                        <URL>
<![CDATA[https://ultrapress.org/changelog/]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-7432]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-7432]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                 <![CDATA[WordPress Unseen Blog is a free WordPress theme
which is light weight, super fast, fully customizable, easy to use and is
best for lead generation for any coaching business. <P>
Unseen Blog Theme is vulnerable to PHP Object Injection.<P>
Affected Versions:<BR> WordPress Unseen Blog Theme versions up to and
including 1.0.0<P>
QID Detection Logic:<BR> This QID sends a HTTP GET request and checks for
vulnerable version of Unseen Blog theme running on the target
application.<P>]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could allow authenticated attackers with Contributor-level access and
```

```
above to inject a PHP Object. No known POP chain is present in the
vulnerable software. If a POP chain is present via an additional plugin or
theme installed on the target system, it could allow the attacker to
delete arbitrary files, retrieve sensitive data, or execute code.<P>]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Customers are advised to refer to <A
HREF="https://ultrapress.org/changelog/" TARGET="_blank">Unseen Blog
Theme Changelog</A> for updates to remediate this vulnerability.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="6">
                        <![CDATA[High_Data_Loss]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="7">
                        <![CDATA[Denial_of_Service]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>152299</QID>
                <VULN_TYPE>Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[WordPress Pretix Widget Plugin: Local File
Inclusion Vulnerability (CVE-2024-9575)]]>
                </TITLE>
                <CATEGORY>Web Application</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-10-
27T18:09:47Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-10-
27T15:39:56Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-10-
27T15:39:56Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2024-10-
10T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[None]]>
```

```
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[wordpress]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Pretix Widget Changelog]]>
                        </ID>
                        <URL>
<![CDATA[https://wordpress.org/plugins/pretix-widget/#developers]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-9575]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-9575]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                   <![CDATA[The pretix widget allows us to easily display
pretix ticket widgets on a website by customizing the display of any
pretix tickets and providing a seamless ticket booking experience for
users. <P>
WordPress pretix widget plugin is vulnerable to Local File Inclusion
vulnerability in Windows.<P>
Affected Versions:<BR> pretix widget plugin versions starting from 1.0.0
up to, and including 1.0.5<P>
QID Detection Logic:<BR> This QID sends a HTTP GET request and checks for
vulnerable version of pretix widget plugin running on the target
application.<P>]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could allow unauthenticated attacker to cause arbitrary .php files of the
system to be included on the page, including possible directory
traversal.<P>]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Customers are advised to upgrade to <A
HREF="https://latepoint.com/changelog/" TARGET="_blank">pretix widget
plugin 1.0.6</A> or later version to remediate this vulnerability.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="5">
```

```
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                    <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Real-Time Threat Indicators (RTIs)

The KnowledgeBase list output includes Real-Time Threat Indicators (RTIs) associated with each vulnerability. RTIs appear as part of vulnerability details under THREAT_INTELLIGENCE. Please note that RTIs are only visible when Threat Protection is enabled for the subscription.

Real-Time Threat Indicators are described below.

RTI (ID)	Description
Zero_Day (1)	Active attack has been observed in the wild and there is no patch from the vendor. An active attack is a prerequisite for this RTI in addition to no patch from the vendor. If a vulnerability is not actively attacked this RTI will not be set (even if there is no patch from the vendor). If a patch becomes available Qualys will remove the Zero Day RTI attribute which helps users to focus only on vulnerabilities that are actively exploited and there is no official patch.
Exploit_Public (2)	Exploit knowledge is well known and a working exploitation code is publicly available. Potential of active attacks is very high. This attribute is set for example when PoC exploit code is available from Exploit-DB, Metasploit, Core, Immunity or other exploit vendors. This RTI does not necessarily indicate that active attacks have been observed in the wild.
Active_Attacks (3)	Active attacks have been observed in the wild. This information is derived from Malware, Exploit Kits, acknowledgment from vendors, US-CERT and similar trusted sources. If there are no patches, Qualys will mark it as Zero Day, in addition, to actively attacked.
High_Lateral_Movement (4)	After a successful compromise, the attacker has high potential to compromise other machines in the network.
Easy_Exploit (5)	The attack can be carried out easily and requires little skills or does not require additional information.
High_Data_Loss (6)	Successful exploitation will result in massive data loss on the host.
Denial_of_Service (7)	Successful exploitation will result in denial of service.
No_Patch (8)	The vendor has not provided an official fix.

RTI (ID)	Description
Malware (9)	Malware has been associated with the vulnerability.
Exploit_Kit (10)	Exploit Kit has been associated with this vulnerability. Exploit Kits are usually cloud based toolkits that help malware writers in identifying vulnerable browsers/plugins and install malware. Users can also search on Exploit Kit name like Angler, Nuclear, Rig and others.
Wormable (11)	Wormable has been associated with this vulnerability. The vulnerability can be used in “worms” - malware that spreads itself without user interaction.
Predicted_High_Risk (12)	Predicted High Risk has been associated with this vulnerability. Qualys Machine Learning Model predicted this vulnerability as a High Risk based on various data sources including NVD, Social network, Dark web, Security Blogs, Code repository, Exploits, etc.
Privilege_Escalation (13)	Successful exploitation allows an attacker to gain elevated privileges.
Unauthenticated_Exploitation (14)	Exploitation of this vulnerability does not require authentication.
Remote_Code_Execution (15)	Successful exploitation allows an attacker to execute arbitrary commands or code on a targeted system or in a target process.
Ransomware (16)	This vulnerability has been exploited in attack vectors where ransomware has been deployed. In other words, this vulnerability is associated with known ransomware.
Solorigate_Sunburst (17)	Solorigate Sunburst has been associated with all the CVEs, used by FireEye's Red Team tools to test the security of their client environments and compromised versions of SolarWinds Orion.
CISA Known Exploited Vulnerabilities (18)	CISA maintains a catalog of the top publicly known vulnerabilities being exploited in the wild and organizations (referred as CISA Known Exploitable Vulnerabilities) are advised to patch affected systems on priority. This RTI indicates that the vulnerability is associated with the CISA catalog and with CVE mappings to respective QIDs. We will add the CISA Known Exploited Vulnerabilities to QIDs within 24hrs of CISA catalog updates with new CVEs. This CISA Directive recommends urgent and prioritized remediation of the vulnerabilities that adversaries are actively exploiting. The timelines are available in CISA's Catalog for each of the CVEs.

Sample - Fetch Basic Details for Vulnerabilities

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&details=Al
l&ids=6666666' \
```

```
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-02T10:55:37Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>6666666</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>
                   <![CDATA[Debian 12 Security Update for webkit2gtk (CVE-
2024-40780)]]>
                </TITLE>
                <CATEGORY>Debian</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
02T02:43:07Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-08-
26T14:08:11Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-08-
26T14:08:11Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2024-08-
15T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[webkit2gtk]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[debian]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[webkit2gtk_Debian12]]>
                        </ID>
                        <URL>
                            <![CDATA[https://security-
tracker.debian.org/tracker/CVE-2024-40780]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
```

```
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-40780]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-40780]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Debian has released a security update for
webkit2gtk to fix the vulnerabilities.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could lead to a security breach or affect integrity, availability, and
confidentiality.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Refer to Debian security advisory <A
HREF='https://security-tracker.debian.org/tracker/CVE-2024-40780'
TARGET='_blank'>CVE-2024-40780</A> for updates and patch information.]]>
                </SOLUTION>
                <PCI_FLAG>0</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>0</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Unix</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - Patchable Vulnerabilities

Vulnerabilities with certain QIDs that are patchable.

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&ids=608087
1&details=All&is_patchable=1' \
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-03T06:03:55Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>6080871</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[VMware Photon OS Security Update for python-
cryptography,coredns,grub2 (PHSA-2023-3.0-0681)]]>
                </TITLE>
                <CATEGORY>PhotonOS</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-06-
25T12:04:37Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-06-
24T12:55:24Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-06-
24T12:55:24Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2023-11-
04T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[photonos]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[vmware]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[PHSA-2023-3.0-0681]]>
                        </ID>
                        <URL>

<![CDATA[https://github.com/vmware/photon/wiki/Security-Update-3.0-681]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
```

```
                            <![CDATA[CVE-2021-28235]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2021-28235]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-4692]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-4692]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-4693]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-4693]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-32082]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-32082]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-23931]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-23931]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[PhotonOS has released a security update for
python-cryptography,coredns,grub2 to fix the vulnerabilities.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could lead to a security breach or affect integrity, availability, and
confidentiality.]]>
                </CONSEQUENCE>
                <SOLUTION>
```

```
                    <![CDATA[Refer to PhotonOS security advisory <A
HREF="https://github.com/vmware/photon/wiki/Security-Update-3.0-681"
TARGET="_blank">PHSA-2023-3.0-0681</A> for updates and patch
information.]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
        </EXPLT_SRC>
                    </EXPLOITS>
                </CORRELATION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="2">
                        <![CDATA[Exploit_Public]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>0</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Unix</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - Vulnerabilities Modified After Date

Vulnerabilities modified by the service after August 20, 2024 and that have discovery method "remote and authenticated".

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&last_modif
ied_by_service_after=2024-08-20&discovery_method=RemoteAndAuthenticated'
\
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-03T11:00:08Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>12681</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Adobe ColdFusion Information Disclosure
Vulnerability (APSA13-03, APSB13-13)]]>
                </TITLE>
                <CATEGORY>CGI</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
03T00:00:01Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2013-05-
14T20:25:21Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2013-05-
14T20:25:21Z</CODE_MODIFIED_DATETIME>
                <BUGTRAQ_LIST>
                    <BUGTRAQ>
                        <ID>
                            <![CDATA[59773]]>
        <VULN_LIST>
            <VULN>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com]]>
                        </URL>
                    </BUGTRAQ>
                </BUGTRAQ_LIST>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2013-05-
14T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[coldfusion]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[adobe]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[APSB13-13]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com]]>
```

```
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2013-3336]]>
                        </ID>
                        <URL>
                            <![CDATA[url.com]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Adobe ColdFusion is an application for
developing Web sites.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[Exploitation allows an unauthorized user to
remotely retrieve files stored on the server.]]>
                </CONSEQUENCE>
                <SOLUTION>
                   <![CDATA[The vendor has released a hotfix to patch this
vulnerability.<P>
Workaround:<BR>
Restrict public access to the CFIDE/administrator, CFIDE/adminapi and
CFIDE/gettingstarted directories.]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[coreimpact]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2013-3336]]>
                                    </REF>
                                    <DESC>
                                       <![CDATA[Adobe ColdFusion l10n.cfm
Remote Code Execution Exploit]]>
                                    </DESC>
                                    <LINK>
                                        <![CDATA[https://url.com/core-
labs/exploits]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[nist-nvd2]]>
                            </SRC_NAME>
```

```
                                <EXPLT_LIST>
                                    <EXPLT>
                                        <REF>
                                            <![CDATA[CVE-2013-3336]]>
                                        </REF>
                                        <DESC>
                                           <![CDATA[Unspecified vulnerability
in Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote attackers to
read arbitrary files via unknown vectors.]]>
                                        </DESC>
                                        <LINK>

<![CDATA[https://url.com/exploits/25305]]>
                                        </LINK>
                                    </EXPLT>
                                </EXPLT_LIST>
                            </EXPLT_SRC>
                            <EXPLT_SRC>
                                <SRC_NAME>
                                    <![CDATA[exploitdb]]>
                                </SRC_NAME>
                                <EXPLT_LIST>
                                    <EXPLT>
                                        <REF>
                                            <![CDATA[CVE-2013-3336]]>
                                        </REF>
                                        <DESC>
                                            <![CDATA[ColdFusion 9-10 -
Credential Disclosure]]>
                                        </DESC>
                                        <LINK>

<![CDATA[https://url.com/exploits/25305]]>
                                        </LINK>
                                    </EXPLT>
                                </EXPLT_LIST>
                            </EXPLT_SRC>
                        </EXPLOITS>
                    </CORRELATION>
                    <PCI_FLAG>1</PCI_FLAG>
                    <THREAT_INTELLIGENCE>
                        <THREAT_INTEL id="12">
                            <![CDATA[Predicted_High_Risk]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="14">
                            <![CDATA[Unauthenticated_Exploitation]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="15">
                            <![CDATA[Remote_Code_Execution]]>
                        </THREAT_INTEL>
                    </THREAT_INTELLIGENCE>
                    <DISCOVERY>
                        <REMOTE>1</REMOTE>
                        <AUTH_TYPE_LIST>
```

```
                        <AUTH_TYPE>Windows</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>19088</QID>
                <VULN_TYPE>Vulnerability or Potential
Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[IBM DB2 Remote Command Server Privilege
Escalation Vulnerability]]>
                </TITLE>
                <CATEGORY>Database</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
03T00:00:01Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2004-04-
08T18:23:47Z</PUBLISHED_DATETIME>
                <BUGTRAQ_LIST>
                    <BUGTRAQ>
                        <ID>
                            <![CDATA[9821]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com/bid/9821]]>
                        </URL>
                    </BUGTRAQ>
                </BUGTRAQ_LIST>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2004-02-
20T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[db2_universal_database]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[ibm]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[IY53894]]>
                        </ID>
                        <URL>

<![CDATA[https://url.com/support/docview.wss?uid=swg1IY53894]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
```

```
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2004-0795]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com/cgi-
bin/cvename.cgi?name=CVE-2004-0795]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[The database server includes a component
called the Remote Command Server to facilitate execution of commands by
remote clients.
<P>
IBM DB2 Remote Command Server is prone to a vulnerability that may permit
authenticated users to gain administrative access to the underlying
database.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[By exploiting this vulnerability, an attacker
may execute arbitrary commands with the escalated privileges of the
&amp;quot;db2admin&amp;quot; account. This issue could be exploited by a Windows
&amp;quot;Guest&amp;quot; account.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Information about this issue is provided in
<A HREF="http://www-01.ibm.com/support/docview.wss?uid=swg1IY53894"
TARGET="_blank">APAR IY53894</A>. IBM has included a fix for this problem
in<A HREF="http://www-
01.ibm.com/support/docview.wss?rs=71&uid=swg27007053" TARGET="_blank">DB2
Version 8 FixPak 5</A>. ]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[metasploit]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2004-0795]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[IBM DB2 db2rcmd.exe
Command Execution Vulnerability]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/rapid7/metasploit-
framework/master/modules/auxiliary/admin/db2/db2rcmd.rb]]>
                                    </LINK>
```

```
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[Metasploit]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2004-0795]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[IBM DB2 db2rcmd.exe
Command Execution Vulnerability - Metasploit Ref :
/modules/auxiliary/admin/db2/db2rcmd]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/rapid7/metasploit-
framework/blob/master//modules/auxiliary/admin/db2/db2rcmd.rb]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[packetstorm]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2004-0795]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[IBM DB2 Db2rcmd.exe
Command Execution]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/files/180775/IBM-DB2-Db2rcmd.exe-Command-
Execution.html]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                    </EXPLOITS>
                </CORRELATION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
```

```
                        <THREAT_INTEL id="6">
                            <![CDATA[High_Data_Loss]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="7">
                            <![CDATA[Denial_of_Service]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="13">
                            <![CDATA[Privilege_Escalation]]>
                        </THREAT_INTEL>
                    </THREAT_INTELLIGENCE>
                    <DISCOVERY>
                        <REMOTE>1</REMOTE>
                        <AUTH_TYPE_LIST>
                            <AUTH_TYPE>Windows</AUTH_TYPE>
                        </AUTH_TYPE_LIST>
                        <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                    </DISCOVERY>
                </VULN>
                </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

DTD

<platform API server>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd

V4.0

/api/4.0/fo/knowledge_base/vuln/?action=list

[GET] [POST]

Download a list of vulnerabilities from Qualys' KnowledgeBase. Several input parameters grant users control over which vulnerabilities to download and the amount of detail to download, and the XML output provides a rich information source for each vulnerability.

Qualys' Sofware-as-a-Service (SaaS) technology includes its KnowledgeBase, with the industry's largest number of vulnerability signatures, that is continuously updated by Qualys' Research and Development team. Qualys is fully dedicated to providing the most accurate security audits in the industry. Each day new and updated signatures are tested in Qualys' own vulnerability labs and then published, making them available to Qualys customers. When Threat Protection is enabled for your subscription, the output will include Samples - Lists the QIDs that exactly matches the given CVE. associated with vulnerabilities.

Authorized Qualys users have the ability to download vulnerability data using the KnowledgeBase API. Please contact Qualys Support or your sales representative if you would like to obtain authorization for your subscription.

Permissions - Your subscription must be granted permission to run this API function. Please contact Qualys Support or your sales representative to receive this authorization.

Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.
Auditor	No permission to download vulnerability data from the KnowledgeBase.

Input Parameters

Several optional input parameters may be specified. When unspecified, the XML output includes all vulnerabilities in the KnowledgeBase, showing basic details for each vulnerability. Several optional parameters allow you specify filters. When filter parameters are specified, these parameters are ANDed by the service to filter the data from the output.

Parameter	Description
action=list	(Required)
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. Supported date format is YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each vulnerability in the XML output. A valid value is: Basic (default), All, or None. Basic includes basic elements plus CVSS Base and Temporal scores. All includes all vulnerability details, including the Basic details.
ids={value}	(Optional) Used to filter the XML output to include only vulnerabilities that have QID numbers matching the QID numbers you specify. **Notes**: - If the QID numbers and number range specified are too large, it is recommended to use `id_min={value}` and `id_max={value}` parameters. - The query string length ranges from 8000 to 10,000 QIDs (Characters). If the length exceeds 10,000, the API may not return a response.
id_min={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number greater than or equal to a QID number you specify.

Parameter	Description
id_max={value}	(Optional) Used to filter the XML output to show only vulnerabilities that have a QID number less than or equal to a QID number you specify.
is_patchable={**0**|1}	(Optional) Used to filter the XML output to show only vulnerabilities that are patchable or not patchable. A vulnerability is considered patchable when a patch exists for it. When 1 is specified, only vulnerabilities that are patchable will be included in the output. When 0 is specified, only vulnerabilities that are not patchable will be included in the output. When unspecified, patchable and unpatchable vulnerabilities will be included in the output.
last_modified_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified after a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified before a certain date and time. When specified vulnerabilities last modified by a user or by the service will be shown. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_user_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_user_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by a user before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
last_modified_by_service_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities last modified by the service before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
published_after={date}	(Optional) Used to filter the XML output to show only vulnerabilities published after a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).

Parameter	Description
published_before={date}	(Optional) Used to filter the XML output to show only vulnerabilities published before a certain date and time. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
discovery_method={value}	(Optional) Used to filter the XML output to show only vulnerabilities assigned a certain discovery method. A valid value is: Remote, Authenticated, RemoteOnly, AuthenticatedOnly, or RemoteAndAuthenticated. When "Authenticated" is specified, the service shows vulnerabilities that have at least one associated authentication type. Vulnerabilities that have at least one authentication type can be detected in two ways: 1) remotely without using authentication, and 2) using authentication.
discovery_auth_types={value}	(Optional) Used to filter the XML output to show only vulnerabilities having one or more authentication types. A valid value is: Windows, Oracle, Unix, SNMP, DB2, HTTP, PANOS, TOMCAT, MARIADB, MongoDB, WEBLOGIC, MySQL, VMware. Multiple values should be comma-separated.
show_pci_reasons={**0**|1}	(Optional) Used to filter the XML output to show reasons for passing or failing PCI compliance (when the CVSS Scoring feature is turned on in the user's subscription). Specify 1 to view the reasons in the XML output. When unspecified, the reasons are not included in the XML output.
show_supported_modules_info={**0**|1}	(Optional) Used to filter the XML output to show Qualys modules that can be used to detect each vulnerability. Specify 1 to view supported modules in the XML output. When unspecified, supported modules are not included in the XML output.
show_disabled_flag={**0**|1}	(Optional) Specify 1 to include the disabled flag for each vulnerability in the XML output.
show_qid_change_log={**0**|1}	(Optional) Specify 1 to include QID changes for each vulnerability in the XML output.
code_modified_after={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified after a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).
code_modified_before={date}	(Optional) Used to filter the XML output. This shows only the QIDs modified before a certain date and time. The supported date format is YYYY-MM-DD [THH:MM:SSZ] format (UTC/GMT).
cloud_agent_scan_type	(Optional) Required for fetching data for Deep Scan QIDs.

Sample - Lists the QIDs that exactly matches the given CVE.

API Request

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/index.php?action=list&c
```

```
ve=CVE-1999-0527' \
--header 'X-Requested-With: curl demo2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-10-28T07:21:55Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>27002</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Writeable Root Directory on FTP Server]]>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2009-07-
08T17:28:46Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-0527]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[The FTP server has a world writeable root
directory.  The root directory of your FTP server can therefore be
written-to by any user.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Writeable FTP servers are commonly abused by
unauthorized users to upload movies, pornography, pirated software and
other &quot;warez&quot;. Sometimes the secondary storage is completely
filled up resulting in performance degradation or even complete failure.
<P>For some FTP servers, the FTP root directory contains configuration
files. Allowing write permissions may allow an anonymous user to overwrite
these configuration files.
<P>In addition for UNIX, unauthorized users could place a
&quot;.forward&quot; or an &quot;.rhosts&quot; file in this directory.
&quot;.forward&quot; files may contain commands to be executed each time
```

```
the anonymous user receives an e-mail message.  &amp;quot;.rhosts&amp;quot; files
contain hostnames from which any user will be able to connect to this host
without a password.  Thus, the unauthorized user can add the .rhosts file
using their own hostname.  They can then log in with rsh, rlogin or rexec
service. These two files are commonly used to compromise servers.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Disable write access for unauthorized users
in the root directory of the FTP server.
<P>For UNIX:<BR>
$ chmod o-w path/to/ftp/root/directory
<P>For Microsoft IIS 6:<BR>
1.  Click Start, point to Administrative Tools, and then click Internet
Information Services (IIS).<BR>
2.  In IIS Manager, expand the local computer, expand the FTP Sites
folder, right-click the FTP site in question, and click Properties.<BR>
3.  Click the Home Directory tab and deselect the Write checkbox; click
OK.<BR>
4.  For advanced permissions, refer to step 2 and click Permissions
instead of Properties; then click Advanced Permissions.<BR><P> For other
versions of IIS, please refer to the Microsoft website.
]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="6">
                        <![CDATA[High_Data_Loss]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="7">
                        <![CDATA[Denial_of_Service]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="14">
                        <![CDATA[Unauthenticated_Exploitation]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>27005</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
```

```
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[World Readable and Writable Directory on
Anonymous FTP]]>
                </TITLE>
                <CATEGORY>File Transfer Protocol</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2020-11-
23T18:43:15Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>1999-01-
01T08:00:00Z</PUBLISHED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-1999-0527]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-0527]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Your FTP server contains a directory with
dangerous permissions. This directory is world writable and world
readable.  If this is an incoming directory, users should not be able to
list the it's contents.
]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[Unauthorized users can write to your FTP
server. This FTP directory can be used as a pirate software repository or
for adult picture exchanges. You also run the risk of receiving virus or
Trojan programs. Do not run unknown files from this area. ]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Unless they are required, remove the
directories. Otherwise, make sure that no hidden directories are used for
illegal purposes.  These hidden directories may be named with control
characters or begin with a dot (.), making it harder to detect and remove
them.
<P>
Frequently monitor your FTP server directories. You can schedule a
repetitive task with the cron command under Unix, which will execute the
following command every week:
<P><DL><DD>find ~ftp/ -print</DD></DL><P>
This will regularly inform you of all files in this area, and advise you
whether or not they are writeable and readable.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
```

```
                        <THREAT_INTEL id="5">
                            <![CDATA[Easy_Exploit]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="6">
                            <![CDATA[High_Data_Loss]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="7">
                            <![CDATA[Denial_of_Service]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="8">
                            <![CDATA[No_Patch]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="14">
                            <![CDATA[Unauthenticated_Exploitation]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="15">
                            <![CDATA[Remote_Code_Execution]]>
                        </THREAT_INTEL>
                    </THREAT_INTELLIGENCE>
                    <DISCOVERY>
                        <REMOTE>1</REMOTE>
                    </DISCOVERY>
                </VULN>
...
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - List all the QIDs for the code modified before and after specific date.

API Request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/?null=null&code_modifie
d_before=2024-10-28&action=list&code_modified_after=2024-10-27' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-10-28T07:32:48Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>152263</QID>
                <VULN_TYPE>Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
```

```
                    <![CDATA[WordPress Unseen Blog Theme: PHP Object
Injection Vulnerability (CVE-2024-7432)]]>
                </TITLE>
                <CATEGORY>Web Application</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-10-
27T18:12:51Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-10-
27T15:03:21Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-10-
27T15:03:21Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>0</PATCHABLE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[None]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[wordpress]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Unseen Blog Changelog]]>
                        </ID>
                        <URL>
<![CDATA[https://ultrapress.org/changelog/]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-7432]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-7432]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                  <![CDATA[WordPress Unseen Blog is a free WordPress theme
which is light weight, super fast, fully customizable, easy to use and is
best for lead generation for any coaching business. <P>
Unseen Blog Theme is vulnerable to PHP Object Injection.<P>
Affected Versions:<BR> WordPress Unseen Blog Theme versions up to and
including 1.0.0<P>
QID Detection Logic:<BR> This QID sends a HTTP GET request and checks for
vulnerable version of Unseen Blog theme running on the target
application.<P>]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
```

```
                    <![CDATA[Successful exploitation of this vulnerability
could allow authenticated attackers with Contributor-level access and
above to inject a PHP Object. No known POP chain is present in the
vulnerable software. If a POP chain is present via an additional plugin or
theme installed on the target system, it could allow the attacker to
delete arbitrary files, retrieve sensitive data, or execute code.<P>]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Customers are advised to refer to <A
HREF="https://ultrapress.org/changelog/" TARGET="_blank">Unseen Blog
Theme Changelog</A> for updates to remediate this vulnerability.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="6">
                        <![CDATA[High_Data_Loss]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="7">
                        <![CDATA[Denial_of_Service]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="8">
                        <![CDATA[No_Patch]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>152299</QID>
                <VULN_TYPE>Potential Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[WordPress Pretix Widget Plugin: Local File
Inclusion Vulnerability (CVE-2024-9575)]]>
                </TITLE>
                <CATEGORY>Web Application</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-10-
27T18:09:47Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-10-
27T15:39:56Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-10-
27T15:39:56Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2024-10-
10T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
```

```
                        <PRODUCT>
                            <![CDATA[None]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[wordpress]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[Pretix Widget Changelog]]>
                        </ID>
                        <URL>
<![CDATA[https://wordpress.org/plugins/pretix-widget/#developers]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-9575]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-9575]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                   <![CDATA[The pretix widget allows us to easily display
pretix ticket widgets on a website by customizing the display of any
pretix tickets and providing a seamless ticket booking experience for
users. <P>
WordPress pretix widget plugin is vulnerable to Local File Inclusion
vulnerability in Windows.<P>
Affected Versions:<BR> pretix widget plugin versions starting from 1.0.0
up to, and including 1.0.5<P>
QID Detection Logic:<BR> This QID sends a HTTP GET request and checks for
vulnerable version of pretix widget plugin running on the target
application.<P>]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could allow unauthenticated attacker to cause arbitrary .php files of the
system to be included on the page, including possible directory
traversal.<P>]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Customers are advised to upgrade to <A
HREF="https://latepoint.com/changelog/" TARGET="_blank">pretix widget
plugin 1.0.6</A> or later version to remediate this vulnerability.]]>
                </SOLUTION>
                <PCI_FLAG>1</PCI_FLAG>
```

```
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="5">
                        <![CDATA[Easy_Exploit]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                    <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - KnowledgeBase API

API Request:

```
curl location
<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/?action=list&details=Non
e&cloud_agent_scan_type=Deep%20Scan%20-%20Windows' \
header 'Content-Type: test/xml' \
header 'X-Requested-With: test' \
header 'Accept-Encoding: *' \
header 'Authorization: Bearer <JWT Token>
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/knowledge_base_vu
ln_list_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-12-11T10:08:37Z</DATETIME>
        <ID_SET>
            <ID>45692</ID>
            <ID>92291</ID>
            <ID>92310</ID>
            <ID>92316</ID>
            <ID>92319</ID>
            <ID>382697</ID>
            <ID>382991</ID>
            <ID>383087</ID>
            <ID_RANGE>383090-383092</ID_RANGE>
            <ID>383097</ID>
            <ID>383116</ID>
            <ID>383138</ID>
            <ID_RANGE>383140-383141</ID_RANGE>
            <ID>383243</ID>
            <ID_RANGE>383249-383250</ID_RANGE>
```

```
<ID>383396</ID>
<ID>383400</ID>
<ID>383414</ID>
<ID>383416</ID>
<ID>383422</ID>
<ID>383426</ID>
<ID>383428</ID>
<ID>383463</ID>
<ID>383478</ID>
<ID>383481</ID>
<ID_RANGE>383568-383569</ID_RANGE>
<ID>383572</ID>
<ID>383578</ID>
<ID>383587</ID>
<ID_RANGE>383592-383593</ID_RANGE>
<ID>383596</ID>
<ID>383598</ID>
<ID>383609</ID>
<ID>383645</ID>
<ID_RANGE>383648-383657</ID_RANGE>
<ID_RANGE>383660-383662</ID_RANGE>
<ID>383664</ID>
<ID_RANGE>383669-383670</ID_RANGE>
<ID_RANGE>383672-383705</ID_RANGE>
<ID>383709</ID>
<ID>383711</ID>
<ID>383717</ID>
<ID_RANGE>383719-383725</ID_RANGE>
<ID_RANGE>383729-383730</ID_RANGE>
<ID_RANGE>383741-383850</ID_RANGE>
<ID_RANGE>383852-383915</ID_RANGE>
<ID_RANGE>383917-383939</ID_RANGE>
<ID>383941</ID>
<ID_RANGE>383943-383946</ID_RANGE>
<ID>383966</ID>
<ID_RANGE>383971-384172</ID_RANGE>
<ID_RANGE>384174-384256</ID_RANGE>
<ID_RANGE>384258-384329</ID_RANGE>
<ID_RANGE>384332-384349</ID_RANGE>
<ID_RANGE>384511-384518</ID_RANGE>
<ID_RANGE>384574-384578</ID_RANGE>
<ID_RANGE>384580-384605</ID_RANGE>
<ID_RANGE>384611-384613</ID_RANGE>
<ID>384615</ID>
<ID_RANGE>384626-384644</ID_RANGE>
```

```
<ID_RANGE>384649-384650</ID_RANGE>
<ID>384652</ID>
<ID_RANGE>384654-384674</ID_RANGE>
<ID>384676</ID>
<ID_RANGE>384678-384687</ID_RANGE>
<ID>384689</ID>
<ID>384692</ID>
<ID>385099</ID>
<ID_RANGE>385106-385108</ID_RANGE>
<ID>385148</ID>
<ID_RANGE>385160-385203</ID_RANGE>
<ID_RANGE>385205-385206</ID_RANGE>
<ID_RANGE>385208-385230</ID_RANGE>
<ID_RANGE>385238-385270</ID_RANGE>
<ID_RANGE>385272-385273</ID_RANGE>
<ID_RANGE>385275-385276</ID_RANGE>
<ID_RANGE>385278-385279</ID_RANGE>
<ID_RANGE>385281-385285</ID_RANGE>
<ID_RANGE>385287-385330</ID_RANGE>
<ID_RANGE>385358-385365</ID_RANGE>
<ID_RANGE>385368-385372</ID_RANGE>
<ID>385374</ID>
<ID>385385</ID>
<ID_RANGE>385397-385401</ID_RANGE>
<ID_RANGE>385403-385424</ID_RANGE>
<ID_RANGE>385432-385436</ID_RANGE>
<ID_RANGE>385448-385451</ID_RANGE>
<ID_RANGE>385456-385477</ID_RANGE>
<ID_RANGE>385479-385484</ID_RANGE>
<ID_RANGE>385486-385493</ID_RANGE>
<ID_RANGE>385496-385501</ID_RANGE>
<ID>385504</ID>
<ID>385508</ID>
<ID>385526</ID>
<ID>385536</ID>
<ID>385593</ID>
<ID>385604</ID>
<ID_RANGE>385609-385611</ID_RANGE>
<ID>385773</ID>
<ID_RANGE>385775-385777</ID_RANGE>
<ID_RANGE>385793-385857</ID_RANGE>
<ID>385865</ID>
<ID>385941</ID>
<ID>385979</ID>
<ID_RANGE>385998-386013</ID_RANGE>
```

```
            <ID>386019</ID>
            <ID_RANGE>386054-386059</ID_RANGE>
            <ID_RANGE>386120-386122</ID_RANGE>
            <ID>386128</ID>
            <ID>386130</ID>
            <ID>386136</ID>
        </ID_SET>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

sample - List the CVSS4 details in the response for a single QID.

API Request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/knowledge_base/vuln/?action=list&details=Al
l&ids=913768' \
--header 'Content-Type: test/xml' \
--header 'X-Requested-With: test' \
--header 'Accept-Encoding: *' \
--header 'Authorization: Bearer<JWT Token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE\_BASE\_VULN\_LIST\_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/knowledge\_base/vuln/knowledge\_base\_vuln\
_list\_…

<RESPONSE>
    <DATETIME>2025-09-29T12:59:24Z</DATETIME>
    <VULN_LIST>
        <VULN>
            <QID>913768</QID>
            <VULN_TYPE>Vulnerability</VULN_TYPE>
            <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
            <TITLE>
                <![CDATA[Common Base Linux Mariner (CBL-Mariner) Security
Update for binutils (57590)]]>
            </TITLE>
            <CATEGORY>CBL-Mariner</CATEGORY>
            <LAST_SERVICE_MODIFICATION_DATETIME>2025-07-
02T12:07:47Z</LAST_SERVICE_MODIFICATION_DATETIME>
            <PUBLISHED_DATETIME>2025-03-20T15:08:30Z</PUBLISHED_DATETIME>
            <CODE_MODIFIED_DATETIME>2025-03-
20T15:08:30Z</CODE_MODIFIED_DATETIME>
            <PATCHABLE>1</PATCHABLE>
            <PATCH_PUBLISHED_DATE>2025-03-
12T00:00:00Z</PATCH_PUBLISHED_DATE>
            <SOFTWARE_LIST>
                <SOFTWARE>
                    <PRODUCT>
                        <![CDATA[cbl_mariner_2]]>
```

```
                    </PRODUCT>
                    <VENDOR>
                        <![CDATA[microsoft]]>
                    </VENDOR>
                </SOFTWARE>
            </SOFTWARE_LIST>
            <VENDOR_REFERENCE_LIST>
                <VENDOR_REFERENCE>
                    <ID>
                        <![CDATA[Mariner_2.0_57590]]>
                    </ID>
                    <URL>
                        <![CDATA[https://github.com/microsoft/CBL-
Mariner/tree/2.0]]>
                    </URL>
                </VENDOR_REFERENCE>
            </VENDOR_REFERENCE_LIST>
            <CVE_LIST>
                <CVE>
                    <ID>
                        <![CDATA[CVE-2025-1744]]>
                    </ID>
                    <URL>
                        <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2025-1744]]>
                    </URL>
                </CVE>
            </CVE_LIST>
            <DIAGNOSIS>
               <![CDATA[CBL-Mariner 2.0 is an internal Linux distribution
for cloud infrastructure and edge products and services of
Microsoft.<BR>CBL-Mariner has released a security update for binutils to
fix the vulnerabilities.<BR><BR><P>QID Detection Logic
(Authenticated):<BR>QID utilizes the target system's package manager, such
as &amp;quot;rpm&amp;quot;, to enumerate packages and map them with vendor
advisories to identify vulnerable versions.<BR>]]>
            </DIAGNOSIS>
            <CONSEQUENCE>
                <![CDATA[Successful exploitation of this vulnerability
could lead to a security breach or could affect integrity, availability,
and confidentiality.]]>
            </CONSEQUENCE>
            <SOLUTION>
               <![CDATA[<P>CBL-Mariner has issued updated packages to fix
this vulnerability. For more information about the vulnerability and
obtaining patches, refer to the following CBL-Mariner 2.0 security
advisories:<A HREF="https://github.com/microsoft/CBL-Mariner/tree/2.0"
TARGET="\_blank">https://github.com/microsoft/CBL-
Mariner/tree/2.0</A></P><P>Patch:<BR>
Following are links for downloading patches to fix the vulnerabilities:
<P><A HREF="https://github.com/microsoft/CBL-Mariner/tree/2.0"
TARGET="\_blank">57590:CBL-Mariner Linux 2\\\\.0</A>]]>
            </SOLUTION>
            <CVSS>
```

```
                <BASE source="service">5.4</BASE>
                <TEMPORAL>4.0</TEMPORAL>

<VECTOR_STRING>CVSS:2.0/AV:A/AC:M/Au:M/C:N/I:C/A:P/E:U/RL:OF/RC:C</VECTOR
_STRING>
                <ACCESS>
                    <VECTOR>2</VECTOR>
                    <COMPLEXITY>2</COMPLEXITY>
                </ACCESS>
                <IMPACT>
                    <CONFIDENTIALITY>1</CONFIDENTIALITY>
                    <INTEGRITY>3</INTEGRITY>
                    <AVAILABILITY>2</AVAILABILITY>
                </IMPACT>
                <AUTHENTICATION>3</AUTHENTICATION>
                <EXPLOITABILITY>1</EXPLOITABILITY>
                <REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
                <REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>
            </CVSS>
            <CVSS_V3>
                <BASE>9.8</BASE>
                <TEMPORAL>8.5</TEMPORAL>

<VECTOR_STRING>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
</VECTOR_STRING>
                <CVSS3_VERSION>3.1</CVSS3_VERSION>
                <ATTACK>
                    <VECTOR>1</VECTOR>
                    <COMPLEXITY>1</COMPLEXITY>
                </ATTACK>
                <IMPACT>
                    <CONFIDENTIALITY>3</CONFIDENTIALITY>
                    <INTEGRITY>3</INTEGRITY>
                    <AVAILABILITY>3</AVAILABILITY>
                </IMPACT>
                <PRIVILEGES_REQUIRED>1</PRIVILEGES_REQUIRED>
                <USER_INTERACTION>1</USER_INTERACTION>
                <SCOPE>1</SCOPE>
                <EXPLOIT_CODE_MATURITY>1</EXPLOIT_CODE_MATURITY>
                <REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
                <REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>
            </CVSS_V3>
            <CVSS_V4>
                <BASE>10.0</BASE>

<VECTOR_STRING>CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/SC:H/VI:H/SI:H/VA:H
/SA:H</VECTOR_STRING>
                <CVSS4_VERSION>4.0</CVSS4_VERSION>
                <ATTACK>
                    <VECTOR>1</VECTOR>
                    <COMPLEXITY>1</COMPLEXITY>
                    <REQUIREMENT>1</REQUIREMENT>
                </ATTACK>
                <IMPACT>
```

```
                    <VULNERABLE>
                        <CONFIDENTIALITY>3</CONFIDENTIALITY>
                        <INTEGRITY>3</INTEGRITY>
                        <AVAILABILITY>3</AVAILABILITY>
                    </VULNERABLE>
                    <SUBSEQUENT>
                        <CONFIDENTIALITY>3</CONFIDENTIALITY>
                        <INTEGRITY>3</INTEGRITY>
                        <AVAILABILITY>3</AVAILABILITY>
                    </SUBSEQUENT>
                </IMPACT>
                <PRIVILEGES_REQUIRED>1</PRIVILEGES_REQUIRED>
                <USER_INTERACTION>1</USER_INTERACTION>
            </CVSS_V4>
            <PCI_FLAG>1</PCI_FLAG>
            <THREAT_INTELLIGENCE>
                <THREAT_INTEL id="4">
                    <![CDATA[High_Lateral_Movement]]>
                </THREAT_INTEL>
                <THREAT_INTEL id="15">
                    <![CDATA[Remote_Code_Execution]]>
                </THREAT_INTEL>
            </THREAT_INTELLIGENCE>
            <DISCOVERY>
                <REMOTE>0</REMOTE>
                <AUTH_TYPE_LIST>
                    <AUTH_TYPE>Unix</AUTH_TYPE>
                </AUTH_TYPE_LIST>
                <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
            </DISCOVERY>
        </VULN>
    </VULN_LIST>
</RESPONSE>undefined</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Real-Time Threat Indicators (RTIs)

The KnowledgeBase list output includes Real-Time Threat Indicators (RTIs) associated with each vulnerability. RTIs appear as part of vulnerability details under THREAT_INTELLIGENCE. Please note that RTIs are only visible when Threat Protection is enabled for the subscription.

Real-Time Threat Indicators are described below.

RTI (ID)	Description
Zero_Day (1)	Active attack has been observed in the wild and there is no patch from the vendor. An active attack is a prerequisite for this RTI in addition to no patch from the vendor. If a vulnerability is not actively attacked this RTI will not be set (even if there is no patch from the vendor). If a patch becomes available Qualys will remove the Zero Day RTI attribute which helps users to focus only on vulnerabilities that are actively exploited and there is no official patch.
Exploit_Public (2)	Exploit knowledge is well known and a working exploitation code is publicly available. Potential of active attacks is very high. This attribute is set for example when PoC exploit code is available from Exploit-DB, Metasploit, Core, Immunity or other exploit vendors. This RTI does not necessarily indicate that active attacks have been observed in the wild.
Active_Attacks (3)	Active attacks have been observed in the wild. This information is derived from Malware, Exploit Kits, acknowledgment from vendors, US-CERT and similar trusted sources. If there are no patches, Qualys will mark it as Zero Day, in addition, to actively attacked.
High_Lateral_Movement (4)	After a successful compromise, the attacker has high potential to compromise other machines in the network.
Easy_Exploit (5)	The attack can be carried out easily and requires little skills or does not require additional information.
High_Data_Loss (6)	Successful exploitation will result in massive data loss on the host.
Denial_of_Service (7)	Successful exploitation will result in denial of service.
No_Patch (8)	The vendor has not provided an official fix.
Malware (9)	Malware has been associated with the vulnerability.
Exploit_Kit (10)	Exploit Kit has been associated with this vulnerability. Exploit Kits are usually cloud based toolkits that help malware writers in identifying vulnerable browsers/plugins and install malware. Users can also search on Exploit Kit name like Angler, Nuclear, Rig and others.
Wormable (11)	Wormable has been associated with this vulnerability. The vulnerability can be used in “worms” - malware that spreads itself without user interaction.
Predicted_High_Risk (12)	Predicted High Risk has been associated with this vulnerability. Qualys Machine Learning Model predicted this vulnerability as a High Risk based on various data sources including NVD, Social network, Dark web, Security Blogs, Code repository, Exploits, etc.
Privilege_Escalation (13)	Successful exploitation allows an attacker to gain elevated privileges.
Unauthenticated_Exploitation (14)	Exploitation of this vulnerability does not require authentication.

RTI (ID)	Description
Remote_Code_Execution (15)	Successful exploitation allows an attacker to execute arbitrary commands or code on a targeted system or in a target process.
Ransomware (16)	This vulnerability has been exploited in attack vectors where ransomware has been deployed. In other words, this vulnerability is associated with known ransomware.
Solorigate_Sunburst (17)	Solorigate Sunburst has been associated with all the CVEs, used by FireEye's Red Team tools to test the security of their client environments and compromised versions of SolarWinds Orion.
CISA Known Exploited Vulnerabilities (18)	CISA maintains a catalog of the top publicly known vulnerabilities being exploited in the wild and organizations (referred as CISA Known Exploitable Vulnerabilities) are advised to patch affected systems on priority. This RTI indicates that the vulnerability is associated with the CISA catalog and with CVE mappings to respective QIDs. We will add the CISA Known Exploited Vulnerabilities to QIDs within 24hrs of CISA catalog updates with new CVEs. This CISA Directive recommends urgent and prioritized remediation of the vulnerabilities that adversaries are actively exploiting. The timelines are available in CISA's Catalog for each of the CVEs.

Sample - Fetch Basic Details for Vulnerabilities

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&details=Al
l&ids=6666666' \
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-02T10:55:37Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>6666666</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>
                   <![CDATA[Debian 12 Security Update for webkit2gtk (CVE-
2024-40780)]]>
```

```
                </TITLE>
                <CATEGORY>Debian</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
02T02:43:07Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-08-
26T14:08:11Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-08-
26T14:08:11Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2024-08-
15T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[webkit2gtk]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[debian]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[webkit2gtk_Debian12]]>
                        </ID>
                        <URL>
                            <![CDATA[https://security-
tracker.debian.org/tracker/CVE-2024-40780]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2024-40780]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2024-40780]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Debian has released a security update for
webkit2gtk to fix the vulnerabilities.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could lead to a security breach or affect integrity, availability, and
confidentiality.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Refer to Debian security advisory <A
```

```
HREF='https://security-tracker.debian.org/tracker/CVE-2024-40780'
TARGET='_blank'>CVE-2024-40780</A> for updates and patch information.]]>
                </SOLUTION>
                <PCI_FLAG>0</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>0</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Unix</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - Patchable Vulnerabilities

Vulnerabilities with certain QIDs that are patchable.

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&ids=608087
1&details=All&is_patchable=1' \
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-03T06:03:55Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>6080871</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[VMware Photon OS Security Update for python-
cryptography,coredns,grub2 (PHSA-2023-3.0-0681)]]>
                </TITLE>
                <CATEGORY>PhotonOS</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-06-
```

```
25T12:04:37Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2024-06-
24T12:55:24Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2024-06-
24T12:55:24Z</CODE_MODIFIED_DATETIME>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2023-11-
04T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[photonos]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[vmware]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[PHSA-2023-3.0-0681]]>
                        </ID>
                        <URL>

<![CDATA[https://github.com/vmware/photon/wiki/Security-Update-3.0-681]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2021-28235]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2021-28235]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-4692]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-4692]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-4693]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
```

```
bin/cvename.cgi?name=CVE-2023-4693]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-32082]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-32082]]>
                        </URL>
                    </CVE>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2023-23931]]>
                        </ID>
                        <URL>
                            <![CDATA[http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2023-23931]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[PhotonOS has released a security update for
python-cryptography,coredns,grub2 to fix the vulnerabilities.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[Successful exploitation of this vulnerability
could lead to a security breach or affect integrity, availability, and
confidentiality.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Refer to PhotonOS security advisory <A
HREF="https://github.com/vmware/photon/wiki/Security-Update-3.0-681"
TARGET="_blank">PHSA-2023-3.0-0681</A> for updates and patch
information.]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
        </EXPLT_SRC>
                    </EXPLOITS>
                </CORRELATION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="2">
                        <![CDATA[Exploit_Public]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="4">
                        <![CDATA[High_Lateral_Movement]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
```

```
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>0</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Unix</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

Sample - Vulnerabilities Modified After Date

Vulnerabilities modified by the service after August 20, 2024 and that have discovery method "remote and authenticated".

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/?action=list&last_modif
ied_by_service_after=2024-08-20&discovery_method=RemoteAndAuthenticated'
\
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/knowledge_base/vuln/knowledge_base_vuln_lis
t_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-09-03T11:00:08Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>12681</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Adobe ColdFusion Information Disclosure
Vulnerability (APSA13-03, APSB13-13)]]>
                </TITLE>
                <CATEGORY>CGI</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
03T00:00:01Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2013-05-
14T20:25:21Z</PUBLISHED_DATETIME>
                <CODE_MODIFIED_DATETIME>2013-05-
14T20:25:21Z</CODE_MODIFIED_DATETIME>
```

```
                <BUGTRAQ_LIST>
                    <BUGTRAQ>
                        <ID>
                            <![CDATA[59773]]>
        <VULN_LIST>
            <VULN>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com]]>
                        </URL>
                    </BUGTRAQ>
                </BUGTRAQ_LIST>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2013-05-
14T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[coldfusion]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[adobe]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[APSB13-13]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2013-3336]]>
                        </ID>
                        <URL>
                            <![CDATA[url.com]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[Adobe ColdFusion is an application for
developing Web sites.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                    <![CDATA[Exploitation allows an unauthorized user to
remotely retrieve files stored on the server.]]>
                </CONSEQUENCE>
                <SOLUTION>
```

```
                    <![CDATA[The vendor has released a hotfix to patch this
vulnerability.<P>
Workaround:<BR>
Restrict public access to the CFIDE/administrator, CFIDE/adminapi and
CFIDE/gettingstarted directories.]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[coreimpact]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2013-3336]]>
                                    </REF>
                                    <DESC>
                                       <![CDATA[Adobe ColdFusion l10n.cfm
Remote Code Execution Exploit]]>
                                    </DESC>
                                    <LINK>
                                        <![CDATA[https://url.com/core-
labs/exploits]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[nist-nvd2]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2013-3336]]>
                                    </REF>
                                    <DESC>
                                       <![CDATA[Unspecified vulnerability
in Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote attackers to
read arbitrary files via unknown vectors.]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/exploits/25305]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[exploitdb]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
```

```
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2013-3336]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[ColdFusion 9-10 -
Credential Disclosure]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/exploits/25305]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                    </EXPLOITS>
                </CORRELATION>
                <PCI_FLAG>1</PCI_FLAG>
                <THREAT_INTELLIGENCE>
                    <THREAT_INTEL id="12">
                        <![CDATA[Predicted_High_Risk]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="14">
                        <![CDATA[Unauthenticated_Exploitation]]>
                    </THREAT_INTEL>
                    <THREAT_INTEL id="15">
                        <![CDATA[Remote_Code_Execution]]>
                    </THREAT_INTEL>
                </THREAT_INTELLIGENCE>
                <DISCOVERY>
                    <REMOTE>1</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Windows</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
            <VULN>
                <QID>19088</QID>
                <VULN_TYPE>Vulnerability or Potential
Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>4</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[IBM DB2 Remote Command Server Privilege
Escalation Vulnerability]]>
                </TITLE>
                <CATEGORY>Database</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2024-09-
03T00:00:01Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2004-04-
08T18:23:47Z</PUBLISHED_DATETIME>
                <BUGTRAQ_LIST>
                    <BUGTRAQ>
```

```
                        <ID>
                            <![CDATA[9821]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com/bid/9821]]>
                        </URL>
                    </BUGTRAQ>
                </BUGTRAQ_LIST>
                <PATCHABLE>1</PATCHABLE>
                <PATCH_PUBLISHED_DATE>2004-02-
20T00:00:00Z</PATCH_PUBLISHED_DATE>
                <SOFTWARE_LIST>
                    <SOFTWARE>
                        <PRODUCT>
                            <![CDATA[db2_universal_database]]>
                        </PRODUCT>
                        <VENDOR>
                            <![CDATA[ibm]]>
                        </VENDOR>
                    </SOFTWARE>
                </SOFTWARE_LIST>
                <VENDOR_REFERENCE_LIST>
                    <VENDOR_REFERENCE>
                        <ID>
                            <![CDATA[IY53894]]>
                        </ID>
                        <URL>

<![CDATA[https://url.com/support/docview.wss?uid=swg1IY53894]]>
                        </URL>
                    </VENDOR_REFERENCE>
                </VENDOR_REFERENCE_LIST>
                <CVE_LIST>
                    <CVE>
                        <ID>
                            <![CDATA[CVE-2004-0795]]>
                        </ID>
                        <URL>
                            <![CDATA[https://url.com/cgi-
bin/cvename.cgi?name=CVE-2004-0795]]>
                        </URL>
                    </CVE>
                </CVE_LIST>
                <DIAGNOSIS>
                    <![CDATA[The database server includes a component
called the Remote Command Server to facilitate execution of commands by
remote clients.
<P>
IBM DB2 Remote Command Server is prone to a vulnerability that may permit
authenticated users to gain administrative access to the underlying
database.]]>
                </DIAGNOSIS>
                <CONSEQUENCE>
                   <![CDATA[By exploiting this vulnerability, an attacker
```

```
may execute arbitrary commands with the escalated privileges of the
&amp;quot;db2admin&amp;quot; account. This issue could be exploited by a Windows
&amp;quot;Guest&amp;quot; account.]]>
                </CONSEQUENCE>
                <SOLUTION>
                    <![CDATA[Information about this issue is provided in
<A HREF="http://www-01.ibm.com/support/docview.wss?uid=swg1IY53894"
TARGET="_blank">APAR IY53894</A>. IBM has included a fix for this problem
in<A HREF="http://www-
01.ibm.com/support/docview.wss?rs=71&uid=swg27007053" TARGET="_blank">DB2
Version 8 FixPak 5</A>. ]]>
                </SOLUTION>
                <CORRELATION>
                    <EXPLOITS>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[metasploit]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2004-0795]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[IBM DB2 db2rcmd.exe
Command Execution Vulnerability]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/rapid7/metasploit-
framework/master/modules/auxiliary/admin/db2/db2rcmd.rb]]>
                                    </LINK>
                                </EXPLT>
                            </EXPLT_LIST>
                        </EXPLT_SRC>
                        <EXPLT_SRC>
                            <SRC_NAME>
                                <![CDATA[Metasploit]]>
                            </SRC_NAME>
                            <EXPLT_LIST>
                                <EXPLT>
                                    <REF>
                                        <![CDATA[CVE-2004-0795]]>
                                    </REF>
                                    <DESC>
                                        <![CDATA[IBM DB2 db2rcmd.exe
Command Execution Vulnerability - Metasploit Ref :
/modules/auxiliary/admin/db2/db2rcmd]]>
                                    </DESC>
                                    <LINK>

<![CDATA[https://url.com/rapid7/metasploit-
framework/blob/master//modules/auxiliary/admin/db2/db2rcmd.rb]]>
                                    </LINK>
```

```
                                    </EXPLT>
                                </EXPLT_LIST>
                            </EXPLT_SRC>
                            <EXPLT_SRC>
                                <SRC_NAME>
                                    <![CDATA[packetstorm]]>
                                </SRC_NAME>
                                <EXPLT_LIST>
                                    <EXPLT>
                                        <REF>
                                            <![CDATA[CVE-2004-0795]]>
                                        </REF>
                                        <DESC>
                                            <![CDATA[IBM DB2 Db2rcmd.exe
Command Execution]]>
                                        </DESC>
                                        <LINK>

<![CDATA[https://url.com/files/180775/IBM-DB2-Db2rcmd.exe-Command-
Execution.html]]>
                                        </LINK>
                                    </EXPLT>
                                </EXPLT_LIST>
                            </EXPLT_SRC>
                        </EXPLOITS>
                    </CORRELATION>
                    <PCI_FLAG>1</PCI_FLAG>
                    <THREAT_INTELLIGENCE>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="5">
                            <![CDATA[Easy_Exploit]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="6">
                            <![CDATA[High_Data_Loss]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="7">
                            <![CDATA[Denial_of_Service]]>
                        </THREAT_INTEL>
                        <THREAT_INTEL id="13">
                            <![CDATA[Privilege_Escalation]]>
                        </THREAT_INTEL>
                    </THREAT_INTELLIGENCE>
                    <DISCOVERY>
                        <REMOTE>1</REMOTE>
                        <AUTH_TYPE_LIST>
                            <AUTH_TYPE>Windows</AUTH_TYPE>
                        </AUTH_TYPE_LIST>
                        <ADDITIONAL_INFO>Patch Available, Exploit
Available</ADDITIONAL_INFO>
                    </DISCOVERY>
                </VULN>
                </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

DTD

<platform API server>/api/4.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	API Status	Release Date
/api/4.0/fo/knowledge_base/vuln/?action=list	Active	Active
/api/3.0/fo/knowledge_base/vuln/?action=list	August 2026	February 2027
/api/2.0/fo/knowledge_base/vuln/?action=list	December 2025	December 2026

KnowledgeBase QVS Download in JSON Format

For API version information, refer to the API Version History section.

V2.0|V3.0

V2.0

/api/2.0/fo/knowledge_base/qvs/?action=list

[GET] [POST]

Use this API endpoint to download Qualys Vulnerability Score (QVS) information from the Vulnerability KnowledgeBase for one or more CVE IDs based on certain criteria. The API output is in JSON format.

The Qualys Vulnerability Score (QVS) is a Qualys-assigned score to a vulnerability based on multiple factors associated with the CVE, such as CVSS, EPSS (Exploit Prediction Scoring System) and external threat indicators like active exploitation, exploit code maturity and much more.

Input Parameters

Use the following input parameters.

Parameter	Description
action=list	(Required) You must specify the list action. **Note:** Specify the list action to retrieve all CVEs published or last modified within the past 90 days from the current date.
details={Basic|All}	(Required) Specify details to show the base QVS in the output. Specify details=All to show the base QVS and contributing factors in the output. **Note:** Specify the details parameter to retrieve all CVEs published or last modified within the past 90 days from the current date.
cve={value}	(Required) Filter the JSON output to only show vulnerabilities associated with the CVE IDs that you specify. The associated vulnerabilities are shown only when the requested CVE is published.
qvs_last_modified_before={date}	(Optional) Show only CVE IDs with a QVS score that was last modified before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-1201T23:12:00Z”.
qvs_last_modified_after={date}	(Optional) Show only CVE IDs with a QVS score that was last modified after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
qvs_min={value}	(Optional) Show only CVEs with a QVS value greater than or equal to the QVS min value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value.

Parameter	Description
qvs_max={value}	(Optional) Show only CVEs with a QVS value less than or equal to the QVS max value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value.
nvd_published_before={date}	(Optional) Show only CVE IDs with a QVS score that was published before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
nvd_published_after={date}	(Optional) Show only CVE IDs with a QVS score that was published after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.

Sample KnowledgeBase QVS Download

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/knowledge_base/qvs/?action=list&cve=CVE-
2021-36764%2CCVE-2021-36765%2CCVE-2021-36798%2CCVE-2017-
0199&details=All'\
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

JSON output:

```
{
{
    "CVE-2021-36764": {
        "base": {
            "id": "CVE-2021-36764",
            "idType": "CVE",
            "qvs": "35",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1628086500
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:N\/I:N\/A:H",
            "epss": [
                "0.00089"
            ]
        }
    },
    "CVE-2021-36765": {
        "base": {
```

```
            "id": "CVE-2021-36765",
            "idType": "CVE",
            "qvs": "35",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1628086500
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:H\/I:N\/A:N",
            "epss": [
                "0.00152"
            ]
        }
    },
    "CVE-2021-36798": {
        "base": {
            "id": "CVE-2021-36798",
            "idType": "CVE",
            "qvs": "41",
            "qvsLastChangedDate": 1704844800,
            "nvdPublishedDate": 1628514900
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:N\/I:N\/A:H",
            "exploitMaturity": [
                "poc"
            ],
            "epss": [
                "0.00246"
            ]
        }
    }
}
{
"CVE-2017-0199": {
        "base": {
            "id": "CVE-2017-0199",
            "idType": "CVE",
            "qvs": "100",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1492009141
```

```
        },
        "contributingFactors": {
            "cvss": "9.3",
            "cvssVersion": "v2",
            "cvssString": "AV:N\/AC:M\/Au:N\/C:C\/I:C\/A:C",
            "threatActors": [
                "Stardust Chollima,Cobalt Spider,APT43,Mythic
Leopard,SectorJ,APT41,Whisper
Spider,SideWinder,Silence,APT34,Kimsuky,Primitive
Bear,TA459,Mustang Panda,Cobalt,Gorgon Group,Gothic
Panda,Codoso,LABYRINTH CHOLLIMA,Pioneer Kitten,TA558,Dropping
Elephant,Subaat,Quilted Tiger,Saaiwc Group,OilRig,Ocean
Buffalo,APT19,China Attribution,Helix Kitten,Slayer Kitten,Lazarus
Group,Velvet Chollima,BlackTech,Leviathan,SectorA,Dark
Pink,CopyKittens,Razor Tiger,Gamaredon,PARASITE,Shadow Crane,Stone
Panda,Labyrinth Chollima,Molerats,Kryptonite
Panda,FIN7,DarkHotel,North Korea Attribution,Unattributed,Ricochet
Chollima,Circuit Panda,RedAlpha,Carbon Spider,Wicked
Panda,CHRYSENE,MuddyWater,Luckycat,GreyEnergy,Static Kitten,APT37"
            ],
            "exploitMaturity": [
                "poc,weaponized"
            ],
            "trending": [

"10302025,11052025,11032025,10152025,10142025,11022025,11082025,11
072025,11102025,10292025,10132025,11012025,10282025,10312025"
            ],
            "malwareName": [

"Leonem,SLoad,Relsloadr,Donoff,Blinky,MalLink,Nemucod,Oneeva,Meter
preter,Emotet,Petya,Pterodo,Powsheldow,IcedID,Amphitryon,Snakekeyl
ogger,Kepavll,Cerber,Cryxos,LokiBot,Powdow,Downlaoder,Valyria,Alie
n,Bladabhindi,Privateloader,Pidief,Aentdwn,Pantera,Farheyt,Relslod
r,DdexLoader,AgentTesla,RTFObfustream,MacroLess,Badur,Razy,Snojan,
DdeExec,FormBook,Stelega,TurtleLoader,Generic,WannaCry,EncDoc,Remc
os,Negasteal,CobaltStrikeBeacon,Skeeyah,Bitrep,Encrypteddoc,Abnorm
al,Sonoko,Ymacco,Dotmer,Loki,Powload,Heuristic,RemoteTemplateInj,M
esdettyLaunch,GenScript,BlackKingdom,Rasftuby,LockerGoga,Stratos,M
adefref,PhishingAdb,Bluteal,Androm,Multiverze,Disco,Znyonm,Upatre,
Phonzy,Rozena,Tiggre,Casur,Occamy,Zpevdo,Johnnie,NanoCore,SDrop,Pe
derr,BadTemplate,Ako,Symmi,Toncteseg,Zenpak,Gluptel,Vigorf,DllHija
ck,Primarypass,Ofckit,CVE-2017-
0199,Risepro,Olemalrtf,Psyme,SpamDocCrypted,Unattributed,Pyfatget,
Malgent,Groooboor,Gozi,Wacatac"
            ],
            "malwareHash": [
```

```
"7f2a499891a72b9f3b0923be0f9db490463639166b41a15fe3bf5387df660f1c"
,
"d73c616eaef3c683005a799b7420bae06bd5cd094d3923409f1611de67d4b82f"
,
"54874f342f9e4d93ccba0208446e6699c489e1f1d99f396c358df63cdfa4535f"
,
"e29ebea9db086b874310403868dc233b6c03e4305bebca507dbd53f36170dba8"
,
"645434d52d7e12dbae40d46fef28870785e74d0126d9cead76f46d65fc283a7f"
,
"34717e10b0f170025c3e380fb0287fe3c1f3347e3071c79c1e39ea94a489e6f7"
            ],
            "rti": [
                "dos,remote"
            ],
            "epss": [
                "0.xxxx"
            ],
            "cisaVuln": [
                "YES"
            ],
            "cisaDueDate": "1651536000000",
            "cisaAddedDate": "1635897600000"
        }
    }
}
}
```


V3.0

/api/3.0/fo/knowledge_base/qvs/?action=list

[GET] [POST]

Use this API endpoint to download Qualys Vulnerability Score (QVS) information from the Vulnerability KnowledgeBase for one or more CVE IDs based on certain criteria. The API output is in JSON format.

The Qualys Vulnerability Score (QVS) is a Qualys-assigned score to a vulnerability based on multiple factors associated with the CVE, such as CVSS, EPSS (Exploit Prediction Scoring System) and external threat indicators like active exploitation, exploit code maturity and much more.

Input Parameters

Use the following input parameters.

Parameter	Description
action=list	(Required) You must specify the list action. **Note:** Specify the list action to retrieve all CVEs published or last modified within the past 90 days from the current date..
details={Basic|All}	(Required) Specify details to show the base QVS in the output. Specify details=All to show the base QVS and contributing factors in the output. **Note:** Specify the details parameter to retrieve all CVEs published or last modified within the past 90 days from the current date.
cve={value}	(Optional) Filter the JSON output to show only the CVEs for which the QVS is recently updated. The associated vulnerabilities are shown only when the requested CVE is published.
qvs_last_modified_before={date}	(Optional) Show only CVE IDs with a QVS score that was modified for the last 15 days before a specific date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-1201T23:12:00Z”.
qvs_last_modified_after={date}	(Optional) Show only CVE IDs with a QVS score that was modified within the next 15 days after a specific date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
qvs_min={value}	(Optional) Show only CVEs with a QVS value greater than or equal to the QVS min value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value. **Note:** This shows only the CVEs with a QVS score that was modified for the last 15 days.
qvs_max={value}	(Optional) Show only CVEs with a QVS value less than or equal to the QVS max value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value. **Note:** This shows only the CVEs with a QVS score that was modified for the last 15 days.
nvd_published_before={date}	(Optional) Show only the CVE IDs with modified QVS scores from the past 15 days that were published before a specified date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
nvd_published_after={date}	(Optional) Show only the CVE IDs where the QVS scores have been updated and published within the next 15 days, starting from a specified date and time.Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.

Sample - KnowledgeBase QVS Download

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&cve=CVE-
2021-36764%2CCVE-2021-36765%2CCVE-2021-36798%2CCVE-2017-
0199&details=All'\
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

JSON output:


```
{
{
    "CVE-2021-36764": {
        "base": {
            "id": "CVE-2021-36764",
            "idType": "CVE",
            "qvs": "35",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1628086500
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:N\/I:N\/A:H",
            "epss": [
                "0.00089"
            ]
        }
    },
    "CVE-2021-36765": {
        "base": {
            "id": "CVE-2021-36765",
            "idType": "CVE",
            "qvs": "35",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1628086500
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:H\/I:N\/A:N",
            "epss": [
                "0.00152"
            ]
```

```
        }
    },
    "CVE-2021-36798": {
        "base": {
            "id": "CVE-2021-36798",
            "idType": "CVE",
            "qvs": "41",
            "qvsLastChangedDate": 1704844800,
            "nvdPublishedDate": 1628514900
        },
        "contributingFactors": {
            "cvss": "7.5",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:N\/I:N\/A:H",
            "exploitMaturity": [
                "poc"
            ],
            "epss": [
                "0.00246"
            ]
        }
    }
}
{
"CVE-2017-0199": {
        "base": {
            "id": "CVE-2017-0199",
            "idType": "CVE",
            "qvs": "100",
            "qvsLastChangedDate": 1664755200,
            "nvdPublishedDate": 1492009141
        },
        "contributingFactors": {
            "cvss": "9.3",
            "cvssVersion": "v2",
            "cvssString": "AV:N\/AC:M\/Au:N\/C:C\/I:C\/A:C",
            "threatActors": [
                "Stardust Chollima,Cobalt Spider,APT43,Mythic
Leopard,SectorJ,APT41,Whisper
Spider,SideWinder,Silence,APT34,Kimsuky,Primitive
Bear,TA459,Mustang Panda,Cobalt,Gorgon Group,Gothic
Panda,Codoso,LABYRINTH CHOLLIMA,Pioneer Kitten,TA558,Dropping
Elephant,Subaat,Quilted Tiger,Saaiwc Group,OilRig,Ocean
Buffalo,APT19,China Attribution,Helix Kitten,Slayer Kitten,Lazarus
Group,Velvet Chollima,BlackTech,Leviathan,SectorA,Dark
```

```
Pink,CopyKittens,Razor Tiger,Gamaredon,PARASITE,Shadow Crane,Stone
Panda,Labyrinth Chollima,Molerats,Kryptonite
Panda,FIN7,DarkHotel,North Korea Attribution,Unattributed,Ricochet
Chollima,Circuit Panda,RedAlpha,Carbon Spider,Wicked
Panda,CHRYSENE,MuddyWater,Luckycat,GreyEnergy,Static Kitten,APT37"
            ],
            "exploitMaturity": [
                "poc,weaponized"
            ],
            "trending": [

"10302025,11052025,11032025,10152025,10142025,11022025,11082025,11
072025,11102025,10292025,10132025,11012025,10282025,10312025"
            ],
            "malwareName": [

"Leonem,SLoad,Relsloadr,Donoff,Blinky,MalLink,Nemucod,Oneeva,Meter
preter,Emotet,Petya,Pterodo,Powsheldow,IcedID,Amphitryon,Snakekeyl
ogger,Kepavll,Cerber,Cryxos,LokiBot,Powdow,Downlaoder,Valyria,Alie
n,Bladabhindi,Privateloader,Pidief,Aentdwn,Pantera,Farheyt,Relslod
r,DdexLoader,AgentTesla,RTFObfustream,MacroLess,Badur,Razy,Snojan,
DdeExec,FormBook,Stelega,TurtleLoader,Generic,WannaCry,EncDoc,Remc
os,Negasteal,CobaltStrikeBeacon,Skeeyah,Bitrep,Encrypteddoc,Abnorm
al,Sonoko,Ymacco,Dotmer,Loki,Powload,Heuristic,RemoteTemplateInj,M
esdettyLaunch,GenScript,BlackKingdom,Rasftuby,LockerGoga,Stratos,M
adefref,PhishingAdb,Bluteal,Androm,Multiverze,Disco,Znyonm,Upatre,
Phonzy,Rozena,Tiggre,Casur,Occamy,Zpevdo,Johnnie,NanoCore,SDrop,Pe
derr,BadTemplate,Ako,Symmi,Toncteseg,Zenpak,Gluptel,Vigorf,DllHija
ck,Primarypass,Ofckit,CVE-2017-
0199,Risepro,Olemalrtf,Psyme,SpamDocCrypted,Unattributed,Pyfatget,
Malgent,Groooboor,Gozi,Wacatac"
            ],
            "malwareHash": [

"7f2a499891a72b9f3b0923be0f9db490463639166b41a15fe3bf5387df660f1c"
,

"d73c616eaef3c683005a799b7420bae06bd5cd094d3923409f1611de67d4b82f"
,

"54874f342f9e4d93ccba0208446e6699c489e1f1d99f396c358df63cdfa4535f"
,

"e29ebea9db086b874310403868dc233b6c03e4305bebca507dbd53f36170dba8"
,

"645434d52d7e12dbae40d46fef28870785e74d0126d9cead76f46d65fc283a7f"
,
```

```
"34717e10b0f170025c3e380fb0287fe3c1f3347e3071c79c1e39ea94a489e6f7"
            ],
            "rti": [
                "dos,remote"
            ],
            "epss": [
                "0.xxxx"
            ],
            "cisaVuln": [
                "YES"
            ],
            "cisaDueDate": "1651536000000",
            "cisaAddedDate": "1635897600000"
        }
    }
}
```


}**Sample - KnowledgeBase QVS last modified before a given date**

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&qvs
_last_modified_before=2024-08-15' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic username:password string'
```

JSON output:


```
{
"CVE-2017-16260": {
"base": {
"id": "CVE-2017-16260",
"idType": "CVE",
"qvs": "72",
"qvsLastChangedDate": 1722988800,
"nvdPublishedDate": 1673475300
}
},
"CVE-2017-16261": {
"base": {
"id": "CVE-2017-16261",
"idType": "CVE",
"qvs": "42",
"qvsLastChangedDate": 1722988800,
"nvdPublishedDate": 1673475300
}
},
```

```
"CVE-2017-16262": {
"base": {
"id": "CVE-2017-16262",
"idType": "CVE",
"qvs": "72",
"qvsLastChangedDate": 1722988800,
"nvdPublishedDate": 1673475300
}
},
"CVE-2023-23948": {
"base": {
"id": "CVE-2023-23948",
"idType": "CVE",
"qvs": "37",
"qvsLastChangedDate": 1722902400,
"nvdPublishedDate": 1676308500
}
},
"CVE-2017-16263": {
"base": {
"id": "CVE-2017-16263",
"idType": "CVE",
"qvs": "72",
"qvsLastChangedDate": 1722988800,
"nvdPublishedDate": 1673475300
}
}
```


Sample - KnowledgeBase QVS last modified after a given date

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&qvs
_last_modified_after=2024-09-05&details=All' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic username:password string'
```

JSON output:


```
{
"CVE-2024-38858": {
"base": {
"id": "CVE-2024-38858",
"idType": "CVE",
"qvs": "30",
"qvsLastChangedDate": 1725494400,
"nvdPublishedDate": 1725279319
},
```

```
"contributingFactors": {
"cvss": "6.1",
"cvssVersion": "v3.x",
"cvssString":
"CVSS:3.1\/AV:N\/AC:L\/PR:N\/UI:R\/S:C\/C:L\/I:L\/A:N",
"trending": [
"09032024,09042024,08272024,08282024"
],
"epss": [
"0.00043"
]
}
},
"CVE-2018-19183": {
"base": {
"id": "CVE-2018-19183",
"idType": "CVE",
"qvs": "41",
"qvsLastChangedDate": 1725494400,
"nvdPublishedDate": 1541989740
},
"contributingFactors": {
"cvss": "7.5",
"cvssVersion": "v3.x",
"cvssString":
"CVSS:3.1\/AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:N\/I:N\/A:H",
"exploitMaturity": [
"poc"
],
"epss": [
"0.00416"
]
}
}
```


Sample - Display CVEs for QVS minimum

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&det
ails=All&qvs_min=95' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic username:password string'
```

JSON output:


```
{
"CVE-2024-38856": {
```

```
"base": {
"id": "CVE-2024-38856",
"idType": "CVE",
"qvs": "95",
"qvsLastChangedDate": 1725956542967,
"nvdPublishedDate": 1722849356
},
"contributingFactors": {
"cvss": "9.8",
"cvssVersion": "v3.x",
"cvssString":
"CVSS:3.1\/AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:H\/I:H\/A:H",
"threatActors": [
"Unattributed"
],
"exploitMaturity": [
"weaponized,poc"
],
"trending": [
"08182024,08232024,08092024,08062024,08072024,08262024,08132024,08
292024,08302024,08152024,08212024,08112024,08202024,08282024,08252
024,08242024,08162024,08042024,08122024"
],
"epss": [
"0.93274"
]
}
},
"CVE-2019-18988": {
"base": {
"id": "CVE-2019-18988",
"idType": "CVE",
"qvs": "95",
"qvsLastChangedDate": 1725956542967,
"nvdPublishedDate": 1581092100
},
"contributingFactors": {
"cvss": "7.0",
"cvssVersion": "v3.x",
"cvssString": "AV:L\/AC:H\/PR:L\/UI:N\/S:U\/C:H\/I:H\/A:H",
"exploitMaturity": [
"poc,weaponized"
],
"trending": [
"07052024"
],
```

```
"epss": [
"0.00358"
]
}
}
```

Sample - Display CVEs for QVS maximum

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&det
ails=All&qvs_max=95' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic username:password string'
```

JSON output:

```
{
    "CVE-2017-16260": {
        "base": {
            "id": "CVE-2017-16260",
            "idType": "CVE",
            "qvs": "71",
            "qvsLastChangedDate": 1725580800,
            "nvdPublishedDate": 1673475300
        },
        "contributingFactors": {
            "cvss": "9.9",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:L\/UI:N\/S:C\/C:H\/I:H\/A:H",
            "exploitMaturity": [
                "poc"
            ],
            "epss": [
                "0.00091"
            ]
        }
    },
    "CVE-2017-16261": {
        "base": {
            "id": "CVE-2017-16261",
            "idType": "CVE",
            "qvs": "41",
            "qvsLastChangedDate": 1725580800,
            "nvdPublishedDate": 1673475300
        },
        "contributingFactors": {
```

```
            "cvss": "8.8",
            "cvssVersion": "v3.x",
            "cvssString":
"AV:N\/AC:L\/PR:L\/UI:N\/S:U\/C:H\/I:H\/A:H",
            "exploitMaturity": [
                "poc"
            ],
            "epss": [
                "0.00091"
            ]
        }
    }
```

Sample - Display CVEs within QVS min and QVS max

API request:

```
curl --location
'https://<qualys_base_url>/api/3.0/fo/knowledge_base/qvs/?action=list&det
ails=All&qvs_min=95&qvs_max=96' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic username:password string'
```

JSON output:

```
{
"CVE-2024-38856": {
"base": {
"id": "CVE-2024-38856",
"idType": "CVE",
"qvs": "95",
"qvsLastChangedDate": 1725958333539,
"nvdPublishedDate": 1722849356
},
"contributingFactors": {
"cvss": "9.8",
"cvssVersion": "v3.x",
"cvssString":
"CVSS:3.1\/AV:N\/AC:L\/PR:N\/UI:N\/S:U\/C:H\/I:H\/A:H",
"threatActors": [
"Unattributed"
],
"exploitMaturity": [
"weaponized,poc"
],
"trending": [
"08182024,08232024,08092024,08062024,08072024,08262024,08132024,08
292024,08302024,08152024,08212024,08112024,08202024,08282024,08252
024,08242024,08162024,08042024,08122024"
```

```
],
"epss": [
"0.93274"
]
}
},
"CVE-2019-18988": {
"base": {
"id": "CVE-2019-18988",
"idType": "CVE",
"qvs": "95",
"qvsLastChangedDate": 1725958333539,
"nvdPublishedDate": 1581092100
},
"contributingFactors": {
"cvss": "7.0",
"cvssVersion": "v3.x",
"cvssString": "AV:L\/AC:H\/PR:L\/UI:N\/S:U\/C:H\/I:H\/A:H",
"exploitMaturity": [
"poc,weaponized"
],
"trending": [
"07052024"
],
"epss": [
"0.00358"
]
}
```


API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/knowledge_base/qvs/?action=list	Active	Active
/api/2.0/fo/knowledge_base/qvs/?action=list	December 2025	December 2026

Editing Vulnerabilities

/api/2.0/fo/knowledge_base/vuln/

[POST]

Edit, reset and list the edited vulnerabilities in the Qualys Vulnerability KnowledgeBase.

Permissions - Managers have permissions to edit vulnerabilities and make API requests to edit a vulnerability, reset a vulnerability and list customized vulnerabilities.

Edit a vulnerability

You can change the severity level and/or add comments to Threat, Impact or Solution. Providing at least one optional parameter is mandatory.

Parameter	Description
action=edit	(Required) POST method is required
qid={value}	(Required) QID of the vulnerability to be edited.
severity={value}	(Optional) Severity level between 1 to 5. Changing the severity level of a vulnerability impacts how the vulnerability appears in reports and how it is eventually prioritized for remediation. For example, by changing a vulnerability from a severity 2 to a severity 5, remediation tickets for the vulnerability could have a higher priority and shorter deadline for resolution.
disable={**0**|1}	(Optional) Specify 1 to disable the vulnerability. Default is 0. When you disable a vulnerability it is globally filtered out from all hosts in all scan reports. The vulnerability is also filtered from host information, asset search results and your dashboard. You may include disabled vulnerabilities in scan reports by changing report filter settings.
threat_comment	(Optional) Threat comments in plain text.
impact_comment	(Optional) Impact comments in plain text.
solution_comment	(Optional) Solution comments in plain text.

Comments added for Threat, Impact, or Solution are appended to the service-provided descriptions in the vulnerability details.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=edit&impact_comment=testimpact&qid=27014"
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2017-03-02T08:51:59Z</DATETIME>
       <TEXT>Custom Vuln Data has been updated successfully</TEXT>
```

```
            <ITEM_LIST>
                <ITEM>
                    <KEY>qid</KEY>
                    <VALUE>27014</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Reset a vulnerability

You can change the vulnerability settings back to original.

Parameter	Description
action=reset	(Required) POST method is required
qid={value}	(Required) QID of the vulnerability to be reset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=reset&qid=27014"
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2017-03-02T08:55:11Z</DATETIME>
        <TEXT>Custom Vuln Data has been reset successfully</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

List customized vulnerabilities

You can list the vulnerabilities that are edited.

Parameter	Description
action=custom	(Required) GET or POST method can be used.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=custom"
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KB_CUSTOM_VULN_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_l
ist_output.dtd">
<KB_CUSTOM_VULN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2017-03-02T08:47:52Z</DATETIME>
        <CUSTOM_VULN_LIST>
            <CUSTOM_VULN_DATA>
                <QID>
                    <![CDATA[27014]]>
                </QID>
                <SEVERITY_LEVEL>5</SEVERITY_LEVEL>

<ORIGINAL_SEVERITY_LEVEL>5</ORIGINAL_SEVERITY_LEVEL>
                <IS_DISABLED>1</IS_DISABLED>
                <UPDATED_DATETIME>
                    <![CDATA[2017-03-02T05:58:40Z]]>
                </UPDATED_DATETIME>
                <UPDATED_BY>
                    <![CDATA[mr_md]]>
                </UPDATED_BY>
                <THREAT_COMMENT>
                    <![CDATA[threat123]]>
                </THREAT_COMMENT>
                <IMPACT_COMMENT>
                    <![CDATA[impact123]]>
                </IMPACT_COMMENT>
                <SOLUTION_COMMENT>
                    <![CDATA[solution123]]>
                </SOLUTION_COMMENT>
            </CUSTOM_VULN_DATA>
        </CUSTOM_VULN_LIST>
    </RESPONSE>
</KB_CUSTOM_VULN_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_list_output.dtd

Static Search Lists

/api/2.0/fo/qid/search_list/static/

Create static search lists and get information about them.

Permissions - as below.

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Create, update, list and delete search lists.
Auditor	No permission to create, update, list and delete search lists.

List static search lists

Input parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
ids={id1,id2...}	(Optional) One or more search list IDs to display. Multiple IDs are comma separated.

Sample - List static search list

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/qid/search_list/static/?action=list&
ids=381"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE STATIC_SEARCH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/qid/search_list/static/static_list_o
utput.dtd">
<STATIC_SEARCH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-06T06:20:03Z</DATETIME>
    <STATIC_LISTS>
      <STATIC_LIST>
        <ID>381</ID>
        <TITLE><![CDATA[static search list]]></TITLE>
        <GLOBAL>Yes</GLOBAL>
        <OWNER>acme_tb</OWNER>
        <CREATED><![CDATA[06/01/2018 at 15:18:42
(GMT+0530)]]></CREATED>
        <MODIFIED_BY>acme_tb</MODIFIED_BY>
        <MODIFIED><![CDATA[06/02/2018 at 15:18:42
(GMT+0530)]]></MODIFIED>
```

```
        <QIDS>
          <QID>1000<QID>
          <QID>1001<QID>
        </QIDS>
       <!-- This list is used in the following option profiles //-
->
        <OPTION_PROFILES>
            <OPTION_PROFILE>
                <ID>135<ID>
                <TITLE><![CDATA[Initial Options]]></TITLE>
            <OPTION_PROFILE>
        </OPTION_PROFILES>
        <!-- This list is used in the following report templates
//-->
        <REPORT_TEMPLATES>
            <REPORT_TEMPLATE>
                <ID>256<ID>
                <TITLE><![CDATA[Scan Report Template]]></TITLE>
            <REPORT_TEMPLATE>
        </REPORT_TEMPLATES>
        <!-- This list is used in the following remediation
policies. //-->
        <REMEDIATION_POLICIES>
            <REMEDIATION_POLICY>
                <ID>655<ID>
                <TITLE><![CDATA[Remediation Policy 1]]></TITLE>
            <REMEDIATION_POLICY>
        </REMEDIATION_POLICIES>
        <!-- This search list is associated with following
distribution groups. //-->
        <DISTRIBUTION_GROUPS>
            <DISTRIBUTION_GROUP>
                <NAME><![CDATA[All]]></NAME>
            <DISTRIBUTION_GROUP>
        </DISTRIBUTION_GROUPS>
        <COMMENTS><![CDATA[This is my first comment for this
list]]></COMMENTS>
      </STATIC_LIST>
   </STATIC_LISTS>
  </RESPONSE>
</SEARCH_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/qid/search_list/static/static_list_output.dtd

Create static search lists

Input parameters

Parameter	Description
action=create	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
title={value}	(Required) A user defined search list title. Maximum is 256 characters (ascii).
qids=(num1, num2...}	(Required) QIDs to include in the search list. Ranges are allowed.
global={**0**|1}	(Optional) Specify 1 to make this a global search list, available to all subscription users.
comments={value}	(Optional) User defined comments.

Sample - Create search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=My+Static+Search+List&qids=68518-68522,48000"
"<qualys_base_url>/api/2.0/fo/qid/search_list/static/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>New search list created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update static search list

Input parameters

Parameter	Description
action=update	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to update.
title={value}	(Optional) The search list title. Maximum is 256 characters (ascii).
global={0|1}	(Optional) Specify 1 to make this a global search list.
qids=(num1, num2...}	(Optional) QIDs/ranges to include in the search list. Multiple entries are comma separated. ***QIDs specified will replace all existing ones defined for the search list, if any.
	qids cannot be specified with add_qids or remove_qids in the same request.
add_qids=(num1, num2...}	(Optional) QIDs/ranges you want to add to the existing ones defined for the search list. When the same QIDs are passed using add_qids and remove_qids in the same request, the QIDs are added to the list.
	add_qids cannot be specified with qids in the same request.
remove_qids=(num1, num2...}	(Optional) QIDs/ranges you want to remove the existing ones defined for the search list. When the same QIDs are passed using add_qids and remove_qids in the same request, the QIDs are added to the list.
	remove_qids cannot be specified with qids in the same request.
comments={value}	(Optional) User defined comments.

Sample - Update static search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=136992&global=1&qids=68518-68522,48000-48004"
"<qualys_base_url>/api/2.0/fo/qid/search_list/static/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>Search list updated successfully</TEXT>
    <ITEM_LIST>
```

```
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Delete static search list

Input parameters

Parameter	Description
action=delete	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to delete.

Sample - Delete static search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&id=136992"
"<qualys_base_url>/api/2.0/fo/qid/search_list/static/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>search list deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Dynamic Search Lists

For API version information, refer to the API Version History section.

V2.0 | V3.0

V2.0

/api/2.0/fo/qid/search_list/dynamic/

Create dynamic search lists and get information about them.

Permissions - as described below

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Create, update, list and delete search lists.
Auditor	No permission to create, update, list and delete search lists.

List dynamic search lists

Input parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
ids={id1,id2...}	(Optional) One or more search list IDs to display. Multiple IDs are comma separated.
show_qids={0|**1**}	(Optional) Set to 0 to hide QIDs defined for each search list in the XML output. By default these QIDs are shown.
show_option_profiles={0|**1**}	(Optional) Set to 0 to hide option profiles associated with each search list in the XML output. By default these option profiles are shown.
show_distribution_groups={0|**1**}	(Optional) Set to 0 to hide distribution groups associated with each search list in the XML output. By default these distribution groups are shown.
show_report_templates={0|**1**}	(Optional) Set to 0 to hide report templates associated with each search list in the XML output. By default these report templates will be shown.
show_remediation_policies={0|**1**}	(Optional) Set to 0 to hide remediation policies associated with each search list in the XML output. By default these remediation policies will be shown.

Sample - List dynamic search list

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/?action=list
&ids=381"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/dynamic_list
_output.dtd">
<SEARCH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2015-01-06T06:20:03Z</DATETIME>
    <DYNAMIC_LISTS>
      <DYNAMIC_LIST>
        <ID>381</ID>
        <TITLE><![CDATA[static search list]]></TITLE>
        <GLOBAL>Yes</GLOBAL>
        <OWNER>acme_tb</OWNER>
        <CREATED><![CDATA[07/27/2015 at 15:18:42
(GMT+0530)]]></CREATED>
        <MODIFIED_BY>acme_tb</MODIFIED_BY>
        <MODIFIED><![CDATA[07/27/2015 at 15:18:42
(GMT+0530)]]></MODIFIED>
        <QIDS>
            <QID>1000<QID>
            <QID>1001<QID>
        </QIDS>
        <CRITERIA>
            <VULNERABILITY_TITLE><![CDATA[NOT
Title]]></VULNERABILITY_TITLE>
            <DISCOVERY_METHOD><![CDATA[Authenticated
Only]]></DISCOVERY_METHOD>
            <AUTHENTICATION_TYPE><![CDATA[HTTP, Oracle,
Unix]]></AUTHENTICATION_TYPE>
            <USER_CONFIGURATION><![CDATA[Disabled,
Edited]]></USER_CONFIGURATION>
          <CATEGORY><![CDATA[NOT Backdoors and trojan horses, DNS
and BIND]]> </CATEGORY>
            <CONFIRMED_SEVERITY><![CDATA[1,
2]]></CONFIRMED_SEVERITY>
            <POTENTIAL_SEVERITY><![CDATA[2,
3]]></POTENTIAL_SEVERITY>
            <INFORMATION_SEVERITY><![CDATA[4,
5]]></INFORMATION_SEVERITY>
            <VENDOR><![CDATA[NOT 2brightsparks,3com,4d]]></VENDOR>
            <PRODUCT><![CDATA[NOT .net_framework]]></PRODUCT>
            <CVSS_BASE_SCORE><![CDATA[2]]></CVSS_BASE_SCORE>

<CVSS_TEMPORAL_SCORE><![CDATA[3]]></CVSS_TEMPORAL_SCORE>
```

```
            <CVSS_ACCESS_VECTOR><![CDATA[Adjacent
Network]]></CVSS_ACCESS_VECTOR>
            <PATCH_AVAILABLE><![CDATA[Yes, No]]></PATCH_AVAILABLE>
<VIRTUAL_PATCH_AVAILABLE><![CDATA[Yes]]></VIRTUAL_PATCH_AVAILABLE>
            <CVE_ID><![CDATA[NOT CVE]]></CVE_ID>
<CVE_ID_FILTER><![CDATAContains]></CVE_ID_FILTER>
            <EXPLOITABILITY><![CDATA[ExploitKits, Immunity -
Dsquare]]> </EXPLOITABILITY>
            <ASSOCIATED_MALWARE><![CDATA[Trend
Micro]]></ASSOCIATED_MALWARE>
            <VENDOR_REFERENCE><![CDATA[NOT
Linux]]></VENDOR_REFERENCE>
          <BUGTRAQ_ID><![CDATA[NOT 15656]]></BUGTRAQ_ID>
<VULNERABILITY_DETAILS><![CDATA[details]]></VULNERABILITY_DETAILS>

<COMPLIANCE_DETAILS><![CDATA[details]]></COMPLIANCE_DETAILS>
            <COMPLIANCE_TYPE><![CDATA[PCI, CobIT, HIPAA, GLBA,
SOX]]></COMPLIANCE_TYPE>
            <QUALYS_TOP_20><![CDATA[Top Internal 10, Top External
10]]></QUALYS_TOP_20>
            <OTHER><![CDATA[Not exploitable due to configuration,
Non-running services, 2008 SANS 20]]></OTHER>
            <NETWORK_ACCESS><![CDATA[NAC / NAM]]></NETWORK_ACCESS>
            <USER_MODIFIED><![CDATA[NOT 07/27/2015-
07/27/2015]]></USER_MODIFIED>
            <PUBLISHED><![CDATA[NOT 06/02/2015-
07/20/2015]]></PUBLISHED>
            <SERVICE_MODIFIED><![CDATA[NOT Previous 1
week]]></SERVICE_MODIFIED>
        </CRITERIA>
        </CRITERIA>
       <!-- This list is used in the following option profiles //-
->
        <OPTION_PROFILES>
            <OPTION_PROFILE>
                <ID>135<ID>
                <TITLE><![CDATA[Initial Options]]></TITLE>
            <OPTION_PROFILE>
        </OPTION_PROFILES>
        <!-- This list is used in the following report templates
//-->
        <REPORT_TEMPLATES>
            <REPORT_TEMPLATE>
                <ID>256<ID>
                <TITLE><![CDATA[Scan Report Template]]></TITLE>
            <REPORT_TEMPLATE>
        </REPORT_TEMPLATES>
```

```
        <!-- This list is used in the following remediation
policies. //-->
        <REMEDIATION_POLICIES>
            <REMEDIATION_POLICY>
                <ID>655<ID>
                <TITLE><![CDATA[Remediation Policy 1]]></TITLE>
            <REMEDIATION_POLICY>
        </REMEDIATION_POLICIES>
        <!-- This search list is associated with following
distribution groups. //-->
        <DISTRIBUTION_GROUPS>
            <DISTRIBUTION_GROUP>
                <ID>226<ID>
                <TITLE><![CDATA[All]]></TITLE>
            <DISTRIBUTION_GROUP>
        </DISTRIBUTION_GROUPS>
        <COMMENTS><![CDATA[This is my first comment for this
list]]></COMMENTS>
      </DYNAMIC_LIST>
   </DYNAMIC_LISTS>
  </RESPONSE>
</SEARCH_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd

Create dynamic search list

Input parameters

Parameter	Description
action=create	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
title={value}	(Required) A user defined search list title. Maximum is 256 characters (ascii).
global={**0**|1}	(Optional) Specify 1 to make this a global search list, available to all subscription users.
comments={value}	(Optional) User defined comments.
{criteria}	(Required) User defined search criteria. See “Search criteria”

Search criteria

Use these parameters to define search criteria for dynamic search lists, using create and update requests. All parameters act as vulnerability filters.

Parameter	Value
vuln_title={value}	Vulnerability title (string); to unset value use update request and set to empty value
not_vuln_title={**0**|1}	Set to 1 for vulnerability title that does not match vuln_title parameter value
discovery_methods={value}	One or more discovery methods: Remote, Authenticated, Remote_Authenticated; by default all methods are included
auth_types={value}	One or more of these authentication types: Windows, Unix, Oracle, SNMP, VMware, DB2, HTTP, MySQL, PANOS, TOMCAT, MARIADB, MongoDB, WEBLOGIC; multiple values are comma separated; to unset value use update request and set to empty value
user_configuration={value}	One or more of these user configuration values: disabled, custom; multiple values are comma separated; to unset value use update request and set to empty value
categories={value}	One or more vulnerability category names (strings); to unset value use update request and set to empty value
not_categories={**0**|1}	Set to 1 for categories that do not match categories parameter values
confirmed_severities={value}	One or more confirmed vulnerability severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
potential_severities={value}	One or more potential vulnerability severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
ig_severities={value}	One or more information gathered severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
vendor_ids={value}	One or more vendor IDs; multiple IDs are comma separated; to unset value use update request and set to empty value
not_vendor_ids={**0**|1}	Set to 1 for vendor IDs that do not match vendor_ids parameter values
products={value}	Vendor product names; multiple names are comma separated; to unset value use update request and set to empty value

Parameter	Value
not_products={**0**|1}	Set to 1 for product names that do not match products parameter values
patch_available={value}	Vulnerabilities with patches: 0 (no), 1 (yes); by default all vulnerabilities with and without patches are included; multiple values are comma separated; to unset value use update request and set to empty value
virtual_patch_available={value}	Vulnerabilities with Trend Micro virtual patches: 0 (no), 1 (yes); by default vulnerabilities with and without these virtual patches are included: multiple values are comma separated; to unset value use update request and set to empty value
cve_ids_filter	(Optional) Filter CVE IDs with the "Exact Match" or "Contains" search criteria: - Set to 1 to filter the CVE IDs that match exactly with the input CVE strings. - Set to 2 to filter the CVE IDs that contain the input CVE string.
cve_ids={value}	One or more CVE IDs; multiple IDs are comma separated; to unset value use update request and set to empty value
not_cve_ids={**0**|1}	Set to 1 for CVE IDs that do not match cve_ids parameter values
exploitability={value}	One or more vendors with exploitability info; multiple references are comma separated; to unset value use update request and set to empty value
malware_associated={value}	One or more vendors with malware info; multiple references are comma separated; to unset value use update request and set to empty value
vendor_refs={value}	One or more vendor references; multiple vendors are comma separated; to unset value use update request and set to empty value
not_vendor_refs={**0**|1}	Set to 1 for vendor references that do not match vendor_refs parameter values
bugtraq_id={value}	Vulnerabilities with a Bugtraq ID number; to unset value use update request and set to empty value
not_bugtraq_id={**0**|1}	Set to 1 for vulnerabilities with Bugtraq IDs that do not match the bugtraq_id parameter value
vuln_details={value}	A string matching vulnerability details; to unset value use update request and set to empty value
compliance_details={value}	A string matching compliance details; to unset value use update request and set to empty value

Parameter	Value
supported_modules={value}	One or more of these Qualys modules: VM, CA-Windows Agent, CA-Linux Agent, WAS, WAF, MD; multiple values are comma separated; to unset value use update request and set to empty value
compliance_types={value}	One or more compliance types: PCI, CobiT, HIPAA, GLBA, SOX; multiple values are comma separated; to unset value use update request and set to empty value
qualys_top_lists={value}	One or more Qualys top lists: Internal_10, External_10; multiple values are comma separated; to unset value use update request and set to empty value
cpe={value}	(Optional) One or more CPE values: Operating System, Application, Hardware, None; multiple values are comma separated.
qids_not_exploitable={**0**|1}	Set to 1 for vulnerabilities that are not exploitable due to configuration.
non_running_services={**0**|1}	Set to 1 for vulnerabilities on non running services.
sans_20={**0**|1}	Set to 1 for vulnerabilities in 2008 SANS 20 list
nac_nam={**0**|1}	Set to 1 for NAC/NAM vulnerabilities
vuln_provider={value}	Provider of the vulnerability if not Qualys; valid value is iDefense
cvss_base={value}	CVSS base score value (matches greater than or equal to this value); to unset value use update request and set to empty value
cvss_temp={value}	CVSS temporal score value (matches greater than or equal to this value); to unset value use update request and set to empty value
cvss_access_vector={value}	CVSS access vector, one of: Undefined, Local, Adjacent_Network, Network; to unset value use update request and set to empty value
cvss_base_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss_base" parameter along with the "cvss_base_operand" parameter in the API request.
cvss_temp_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss_temp" parameter along with the "cvss_temp_operand" parameter in the API request.

Parameter	Value
cvss3_base={value}	CVSS3 base score value assigned to the CVEs by NIST (matches greater than, less than, or equal to this value); to unset value use update request and set to empty value.
cvss3_temp={value}	CVSS3 temporal score value assigned to the CVEs by NIST (matches greater than, less than, or equal to this value); to unset value use update request and set to empty value.
cvss3_base_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss3_base" parameter along with the "cvss3_base_operand" parameter in the API request.
cvss3_temp_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss3_temp" parameter along with the "cvss3_temp_operand" parameter in the API request.

User modified filters

The user_modified* parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
user_modified_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
user_modified_date_today={0|1}	set to 1 for modified by user today; set to 0 for not modified by user today
user_modified_date_in previous={value}	one of: Year, Month, Week, Quarter
user_modified_date_within_last_days={value}	number of days: 1-9999
not_user_modified={**0**|1}	set to 1 to set the “not” flag for one of the user_modified* parameters

Service modified filters

These parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
service_modified_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
service_modified_date_today={0|1}	set to 1 for modified by our service today; set to 0 for not modified by our service today
service_modified_date_in previous={value}	one of: Year, Month, Week, Quarter

Parameter	Value
service_modified_date_within_last_days ={value}	number of days: 1-9999
not_service_modified={**0**|1}	set to 1 to set the "not" flag for one of the service_modified* parameters

Published filters

These parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
published_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
published_date_today={0|1}	set to 1 for published today; set to 0 for not published today
published_date_in previous={value}	one of: Year, Month, Week, Quarter
published_date_within_last_days={value}	number of days: 1-9999
not_published={**0**|1}	set to 1 to set the "not" flag for one of the published* parameters

Sample - Create dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=My+Dynamic+Search+List&global=1&published_dat
e_within_last_days=7&patch_available=1"
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>New search list created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create dynamic search list, CVSS scores

API request:

Request for CVSS2 base scores: greater than equal to 3, CVSS 2 temporal scores less than 2, CVSS3 base scores greater than or equal to 2, CVSS3 temporal scores less than 2.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2" -d
"action=create&title=mytest_DL313&cvss_base=3&cvss_base_operand=1&
cvss_temp=2&cvss_temp_operand=2&cvss3_base=2&cvss3_base_operand=1&
cvss3_temp=2&cvss3_temp_operand=2"
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/"
```

Update dynamic search list

Input parameters

Parameter	Description
action=update	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to update.
title={value}	(Optional) The search list title. Maximum is 256 characters (ascii).
global={0|1}	(Optional) Specify 1 to make this a global search list.
comments={value}	(Optional) User defined comments.
{criteria}	(Optional) See "Search criteria" Only criteria specified in an update request will overwrite existing criteria, if any. For example, if a search list has confirmed_severities=3,4 and you make an update request with confirmed_severities=5, the search list will be updated to confirmed_severities=5.
unset_user_modified_date={value}	(Optional) Set to empty value to unset the user modified date in the search list parameters.
unset_published_date={value}	(Optional) Set to empty value to unset the published date in the search list parameters.
unset_service_modified_date={value}	(Optional) Set to empty value to unset the service modified date in the search list parameters.

Sample - Update dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=136992"
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>Search list updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Delete dynamic search list

Input parameters

Parameter	Description
action=delete	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to delete.

Sample - Delete dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&id=123456"
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>search list deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>123456</VALUE>
      </ITEM>
```

```
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/qid/search_list/dynamic/

Create dynamic search lists and get information about them.

Permissions - as described below

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Create, update, list and delete search lists.
Auditor	No permission to create, update, list and delete search lists.

List dynamic search lists

Input parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
ids={id1,id2...}	(Optional) One or more search list IDs to display. Multiple IDs are comma separated.
show_qids={0|**1**}	(Optional) Set to 0 to hide QIDs defined for each search list in the XML output. By default these QIDs are shown.
show_option_profiles={0|**1**}	(Optional) Set to 0 to hide option profiles associated with each search list in the XML output. By default these option profiles are shown.
show_distribution_groups={0|**1**}	(Optional) Set to 0 to hide distribution groups associated with each search list in the XML output. By default these distribution groups are shown.
show_report_templates={0|**1**}	(Optional) Set to 0 to hide report templates associated with each search list in the XML output. By default these report templates will be shown.
show_remediation_policies={0|**1**}	(Optional) Set to 0 to hide remediation policies associated with each search list in the XML output. By default these remediation policies will be shown.

Sample - List dynamic search list

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/?action=list
&ids=381"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/dynamic_list_output
.dtd">
<SEARCH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2015-01-06T06:20:03Z</DATETIME>
    <DYNAMIC_LISTS>
      <DYNAMIC_LIST>
        <ID>381</ID>
        <TITLE><![CDATA[static search list]]></TITLE>
        <GLOBAL>Yes</GLOBAL>
        <OWNER>acme_tb</OWNER>
        <CREATED><![CDATA[07/27/2015 at 15:18:42 (GMT+0530)]]></CREATED>
        <MODIFIED_BY>acme_tb</MODIFIED_BY>
     <MODIFIED><![CDATA[07/27/2015 at 15:18:42 (GMT+0530)]]></MODIFIED>
        <QIDS>
            <QID>1000<QID>
            <QID>1001<QID>
        </QIDS>
        <CRITERIA>
            <VULNERABILITY_TITLE><![CDATA[NOT
Title]]></VULNERABILITY_TITLE>
            <DISCOVERY_METHOD><![CDATA[Authenticated
Only]]></DISCOVERY_METHOD>
            <AUTHENTICATION_TYPE><![CDATA[HTTP, Oracle,
Unix]]></AUTHENTICATION_TYPE>
            <USER_CONFIGURATION><![CDATA[Disabled,
Edited]]></USER_CONFIGURATION>
            <CATEGORY><![CDATA[NOT Backdoors and trojan horses, DNS and
BIND]]> </CATEGORY>
            <CONFIRMED_SEVERITY><![CDATA[1, 2]]></CONFIRMED_SEVERITY>
            <POTENTIAL_SEVERITY><![CDATA[2, 3]]></POTENTIAL_SEVERITY>
            <INFORMATION_SEVERITY><![CDATA[4, 5]]></INFORMATION_SEVERITY>
            <VENDOR><![CDATA[NOT 2brightsparks,3com,4d]]></VENDOR>
            <PRODUCT><![CDATA[NOT .net_framework]]></PRODUCT>
            <CVSS_BASE_SCORE><![CDATA[2]]></CVSS_BASE_SCORE>
            <CVSS_TEMPORAL_SCORE><![CDATA[3]]></CVSS_TEMPORAL_SCORE>
            <CVSS_ACCESS_VECTOR><![CDATA[Adjacent
Network]]></CVSS_ACCESS_VECTOR>
            <PATCH_AVAILABLE><![CDATA[Yes, No]]></PATCH_AVAILABLE>
<VIRTUAL_PATCH_AVAILABLE><![CDATA[Yes]]></VIRTUAL_PATCH_AVAILABLE>
            <CVE_ID><![CDATA[NOT CVE]]></CVE_ID>
<CVE_ID_FILTER><![CDATAContains]></CVE_ID_FILTER>
            <EXPLOITABILITY><![CDATA[ExploitKits, Immunity - Dsquare]]>
</EXPLOITABILITY>
            <ASSOCIATED_MALWARE><![CDATA[Trend
Micro]]></ASSOCIATED_MALWARE>
            <VENDOR_REFERENCE><![CDATA[NOT Linux]]></VENDOR_REFERENCE>
            <BUGTRAQ_ID><![CDATA[NOT 15656]]></BUGTRAQ_ID>
<VULNERABILITY_DETAILS><![CDATA[details]]></VULNERABILITY_DETAILS>
```

```
            <COMPLIANCE_DETAILS><![CDATA[details]]></COMPLIANCE_DETAILS>
            <COMPLIANCE_TYPE><![CDATA[PCI, CobIT, HIPAA, GLBA,
SOX]]></COMPLIANCE_TYPE>
            <QUALYS_TOP_20><![CDATA[Top Internal 10, Top External
10]]></QUALYS_TOP_20>
            <OTHER><![CDATA[Not exploitable due to configuration, Non-
running services, 2008 SANS 20]]></OTHER>
            <NETWORK_ACCESS><![CDATA[NAC / NAM]]></NETWORK_ACCESS>
            <USER_MODIFIED><![CDATA[NOT 07/27/2015-
07/27/2015]]></USER_MODIFIED>
            <PUBLISHED><![CDATA[NOT 06/02/2015-07/20/2015]]></PUBLISHED>
            <SERVICE_MODIFIED><![CDATA[NOT Previous 1
week]]></SERVICE_MODIFIED>
        </CRITERIA>
        </CRITERIA>
        <!-- This list is used in the following option profiles //-->
        <OPTION_PROFILES>
            <OPTION_PROFILE>
                <ID>135<ID>
                <TITLE><![CDATA[Initial Options]]></TITLE>
            <OPTION_PROFILE>
        </OPTION_PROFILES>
        <!-- This list is used in the following report templates //-->
        <REPORT_TEMPLATES>
            <REPORT_TEMPLATE>
                <ID>256<ID>
                <TITLE><![CDATA[Scan Report Template]]></TITLE>
            <REPORT_TEMPLATE>
        </REPORT_TEMPLATES>
       <!-- This list is used in the following remediation policies. //-->
        <REMEDIATION_POLICIES>
            <REMEDIATION_POLICY>
                <ID>655<ID>
                <TITLE><![CDATA[Remediation Policy 1]]></TITLE>
            <REMEDIATION_POLICY>
        </REMEDIATION_POLICIES>
        <!-- This search list is associated with following distribution
groups. //-->
        <DISTRIBUTION_GROUPS>
            <DISTRIBUTION_GROUP>
                <ID>226<ID>
                <TITLE><![CDATA[All]]></TITLE>
            <DISTRIBUTION_GROUP>
        </DISTRIBUTION_GROUPS>
        <COMMENTS><![CDATA[This is my first comment for this
list]]></COMMENTS>
      </DYNAMIC_LIST>
   </DYNAMIC_LISTS>
  </RESPONSE>
</SEARCH_LIST_OUTPUT>
```

Sample - List dynamic search list for deep Scan QIDs

API request:

```
curl location
<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/?action=list&ids=634
3529&show_qids=0' \
header 'Content-Type: test/xml' \
header 'X-Requested-With: test' \
header 'Authorization: Bearer <JWT Token>'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/dynamic_list_output.
dtd">
<DYNAMIC_SEARCH_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-12-11T09:06:19Z</DATETIME>
        <DYNAMIC_LISTS>
            <DYNAMIC_LIST>
                <ID>6343529</ID>
                <TITLE>
                    <![CDATA[2 Deep Scan API Testing]]>
                </TITLE>
                <GLOBAL>Yes</GLOBAL>
                <OWNER>
                    <![CDATA[Amol Zambare (vmdrxaz7)]]>
                </OWNER>
                <CREATED>2025-12-11T08:46:28Z</CREATED>
                <MODIFIED_BY>
                    <![CDATA[Amol Zambare (vmdrxaz7)]]>
                </MODIFIED_BY>
                <MODIFIED>2025-12-11T08:54:45Z</MODIFIED>
                <CRITERIA>
                    <DISCOVERY_METHOD>
                        <![CDATA[All]]>
                    </DISCOVERY_METHOD>
                    <CLOUD_AGENT_SCAN_TYPE>
                        <![CDATA[Deep Scan - Windows]]>
                    </CLOUD_AGENT_SCAN_TYPE>
                    <PROVIDER>
                        <![CDATA[iDefense]]>
                    </PROVIDER>
                </CRITERIA>
            </DYNAMIC_LIST>
        </DYNAMIC_LISTS>
    </RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>
```

Sample - List dynamic search list for CVSS4 Base Score

API request:

```
curl --location '
/api/3.0/fo/qid/search_list/dynamic/?action=list&ids=6331504&show_qids=0'
\
--header 'Content-Type: test/xml' \
```

```
--header 'X-Requested-With: test' \
--header 'Authorization: Bearer '
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/dynamic_list_output
.dtd">
<DYNAMIC_SEARCH_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-12-09T07:01:26Z</DATETIME>
        <DYNAMIC_LISTS>
            <DYNAMIC_LIST>
                <ID>6331504</ID>
                <TITLE>
                    <![CDATA[Dynamic SL to Test CVSS V4 Phase 2 via API
11]]>
                </TITLE>
                <GLOBAL>Yes</GLOBAL>
                <OWNER>
                    <![CDATA[user name (vmdrxaz7)]]>
                </OWNER>
                <CREATED>2025-12-09T06:04:59Z</CREATED>
                <MODIFIED_BY>
                    <![CDATA[user name (vmdrxaz7)]]>
                </MODIFIED_BY>
                <MODIFIED>2025-12-09T06:04:59Z</MODIFIED>
                <CRITERIA>
                    <DISCOVERY_METHOD>
                        <![CDATA[All]]>
                    </DISCOVERY_METHOD>
                    <CVSS4_BASE_SCORE>
                        <![CDATA[5]]>
                    </CVSS4_BASE_SCORE>
                    <CVSS4_BASE_SCORE_OPERAND>
                        <![CDATA[2]]>
                    </CVSS4_BASE_SCORE_OPERAND>
                    <CVSS4_VERSION>4</CVSS4_VERSION>
                </CRITERIA>
            </DYNAMIC_LIST>
        </DYNAMIC_LISTS>
    </RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>DTD
```

<platform API server>/api/3.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd

Create dynamic search list

Input parameters

Parameter	Description
action=create	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
title={value}	(Required) A user defined search list title. Maximum is 256 characters (ascii).
global={**0**|1}	(Optional) Specify 1 to make this a global search list, available to all subscription users.
comments={value}	(Optional) User defined comments.
{criteria}	(Required) User defined search criteria. See "Search criteria"
cloud_agent_scan_type={}	(Optional) Required for creating dynamic search list for Deep Scan QIDs.

Search criteria

Use these parameters to define search criteria for dynamic search lists, using create and update requests. All parameters act as vulnerability filters.

Parameter	Value
vuln_title={value}	Vulnerability title (string); to unset value use update request and set to empty value
not_vuln_title={**0**|1}	Set to 1 for vulnerability title that does not match vuln_title parameter value
discovery_methods={value}	One or more discovery methods: Remote, Authenticated, Remote_Authenticated; by default all methods are included
auth_types={value}	One or more of these authentication types: Windows, Unix, Oracle, SNMP, VMware, DB2, HTTP, MySQL, PANOS, TOMCAT, MARIADB, MongoDB, WEBLOGIC; multiple values are comma separated; to unset value use update request and set to empty value
user_configuration={value}	One or more of these user configuration values: disabled, custom; multiple values are comma separated; to unset value use update request and set to empty value
categories={value}	One or more vulnerability category names (strings); to unset value use update request and set to empty value
not_categories={**0**|1}	Set to 1 for categories that do not match categories parameter values

Parameter	Value
confirmed_severities={value}	One or more confirmed vulnerability severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
potential_severities={value}	One or more potential vulnerability severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
ig_severities={value}	One or more information gathered severities (1-5); multiple severities are comma separated; to unset value use update request and set to empty value
vendor_ids={value}	One or more vendor IDs; multiple IDs are comma separated; to unset value use update request and set to empty value
not_vendor_ids={**0**|1}	Set to 1 for vendor IDs that do not match vendor_ids parameter values
products={value}	Vendor product names; multiple names are comma separated; to unset value use update request and set to empty value
not_products={**0**|1}	Set to 1 for product names that do not match products parameter values
patch_available={value}	Vulnerabilities with patches: 0 (no), 1 (yes); by default all vulnerabilities with and without patches are included; multiple values are comma separated; to unset value use update request and set to empty value
virtual_patch_available={value}	Vulnerabilities with Trend Micro virtual patches: 0 (no), 1 (yes); by default vulnerabilities with and without these virtual patches are included: multiple values are comma separated; to unset value use update request and set to empty value
cve_ids_filter	(Optional) Filter CVE IDs with the “Exact Match” or “Contains” search criteria: - Set to 1 to filter the CVE IDs that match exactly with the input CVE strings. - Set to 2 to filter the CVE IDs that contain the input CVE string.
cve_ids={value}	One or more CVE IDs; multiple IDs are comma separated; to unset value use update request and set to empty value
not_cve_ids={**0**|1}	Set to 1 for CVE IDs that do not match cve_ids parameter values
exploitability={value}	One or more vendors with exploitability info; multiple references are comma separated; to unset value use update request and set to empty value

Parameter	Value
malware_associated={value}	One or more vendors with malware info; multiple references are comma separated; to unset value use update request and set to empty value
vendor_refs={value}	One or more vendor references; multiple vendors are comma separated; to unset value use update request and set to empty value
not_vendor_refs={**0**|1}	Set to 1 for vendor references that do not match vendor_refs parameter values
bugtraq_id={value}	Vulnerabilities with a Bugtraq ID number; to unset value use update request and set to empty value
not_bugtraq_id={**0**|1}	Set to 1 for vulnerabilities with Bugtraq IDs that do not match the bugtraq_id parameter value
vuln_details={value}	A string matching vulnerability details; to unset value use update request and set to empty value
compliance_details={value}	A string matching compliance details; to unset value use update request and set to empty value
supported_modules={value}	One or more of these Qualys modules: VM, CA-Windows Agent, CA-Linux Agent, WAS, WAF, MD; multiple values are comma separated; to unset value use update request and set to empty value
compliance_types={value}	One or more compliance types: PCI, CobiT, HIPAA, GLBA, SOX; multiple values are comma separated; to unset value use update request and set to empty value
qualys_top_lists={value}	One or more Qualys top lists: Internal_10, External_10; multiple values are comma separated; to unset value use update request and set to empty value
cpe={value}	(Optional) One or more CPE values: Operating System, Application, Hardware, None; multiple values are comma separated.
qids_not_exploitable={**0**|1}	Set to 1 for vulnerabilities that are not exploitable due to configuration.
non_running_services={**0**|1}	Set to 1 for vulnerabilities on non running services.
sans_20={**0**|1}	Set to 1 for vulnerabilities in 2008 SANS 20 list
nac_nam={**0**|1}	Set to 1 for NAC/NAM vulnerabilities
vuln_provider={value}	Provider of the vulnerability if not Qualys; valid value is iDefense
cvss_base={value}	CVSS base score value (matches greater than or equal to this value); to unset value use update request and set to empty value

Parameter	Value
cvss_temp={value}	CVSS temporal score value (matches greater than or equal to this value); to unset value use update request and set to empty value
cvss_access_vector={value}	CVSS access vector, one of: Undefined, Local, Adjacent_Network, Network; to unset value use update request and set to empty value
cvss_base_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss_base" parameter along with the "cvss_base_operand" parameter in the API request.
cvss_temp_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss_temp" parameter along with the "cvss_temp_operand" parameter in the API request.
cvss3_base={value}	CVSS3 base score value assigned to the CVEs by NIST (matches greater than, less than, or equal to this value); to unset value use update request and set to empty value.
cvss3_temp={value}	CVSS3 temporal score value assigned to the CVEs by NIST (matches greater than, less than, or equal to this value); to unset value use update request and set to empty value.
cvss3_base_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss3_base" parameter along with the "cvss3_base_operand" parameter in the API request.
cvss3_temp_operand={value}	Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss3_temp" parameter along with the "cvss3_temp_operand" parameter in the API request.
cvss4_base={value}	(Optional) CVSS4 base score value assigned to the CVEs by NIST (matches greater than or less than the value)
cvss4_base_operand={value}	(Optional) Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss4_base" parameter along with the "cvss4_base_operand" parameter in the API request.

User modified filters

The user_modified* parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
user_modified_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
user_modified_date_today={0|1}	set to 1 for modified by user today; set to 0 for not modified by user today
user_modified_date_in previous={value}	one of: Year, Month, Week, Quarter
user_modified_date_within_last_days={value}	number of days: 1-9999
not_user_modified={**0**|1}	set to 1 to set the "not" flag for one of the user_modified* parameters

Service modified filters

These parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
service_modified_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
service_modified_date_today={0|1}	set to 1 for modified by our service today; set to 0 for not modified by our service today
service_modified_date_in previous={value}	one of: Year, Month, Week, Quarter
service_modified_date_within_last_days={value}	number of days: 1-9999
not_service_modified={**0**|1}	set to 1 to set the "not" flag for one of the service_modified* parameters

Published filters

These parameters are mutually exclusive, only one of these can be passed per request.

Parameter	Value
published_date_between={value}	date range in format (mm/dd/yyyy-mm/dd/yyyy)
published_date_today={0|1}	set to 1 for published today; set to 0 for not published today
published_date_in previous={value}	one of: Year, Month, Week, Quarter
published_date_within_last_days={value}	number of days: 1-9999
not_published={**0**|1}	set to 1 to set the "not" flag for one of the published* parameters

Sample - Create dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=My+Dynamic+Search+List&global=1&published_date_withi
n_last_days=7&patch_available=1"
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>New search list created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create dynamic search list, CVSS scores

API request:

Request for CVSS2 base scores: greater than equal to 3, CVSS 2 temporal scores less than 2, CVSS3 base scores greater than or equal to 2, CVSS3 temporal scores less than 2.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2" -d
"action=create&title=mytest_DL313&cvss_base=3&cvss_base_operand=1&cvss_te
mp=2&cvss_temp_operand=2&cvss3_base=2&cvss3_base_operand=1&cvss3_temp=2&c
vss3_temp_operand=2"
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/"
```

Sample - Create dynamic search list for deep scan QIDs

API request:

```
curl location <qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/' \
header 'X-Requested-With: Curl' \
header 'Content-Type: application/x-www-form-urlencoded' \
header 'Authorization: Bearer <JWT Token>' \
data-urlencode 'action=create' \
data-urlencode 'title=2 Deep Scan API Testing' \
data-urlencode 'global=1' \
data-urlencode 'cloud_agent_scan_type=Deep Scan - Windows'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
```

```
            <DATETIME>2025-12-11T08:46:29Z</DATETIME>
            <TEXT>New search list created successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>6343529</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Create dynamic search list for CVSS4 Base Score

API request:

```
curl location <qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/' \
header 'X-Requested-With: Curl' \
header 'Content-Type: application/x-www-form-urlencoded' \
header 'Authorization: Bearer <JWT Token>' \
data-urlencode 'action=create' \
data-urlencode 'title=2 Deep Scan API Testing' \
data-urlencode 'global=1' \
data-urlencode 'cvss4_base=3' \
data-urlencode 'cvss4_base_operand=1'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-09T06:04:59Z</DATETIME>
        <TEXT>New search list created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>6331504</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Update dynamic search list

Input parameters

Parameter	Description
action=update	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to update.

Parameter	Description
title={value}	(Optional) The search list title. Maximum is 256 characters (ascii).
global={0|1}	(Optional) Specify 1 to make this a global search list.
comments={value}	(Optional) User defined comments.
{criteria}	(Optional) See "Search criteria" Only criteria specified in an update request will overwrite existing criteria, if any. For example, if a search list has confirmed_severities=3,4 and you make an update request with confirmed_severities=5, the search list will be updated to confirmed_severities=5.
unset_user_modified_date={value}	(Optional) Set to empty value to unset the user modified date in the search list parameters.
unset_published_date={value}	(Optional) Set to empty value to unset the published date in the search list parameters.
unset_service_modified_date={value}	(Optional) Set to empty value to unset the service modified date in the search list parameters.
cloud_agent_scan_type={value}	(Optional) Required for updating dynamic search list for Deep Scan QIDs.
cvss4_base={value}	(Optional) CVSS4 base score value assigned to the CVEs by NIST (matches greater than or less than the value)
cvss4_base_operand={value}	(Optional) Set the value to 1 to use the greater than equal to operand. Set the value to 2 to use the less than operand. You must always specify the "cvss4_base" parameter along with the "cvss4_base_operand" parameter in the API request.

Sample - Update dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=136992"
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>Search list updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
```

```
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update dynamic search list Deep Scan QIDs

API request:

```
curl location <qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/' \
header 'X-Requested-With: Curl' \
header 'Content-Type: application/x-www-form-urlencoded' \
header 'Authorization: Bearer <JWT Token>' \
data-urlencode 'action=update' \
data-urlencode 'title=2 Deep Scan API Testing' \
data-urlencode 'global=1' \
data-urlencode 'vuln_provider=iDefense' \
data-urlencode 'cloud_agent_scan_type=Deep Scan - Windows' \
data-urlencode 'id=xxxxxxx'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T08:54:46Z</DATETIME>
        <TEXT>search list updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>6343529</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update dynamic search list for CVSS4 for Base Score

API request:

```
curl --location '<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/' \
--header 'X-Requested-With: Curl' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer<JWT Token>' \
--data-urlencode 'action=update' \
--data-urlencode 'title=Dynamic SL to Test CVSS V4 Phase 2 via API' \
--data-urlencode 'id=6331504' \
--data-urlencode 'global=1' \
--data-urlencode 'cvss4_base=3' \
--data-urlencode 'cvss4_base_operand=1'
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.p04.eng.sjc01.qualys.com/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-09T09:25:34Z</DATETIME>
        <TEXT>search list updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>6331504</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Delete dynamic search list

Input parameters

Parameter	Description
action=delete	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
id={id}	(Required) The ID of the search list you want to delete.

Sample - Delete dynamic search list

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&id=123456"
"<qualys_base_url>/api/3.0/fo/qid/search_list/dynamic/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>search list deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>123456</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	API Status	Release Date
api/3.0/fo/qid/search_list/dynamic/	Active	Active
api/2.0/fo/qid/search_list/dynamic/	August 2026	February 2027

Vendor IDs and References

/api/2.0/fo/vendor/?action=list_vendors

/api/2.0/fo/vendor/?action=list_vendor_references

List vendor IDs and names. This vendor information may be defined as part of dynamic search list query criteria.

Permissions - All users except Auditors have permission to run this API.

Input Parameters

Parameter	Description
action={value}	(Required) Set to "list_vendors" to list vendor IDs and names. Set to "list_vendor_references" to list vendor references for QIDs.
echo_request={**0**|1}	(Optional) Specify 1 to show input parameters in XML output.
ids={id1,id2,...}	(Optional for action=list) One or more vendors IDs to list those vendors only.
qids={id1,id2,...}	(Optional for action=list_vendor_references) One or more QIDs to list vendors references for those QIDs only.

Sample - List vendor IDs and names

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/vendor/?action=list_vendors&ids=458,
1967"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VENDOR_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/vendor/vendor_list_output.dtd">
<VENDOR_LIST_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2015-09-02T09:23:52Z</DATETIME>
        <VENDORS>
            <VENDOR>
                <ID>458</ID>
                <NAME>
                    <![CDATA[3com]]>
                </NAME>
            </VENDOR>
            <VENDOR>
                <ID>1967</ID>
                <NAME>
                    <![CDATA[2glux]]>
                </NAME>
            </VENDOR>
        </VENDORS>
    </RESPONSE>
</VENDOR_LIST_OUTPUT>
```

DTD

```
<!-- QUALYS VENDOR_LIST_OUTPUT DTD -->
<!ELEMENT VENDOR_LIST_OUTPUT (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
                   POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, VENDORS?)>
<!ELEMENT VENDORS (VENDOR+)>
<!ELEMENT VENDOR (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME  (#PCDATA)>

<!-- EOF -->
```

Sample - List vendor references for qids

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"<qualys_base_url>/api/2.0/fo/vendor/?action=list_vendor_reference
s"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VENDOR_REFERENCE_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/vendor/vendor_reference_list_output.
dtd">
<VENDOR_REFERENCE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2015-09-02T09:27:34Z</DATETIME>
        <VENDOR_REFERENCES>
            <VENDOR_REFERENCE>
                <QID>195464</QID>
                <REFERENCE_INFO>
                    <REFERENCE>
                        <![CDATA[USN-2186-1]]>
                    </REFERENCE>
                    <URL>

<![CDATA[https://lists.ubuntu.com/archives/ubuntu-security-
announce/2014-April/002483.html]]>
                    </URL>
                </REFERENCE_INFO>
            </VENDOR_REFERENCE>
            <VENDOR_REFERENCE>
                <QID>115844</QID>
                <REFERENCE_INFO>
                    <REFERENCE>
                        <![CDATA[RHSA-2008-0508]]>
                    </REFERENCE>
                    <URL>
                       <![CDATA[http://rhn.redhat.com/errata/RHSA-
2008-0508.html]]>
                    </URL>
                </REFERENCE_INFO>
                <REFERENCE_INFO>
                    <REFERENCE>
                        <![CDATA[RHSA-2008-0519]]>
                    </REFERENCE>
                    <URL>
                       <![CDATA[http://rhn.redhat.com/errata/RHSA-
2008-0519.html]]>
                    </URL>
                </REFERENCE_INFO>
```

```
            </VENDOR_REFERENCE>
        </VENDOR_REFERENCES>
...
    </RESPONSE>
</VENDOR_REFERENCE_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/vendor/vendor_reference_list_output.dtd

Manage Containerized Scanner Appliance

Use the Containerized Scanner Appliance API (/api/2.0/fo/appliance/QCSS) to create, update, list, and delete containerized scanner appliances.

Tell me about permissions. Managers can perform all actions (create, update, list, and delete). Unit Managers and Scanners must have the “Manage containerized appliances” permission to create, update, list, and delete containerized scanners. This permission is only available to Scanner users when your subscription is configured to allow it.

Create New Containerized Scanner Appliance

/api/2.0/fo/appliance/qcss/?action=create

[POST]

Create a new containerized scanner appliance in your account.

Input Parameters

Parameter	Description
action={value}	(Required) Specify action to create, list, update, or delete a containerized scanner
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
name={string}	(Required) The friendly name. This name can't already be assigned to an appliance in your account. It can be a maximum of 32 characters, spaces are not allowed
polling_interval={value}	(Optional) The polling interval, in seconds. A valid value is 60 to 3600 (we recommend 180 which is the default). This is the frequency that the containerized scanner will attempt to connect to our Cloud Security Platform. The appliance calls home to provide health updates/heartbeats to the platform, to get software updates from the platform, to learn if new scan jobs have been requested by users, and to upload scan results data to the platform, if applicable.
asset_group_id={value}	(Required for Unit Managers and Scanners) The ID of an asset group the containerized scanner will be assigned to.

Sample - Create Containerized Scanner Appliance

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/2.0/fo/appliance/qcss/?action=creat
e&echo_
request=1&name=QcssScannerApi1 ' \
--header 'X-Requested-With: abc' \
--header 'Authorization: Basic cXdlYl9ybTI6UWF0ZW1wMTIzIw==='
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_CREATE_OUTPUT SYSTEM
"https://

<qualys_base_url>/api/2.0/fo/appliance/appliance_create_output.d
td">
  <APPLIANCE_CREATE_OUTPUT>
    <REQUEST>
      <DATETIME>2024-03-27T10:53:48Z</DATETIME>
      <USER_LOGIN>qweb_rm2</USER_LOGIN>
      <RESOURCE>https://

        <qualys_base_url>/api/2.0/fo/appliance/qcss/
```

```
      </RESOURCE>
      <PARAM_LIST>
        <PARAM>
          <KEY>action</KEY>
          <VALUE>create</VALUE>
        </PARAM>
        <PARAM>
          <KEY>echo_request</KEY>
          <VALUE>1</VALUE>
        </PARAM>
        <PARAM>
          <KEY>name</KEY>
          <VALUE>QcssScannerApi1</VALUE>
        </PARAM>
      </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
      <DATETIME>2024-03-27T10:53:48Z</DATETIME>
      <APPLIANCE>
        <ID>1227168</ID>
        <FRIENDLY_NAME>QcssScannerApi1</FRIENDLY_NAME>
        <ACTIVATION_CODE>11111111111111</ACTIVATION_CODE>
        <REMAINING_QVSA_LICENSES>983</REMAINING_QVSA_LICENSES>
      </APPLIANCE>
    </RESPONSE>
</APPLIANCE_CREATE_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/appliance/qcss/?action=create

List Containerized Scanner Appliance

/api/2.0/fo/appliance/qcss/?action=list

[POST]

List the containerized scanner appliance in your account.

Input Parameters

Parameter	Description
action=list	(Required) Specify action to list scanner appliances.
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.

Parameter	Description
output_mode={brief|full}	(Optonal) The amount of detail provided for each scanner appliance in the output: brief (default) or full. The "brief" output includes this information for each appliance: appliance ID, friendly name, software version, the number of running scans, and heartbeat check status (online or offline). The "full" output includes the full appliance information, including the same details available in the Qualys user interface.
scan_detail={0|1}	(Optional) Set to 1 to include scan details for scans currently running on the scanner appliance. Set to 0 (default) to not include scan details. Scan detail includes scan ID, title, scan reference, scan type and scan date.
include_cloud_info={0|1}	(Optional) When specified output_mode=full is required) Set to 1 to include cloud information in the output for containerized scanner appliances deployed on cloud platforms e.g. Amazon EC2, Microsoft Azure Cloud Platform and Google Cloud Platform. Set to 0 (default) to not include cloud info.
busy={0|1}	(Optional) By default all scanner appliances in the user account are shown. Set to 0 to show only appliances which are not currently running scans. Set to 1 (default) to show only appliances which are currently running scans.
scan_ref={value}	(Optional) Specify a scan reference code to show only the scanner appliances running a particular scan. You may enter a valid scan reference code for a currently running scan. The scan reference code starts with a string that identifies the scan type: "scan/" for a vulnerability scan, "compliance/" for a compliance scan, "was/" for a web application scan, "qscap/" for an FDCC scan, or "map/" for a network map.
name={string}	(Optional) List only scanner appliances (physical and containerized) that have names matching the string provided. Tip - Substring match is supported. For example, if you have 2 appliances named "myscanner" and "anotherscanner" and you supply the string "name=scan" both appliance both appliances will be returned in the XML output.
ids={id1,id2,...}	(Optional) List only scanner appliances (physical and containerized) that have certain IDs. Multiple IDs are comma separated.
include_license_info={0|1}	(Optional) Set to 1 to return containerized scanner license information in the XML output. This tells you the number of licenses you have and the number used. This information is not returned by default. When specified the XML output will include the LICENSE_INFO element.

Parameter	Description
type={physical | containerized | virtual | offline}	(Optional) Type of scanner appliances: physical, containerized, virtual, or offline. Type appears when output_mode=full is specified in API request.
platform_provider	(Optional) Specify a platform to show scanners deployed on that platform. The valid values are: ec2, ec2_compat, gce, azure, vCenter. ec2 - Amazon EC2, ec2_compat - OpenStack, gce - Google Cloud Platform, azure - Microsoft Azure Cloud Platform, vCenter - VMware vCenter

Sample - List Containerized Scanner Appliance

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/2.0/fo/appliance/qcss/?action=list&
output_mode=full' \
--header 'X-Requested-With: abc' \
--header 'Authorization: Basic cXdlYl9ybTI6UWF0ZW1wMTIzIw=='
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/2.0/fo/appliance/appliance_list_output.dtd
">
<APPLIANCE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-03-28T04:56:15Z</DATETIME>
        <APPLIANCE_LIST>
            <APPLIANCE>
                <ID>1227190</ID>
                <UUID>2c951232-e993-f1a3-8064-888ae369b2bf</UUID>
                <NAME>QcssScannerApi2</NAME>
                <NETWORK_ID>0</NETWORK_ID>
                <SOFTWARE_VERSION>0</SOFTWARE_VERSION>
                <RUNNING_SLICES_COUNT>0</RUNNING_SLICES_COUNT>
                <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
                <STATUS>Offline</STATUS>
                <MODEL_NUMBER>qcss</MODEL_NUMBER>
                <TYPE>Containerized</TYPE>
                <SERIAL_NUMBER>0</SERIAL_NUMBER>
                <ACTIVATION_CODE>70105819066298</ACTIVATION_CODE>
                <INTERFACE_SETTINGS>
                    <INTERFACE>lan</INTERFACE>
                    <IP_ADDRESS></IP_ADDRESS>
                    <NETMASK>128.0.0.0</NETMASK>
                    <GATEWAY>128.0.0.0</GATEWAY>
                    <LEASE>Static</LEASE>
                    <IPV6_ADDRESS></IPV6_ADDRESS>
```

```
        <SPEED></SPEED>
        <DUPLEX>Unknown</DUPLEX>
        <DNS>
            <DOMAIN></DOMAIN>
            <PRIMARY>128.0.0.0</PRIMARY>
            <SECONDARY>128.0.0.0</SECONDARY>
        </DNS>
    </INTERFACE_SETTINGS>
    <INTERFACE_SETTINGS>
        <SETTING>Disabled</SETTING>
        <INTERFACE>wan</INTERFACE>
        <IP_ADDRESS></IP_ADDRESS>
        <NETMASK>128.0.0.0</NETMASK>
        <GATEWAY>128.0.0.0</GATEWAY>
        <LEASE>Static</LEASE>
        <SPEED></SPEED>
        <DUPLEX>Unknown</DUPLEX>
        <DNS>
            <PRIMARY>128.0.0.0</PRIMARY>
            <SECONDARY>128.0.0.0</SECONDARY>
        </DNS>
    </INTERFACE_SETTINGS>
    <PROXY_SETTINGS>
        <SETTING>Disabled</SETTING>
        <PROXY>
            <IP_ADDRESS>128.0.0.0</IP_ADDRESS>
            <PORT></PORT>
            <USER></USER>
        </PROXY>
    </PROXY_SETTINGS>
    <VLANS>
        <SETTING>Disabled</SETTING>
    </VLANS>
    <STATIC_ROUTES />
    <ML_LATEST>12.11.28-1</ML_LATEST>
    <ML_VERSION updated="no"></ML_VERSION>
    <VULNSIGS_LATEST>2.5.993-3</VULNSIGS_LATEST>
    <VULNSIGS_VERSION updated="no"></VULNSIGS_VERSION>
    <ASSET_GROUP_COUNT>0</ASSET_GROUP_COUNT>
    <ASSET_GROUP_LIST />
    <LAST_UPDATED_DATE>N/A</LAST_UPDATED_DATE>
    <POLLING_INTERVAL>180 seconds</POLLING_INTERVAL>
    <USER_LOGIN>qweb_rm2</USER_LOGIN>
    <HEARTBEATS_MISSED>0</HEARTBEATS_MISSED>
    <SS_CONNECTION>Inactive</SS_CONNECTION>
  <SS_LAST_CONNECTED>2023-03-29T04:54:37Z</SS_LAST_CONNECTED>
    <USER_LIST />
    <UPDATED>No</UPDATED>
    <COMMENTS>
        <![CDATA[]]>
    </COMMENTS>
    <MAX_CAPACITY_UNITS></MAX_CAPACITY_UNITS>
    <CPU_INFO></CPU_INFO>
    <MEMORY_INFO></MEMORY_INFO>
```

```
                <REGION_INFO></REGION_INFO>
            </APPLIANCE>
        </APPLIANCE_LIST>
    </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/appliance/qcss/?action=list

Update Containerized Scanner Appliance

/api/2.0/fo/appliance/qcss/?action=update

[POST]

Update the containerized scanner appliance details in your account.

Input Parameters

Parameter	Description
action=update	(Required) Specify action to update scanner appliance.
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
id={id}	(Required) A valid ID of a containerized scanner.
name={string}	(Optional) The friendly name. This name can't already be assigned to an appliance in your account. It can be a maximum of 32 characters, spaces are not allowed.
polling_interval={value}	The polling interval, in seconds. A valid value is 60 to 3600 (we recommend 180 which is the default). This is the frequency that the containerized scanner will attempt to connect to our Cloud Security Platform. The appliance calls home to provide health updates/heartbeats to the platform, to get software updates from the platform, to learn if new scan jobs have been requested by users, and to upload scan results data to the platform, if applicable.
comment={value}	(Optional) User-defined comments.
set_tags= {value}	(Optional) Specify tag to be assigned to the scanner appliance. Both containerized and physical scanners can be tagged. These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.

Parameter	Description
add_tags= {value}	(Optional) Specify tag to be added to the existing list of tags assigned to the scanner. Multiple entries are comma separated. These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
remove_tags= {value}	(Optional) Specify tag to be removed from the existing list of tags assigned to scanner. Multiple tags are comma separated. These parameters are mutually exclusive and cannot be specified in the same request: set_tags and add_tags, remove_tags.
tag_set_by= {id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names.
enable_ipv6=0	(Optional) Enable or disable IPv6 on LAN. Specify 1 to enable IPv6 and 0 to disable it.

Sample - Update Containerized Scanner Appliance

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/2.0/fo/appliance/qcss/?action=updat
e&echo_
request=1&name=QcssScannerApi1_updated&id=1227168' \
--header 'X-Requested-With: abc' \
--header 'Authorization: Basic cXdlYl9ybTI6UWF0ZW1wMTIzIw==='
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://
<qualys_base_url>/api/2.0/simple_return.dtd">
  <SIMPLE_RETURN>
    <REQUEST>
      <DATETIME>2024-03-27T11:05:26Z</DATETIME>
      <USER_LOGIN>qweb_rrr</USER_LOGIN>
      <RESOURCE>https://
        <qualys_base_url>/api/2.0/fo/appliance/qcss/
        </RESOURCE>
        <PARAM_LIST>
          <PARAM>
            <KEY>action</KEY>
            <VALUE>update</VALUE>
          </PARAM>
```

```
        <PARAM>
          <KEY>echo_request</KEY>
          <VALUE>1</VALUE>
        </PARAM>
        <PARAM>
          <KEY>name</KEY>
          <VALUE>QcssScannerApi1_updated</VALUE>
        </PARAM>
        <PARAM>
          <KEY>id</KEY>
          <VALUE>1227168</VALUE>
        </PARAM>
      </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
      <DATETIME>2024-03-27T11:05:26Z</DATETIME>
      <TEXT>Containerized scanner updated successfully</TEXT>
      <ITEM_LIST>
        <ITEM>
          <KEY>ID</KEY>
          <VALUE>1227168</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
  </SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/fo/appliance/qcss/?action=update

Delete Containerized Scanner Appliance

/api/2.0/fo/appliance/qcss/?action=delete

[POST]

Delete the containerized scanner appliance in your account.

Input Parameters

Parameter	Description
action=delete	(Required) Specify action to delete containerized scanner.
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
id={id}	(Required) A valid ID of a containerized scanner.

Sample - Delete Containerized Scanner Appliance

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/2.0/fo/appliance/qcss/?action=delet
e&echo_request=1&id=1111111' \
--header 'X-Requested-With: abc' \
--header 'Authorization: Basic cXdlYl9ybTI6UWF0ZW1wMTIzIw=='
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <REQUEST>
        <DATETIME>2024-03-27T11:10:22Z</DATETIME>
        <USER_LOGIN>qweb_rm2</USER_LOGIN>

<RESOURCE>https://<qualys_base_url>/api/2.0/fo/appliance/qcss/</RESOURCE>
        <PARAM_LIST>
            <PARAM>
                <KEY>action</KEY>
                <VALUE>delete</VALUE>
            </PARAM>
            <PARAM>
                <KEY>echo_request</KEY>
                <VALUE>1</VALUE>
            </PARAM>
            <PARAM>
                <KEY>id</KEY>
                <VALUE>1227168</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2024-03-27T11:10:22Z</DATETIME>
        <TEXT>Containerized scanner deleted successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1227168</VALUE>
            </ITEM>
```

```
            <ITEM>
                <KEY>DEACTIVATED_SCHEDULED_SCANS</KEY>
                <VALUE>None</VALUE>
            </ITEM>
            <ITEM>
                <KEY>AFFECTED_ASSET_GROUPS</KEY>
                <VALUE>None</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/fo/appliance/qcss/?action=delete

Scan Authentication

Create, edit, list, delete authentication records for authenticated (trusted) scanning of various technologies (i.e. Windows, Unix, Docker, Oracle, etc).

Permissions

User Permissions Summary

List Auth Records

List Authentication Records

List Authentication Records by Type

Auth Record types

DataStax Record - Apache, MIIS, IBM Websphere, Tomcat

Azure MS SQL Record

Apache Cassandra Record

DataStax Record

Docker Record

HTTP Record

IBM DB2 Record

InformixDB Record

JBoss Server record

Kubernetes Record

MariaDB Record

MarkLogic Record

MongoDB Record

MS SQL Record

MySQL Record

Neo4j Record

Nginx Record

Oracle Record

Oracle Listener Record

Oracle WebLogic Server Record

Palo Alto Firewall Record

PostgreSQL Record

SAP Hana Record

SAP IQ Record

SNMP Record

Sybase Record

Unix Record

VMware Record

VMware NSX Record

Windows Record

MS Exchange Server

Oracle HTTP Server Record

vCenter - ESXi Mapping Records

Network SSH Record

User Permissions Summary

A summary is provided below. For complete details, see "Managing Authentication Records" in Qualys online help.

Maximum Records per request

A maximum of 1,000 authentication records can be processed per request. If the requested list identifies more than 1,000 authentication records, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of records.

View Record List

User Role	Permissions
Manager	View all authentication records in subscription.
Unit Manager	View authentication records which contain hosts in the user's business unit.
Scanner	View authentication records which contain hosts in the user's assigned asset groups.
Auditor, Reader	No permissions.

Create Record

User Role	Permissions
Manager	Create authentication records for hosts in the subscription.
Unit Manager	Create authentication records for hosts in the user's business unit. The permission "create/edit authentication records" must be granted in the user's account.
Auditor, Scanner, Reader	No permissions.

Update/Delete Record

User Role	Permissions
Manager	Update and delete authentication records.
Unit Manager	Update and delete authentication records. The permission "create/edit authentication records/vaults" must be granted in the user's account. To edit a record, at least one host in the record must be in the user's business unit. To delete a record, all hosts in the record must also be in the user's business unit.
Auditor, Scanner, Reader	No permissions.

List Authentication Records

For API version information, refer to API Version History section.

V2.0| V3.0

V2.0

/api/2.0/fo/auth/?action=list

[GET] [POST]

List all authentication records visible to the user for all technologies (i.e. Windows, Unix, Docker, etc).

A maximum of 1,000 authentication records can be processed per request. If the requested list identifies more than 1,000 authentication records, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
title={value}	(Optional) Show only authentication records which have a certain string in the record title.
comments={value}	(Optional) Show only authentication records which have a certain string in the record comments.
ids={value}	(Optional) Show only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. One or more IDs/ranges may be specified. An ID range entry is specified with a hyphen (for example, 3000-3250). Valid IDs are required.
id_min={value}	(Optional) Show only authentication records which have a minimum ID value. A valid ID is required.
id_max={value}	(Optional) Show only authentication records which have a maximum ID value. A valid ID is required.

DTD for list records

<platform API server>/api/2.0/fo/auth/auth_records.dtd

Sample - List authentication records, multiple technologies

```
<AUTH_ LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-05-21T13:32:17Z</DATETIME>
    <AUTH_RECORDS>
      <AUTH_UNIX_RECORDS>
        <ID_SET>
          <ID_RANGE>17-41</ID_RANGE>
          <ID_RANGE>62-119</ID_RANGE>
        </ID_SET>
      </AUTH_UNIX_RECORDS>
      <AUTH_WINDOWS_RECORDS>
        <ID_SET>
          <ID_RANGE>1-6</ID_RANGE>
        </ID_SET>
      </AUTH_WINDOWS_RECORDS>
      <AUTH_ORACLE_RECORDS>
        <ID_SET>
          <ID>7</ID>
        </ID_SET>
      </AUTH_ORACLE_RECORDS>
      <AUTH_SNMP_RECORDS>
        <ID_SET>
          <ID>4114</ID>
          <ID_RANGE>4117-4121</ID_RANGE>
        </ID_SET>
      </AUTH_SNMP_RECORDS>
      <AUTH_IBM_DB2_RECORDS>
        <ID_SET>
          <ID>6</ID>
        </ID_SET>
      </AUTH_IBM_DB2_RECORDS>
    </AUTH_RECORDS>
  </RESPONSE>
</AUTH_LIST_OUTPUT>
```

V3.0

/api/3.0/fo/auth/?action=list

[GET] [POST]

List all authentication records visible to the user for all technologies (i.e. Windows, Unix, Docker, etc).

A maximum of 1,000 authentication records can be processed per request. If the requested list identifies more than 1,000 authentication records, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
title={value}	(Optional) Show only authentication records which have a certain string in the record title.
comments={value}	(Optional) Show only authentication records which have a certain string in the record comments.
ids={value}	(Optional) Show only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. One or more IDs/ranges may be specified. An ID range entry is specified with a hyphen (for example, 3000-3250). Valid IDs are required.
id_min={value}	(Optional) Show only authentication records which have a minimum ID value. A valid ID is required.
id_max={value}	(Optional) Show only authentication records which have a maximum ID value. A valid ID is required.

DTD for list records

<platform API server>/api/3.0/fo/auth/auth_records.dtd

Sample - List all authentication records, multiple samples

API Request

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#"
-d "action=list" "https://<qualys_base_url>/api/3.0/fo/auth/">
```

XML Response

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/auth/auth_records.dtd”
<auth_records_output>
  <response>
    <datetime>2024-08-23T13:47:54Z</datetime>
    <auth_records>
      <auth_unix_ids>
        <id_set>
```

```
    <id>679711</id>
    <id>712175</id>
    <id>958037</id>
    <id>969642</id>
   ...
    <id_range>2132864-2132865</id_range>
    <id_range>4706061-4706062</id_range>
    <id_range>4706066-4706069</id_range>
  </id_set>
</auth_unix_ids>
<auth_windows_ids>
  <id_set>
    <id>679712</id>
    <id>712176</id>
    <id>958039</id>
    <id>965457</id>
    ...
    <id_range>4704738-4704739</id_range>
  </id_set>
</auth_windows_ids>
<auth_oracle_ids>
  <id_set>
    <id>768181</id>
    <id>971683</id>
    <id>1371740</id>
    <id>1371746</id>
    <id>1403716</id>
    <id>5190863</id>
    <id_range>5190867-5190868</id_range>
  </id_set>
</auth_oracle_ids>
<auth_snmp_ids>
  <id_set>
    <id>2118698</id>
  </id_set>
</auth_snmp_ids>
<auth_ms_sql_ids>
  <id_set>
    <id>2047865</id>
    <id>2266695</id>
    <id>2266910</id>
    ...
    <id_range>4713871-4713872</id_range>
    <id_range>5089353-5089356</id_range>
    <id_range>5089363-5089368</id_range>
```

```
  </id_set>
</auth_ms_sql_ids>
<auth_ibm_db2_ids>
  <id_set>
    <id>2134085</id>
  </id_set>
</auth_ibm_db2_ids>
<auth_vmware_ids>
  <id_set>
    <id>1420676</id>
    <id>1424399</id>
    <id_range>2444361-2444363</id_range>
  </id_set>
</auth_vmware_ids>
<auth_apache_ids>
  <id_set>
    <id>5096496</id>
    <id>5096516</id>
  </id_set>
</auth_apache_ids>
<auth_sybase_ids>
  <id_set>
    <id>1033098</id>
    <id>1033101</id>
    <id>5243997</id>
    <id>5244016</id>
    ...
    <id_range>5238874-5238875</id_range>
    <id_range>5240379-5240380</id_range>
  </id_set>
</auth_sybase_ids>
<auth_mysql_ids>
  <id_set>
    <id>5145480</id>
    <id>5190357</id>
  </id_set>
</auth_mysql_ids>
<auth_tomcat_ids>
  <id_set>
    <id>712177</id>
    <id>712187</id>
    <id>712226</id>
    ...
  </id_set>
</auth_tomcat_ids>
```

```
<auth_oracle_weblogic_ids>
  <id_set>
    <id>1726135</id>
    <id>2134083</id>
  </id_set>
</auth_oracle_weblogic_ids>
<auth_postgresql_ids>
  <id_set>
    <id>1026647</id>
    <id>4706073</id>
    <id>4706075</id>
    <id>4706077</id>
    ...
  </id_set>
</auth_postgresql_ids>
<auth_mongodb_ids>
  <id_set>
    <id>2157859</id>
    <id>2230895</id>
    <id>2283004</id>
    <id>2338797</id>
    <id>2455264</id>
    ...
    <id_range>2455458-2455460</id_range>
    <id_range>2455464-2455465</id_range>
    <id_range>2456530-2456535</id_range>
    <id_range>5190864-5190866</id_range>
  </id_set>
</auth_mongodb_ids>
<auth_vcenter_ids>
  <id_set>
    <id>1423522</id>
    <id>2118903</id>
    <id>2442690</id>
    <id>4684441</id>
    <id_range>2444364-2444365</id_range>
  </id_set>
</auth_vcenter_ids>
<auth_mariadb_ids>
  <id_set>
    <id>5238876</id>
  </id_set>
</auth_mariadb_ids>
<auth_informixdb_ids>
  <id_set>
```

```
    <id_range>1027159-1027160</id_range>
    <id>4747926</id>
  </id_set>
</auth_informixdb_ids>
<auth_network_ssh_ids>
  <id_set>
    <id>1043882</id>
    <id>1043889</id>
    <id>1044112</id>
    ...
    <id_range>1044121-1044123</id_range>
    <id_range>1044158-1044159</id_range>
    <id_range>1051721-1051722</id_range>
  </id_set>
</auth_network_ssh_ids>
<auth_nginx_ids>
  <id_set>
    <id>2134081</id>
    <id>2473317</id>
  </id_set>
</auth_nginx_ids>
<auth_infoblox_ids>
  <id_set>
    <id>2473315</id>
    <id>4675302</id>
    <id>4675307</id>
    <id>4675316</id>
    ...
  </id_set>
</auth_infoblox_ids>
<auth_bind_ids>
  <id_set>
    <id>4703222</id>
  </id_set>
</auth_bind_ids>
<auth_cisco_apic_ids>
  <id_set>
    <id>4673926</id>
    <id>4673946</id>
    <id>4675278</id>
    ...
  </id_set>
</auth_cisco_apic_ids>
<auth_cassandra_ids>
  <id_set>
```

```
            <id>4703223</id>
            <id>4713982</id>
            <id>4724463</id>
            <id>5207337</id>
            ...
          </id_set>
        </auth_cassandra_ids>
        <auth_marklogic_ids>
          <id_set>
            <id>4702420</id>
            <id>4706451</id>
            <id>4713859</id>
            <id>4714410</id>
            ...
            <id_range>4714287-4714288</id_range>
            <id_range>4714384-4714387</id_range>
          </id_set>
        </auth_marklogic_ids>
        <auth_datastax_ids>
          <id_set>
            <id>5291284</id>
            <id>5295929</id>
            <id>5296333</id>
            <id>5305719</id>
            ...
          </id_set>
        </auth_datastax_ids>
      </auth_records>
    </response>
  </auth_records_output>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/auth/?action=list	Active	Active
/api/2.0/fo/auth/?action=list	December 2025	December 2026

List Authentication Records by Type

/api/2.0/fo/auth/<type>

{GET] [POST}

List authentication records visible to the user for a specific technology (i.e. Unix, Windows, Docker, Sybase etc).

<type> will be a supported technology like: docker, http, ibm_db2, mongodb, ms_exchange, ms_sql, mysql, oracle, oracle_listener, oracle_weblogic, palo_alto_firwall, postgresql, snmp, sybase, unix (for Unix, Cisco, Checkpoint Firewall), network_ssh, vmware, windows. For application servers: apache, ms_iis, ibm_websphere, tomcat.

A maximum of 1,000 authentication records can be processed per request. If the requested list identifies more than 1,000 authentication records, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
title={value}	(Optional) how only authentication records which have a certain string in the record title.
comments={value}	(Optional) Show only authentication records which have a certain string in the record comments.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each authentication record. A valid value is: None - show record ID only Basic (default) - show record ID and all authentication record attributes All - show record ID and all authentication record attributes and a glossary section with the user name and login for each record owner
ids={value}	(Optional) Show only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. One or more IDs/ranges may be specified. An ID range entry is specified with a hyphen (for example, 3000-3250). Valid IDs are required.
id_min={value}	(Optional) Show only authentication records which have a minimum ID value. A valid ID is required.

Parameter	Description
id_max={value}	(Optional) Show only authentication records which have a maximum ID value. A valid ID is required.
Oracle Records	
template_auth_id={value}	(Optional) Specify the template ID for an Oracle system record template to only show Oracle records associated with the specified template.
template_auth_name={value}	(Optional) Specify the template name for an Oracle system record template to only show Oracle records associated with the specified template.
is_template={0|1}	(Optional) By default, template records and regular Oracle records are listed. Set to 0 to list only regular Oracle records or set to 1 to list only Oracle system record templates.
status={0|1}	(Optional) By default, active and inactive auth records are listed. Set to 0 to list only inactive records or set to 1 to list only active records.
is_system_created={0|1}	(Optional) By default, user created records and system created auth records are listed. Set to 0 to list only user created records or set to 1 to list only system created records.
MongoDB Records	
template_auth_id={value}	(Optional) Specify the template ID for an MongoDB system record template to only show MongoDB records associated with the specified template.
template_auth_name={value}	(Optional) Specify the template name for an MongoDB system record template to only show MongoDB records associated with the specified template.
is_template={0|1}	(Optional) By default, template records and regular MongoDB records are listed. Set to 0 to list only regular MongoDB records or set to 1 to list only MongoDB system record templates.
status={0|1}	(Optional) By default, active and inactive auth records are listed. Set to 0 to list only inactive records or set to 1 to list only active records.
is_system_created={0|1}	(Optional) By default, user created records and system created auth records are listed. Set to 0 to list only user created records or set to 1 to list only system created records.

DTD for list record type

<platform API server>/api/2.0/fo/auth/<type>/

where <type> is the authentication record type, such as unix, windows, oracle, etc.

Sample - List Unix and Cisco records

```
<AUTH_UNIX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-05-21T13:32:17Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>678</ID>
        <TITLE><![CDATA[My Ubuntu credentials]]></TITLE>
        <USERNAME><![CDATA[bumbler]]></USERNAME>
        <ROOT_TOOL>Sudo</ROOT_TOOL>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP_RANGE>10.10.10.168-10.10.10.195</IP_RANGE>
        </IP_SET>
        <CREATED>
            <DATETIME>2017-04-20T01:01:01</DATETIME>
            <BY>quays_es11</BY>
        </CREATED>
        <LAST_MODIFIED>
            <DATETIME>2017-04-20T01:01:01</DATETIME>
            <BY>quays_es11</BY>
        </LAST_MODIFIED>
        </COMMENTS><![CDATA[Development lab]]></COMMENTS>
      </AUTH_UNIX>
      ...
    </AUTH_UNIX_LIST>
    <WARNING_LIST>
        <WARNING>
            <CODE>1980</CODE>
            <TEXT>1000 record limit exceeded. Use URL to get next
batch of records.</TEXT>

<URL><qualys_base_url>/api/2.0/fo/auth/?action=list&id_min=3457</U
RL>
        </WARNING>
    </WARNING_LIST>
    <GLOSSARY>
        <USER_LIST>
            <USER>
                <USER_LOGIN>quays_es11</USER_LOGIN>
                <FIRST_NAME>Ernie</FIRST_NAME>
                <LAST_NAME>Smith</LAST_NAME>
            </USER>
        </USER_LIST>
    </GLOSSARY>
```

```
  </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample list Oracle record

This sample shows details for a single Oracle record specified by ID. The XML output identifies whether the record is system created, is active and is a template. In this example, the record listed is not system created. It is active and it is a template record.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=2237956"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/auth_oracle_list_out
put.dtd">
<AUTH_ORACLE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-23T18:44:27Z</DATETIME>
    <AUTH_ORACLE_LIST>
      <AUTH_ORACLE>
        <ID>2237956</ID>
        <TITLE><![CDATA[OracleRecordTemplate]]></TITLE>
        <USERNAME><![CDATA[OracleUser]]></USERNAME>
        <CREATED>
          <DATETIME>2020-04-23T18:43:59Z</DATETIME>
          <BY>rey_pt11</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-04-23T18:43:59Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
        <COMMENTS><![CDATA[my comments]]></COMMENTS>
      </AUTH_ORACLE>
    </AUTH_ORACLE_LIST>
  </RESPONSE>
</AUTH_ORACLE_LIST_OUTPUT>
```

Sample list MongoDB record

This sample shows details for a single MongoDB record specified by ID. The XML output identifies whether the record is system created, is active and is a template. In this example, the record listed is not system created. It is active and it is a template record.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=6847704"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

XML Output

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb_list_o
utput.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
<RESPONSE>
     <DATETIME>2023-01-05T12:47:03Z</DATETIME>
     <AUTH_MONGODB_LIST>
          <AUTH_MONGODB>
               <ID>6847704</ID>
               <TITLE>
                         <![CDATA[MongoDB system record template]]>
                    </TITLE>
                    <USERNAME>
                         <![CDATA[root]]>
                    </USERNAME>
                    <CREDENTIAL_TYPE>
                         <![CDATA[local]]>
                    </CREDENTIAL_TYPE>
                    <LOGIN_TYPE>
                         <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <REQUIRE_CERT>
                         <![CDATA[0]]>
                    </REQUIRE_CERT>
                    <CREATED>
                         <DATETIME>2023-01-05T07:16:46Z</DATETIME>
                         <BY>vt_sm1</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                         <DATETIME>2023-01-05T07:16:46Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                    <IS_TEMPLATE>1</IS_TEMPLATE>
               </AUTH_MONGODB>
          </AUTH_MONGODB_LIST>
     </RESPONSE>
</AUTH_MONGODB_LIST_OUTPUT>
```

Apache Cassandra Record

/api/2.0/fo/auth/cassandra

[POST]

Create, update, list and delete Apache Cassandra records for authenticated scans of Apcche Cassandra instances. Compliance scans are supported (using PC).

Both basic and vault based authentication are supported. For the Vault based authentication, see Vault Support matrix for the supported vaults.

Input Parameters

Parameter	Description
action={action}	Specify any one of the following: create, update, list, delete.
title={value}	(Required to create a record) A title for the record. Optional to update record.
ips={value}	(Required) Optional to update record. IPs to be added to your Apache Cassandra record. You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed
username={value}	(Optional) The username to be used for authentication to Apache Cassandra.
password={value}	(Optional) The password to be used for authentication to Apache Cassandra.
login_type={basic|vault}	(Required) The login type is basic by default. You can choose vault (for vault based authentication). Set to vault if a third party vault is used to retrieve the password. **Note**: For vault based authentication, vault parameters need to be provided in the record.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix in the API user guide.
port={value}	(Optional) The port number that the Apache Cassandra database instance is running on.
ssl_verify_with_host={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
require_cert={0|1}	(Optional) Set this to 1 when you want to authenticate the Apache Cassandra instance via certificate and private_key. Enabling this from API switch on the Require Certificate toggle on UI.
certificate={value}	(Required) Certificate content if require_cert is set to 1.
private_key={value}	(Required) private_key details if require_cert is set to 1.
hosts={value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.

Parameter	Description
confpath={value}	(Optional) The full path to Apache Cassandra yaml/yuml file.
basepath={value}	(Optional) The base path to Apache Cassandra installation.
cleartext={0|1}	(Optional) Set to 1 to send user credentials in clear text.
ids={value}	(Required to update record) Apache Cassandra Record IDs to update. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
passphrase={value}	(Optional) Specify password passphrase. If a client certificate is required, the private key specifies the client certificate. If this key is protected by a passphrase, you can provide it via this parameter.
use_vault_passphrase={0|1}	(Optional) Set to 1 if you want to store passphrase to vault. Enabling this from API switches the Get passphrase from vault toggle to Yes on the UI.
pp_vault_type={value}	(Required if use_vault_passphrase parameter is set to 1) If the passphrase is stored in a vault, this parameter indicates its vault type. Enter the type of the vault that stores the passphrase.
pp_vault_record={value}	(Required if use_vault_passphrase parameter is set to 1) If the passphrase is stored in a vault, this parameter indicates its vault ID. Enter the ID of the vault that stores the passphrase.
pp_<vault_parameters>={value}	Optional) If use_vault_passphrase parameter is set to 1 then all vault parameter fields must be added with prefix 'pp_' For example, pp_vault_type,pp_vault_record. Vault specific parameters required depend on the vault type you've selected. See “Vault Definition” in the API user guide

Sample- Create Apache Cassandra Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=create&title=apache_cassandra_API_create&login_type=basic&usernam
e=test&password=abc123&ips=1.1.1.6&port=12"
"https://<qualys_base_url>/api/2.0/fo/auth/cassandra/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2024-04-18T10:02:08Z</DATETIME>
```

```
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>4547904</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample- Update Apache Cassandra Record

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=update&title=apache_cassandra_API_update&login_type=basic&usernam
e=testupdate&ids=4547904"
"https://<qualys_base_url>/api/2.0/fo/auth/cassandra/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2024-04-18T10:06:56Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>4547904</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample- Delete Apache Cassandra Record

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=delete&ids=4545330"
"https://<qualys_base_url>/api/2.0/fo/auth/cassandra/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2024-04-18T10:37:21Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4545330</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample-List Apache Cassandra Records

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&ids=4547904"
"https://<qualys_base_url>/api/2.0/fo/auth/cassandra/"
```

XML Response

```
"<?xml version=""1.0"" encoding=""UTF-8"" ?>
<!DOCTYPE AUTH_CASSANDRA_LIST_OUTPUT SYSTEM
""https://<qualys_base_url>/api/2.0/fo/auth/cassandra/auth_cassandra_list
_output.dtd"">
<AUTH_CASSANDRA_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2024-04-18T10:22:00Z</DATETIME>
    <AUTH_CASSANDRA_LIST>
      <AUTH_CASSANDRA>
        <ID>4547904</ID>
        <TITLE><![CDATA[apache_cassandra_API_update]]></TITLE>
        <USERNAME><![CDATA[testupdate]]></USERNAME>
        <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
        <IP_SET>
          <IP>1.1.1.6</IP>
        </IP_SET>
        <REQUIRE_CERT><![CDATA[0]]></REQUIRE_CERT>
        <PORT><![CDATA[12]]></PORT>
        <SSL_VERIFY_WITH_HOST><![CDATA[0]]></SSL_VERIFY_WITH_HOST>
        <CLEARTEXT><![CDATA[0]]></CLEARTEXT>
        <USE_VAULT_PASSPHRASE><![CDATA[0]]></USE_VAULT_PASSPHRASE>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2024-04-18T10:02:08Z</DATETIME>
          <BY>vsh_sm</BY>
        </CREATED>
```

```
        <LAST_MODIFIED>
          <DATETIME>2024-04-18T10:09:27Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_CASSANDRA>
    </AUTH_CASSANDRA_LIST>
  </RESPONSE>
</AUTH_CASSANDRA_LIST_OUTPUT>
```

DTDs for Apache Cassandra records

<platform API server>/api/2.0/fo/auth/cassandra/auth_cassandra_list

DataStax Record

/api/2.0/fo/auth/datastax/

[POST]

Create, update, list and delete DataStax records for authenticated scans of DataStax instances. Compliance scans are supported (using PC).

Both basic and vault based authentication are supported. For the Vault based authentication, see Vault Support matrix for the supported vaults.

Input Parameters

Parameter	Description
action={action}	Specify any one of the following: create, update, list, delete.
title={value}	(Required to create a record) A title for the record. Optional to update record.
ips={value}	(Required) Optional to update record. IPs to be added to your DataStax record. You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed
username={value}	(Optional) The username to be used for authentication to DataStax.
password={value}	(Optional) The password to be used for authentication to DataStax.
login_type={basic|vault}	(Required) The login type is basic by default. You can choose vault (for vault based authentication). Set to vault if a third party vault is used to retrieve the password. **Note**: For vault based authentication, vault parameters need to be provided in the record.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix in the API user guide.
port={value}	(Optional) The port number that the DataStax database instance is running on.
ssl_verify_with_host={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
hosts={value}	(Required if ssl_verify_with_host=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
require_cert={0|1}	(Optional) Set this to 1 when you want to authenticate the DataStax instance via certificate and private_key. Enabling this from API switch on the Require Certificate toggle on UI.
certificate={value}	(Required) Certificate content if require_cert is set to 1.
private_key={value}	(Required) private_key details if require_cert is set to 1.
confpath={value}	(Optional) The full path to DataStax yaml/yuml file.

Parameter	Description
basepath={value}	(Optional) The base path to DataStax installation.
dseconfpath={value}	(Optional) Configuration path of DataStax conf file.
cleartext={0|1}	(Optional) Set to 1 to send user credentials in clear text.
ids={value}	(Required to update record) DataStax Record IDs to update. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
passphrase={value}	(Optional) Specify password passphrase. If a client certificate is required, the private key specifies the client certificate. If this key is protected by a passphrase, you can provide it via this parameter.
use_vault_passphrase={0|1}	(Optional) Set to 1 if you want to store passphrase to vault. Enabling this from API switches the Get passphrase from vault toggle to Yes on the UI.
pp_vault_type={value}	(Required if use_vault_passphrase parameter is set to 1) If the passphrase is stored in a vault, this parameter indicates its vault type. Enter the type of the vault that stores the passphrase.
pp_vault_record={value}	(Required if use_vault_passphrase parameter is set to 1) If the passphrase is stored in a vault, this parameter indicates its vault ID. Enter the ID of the vault that stores the passphrase.
pp_<vault_parameters>={value}	Optional) If use_vault_passphrase parameter is set to 1 then all vault parameter fields must be added with prefix 'pp_' For example, pp_vault_type,pp_vault_record. Vault specific parameters required depend on the vault type you've selected. See “Vault Definition” in the API user guide.

Sample- Create DataStax Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=create&title=datastax_API&login_type=basic&username=test&password
=abc123&ips=1.1.1.2&port=12"
"https://<qualys_base_url>/api/2.0/fo/auth/datastax/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2024-08-23T13:40:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
```

```
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>5380731</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample- Update DataStax Record

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=update&title=datastax_APIupdate&login_type=basic&username=testupd
ate&password=abc12312&ids=5380731&port=12"
"https://<qualys_base_url>/api/2.0/fo/auth/datastax/"
```

XML Response

```
<?xml version="1.0" encoding="utf-8"?>
<batch_return>
  <response>
    <datetime>2024-08-23T13:43:33Z</datetime>
    <batch_list>
      <batch>
        <text>Successfully Updated</text>
        <id_set>
          <id>5380731</id>
        </id_set>
      </batch>
    </batch_list>
  </response>
</batch_return>
```

Sample- List DataStax Record

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&ids=5380731"
"https://<qualys_base_url>/api/2.0/fo/auth/datastax/"
```

XML Response

```
<?xml version="1.0" encoding="utf-8"?>
<auth_datastax_list_output>
  <response>
    <datetime>2024-08-23T13:44:50Z</datetime>
    <auth_datastax_list>
      <auth_datastax>
        <id>5380731</id>
        <title>datastax_APIupdate</title>
        <username>testupdate</username>
```

```
        <ip_set>
          <ip>1.1.1.1</ip>
        </ip_set>
        <require_cert>0</require_cert>
        <port>12</port>
        <ssl_verify_with_host>0</ssl_verify_with_host>
        <login_type>basic</login_type>
        <created>
          <datetime>2024-08-23T13:40:49Z</datetime>
          <by>xx_xx</by>
        </created>
        <last_modified>
          <datetime>2024-08-23T13:43:33Z</datetime>
        </last_modified>
      </auth_datastax>
    </auth_datastax_list>
  </response>
</auth_datastax_list_output>
```

Sample- Delete DataStax Record

API Request

```
curl-s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=delete&ids=5380731"
"https://<qualys_base_url>/api/2.0/fo/auth/datastax/"
```

XML Response

```
<?xml version="1.0" encoding="utf-8"?>
<batch_return>
  <response>
    <datetime>2024-08-23T13:52:18Z</datetime>
    <batch_list>
      <batch>
        <text>Successfully Deleted</text>
        <id_set>
          <id>5380731</id>
        </id_set>
      </batch>
    </batch_list>
  </response>
</batch_return>
```

DTDs for DataStax records

<platform API server>/api/2.0/fo/auth/datastax/auth_datastax_list_output.dtd

Application Server Records

/api/2.0/fo/auth/{web app server}/

where {web app server} is one of apache, ms_iis, ibm_websphere, tomcat

[POST]

Create, update, list and delete application server records for authenticated scans of web application servers. Application Server records are used to authenticate to various web app servers.

Instance discovery and auto record creation is supported for Apache Web Server, IBM WebSphere, JBoss, Tomcat, Oracle and MongoDB. Learn more about instance discovery and auto record creation in online help (log in to your Qualys account, go to Help > Online Help and search for System Authentication Records).

Supported servers

API URL (/api/2.0/fo...)	Supported Versions
/auth/apache/	- Apache HTTP Server 2.2 and 2.4 - IBM HTTP Server 7.x, 8.x and 9.x - VMware vFabric Web Server 5.x - Pivotal Web Server 6.x Compliance scans are supported (using PC)
/auth/ms_iis/	MS IIS 6.0, 7.x, 8.x and 10 for Windows Compliance scans are supported (using PC)
/auth/ibm_websphere/	IBM WebSphere Application Server 7.x, 8.x and 9.x Compliance scans are supported (using PC)
/auth/tomcat/	Windows: - Apache Tomcat 7.x, 8.x and 9.x Unix: - Apache Tomcat 6.x, 7.x, 8.x and 9.x - VMware vFabric tc Server 2.9.x - Pivotal tc Server 3.x Vulnerability and Compliance scans are supported (using VM, PC)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required for create) The title of the Server record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional) User defined notes about the Server record. The comments may include a maximum of 1999 characters (ascii); if comments have 2000 or more characters an error is returned and comments are not saved. Tags (such as <script>) cannot be included; if tags are included an error is returned and the request fails.
Application Server	
unix_apache_config_file={value}	(Required to create an Apache Web Server record; valid only for this record). The path to the Apache configuration file.
unix_apache_control_command={value}	(Required to create an Apache Web Server record; valid only for this record) The path to the Apache control command. For IBM HTTP Server, enter the path to the IBM HTTP Server "bin" directory or the specific location of "apachectl". For VMware vFabric Web Server, enter the path to the VMware vFabric global "bin" directory or the specific location of "httpdctl" for a web server instance.
windows_apache_config_file={value}	(Required to create Apache HTTP and IBM HTTP server records; valid only for this record). The Windows path to the Apache HTTP and IBM HTTP server configuration file.
windows_apache_control_command={value}	(Required to create Apache HTTP and IBM HTTP server records; valid only for this record) The Windows path to the Apache HTTP and IBM HTTP server control command. For IBM HTTP Server, enter the path to the IBM HTTP Server "bin" directory or the specific location of "apachectl".
unix_installation_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record) The directory where the WebSphere application is installed.

Parameter	Description
unix_dir_mode={value}	(Optional for IBM WebSphere App Server record; valid only for this record) Specify the Unix directory mode. Valid values are installation_dir (for installation directory) and server_dir (for server directory). When not specified, installation_dir is used.
windows_installation_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record) The Windows directory where the WebSphere application is installed.
installation_path={value}	(Required to create Tomcat Server record on UNIX; valid only for this record) The directory where the tomcat server is installed. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_HOME) /opt/vmware/vfabric-tc-server-standard /opt/pivotal/pivotal-tc-server-standard
instance_path={value}	(Optional to create or update Tomcat Server record on UNIX; valid only for this record) The directory where the tomcat server instance(s) are installed. You can specify a single tomcat instance (use with auto_discover_instances=0), or multiple instances (use with auto_discover_instances=1). Leave unspecified when the instance directory is the same as the installation directory or when your targets have different types of tomcat servers. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_BASE) /opt/vmware/vfabric-tc-server-standard/tc1 /opt/pivotal/pivotal-tc-server-standard/tc1
auto_discover_instances={**0**|1}	(Optional to create or update Tomcat Server record; valid only for this record) Specify auto_discover_instances=1 and we'll find all tomcat server instances for you. Applies to VMware vFabric and Pivotal when you've specified a directory with multiple instances or you did not specify an instance. When unspecified (auto_discover_instances=0), we will not auto discover instances. Applies to Apache Tomcat or when you've specified a single instance.
installation_path_windows	(Required to create Tomcat Server record on Windows; valid only for this record) The directory where the tomcat server is installed. Example: C:\tomcat\apache-tomcat-8.5.11

Parameter	Description
instance_path_windows	(Optional to create or update Tomcat Server record on UNIX; valid only for this record) The directory where the tomcat server instance(s) are installed. Example: C:\tomcat\apache-tomcat-8.5.11
service_name	(Optional) The Tomcat service name that identifies the server instance to be authenticated to.
Apache Server only	
status={0|1}	(Optional to list, create, update Apache records). For list request (action set to list) - By default active and inactive auth records are listed. Set to 0 to list only inactive records or set to 1 to list only active records. For create/update request (action set to create or update) - By default a new record is set to active (1). Set to 0 for inactive record, or 1 for active record. For update action, this parameter is valid only when user created records are specified in the request.
is_system_created={0|1}	(Optional to list Apache records) By default user created records and system created auth records are listed. Set to 0 to list only user created records, or set to 1 to list only system created records.
Target Hosts	
ips={value}	(Required to create record) Add IP addresses of the hosts you want to scan using this record.
add_ips={value}	(Optional and valid only to update record) Add IP address(es) to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create Apache record

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&title=Apache+Record&unix_apache_config_file=/opt/IB
M/HTTPServer/conf/httpd.conf1&unix_apache_control_command=/opt/IBM
/HTTPServer/bin2&ips=10.10.25.25"
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

Sample - Update Apache record

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=update&ids=1234&unix_apache_config_file=/opt/IBM/HTTPServe
r/conf/httpd.conf2"
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

DTDs for server records

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/apache/auth_apache_list_output.dtd

<platform API server>/api/2.0/fo/auth/ms_iis/auth_ms_iis_list_output.dtd

<platform API server>/api/2.0/fo/auth/ibm_websphere/
auth_ibm_websphere_list_output.dtd

<platform API server>/api/2.0/fo/auth/tomcat./auth_tomcat_list_output.dtd

Azure MS SQL Record

/api/2.0/fo/auth/azure_ms_sql/

[POST]

Create, update, list, and delete Azure MS SQL records for compliance scans (using PC).Compliance scans are supported (using PC).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Set to 1 to view the request's input parameters (names and values) in the XML output. By default parameters are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional) User defined comments. Maximum of 1999 characters.
Login credentials	
provider_name={value}	(Optional) Name of the cloud service provider. The only value supported is azure. This value will be passed by default.
login_type={**basic**|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The username to be used for authentication to Azure MS SQL. The username must contain '@'.
password={value}	(Required to create record, optional to update record) when login_type=basic, specify the password to be used for authentication to Azure MS SQL. Maximum 100 characters (ascii).
instance_name={value}	(Optional to create or update record) The name of the database instance to be scanned. This is the instance name assigned to the TCP/IP port. Important: This is not the host name that is assigned to the Azure MS SQL Server instance name. The only value supported is MSSQLSERVER. This value will be passed by default. Currently, we do not support named instances for this parameter.

Parameter	Description
database_name={value}	(Optional to create or update record) The database name of the Azure MS SQL database to be scanned. The database name may contain a maximum of 128 characters. These parameters are mutually exclusive: database_name and auto_discover_databases=1.
auto_discover_databases={**0**|1}	(Optional to create or update record) The database name of the Azure MS SQL database to be scanned. The database name may contain a maximum of 128 characters. These parameters are mutually exclusive: database_name and auto_discover_databases=1.
port={value}	(Required to create record, optional to update record) The port number assigned to the database instance to be scanned.
Vaults	
vault_type={value}	(Required to create record when login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix.
vault_id={value}	(Required only when action=create and login_type=vault) The ID of the vault you want to use.
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.
Target Hosts	
ips={value}	(Required to create record) IPs to be added to your Azure MS SQL Record record. You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. (Optional to update record) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.
add_ips={value}	(Optional and valid only to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional and valid to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - List Azure MS SQL Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ids=4620763"
"https://qualysapi.qualys.com/api/2.0/fo/auth/azure_ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_AZURE_MS_SQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/azure_ms_sql/dtd/aut
h_list_output.dtd">
<AUTH_AZURE_MS_SQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-04-23T13:53:08Z</DATETIME>
    <AUTH_AZURE_MS_SQL_LIST>
      <AUTH_AZURE_MS_SQL>
        <ID>4620763</ID>
        <TITLE><![CDATA[AzureMSSQL_Auth_API]]></TITLE>
        <PROVIDER_NAME><![CDATA[Azure]]></PROVIDER_NAME>
        <USERNAME><![CDATA[john_user@qualys.com]]></USERNAME>
        <INSTANCE><![CDATA[MSSQLSERVER]]></INSTANCE>
        <DATABASE><![CDATA[testdb]]></DATABASE>
        <PORT>42</PORT>
        <IP_SET>
          <IP>1.1.1.4</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2021-04-01T11:47:51Z</DATETIME>
          <BY>up_at</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2021-04-01T11:47:51Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_AZURE_MS_SQL>
    </AUTH_AZURE_MS_SQL_LIST>
  </RESPONSE>
</AUTH_AZURE_MS_SQL_LIST_OUTPUT>
```

Sample - Create Azure MS SQL Record (with basic login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&title=my-azuremssql-record&ips=1.1.1.4&port=42
&database_name=dbname"
"https://qualysapi.qualys.com/api/2.0/fo/auth/azure_ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-04-23T11:47:51Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>4620763</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Azure MS SQL Record (with auto_discover_databases=1)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&auto_discover_databases=1&ids=207024"
"https://qualysapi.qualys.com/api/2.0/fo/auth/azure_ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-04-26T22:22:41Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>207024</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Azure MS SQL Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=delete&ids=4620768"
"https://qualysapi.qualys.com/api/2.0/fo/auth/azure_ms_sql/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-04-26T13:12:51Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4620768</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “azure_ms_sql”

<platform API server>/api/2.0/batch_return.dtd
<platform API server>/api/2.0/fo/auth/azure_ms_sql/dtd/auth_list_output.dtd

Cisco APIC 4.x Authentication Record

/api/2.0/fo/auth/cisco_apic/

[POST]

Create, update, and list, Cisco APIC 4.x authentication records, for the PC/SCA modules.

Input Parameters

Parameter	Required/ Optional	Data Type	Description
action	Required	String	Specify to list, create, update, delete, authentication records.
ids	Required	Integer	Specify a single or comma separated valid Cisco APIC type authentication record ID(s).
title	Required	Alpha-Numeric	Specify the title for the authentication record.
ips	Required	Integer	Specify the IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.
username	Required	String	Specify username for authentication login.
password	Required	String	Specify password for authentication login.
port	Required	Integer	Specify port number required on Cisco APIC devices.
ssl_verify	Optional	Integer	SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
Require Certificate	Optional	Alpha-Numeric	It contains two textfields, certificate and privatekey.
use_ad_hashicorp {0|1}	Optional	boolean	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
Vault Parameter			**Note:** The vault parameters are supported on the following vault types (Secret server Vault, Quest Vault, Hashicorp Vault, CyberArk AIM Vault, CyberArk PIM Vault, and AzureKey Vault).
vault_type	Required	String	Specify if create, and login_type=vault. (private key only supports "Cyber-Ark AIM" and "BeyondTrust PBPS", whereas passphrase does not support "BeyondTrust PBPS").

Parameter	Required/ Optional	Data Type	Description
vault_id	Required	Integer	Specify if create, and login_type=vault. The ID of the vault to be used to retrieve the password for login.
file	Required	String	Specify to create, if vault_type= "Cyber-Ark AIM" or "Cyber-ARK PIM Suite".
folder	Required	String	Specify to create, if vault_type="Cyber-Ark AIM" or "Cyber-ARK PIM Suite.
secret_name	Required	String	Specify to create, if vault_type="Thycotic Secret Server".
system_name	Required	String	Specify if yes(Quest) / no(BeyondTrust PBPS) (create, and vault_type="Quest Vault" or "BeyondTrust PBPS").
account_name	Required	String	Specify to create, if vault_type="BeyondTrust PBPS".

Sample - List Cisco APIC auth records API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d "action=list"
"http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_CISCO_APIC_LIST_OUTPUT SYSTEM
"https://qualys_base_url/api/2.0/fo/auth/cisco_apic/auth_cisco_apic_list_
output.dtd">
<AUTH_CISCO_APIC_LIST_OUTPUT>
  <RESPONSE>
    <AUTH_CISCO_APIC_LIST>
      <AUTH_CISCO_APIC>
        <ID>7850382</ID>
        <TITLE><![CDATA[user 1]]></TITLE>
        <USERNAME><![CDATA[user 1]]></USERNAME>
        <PORT>444</PORT>
        <WINDOWS_DOMAIN><![CDATA[aaaa]]></WINDOWS_DOMAIN>
        <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
        <IP_SET>
          <IP>3.3.3.3</IP>
        </IP_SET>
        <REQUIRE_CERT><![CDATA[1]]></REQUIRE_CERT>
        <DOMAIN><![CDATA[aaaa]]></DOMAIN>
        <PORT><![CDATA[444]]></PORT>
        <SSL_VERIFY_WITH_HOST><![CDATA[1]]></SSL_VERIFY_WITH_HOST>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <BY>vt_sm1</BY>
```

```
        </CREATED>
      </AUTH_CISCO_APIC>
    </AUTH_CISCO_APIC_LIST>
  </RESPONSE>
</AUTH_CISCO_APIC_LIST_OUTPUT>
```

DTD Output:

DTD: <qualys_base_url>/api/2.0/fo/auth/auth_cisco_apic_list_output.dtd

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!ELEMENT AUTH_RECORDS_OUTPUT (REQUEST?, RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, AUTH_RECORDS?, WARNING_LIST?)>

<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?,
AUTH_SAPIQ_IDS?,AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?,
AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?,
AUTH_INFOBLOX_IDS?, AUTH_CISCO_APIC_IDS?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_WEBSPHERE_IDS (ID_SET)>
<!ELEMENT AUTH_HTTP_IDS (ID_SET)>
```

```
<!ELEMENT AUTH_SYBASE_IDS (ID_SET)>
<!ELEMENT AUTH_MYSQL_IDS (ID_SET)>
<!ELEMENT AUTH_TOMCAT_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>
<!ELEMENT AUTH_POSTGRESQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAPIQ_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_HANA_IDS (ID_SET)>
<!ELEMENT AUTH_NEO4J_IDS (ID_SET)>
<!ELEMENT AUTH_AZURE_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_NETWORK_SSH_IDS (ID_SET)>
<!ELEMENT AUTH_NGINX_IDS (ID_SET)>
<!ELEMENT AUTH_INFOBLOX_IDS (ID_SET)>
<!ELEMENT AUTH_CISCO_APIC_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!-- EOF -->
```

Sample - Create Cisco APIC auth records Request API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d
"action=create&ips=3.3.3.3&title=testciscoapic&username=admin&password=ab
c123&port=443" "http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2023-08-09T11:03:04Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>7850988</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Cisco APIC auth records Request API

API Request:

```
curl -u "<token>" -H "X-Requested-With: curl" -d
"action=update&ids=7850382&title=testciscoapic"
"http://qualys_base_url/api/2.0/fo/auth/cisco_apic/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2023-08-09T10:48:33Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>7850382</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD Output:

DTD: <qualys_base_url>/api/2.0/fo/auth/auth_cisco_apic_list_output.dtd

```
<!-- QUALYS AUTH_CISCO_APIC_LIST_OUTPUT DTD -->

<!ELEMENT AUTH_CISCO_APIC_LIST_OUTPUT (REQUEST?, RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
```

```
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (AUTH_CISCO_APIC_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_CISCO_APIC_LIST (AUTH_CISCO_APIC+)>

<!ELEMENT AUTH_CISCO_APIC (ID,
TITLE,USERNAME,SSL_VERIFY?,HOSTS?,REQUIRE_CERT?,CERTIFICATE?,PRIVATE_KEY?
,IP_SET?,PORT?,LOGIN_TYPE?,DIGITAL_VAULT?,NETWORK_ID?,CREATED,LAST_MODIFI
ED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT REQUIRE_CERT (#PCDATA)>
<!ELEMENT HOSTS (#PCDATA)>
<!ELEMENT CERTIFICATE (#PCDATA)>
<!ELEMENTPRIVATE_KEY (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?,
VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
```

```
        <!ELEMENT WARNING_LIST (WARNING+)>
        <!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
        <!ELEMENT CODE (#PCDATA)>
        <!ELEMENT TEXT (#PCDATA)>
        <!ELEMENT URL (#PCDATA)>
        <!ELEMENT ID_SET (ID|ID_RANGE)+>
        <!ELEMENT ID_RANGE (#PCDATA)>

        <!ELEMENT GLOSSARY (USER_LIST?)>
        <!ELEMENT USER_LIST (USER+)>
        <!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
        <!ELEMENT FIRST_NAME (#PCDATA)>
        <!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

DTDs for auth type “cisco_apic”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/auth_cisco_apic_list_output.dtd

DNS BIND Authentication Record

/api/2.0/fo/auth/bind/

[POST]

Create, update, and list, DNS BIND authentication records, for the PC/SCA modules.

Input Parameters

Parameter	Required/ Optional	Data Type	Description
action	Required	String	Specify to list, create, update, delete, authentication records.
ids	Required	Integer	Specify a single or comma separated valid DNS BIND type authentication record ID(s).
title	Required	Alpha-Numeric	Specify the title for the authentication record.
ips	Required	Integer	Specify the IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.
unix_bin_path	Required	Path	Specify absolute path of the DNS BIND Base64 encoded binary file location. Base64 encoded binary file path. Example- "/usr/sbin/named".
unix_conf_path	Required	Path	Specify absolute path of the DNS BIND Base64 encoded configuration file path. Example- "/etc/named.conf".
base_directory	Optional	Path	Specify Base64 encoded base directory. In BIND configuration file, if an include file is relative path, it is relative to this base_dir. Optional field, if not present, it will be derived from conf_path. Example- If conf_path is /etc/named.conf and if base_dir is not specified, then base_dir is set to "/etc". It must be absolute path if specified.
chroot_directory	Optional	Path	Specify Base64 encoded chroot directory. Optional field, only needed if BIND runs in a self contained environment. If present, must be absolute path and it will be prefixed to all other 3 paths. Example- If chroot_dir is "/var/bind" and if bin_path is "/usr/sbin/named", then the final bin_path will be "/var/bind/usr/sbin/named".

Sample - List DNS BIND auth records API

API Request:

```
curl" -d "action=list" "http://qualys_base_url/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_BIND_LIST_OUTPUT SYSTEM
"https://qualys_base_url/api/2.0/fo/auth/bind/auth_bind_list_output.dtd">
<AUTH_BIND_LIST_OUTPUT>
    <AUTH_BIND_LIST>
      <AUTH_BIND>
        <ID>7882778</ID>
        <TITLE><![CDATA[user_1]]></TITLE>
        <IP_SET>
          <IP>40.40.40.6</IP>
        </IP_SET>
        <UNIX_BIN_PATH><![CDATA[/usr/bin/bind]]></UNIX_BIN_PATH>
        <UNIX_CONF_PATH><![CDATA[/etc/bind/bind.conf]]></UNIX_CONF_PATH>
        <BASE_DIRECTORY><![CDATA[/etc/bind]]></BASE_DIRECTORY>
        <CHROOT_DIRECTORY><![CDATA[/etc/bind]]></CHROOT_DIRECTORY>
        <CREATED>
          <DATETIME>2023-08-14T16:15:57Z</DATETIME>
          <BY>vt_sm1</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2023-08-14T16:15:57Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_BIND>
    </AUTH_BIND_LIST>
  </RESPONSE>
</AUTH_BIND_LIST_OUTPUT>
```

Sample - Create DNS BIND auth records Request API

API Request:

```
curl" -d
"action=create&ips=40.40.40.6&title=user_1bind2c&unix_bin_path=/etc&unix_
conf_path=/etc/bind" "http://qualys_base_url:48443/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>7882779</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update DNS BIND auth records Request API

API Request:

```
curl" -d "action=update&ids=7882778&title=testbind"
"http://qualys_base_url:48443/api/2.0/fo/auth/bind/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualys_base_url/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>7882778</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD Output:

Auth Record list output DTD

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!ELEMENT AUTH_RECORDS_OUTPUT (REQUEST?, RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, AUTH_RECORDS?, WARNING_LIST?)>

<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?,
```

```
AUTH_SAPIQ_IDS?,AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?,
AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?,
AUTH_INFOBLOX_IDS?, AUTH_BIND_IDS?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_WEBSPHERE_IDS (ID_SET)>
<!ELEMENT AUTH_HTTP_IDS (ID_SET)>
<!ELEMENT AUTH_SYBASE_IDS (ID_SET)>
<!ELEMENT AUTH_MYSQL_IDS (ID_SET)>
<!ELEMENT AUTH_TOMCAT_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>
<!ELEMENT AUTH_POSTGRESQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAPIQ_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_HANA_IDS (ID_SET)>
<!ELEMENT AUTH_NEO4J_IDS (ID_SET)>
<!ELEMENT AUTH_AZURE_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_NETWORK_SSH_IDS (ID_SET)>
<!ELEMENT AUTH_NGINX_IDS (ID_SET)>
<!ELEMENT AUTH_INFOBLOX_IDS (ID_SET)>
<!ELEMENT AUTH_BIND_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!-- EOF -->
```

DTD: <qualys_base_url>/api/2.0/fo/auth/auth_bind_list_output.dtd

Auth Infoblox list output DTD

```
<!-- QUALYS AUTH_BIND_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_BIND_LIST_OUTPUT (REQUEST?, RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (AUTH_BIND_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_BIND_LIST (AUTH_BIND+)>

<!ELEMENT AUTH_BIND (ID,
TITLE,IP_SET?,UNIX_BIN_PATH?,UNIX_CONF_PATH?,BASE_DIRECTORY?,CHROOT_DIREC
TORY?,NETWORK_ID?,CREATED,LAST_MODIFIED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT UNIX_BIN_PATH (#PCDATA)>
<!ELEMENT UNIX_CONF_PATH (#PCDATA)>
<!ELEMENT BASE_DIRECTORY (#PCDATA)>
<!ELEMENT CHROOT_DIRECTORY (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
```

```
      <!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

DTDs for auth type “dns_bind”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/auth_bind_list_output.dtd

Docker Record

/api/2.0/fo/auth/docker/

[POST]

Create, update, list and delete Docker records for compliance scans (using PC). This record is used to authenticate to a Docker daemon (version 1.9 to 1.12) running on a Linux host.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Set to 1 to echo the request's input parameters (names and values) in the XML output. By default parameters are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) The record title.
comments={value}	(Optional) User defined comments.
Docker	
docker_deamon_conf_file={value}	(Optional to create or update record) Location of the configuration file for the docker daemon.
docker_command={value}	(Optional) The docker command to connect to a local docker daemon.
Target Hosts	
ips={value}	(Required to create record) IPs to be added to your docker record.
add_ips={value}	(Optional and valid only to update record) IPs to be added to an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={1|0}	(Optional) By default, the parameter is set to 0

Sample - Create Docker record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d
"action=create&title=docker_sample&ips=10.10.30.159&docker_deamon_
conf_file=/etc/docker/daemon.json&docker_command=/usr/bin/docker&e
cho_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/docker/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <REQUEST>
    <DATETIME>2018-03-09T06:09:46Z</DATETIME>
    <USER_LOGIN>username</USER_LOGIN>
<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/docker/</RE
SOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>create</VALUE>
      </PARAM>
      <PARAM>
        <KEY>title</KEY>
        <VALUE>docker_sample</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ips</KEY>
        <VALUE>10.10.30.159</VALUE>
      </PARAM>
      <PARAM>
        <KEY>docker_deamon_conf_file</KEY>
        <VALUE>/etc/docker/daemon.json</VALUE>
      </PARAM>
      <PARAM>
        <KEY>docker_command</KEY>
        <VALUE>/usr/bin/docker</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
```

```
  <RESPONSE>
    <DATETIME>2018-03-09T06:09:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Docker Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d
"action=update&ids=72685&add_ips=10.10.26.26"
"https://qualysapi.qualys.com/api/2.0/fo/auth/docker/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-09T06:12:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “docker”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/docker/auth_docker_list_output.dtd

HTTP Record

/api/2.0/fo/auth/http/

[POST]

Create, update and delete HTTP records for authenticated scans of protected portions of web sites and devices, like printers and routers, that require HTTP protocol level authentication. Authenticated scans are supported using VM and PC.

How it works - During an authenticated scan, if we come across a web page that requires HTTP authentication then we'll check to see if an HTTP record exists in your account with applicable credentials. If yes, we'll use the credentials in the record to perform HTTP authentication. (Note this is not Form-based authentication.)

Input Parameters

Parameter	Description
ips={value}	(Optional) Add IP addresses of the hosts you want to scan using this record.
action={value}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Set to 1 to echo the request's input parameters (names and values) in the XML output. By default parameters are not included.
comments={value}	(Optional for create or update request) User-defined comments.
ids={value}	(Required to update or delete record) One or more HTTP record IDs.
title={value}	(Required for a create request; Optional for an update request; otherwise invalid) The HTTP record title.
username={value}	(Required to create record, optional to update record) The user name to be used for authentication.
password={value}	(Required to create record, optional to update record) The password to be used for authentication. Maximum 100 characters (ascii).
ssl={**0**|1}	(Optional to create or update record) Specify 1 if you want to attempt authentication over SSL only. In this case authentication is attempted only when the form is submitted via a link that uses https://...
vhost={value} - or - realm={value} - or - ips={value}	(Required to create record; optional to update record) Specify the protected device or web page you want to authenticate against. You can specify a virtual host (an FQDN such as vhost=bank.qualys.com) or the name of a realm (realm=My+Homepage) or an IP address.

Parameter	Description
Login credentials	
login_type={basic|vault}	(Optional) The login type is basic by default. Specify login_type=vault to use an authentication vault.
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a HTTP account. If login_type=vault is specified, this is the username of a vault account.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to HTTP server. Maximum 100 characters (ascii).
Vault	
vault_type={value}	(Required only when action=create and login_type= vault) The vault to be used for authentication. See Vault Support matrix.
vault_id={value}	(Required only when action=create and login_type= vault) The ID of the vault you want to use.
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.

Sample - Create HTTP record, realm

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&username=jsmith&password=<PASSWORD>&title=My+HTTP+R
ecord+1&realm=My+Homepage"
"https://qualysapi.qualys.com/api/2.0/fo/auth/http/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-03T07:51:48Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>55111</ID>
        </ID_SET>
      </BATCH>
```

```
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Create HTTP record, virtual host

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&username=jsmith&password=<PASSWORD>&title=My+HTTP+R
ecord+2&vhost=bank.us.corp1.com"
"https://qualysapi.qualys.com/api/2.0/fo/auth/http/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-03T08:02:44Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>55112</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN
```

DTDs for auth type “http”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/http/auth_http_list_output.dtd

IBM DB2 Record

/api/2.0/fo/auth/ibm_db2/

[POST]

Create, update, list and delete IBM DB2 records for vulnerability and compliance scans (using VM, PC). This record is used for authenticated scanning of one or more DB2 instances on a single host. Want to scan multiple instances? See "Multiple DB2 Instances" in online help.

Requirement - You must set up target hosts per the Qualys User Guide.

Download Qualys User Guide - IBM DB2 Authentication (.zip)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
vault_id={value}	(Required only when action=create and login_type=vault) The ID of the vault you want to use to retrieve the password for login.
vault_type={value}	(Required only when action=create and login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See “Vault Support Matrix” in the API User Guide. The following vault types are supported for IBM DB2 at this time: ARCON PAM, CA Access Control, CyberArk AIM, CyberArk PIM Suite, HashiCorp, Lieberman ERPM, Quest Vault, Thycotic Secret Server
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you’ve selected. See “Vault Definition” in the API User Guide to know which parameters are required for each vault type.
title={value}	(Required to create record) The title for the record. The title must be unique and may include a maximum of 255 characters (ascii).

Parameter	Description
comments={value}	(Optional) User defined notes about the record. Maximum of 1999 characters (ascii).
pc_only={**0**|1}	(Optional) Specify pc_only=1 if the record will be used for compliance scans only. See "Sample - Create IBM DB2 Record with Vault."
Login Credentials	
login_type={basic|vault}	(Optional) The login type is basic by default. Specify login_type=vault to use a third party vault to retrieve the password for authentication. Vault parameters need to be provided in the record.
username={value}	(Required to create record, optional to update record) The user name for a DB2 database account. A maximum of 13 characters (ascii) may be specified.
password={value}	(Required to create record, optional to update record) The password for a DB2 database account. Maximum 100 characters (ascii).
database={value}	(Required to create record, optional to update record) The name of the DB2 database. A maximum of 8 characters (ascii) may be specified.
port={value}	(Required to create record, optional to update record) The port the database instance is running on.
Target Hosts	
ips={value}	(Required to create record, optional to update record) Add IP addresses of the hosts you want to scan using this record. Overwrites (replaces) the IP address(es) in the IP list for an existing authentication record. The IPs you specify are added, and any existing IPs are removed. You may enter a combination of IPs and IP ranges.
add_ips={value}	(Optional to update record) Add IP address(es) to the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges.
remove_ips={value}	(Optional and valid to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
OS Parameters	
win_db2dir={value} unix_db2dir={value}	The path to the DB2 runtime library if you want the service to perform OS-dependent compliance checks. This is the location where DB2 has been installed on the server. Maximum of 255 characters.

Parameter	Description
win_prilogfile={value} unix_prilogfile={value}	The path to the primary archive location if you want the service to perform OS-dependent compliance checks. This is the directory where the primary log files are located. Maximum of 255 characters.
win_seclogfile={value} unix_seclogfile={value}	The path to the secondary archive location if you want the service to perform OS-dependent compliance checks. Maximum of 255 characters. This parameter specifies the number of secondary log files that are created and used for recovery log files (only as needed). It is set by the DB2 logsecond parameter.
win_terlogfile={value} unix_terlogfile={value}	The path to the tertiary archive location if you want the service to perform OS-dependent compliance checks. Maximum 255 characters. This parameter specifies a path to which DB2 will try to archive log files if thelog files cannot be archived to either the primary or the secondary (if set) archivedestinations because of a media problem affecting those destinations. It is set by the DB2 failarchpath parameter.
win_mirlogfile={value} unix_mirlogfile={value}	The path to the mirror archive location if you want the service to perform OS-dependent compliance checks. Maximum 255 characters. If mirrorlogpath is configured, DB2 will create active log files in both the log path and the mirror log path. All log data will be written to both paths. The mirror log path has a duplicate set of active log files. If the active log files are destroyed by a disk error or human error, the database can still function.

Sample - Create IBM DB2 Record with Vault

In this sample, we're creating a new record and specifying a CyberArk AIM vault.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=create&title=MyDB2Record&username=joe_user&login_type=vaul
t&vault
_id=45014&vault_type=CyberArk
AIM&folder=Root\Windows7&file=rd.txt&database=db2&port=1234&ips=10
.11.12.
13" "https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_db2/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
```

```
<RESPONSE>
<DATETIME>2021-10-11T11:48:03Z</DATETIME>
<BATCH_LIST>
<BATCH>
<TEXT>Successfully Created</TEXT>
<ID_SET>
<ID>112491</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

Multiple DB2 Instances

The service has the ability to authenticate to multiple DB2 instances on a single host during scanning. For a vulnerability scan, an instance "uniqueness" is defined by an IP address and port. For a compliance scan, an instance "uniqueness" is defined by an IP address, port and database name. The setting for "pc_only" has an impact on how the services determines the uniqueness of a DB2 instance.

Let's say you want to define these DB2 records in your account.

	IP Address	Port	Database Name	pc_only=0|1
Record 1	10.10.31.178	5000	SAMPLE	pc_only=0
Record 2	10.10.30.159	5000	TOOLS	pc_only=0
Record 3	10.10.30.159	5000	SAMPLE	pc_only=1

Record 1 and Record 2 will be used for vulnerability scans and compliance scans. You'll notice Records 2 and 3 have the same IP address and port but different database names - this is allowed because Record 3 is used for compliance scans only.

DB2 Paths

When specifying the path to configuration files, these special characters are not allowed:

For Windows:

; & | # % ? ! * ` ( ) [ ] " ' > < = ^ /

For Unix:

; & | # % ? ! * ` ( ) [ ] " ' > < = ^ \

DTDs for auth type "ibm_db2"

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/ibm_db2/auth_ibm_db2_list_output.dtd

InformixDB Record

/api/2.0/fo/auth/informixdb/

[POST]

Create, update, list and delete InformixDB authentication records. Compliance scans are supported (using PC).

- Unix authentication is required for compliance scans using the PC app. Make sure the IP addresses you define in your InformixDB records are also defined in Unix records.

- We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to InformixDB instances.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
InformixDB	
ssl_verify={0|1}	(Optional to create or update record, and valid for server that supports SSL) Specify 1 for a complete SSL certificate validation. - If ssl_verify=0, the Qualys scanners authenticate with Informix Servers that don't use SSL or InformixDB servers that use SSL. However, in the SSL case, the server SSL certificate verification will be skipped. - If unspecified (or ssl_verify=1), the Qualys scanners will only send a login request after verifying that a connection to the InformixDB server uses SSL, the server SSL certificate is valid and matches the scanned host.
hosts={value}	(Optional to create or update record) A list of FQDNs for the hosts that correspond to all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
database_name={value}	(Required to create record, optional to update record) The database name to authenticate to. Specify a valid InformixDB database name. Maximum 255 characters.

Parameter	Description
port={value}	(Required to create record, optional to update record) The port the database name is running on. Valid range is 1-65535. The standard port for InformixDB is 1526.
unix_config_dir={value}	(Optional to create or update record) The path to the Unix informixdb installation directory. Access to this directory is required to run certain checks on Unix hosts.
unix_on_config_dir={value}	(Optional to create or update record) The absolute path to the Unix file that contains configuration parameters of the database server.
unix_sql_host_dir={value}	(Optional to create or update record) The absolute path to the Unix file that contains database connectivity information.
Login credentials	
login_type={basic}	(Optional) The login type is basic by default. We are not supporting vault based authentication.
username={value}	(Required to create record, optional to update record) The username to be used for authentication to InformixDB server.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to InformixDB server. Maximum 100 characters (ascii).
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - Create InformixDB record (with basic login and without ssl_verify)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=my-informixdb-record&username=informix-
admin&password=<PASSWORD>&ips=10.10.10.11&comments=informix-basic-
ipv4&unix_config_dir=/opt/informix/&port=1526&ssl_verify=0&unix_on
_config_dir=/opt/Informix/etc/onconfig.demo&unix_sql_host_dir=opt/
Informix/etc/sqlhosts.demo&database_name=dbname&login_type=basic"
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/informixdb/"
```

XML output:

```
<BATCH_RETURN>
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-01-30T15:45:05Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>43025</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create InformixDB record (with ssl_verify)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=my-informixdb-record&username=informix-
admin&password=<PASSWORD>&ips=10.10.10.11&comments=informix-basic-
ipv4&unix_config_dir=/opt/informix/&port=1526&ssl_verify=1&unix_on
_config_dir=/opt/Informix/etc/onconfig.demo&unix_sql_host_dir=opt/
Informix/etc/sqlhosts.demo&database_name=dbname&login_type=basic&h
osts=mlinformixdb32e.s2012r2.qualys.com,mlinformixdb32e.s2008r2.qu
alys.com"
"https://qualysapi.qualys.com/api/2.0/fo/auth/informixdb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-01-30T15:47:01Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>43026</ID>
```

```
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List InformixDB record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&details=Basic"
"https://qualysapi.qualys.com/api/2.0/fo/auth/informixdb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_INFORMIXDB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/fo/auth/informixdb/auth_informixdb_l
ist_output.dtd">
<AUTH_INFORMIXDB_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-01-30T15:19:02Z</DATETIME>
        <AUTH_INFORMIXDB_LIST>
            <AUTH_INFORMIXDB>
                <ID>40034</ID>
                <TITLE><![CDATA[InformixDB1]]></TITLE>
                <USERNAME><![CDATA[root]]></USERNAME>
                <DATABASE><![CDATA[informixdb]]></DATABASE>
            ...
            </AUTH_INFORMIXDB>
        </AUTH_INFORMIXDB_LIST>
    </RESPONSE>
</AUTH_INFORMIXDB_LIST_OUTPUT>
```

Sample - Update InformixDB record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&ids=41026&title=API-informixdb-basic-login-
updated&username=admin-updated-again&password=<updated-
password>&database_name=new-admin&comments=informixdb-basic-login-
ipv4-updated&unix_config_dir=/opt/informixdb/updated/again"
"https://qualysapi.qualys.com/api/2.0/fo/auth/informixdb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
```

```
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-01-30T16:00:16Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>43025</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete InformixDB record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=delete&ids=43023,43024"
"https://qualysapi.qualys.com/api/2.0/fo/auth/informixdb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://10.114.69.159:46445/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-01-30T15:41:46Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID_RANGE>43023-43024</ID_RANGE>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “informixdb”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/informixdb/auth_informixdb_list_output.dtd

Infoblox Record

/api/2.0/fo/auth/infoblox

[POST]

Create, update, list and delete Infoblox authentication records. Infoblox authentication records are available for the PC/SCA module.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
ids={value}	(Required to edit or delete record) Record IDs to edit/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
ips={value}	(Required to create record) The IP address(es) for the Infoblox devices you want to authenticate to. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
api_version{value}	(Required) API version required on Infoblox devices.
ssl_verify={**0**|1}	(Required) By default set to 0. When set to 1 our service will verify the certificate of the web server. When set to 0, our service will not verify the certificate of the web server.
Login credentials	
login_type={**basic**|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication). **Note** - Required when updating details for HashiCorp and Wallix Authentication Vaults.
username={value}	(Required to create record, optional to update record) The username to be used for authentication to Infoblox server.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to Infoblox server.
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
Vault	

Parameter	Description
vault_type={value}	(Required to create record when login_type=vault) The vault type to be used for authentication. See Vault Support matrix.
vault_id={value}	(Required to create record when login_type=vault and you want to retrieve private key from vault) The vault ID where you want to retrieve the private key from. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.

Sample - Create Infoblox record (with basic login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&ips=10.20.30.40&title=Infoblox_Auth11&api_version=1
v2.0123&ssl_verify=false&username=joe_user&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-06-29T10:50:19Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List Infoblox record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_INFOBLOX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/auth_infobl
ox_list_output.dtd">
<AUTH_INFOBLOX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-06-29T11:13:21Z</DATETIME>
    <AUTH_INFOBLOX_LIST>
      <AUTH_INFOBLOX>
        <ID>6317683</ID>
        <TITLE><![CDATA[Infoblox_Auth_update]]></TITLE>
        <USERNAME><![joe_user]></USERNAME>
        <SSL_VERIFY><![CDATA[true]]></SSL_VERIFY>
        <IP_SET>
          <IP>1.1.1.1</IP>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <API_VERSION><![CDATA[1v2.0124]]></API_VERSION>
        <SSL_VERIFY><![CDATA[true]]></SSL_VERIFY>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2022-06-29T10:50:19Z</DATETIME>
          <BY>scan_at</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2022-06-29T11:10:12Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[added]]></COMMENTS>
      </AUTH_INFOBLOX>
    </AUTH_INFOBLOX_LIST>
  </RESPONSE>
</AUTH_INFOBLOX_LIST_OUTPUT>
```

Sample - Update Infoblox record (with basic login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&add_ips=10.20.30.40&title=Infoblox_Auth_update&api_
version=1v2.0124&ssl_verify=true&comments=added&ids=6317685"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2022-06-29T11:10:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Infoblox record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
 "action=delete&ids=6317685"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-06-29T11:18:52Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Infoblox record (with Vault login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&ips=10.20.30.40&title=Infoblox_Auth_With_Vault&logi
n_type=vault&api_version=1v2.0123&username=joe_user&vault_type=Has
hiCorp&vault_id=1062779&secret_kv_name=admin&secret_kv_key=Infoblo
x_vault_secret&ssl_verify=0"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
<RESPONSE>
<DATETIME>2022-07-14T07:46:29Z</DATETIME>
<BATCH_LIST>
<BATCH>
<TEXT>Successfully Created</TEXT>
<ID_SET>
<ID>1898844</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

Sample - Update Infoblox record (with Vault login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&add_ips=10.20.30.40&title=Infoblox_Auth_update&api_
version=1v2.0125&ssl_verify=1&comments=added&ids=1898844"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
<RESPONSE>
<DATETIME>2022-07-14T07:46:29Z</DATETIME>
<BATCH_LIST>
<BATCH>
<TEXT>Successfully Updated</TEXT>
<ID_SET>
<ID>1898844</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

Sample - Update Details for HashiCorp and Wallix Authentication Vaults

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"<username>:<password>" -d
"action=update&ids=6975476&add_ips=1.1.1.94&login_type=vault&vault
_type=HashiCorp&secret_kv_name=secret&secret_kv_key=key"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-08-22T10:21:50Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>6975476</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “Infoblox”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/infoblox/auth_infoblox_list_output.dtd

JBoss Server record

/api/2.0/fo/auth/jboss/

[POST]

Create, update, list and delete JBoss Server records for vulnerability and compliance scans (using VM, PC). Supports Windows and Unix platforms.

Supported technologies:

Windows - WildFly/JBoss EAP

Unix - WildFly/JBoss EAP

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required) Specify a single or comma separated valid JBoss type auth record ID(s).
title={value}	(Required to create record) A title for the record. The title must be unique.
comment={value}	(Optional to create or update record) User defined comments.
Windows platform	
windows_working_mode={value}	(Optional) Input values should be standalone_mode or domain_controller_mode.
windows_home_path={value}	Required if windows working mode is selected.
windows_base_path={value}	Required if windows working mode is selected.
windows_conf_dir_path={value}	Required if windows working mode is selected.
windows_conf_file_path={value}	Required if windows working mode is selected.
windows_conf_host_file_path={value}	Required if selected Windows working mode is domain controller.
Unix platform	
unix_working_mode={value}	(Optional) Input values should be standalone_mode or domain_controller_mode.
unix_home_path={value}	Required if Unix working mode is selected.

Parameter	Description
unix_base_path={value}	Required if Unix working mode is selected.
unix_conf_dir_path={value}	Required if Unix working mode is selected.
unix_conf_file_path={value}	Required if Unix working mode is selected.
unix_conf_host_file_path={value}	Required if selected Unix working mode is domain controller.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional and valid only to update record) IPs to be added to an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create JBoss Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=jbos_rec&windows_working_mode=standalone_mode
&windows_base_path=c:\&windows_home_path=c:\&windows_conf_file_pat
h=c:\&windows_conf_dir_path=c:\&comment=record
creation&ips=10.10.10.224"
"https://qualysapi.qualys.com/api/2.0/fo/auth/jboss/"
```

XML output:

```
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-08-03T10:42:32Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>296004</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
```

```
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List JBoss Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&ids=296004"
"https://qualysapi.qualys.com/api/2.0/fo/auth/jboss/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_JBOSS_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/jboss/auth_jboss_lis
t_output.dtd">
<AUTH_JBOSS_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-08-03T10:44:39Z</DATETIME>
    <AUTH_JBOSS_LIST>
      <AUTH_JBOSS>
        <ID>296004</ID>
        <TITLE><![CDATA[jboss_record]]></TITLE>
        <IP_SET>
          <IP>10.10.10.224</IP>
        </IP_SET>
        <WINDOWS>
          <HOME_PATH><![CDATA[c:\]]></HOME_PATH>
          <DOMAIN_MODE><![CDATA[true]]></DOMAIN_MODE>
          <BASE_PATH><![CDATA[c:\]]></BASE_PATH>
          <CONF_DIR_PATH><![CDATA[c:\]]></CONF_DIR_PATH>
          <CONF_FILE_PATH><![CDATA[c:\]]></CONF_FILE_PATH>
          <CONF_HOST_FILE_PATH><![CDATA[c:\]]></CONF_HOST_FILE_PAT
H>
        </WINDOWS>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-08-03T10:42:32Z</DATETIME>
          <BY>abc_pk</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-08-03T10:43:58Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[record creation]]></COMMENTS>
      </AUTH_JBOSS>
    </AUTH_JBOSS_LIST>
```

```
  </RESPONSE>
</AUTH_JBOSS_LIST_OUTPUT>
```

Sample record configurations

We have sample JBoss record configurations in our online help. Log in to your Qualys account and select Help > Online Help and search for JBoss.

DTDs for auth type “jboss”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/jboss/auth_jboss_list_output.dtd

Kubernetes Record

/api/2.0/fo/auth/kubernetes/

[POST]

Create, update, list and delete Kubernetes records for compliance scans (using PC). This record is used to authenticate to a Kubernetes application (version 1.x) running on a Unix host.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Set to 1 to echo the request's input parameters (names and values) in the XML output. By default parameters are not included.
details={Basic}	(Optional) Default value is Basic. You can choose from None, Basic, and All.
ids={value}	(Required to list, update or delete record and optional to create record) Kubernetes authentication record IDs. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma-separated.
title={value}	(Required to create record) The title of the record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional) User-defined notes about the record. Maximum of 1999 characters (ascii).
Kubernetes	
unix_bin_path= {value}	(Optional) Absolute path of the 'kubectl' command.
unix_conf_path={value}	(Optional) Absolute path of the Kubernetes configuration file.
Target Hosts	
ips={value}	(Required to create record) The IP addresses for the Kubernetes targets you want to authenticate to. Multiple entries are comma-separated. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional and valid only to update record) IPs to be added to an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.

Parameter	Description
remove_ips={value}	(Optional and valid to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional, and valid when the Networks feature is enabled) The network ID for the record. By default, the parameter is set to 0.

Sample - Create Kubernetes record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=kubernetes auth
record&unix_bin_path=/usr/bin/kubectl&unix_conf_path=/root/kube/co
nfig&ips=10.10.10.10&comments=kube auth record"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "https://qualysapi.qualys.com
/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-08-30T11:30:58Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>94170</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Kubernetes Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=10001&title=kubernetes auth
record&unix_bin_path=/usr/bin/kubectl&unix_conf_path=/root/kube/co
nfig"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "https://qualysapi.qualys.com
/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-08-30T12:30:58Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>94170</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “kubernetes”

<platform API server>/api/2.0/fo/auth/auth_records.dtd

<platform API server>/api/2.0/fo/auth/kubernetes/auth_kubernetes_list_output.dtd

MariaDB Record

/api/2.0/fo/auth/mariadb/

[POST]

Create, update, list and delete MariaDB authentication records. Compliance scans are supported (using PC).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
ssl_verify={**0**|1}	(Optional to create or update record, and valid for server that supports SSL) Specify 1 for a complete SSL certificate validation. - If unspecified (or ssl_verify=0), Qualys scanners authenticate with MySQL Servers that don't use SSL or MariaDB servers that use SSL. However, in the SSL case, the server SSL certificate verification will be skipped. - If ssl_verify=1, the Qualys scanners will only send a login request after verifying that a connection the MariaDB server uses SSL, the server SSL certificate is valid and matches the scanned host.
hosts={value}	(Optional to create or update record) A list of FQDNs for the hosts that correspond to all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
database={value}	(Required to create record, optional to update record) The database name to authenticate to. Specify a valid MariaDB database name.
port={value}	(Required to create record, optional to update record) The port the database name is running on. The default is 3306.

Parameter	Description
windows_config_file={value}	(Optional to create or update record) The path to the Windows mariadb config file. Access to this config file is required to run certain checks on Windows hosts.
	Note: You must include one or both of these parameters in a create request: windows_config_file and unix_config_file.
unix_config_file={value}	(Optional to create or update record) The path to the Unix mariadb config file. Access to this config file is required to run certain checks on Unix hosts.
	Note: You must include one or both of these parameters in a create request: windows_config_file and unix_config_file.
client_cert={value}	(Optional to create or update record) PEM-encoded X.509 certificate. Specify if certificate authentication is required by your server to establish an SSL connection.
client_key={value}	(Optional to create or update record) PEM-encoded RSA private key. Specify if certificate authentication is required by your server to establish an SSL connection.
Login credentials	
login_type={**basic**|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The username to be used for authentication to MariaDB server.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to MariaDB server.
Vault	
vault_type={value}	(Required to create record when login_type=vault) The vault type to be used for authentication. See Vault Support matrix.
vault_id={value}	(Required to create record when login_type=vault and you want to retrieve private key from vault) The vault ID where you want to retrieve the private key from. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.

Parameter	Description
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - Create MariaDB record (with basic login)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=MariaDB_Auth1&username=root&password=<PASSWOR
D>&ips=10.10.31.86&echo_request=0&unix_config_file=/etc/my.cnf&por
t=22&database=mariadb"
"<qualys_base_url>/api/2.0/fo/auth/mariadb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-07-17T21:56:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>284866</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List MariaDB records

Use the new MariaDB Authentication Record List API (/api/2.0/fo/auth/mariadb/?action=list) to list MariaDB records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mariadb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MARIADB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mariadb/auth_mariadb
_list_output.dtd">
<AUTH_MARIADB_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-07-17T21:57:32Z</DATETIME>
    <AUTH_MARIADB_LIST>
      <AUTH_MARIADB>
        <ID>284866</ID>
        <TITLE><![CDATA[MariaDB_Auth1]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <DATABASE><![CDATA[mariadb]]></DATABASE>
        <PORT>22</PORT>
        <IP_SET>
          <IP>10.10.31.86</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <SSL_VERIFY>false</SSL_VERIFY>
        <WINDOWS_CONF_FILE><![CDATA[]]></WINDOWS_CONF_FILE>
        <UNIX_CONF_FILE><![CDATA[/etc/my.cnf]]></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-07-17T21:56:47Z</DATETIME>
          <BY>seenu_yn</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-07-17T21:56:47Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MARIADB>
    </AUTH_MARIADB_LIST>
  </RESPONSE>
</AUTH_MARIADB_LIST_OUTPUT>
```

DTDs for auth type “mariadb”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/mariadb/auth_mariadb_list_output.dtd

MarkLogic Record

/api/2.0/fo/auth/marklogic

[POST]

Create, update, list, and delete MarkLogic records for authenticated scans of MarkLogic instances. Compliance scans are supported (using PC).

Input Parameters

Parameter	Description
action={action}	Specify any one of the following: create, update, list, delete.
title={value}	(Required to create and update a record) A title for the record.
ips={value}	(Required) IPs to be added to your MarkLogic record.You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.
ids={value}	(Required) MarkLogic Record IDs to edit and delete. Specify record IDs and/or ID ranges. Multiple entries are comma separated.
username={value}	((Required) The username to be used for authentication to MarkLogic.
password={value}	(Required) The password to be used for authentication to MarkLogic.
port={value}	(Required)The port number that the MarkLogic database instance is running on. It is the target configuration port.
ssl_verify_with_host={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
hosts={value}	(Required if ssl_verify_with_host=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
require_cert={0|1}	(Optional) Set this to 1 when you want to authenticate the MarkLogic instance via certificate and private_key. Enabling this from API switch on the Require Certificate toggle on UI.
certificate={value}	(Optional) Certificate content if require_cert is set to 1.
private_key={value}	(Optional) private_key details if require_cert is set to 1.
unix_installation_path={value}	(Optional) Unix installation path to MarkLogic.
unix_conf_path={value}	(Optional) Unix configuration path to MarkLogic.
window_installation_path={value}	(Optional) Windows installation path to MarkLogic
window_conf_path={value}	(Optional) Windows configuration path to MarkLogic
admin_port={value}	(Optional) Administrator configuration path to MarkLogic

Parameter	Description
admin_ssl_verify_with_host ={value}	(Required if ssl_verify_with_host=1)(Optional) SSL verification is for admin server. Set to 1 if you want to verify the server's certificate is valid and trusted.
admin_hosts={value}	(Required if admin_ssl_verify_with_host=1)A list of FQDNs for all admin server host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.

Sample- Create MarkLogic Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password" -d
"action=create&title=marklogic_api1&username=test&password=abc&port=78&ip
s=1.1.1.1&ssl_verify_with_host=1&hosts=abc.com&require_cert=1&certificate
=-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjETMBEGA1UEC
AwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERpbWkxDTALBgNVBAsMBE
5TQlUxEDAOBgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0BCQEWDGRpbWlAZGltaS5mcjAeFw0
xNDAxMjgyMDM2NTVaFw0yNDAxMjYyMDM2NTVaMFsxCzAJBgNVBAYTAkZSMRMwEQYDVQQIDApT
b21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFDASBgNVBAMMC
3d3dy5kaW1pLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98
KW68lz8pGaRRcYersNGqPjpifMVjjE8LuCoXgPU0HePnNTUjpShBnynKCvrtWhN+haKbSp+QW
XSxiTrW99HBfAl1MDQyWcukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p1NCvw+6B
/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNuUVD0V09dc5CDYBaKjqetwwv6DFk/GRd
OSEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6DauZkChSRyc/Whvurx6o85D6qpzyw
o8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAG
G+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+tugFtyN
+cXe1wxUqeA7X+yS3bgwHwYDVR0jBBgwFoAUhMwqkbBrGp87HxfvwgPnlGgVR64wDQYJKoZIh
vcNAQEFBQADggEBAIEEmqqhEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplt7YVmevBFNO
c0+1ZyR4tXgi4+5MHGzhYCIVvHo4hKqYm+J+o5mwQInf1qoAHuO7CLD3WNa1sKcVUVvepIxc/
1aHZrG+dPeEHt0MdFfOw13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1fBtuqUsvA8NWSIyz
Q16fyGve+ANf6vXvUizyvwDrPRv/kfvLNa3ZPnLMMxU98MvhPXy3PkB8++6U4Y3vdk2Ni2WYY
lIls8yqbM4327IKmkDc2TimS8u60CT47mKU7aDYcbTV5RDkrlaYwm5yqlTIglvCv7o=-----
END CERTIFICATE-----&private_key=-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvpnaPKLIKdvx98KW68lz8pGaRRcYersNGqPjpifMVjjE8LuCoXgPU0HeP
nNTUjpShBnynKCvrtWhN+haKbSp+QWXSxiTrW99HBfAl1MDQyWcukoEb9Cw6INctVUN4iRvkn
9T8E6q174RbcnwA/7yTc7p1NCvw+6B/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNuU
VD0V09dc5CDYBaKjqetwwv6DFk/GRdOSEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os
6DauZkChSRyc/Whvurx6o85D6qpzywo8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwIDAQABA
oIBAFml8cD9a5pMqlW3f9btTQz1sRL4Fvp7CmHSXhvjsjeHwhHckEe0ObkWTRsgkTsm1XLu5W
8IITnhn0+1iNr+78eB+rRGngdAXh8diOdkEy+8/Cee8tFI3jyutKdRlxMbwiKsouVviumoq3f
xOGQYwQ0Z2l/PvCwy/Y82ffq3ysC5gAJsbBYsCrg14bQo44ulrELe4SDWs5HCjKYbEI2b8cOM
ucqZSOtxg9niLN/je2bo/I2HGSawibgcOdBms8k6TvsSrZMr3kJ5O6J+77LGwKH37brVgbVYv
bq6nWPL0xLG7dUv+7LWEo5qQaPy6aXb/zbckqLqu6/EjOVeydG5JQECgYEA9kKfTZD/WEVAre
A0dzfeJRu8vlnwoagL7cJaoDxqXos4mcr5mPDTkbWgFkLFFH/AyUnPBlK6BcJp1XK67B13ETU
a3i9Q5t1WuZEobiKKBLFm9DDQJt43uKZWJxBKFGSvFrYPtGZst719mZVcPct2CzPjEgN3Hlpt
6fyw3eOrnoECgYEAxiOujwXCOmuGaB7+OW2tR0PGEzbvVlEGdkAJ6TC/HoKM1A8r2u4hLTEJJ
CrLLTfw++4IddHE2dLeR4Q7O58SfLphwgPmLDezN7WRLGr7Vyfuv7VmaHjGuC3Gv9agnhWDlA
2QgBG9/R9oVfL0Dc7CgJgLeUtItCYC31bGT3yhV0MCgYEA4k3DG4L+RN4PXDpHvK9IpA1jXAJ
HEifeHnaW1d3vWkbSkvJmgVf+9U5VeV+OwRHN1qzPZV4suRI6M/8lK8rAGr4UnM4aqK4K/qkY
4G05LKrik9Ev2CgqSLQDRA7CJQ+Jn3Nb50qg6hFnFPafN+J77juWln08wFYV4Atpdd+9XQECg
```

```
YBxizkZFL+9IqkfOcONvWAzGo+Dq1N0L3J4iTIkw56CKWXyj88d4qB4eUU3yJ4uB4S9miaW/e
LEwKZIbWpUPFAn0db7i6h3ZmP5ZL8QqS3nQCb9DULmU2/tU641eRUKAmIoka1g9sndKAZuWo+
o6fdkIb1RgObk9XNn8R4rpsv+aQKBgB+CIcExR30vycv5bnZN9EFlIXNKaeMJUrYCXcRQNvrn
UIUBvAO8+jAeCdLygS5RtgOLZib0IVErqWsP3EI1ACGuLts0vQ9GFLQGaN1SaMS40C9kvns1m
lDuLhIhYpJ8UsCVt5snWo2N+M+6ANh5tpWdQnEK6zILh4tRbuzaiHgb-----END RSA
PRIVATE KEY-----&"
"https://qualysapi.qualys.com/api/2.0/fo/auth/marklogic/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE BATCH_RETURN SYSTEM "
https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
   <RESPONSE>
      <DATETIME>2024-06-04T05:20:20Z</DATETIME>
      <BATCH_LIST>
         <BATCH>
            <TEXT>Successfully Created</TEXT>
            <ID_SET>
               <ID>4706058</ID>
            </ID_SET>
         </BATCH>
      </BATCH_LIST>
   </RESPONSE>
</BATCH_RETURN>
```

Sample- Update MarkLogic Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password" -d
"action=update&ids=4706058&port=99"
"https://<qualys_base_url>/api/2.0/fo/auth/marklogic/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
   <RESPONSE>
      <DATETIME>2024-06-04T09:13:18Z</DATETIME>
      <BATCH_LIST>
         <BATCH>
            <TEXT>Successfully Updated</TEXT>
            <ID_SET>
               <ID>4706058</ID>
            </ID_SET>
         </BATCH>
      </BATCH_LIST>
   </RESPONSE>
</BATCH_RETURN>
```

Sample- Delete MarkLogic Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password" -d
"action=delete&ids=4706058"
"https://qualysapi.qualys.com/api/2.0/fo/auth/marklogic/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
   <RESPONSE>
      <DATETIME>2024-06-04T09:13:55Z</DATETIME>
      <BATCH_LIST>
         <BATCH>
            <TEXT>Successfully Deleted</TEXT>
            <ID_SET>
               <ID>4706058</ID>
            </ID_SET>
         </BATCH>
      </BATCH_LIST>
   </RESPONSE>
</BATCH_RETURN>
```

Sample- List MarkLogic Record

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password" -d
"action=list&ids=5106487"
"https://qualysapi.qualys.com/api/2.0/fo/auth/marklogic/"
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MARKLOGIC_LIST_OUTPUT SYSTEM
https://qualysapi.qualys.com/api/2.0/fo/auth/marklogic/auth_marklogic_lis
t_output.dtd>
<AUTH_MARKLOGIC_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-07-02T08:06:10Z</DATETIME>
        <AUTH_MARKLOGIC_LIST>
            <AUTH_MARKLOGIC>
                <ID>5106487</ID>
                <TITLE>
                    <![CDATA[marklogic ]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[test]]>
                </USERNAME>
                <IP_SET>
                    <IP>1.1.1.1</IP>
```

```
                </IP_SET>
                <REQUIRE_CERT>
                    <![CDATA[1]]>
                </REQUIRE_CERT>
                <PORT>
                    <![CDATA[8001]]>
                </PORT>
                <SSL_VERIFY_WITH_HOST>
                    <![CDATA[1]]>
                </SSL_VERIFY_WITH_HOST>
                <HOSTS>
                    <![CDATA[abc.com]]>
                </HOSTS>
                <CERTIFICATE>
                    <![CDATA[-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjETMBEGA1UEC
AwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERpbWkxDTALBgNVBAsMBE
5TQlUxEDAOBgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0BCQEWDGRpbWlAZGltaS5mcjAeFw0
xNDAxMjgyMDM2NTVaFw0yNDAxMjYyMDM2NTVaMFsxCzAJBgNVBAYTAkZSMRMwEQYDVQQIDApT
b21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFDASBgNVBAMMC
3d3dy5kaW1pLmZyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98
KW68lz8pGaRRcYersNGqPjpifMVjjE8LuCoXgPU0HePnNTUjpShBnynKCvrtWhN+haKbSp+QW
XSxiTrW99HBfAl1MDQyWcukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p1NCvw+6B
/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNuUVD0V09dc5CDYBaKjqetwwv6DFk/GRd
OSEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6DauZkChSRyc/Whvurx6o85D6qpzyw
o8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwIDAQABo3sweTAJBgNVHRMEAjAAMCwGCWCGSAG
G+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+tugFtyN
+cXe1wxUqeA7X+yS3bgwHwYDVR0jBBgwFoAUhMwqkbBrGp87HxfvwgPnlGgVR64wDQYJKoZIh
vcNAQEFBQADggEBAIEEmqqhEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplt7YVmevBFNO
c0+1ZyR4tXgi4+5MHGzhYCIVvHo4hKqYm+J+o5mwQInf1qoAHuO7CLD3WNa1sKcVUVvepIxc/
1aHZrG+dPeEHt0MdFfOw13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1fBtuqUsvA8NWSIyz
Q16fyGve+ANf6vXvUizyvwDrPRv/kfvLNa3ZPnLMMxU98MvhPXy3PkB8++6U4Y3vdk2Ni2WYY
lIls8yqbM4327IKmkDc2TimS8u60CT47mKU7aDYcbTV5RDkrlaYwm5yqlTIglvCv7o=-----
END CERTIFICATE-----]]>
                </CERTIFICATE>
                <PRIVATE_KEY>
                    <![CDATA[-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvpnaPKLIKdvx98KW68lz8pGaRRcYersNGqPjpifMVjjE8LuCoXgPU0HeP
nNTUjpShBnynKCvrtWhN+haKbSp+QWXSxiTrW99HBfAl1MDQyWcukoEb9Cw6INctVUN4iRvkn
9T8E6q174RbcnwA/7yTc7p1NCvw+6B/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNuU
VD0V09dc5CDYBaKjqetwwv6DFk/GRdOSEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os
6DauZkChSRyc/Whvurx6o85D6qpzywo8xwNaLZHxTQPgcIA5su9ZIytv9LH2E+lSwwIDAQABA
oIBAFml8cD9a5pMqlW3f9btTQz1sRL4Fvp7CmHSXhvjsjeHwhHckEe0ObkWTRsgkTsm1XLu5W
8IITnhn0+1iNr+78eB+rRGngdAXh8diOdkEy+8/Cee8tFI3jyutKdRlxMbwiKsouVviumoq3f
xOGQYwQ0Z2l/PvCwy/Y82ffq3ysC5gAJsbBYsCrg14bQo44ulrELe4SDWs5HCjKYbEI2b8cOM
ucqZSOtxg9niLN/je2bo/I2HGSawibgcOdBms8k6TvsSrZMr3kJ5O6J+77LGwKH37brVgbVYv
bq6nWPL0xLG7dUv+7LWEo5qQaPy6aXb/zbckqLqu6/EjOVeydG5JQECgYEA9kKfTZD/WEVAre
A0dzfeJRu8vlnwoagL7cJaoDxqXos4mcr5mPDTkbWgFkLFFH/AyUnPBlK6BcJp1XK67B13ETU
a3i9Q5t1WuZEobiKKBLFm9DDQJt43uKZWJxBKFGSvFrYPtGZst719mZVcPct2CzPjEgN3Hlpt
6fyw3eOrnoECgYEAxiOujwXCOmuGaB7+OW2tR0PGEzbvVlEGdkAJ6TC/HoKM1A8r2u4hLTEJJ
CrLLTfw++4IddHE2dLeR4Q7O58SfLphwgPmLDezN7WRLGr7Vyfuv7VmaHjGuC3Gv9agnhWDlA
2QgBG9/R9oVfL0Dc7CgJgLeUtItCYC31bGT3yhV0MCgYEA4k3DG4L+RN4PXDpHvK9IpA1jXAJ
HEifeHnaW1d3vWkbSkvJmgVf+9U5VeV+OwRHN1qzPZV4suRI6M/8lK8rAGr4UnM4aqK4K/qkY
4G05LKrik9Ev2CgqSLQDRA7CJQ+Jn3Nb50qg6hFnFPafN+J77juWln08wFYV4Atpdd+9XQECg
```

```
YBxizkZFL+9IqkfOcONvWAzGo+Dq1N0L3J4iTIkw56CKWXyj88d4qB4eUU3yJ4uB4S9miaW/e
LEwKZIbWpUPFAn0db7i6h3ZmP5ZL8QqS3nQCb9DULmU2/tU641eRUKAmIoka1g9sndKAZuWo+
o6fdkIb1RgObk9XNn8R4rpsv+aQKBgB+CIcExR30vycv5bnZN9EFlIXNKaeMJUrYCXcRQNvrn
UIUBvAO8+jAeCdLygS5RtgOLZib0IVErqWsP3EI1ACGuLts0vQ9GFLQGaN1SaMS40C9kvns1m
lDuLhIhYpJ8UsCVt5snWo2N+M+6ANh5tpWdQnEK6zILh4tRbuzaiHgb-----END RSA
PRIVATE KEY-----]]>
                </PRIVATE_KEY>
                <UNIX_INSTALLATION_PATH>
                    <![CDATA[/opt/MarkLogic]]>
                </UNIX_INSTALLATION_PATH>
                <UNIX_CONF_PATH>
                    <![CDATA[/opt/MarkLogic]]>
                </UNIX_CONF_PATH>
                <WINDOW_INSTALLATION_PATH>
                    <![CDATA[C:\Program Files\MarkLogic]]>
                </WINDOW_INSTALLATION_PATH>
                <WINDOW_CONF_PATH>
                    <![CDATA[C:\Program Files\MarkLogic\Data]]>
                </WINDOW_CONF_PATH>
                <ADMIN_PORT>
                    <![CDATA[8002]]>
                </ADMIN_PORT>
                <ADMIN_SSL_VERIFY_WITH_HOST>
                    <![CDATA[1]]>
                </ADMIN_SSL_VERIFY_WITH_HOST>
                <ADMIN_HOSTS>
                    <![CDATA[host.domain1, host.domain2]]>
                </ADMIN_HOSTS>
                <LOGIN_TYPE>
                    <![CDATA[basic]]>
                </LOGIN_TYPE>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2024-07-02T08:01:23Z</DATETIME>
                    <BY>quay_sm</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2024-07-02T08:01:23Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_MARKLOGIC>
        </AUTH_MARKLOGIC_LIST>
    </RESPONSE>
</AUTH_MARKLOGIC_LIST_OUTPUT>
```

DTDs for MarkLogic records

<platform API server>/api/2.0/fo/auth/auth_marklogic_list_output.dtd

Microsoft SharePoint Record

/api/2.0/fo/auth/microsoft_sharepoint/

[POST]

List, create, update, and delete Microsoft SharePoint records for authenticated scans of Microsoft SharePoint instances running on Windows and Database. Microsoft SharePoint version 2010, 2013,2016, and 2019 are supported.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Microsoft SharePoint	
db_local={0|1}	(Optional to create or update record) Set to 1 when login credentials are for a MS SQL Server database account. Set to 0 when login credentials are for a Microsoft Windows operating system account that is associated with a MS SQL Server database account. When db_local is not specified during a create request, the flag is set to 1.
windows_domain={value}	(Required when db_local=0, otherwise invalid) The domain name where the login credentials are stored when the login credentials are for a Microsoft Windows operating system account that is associated with a MS SQL Server database account. The domain name may include 1-256 characters (ascii). For an update request when the credentials for the record are for a Microsoft Windows account (db_local=0) and you want to change the record to use credentials for a MS SQL Server account (db_local=1), then you must set windows_domain='' (the empty string) to clear the current parameter setting.
kerberos={0|1}	(Optional to create or update record) When not specified, Kerberos is enabled allowing the scanning engine to try Kerberos when negotiating authentication to target hosts. Specify kerberos=0 if you do not want Kerberos attempted.

Parameter	Description
ntlmv2={0|1}	(Optional to create or update record) When not specified, NTLMv2 is enabled allowing the scanning engine to try NTLMv2 when negotiating authentication to target hosts. Specify ntlmv2=0 if you do not want NTLMv2 attempted.
ntlmv1={0|1}	(Optional to create or update record) When not specified, NTLMv1 will not be attempted. Specify ntlmv1=1 to try NTMLv1 when negotiating authentication to target hosts.
Login credentials	
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a MS SQL Server database user account used for SharePoint. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(For create request, password or login_type=vault is required) The password of the MS SQL Server database user account to be used for authentication. Maximum 100 characters (ascii).
login_type={value}	(For create request, password or login_type=vault is required) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix.
secret_name={value}	(Required if vault type is Thycotic Secret Server) Specify the secret name that contains the password to be used for authentication. The scanning engine will perform a search for the secret name and then get the password from the secret returned by the search. A single exact match of the secret name must be found in order for authentication to be successful. The secret name may contain a maximum of 256 characters, and must not contain multibyte characters.
system_name={value}	(Optional if vault type is BeyondTrust PBPS or Quest Vault) The managed system name (also known as asset name). When not specified, we'll attempt to auto-discover the system name at scan time.
account_name={value}	(Optional if vault type is BeyondTrust PBPS) The account name. When not specified, we'll try the username specified in the authentication record.

Parameter	Description
folder={value}	(Required if vault type is CyberArk AIM and Cyber-ARK PIM Suite) Specify the name of the folder in the secure digital safe where the password to be used for authentication should be stored. The folder name can contain a maximum of 169 characters. Entering a trailing /, as in folder/, is optional (when specified, the service removes the trailing / and does not save it in the folder name). The maximum length of a folder name with a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a folder name: / : * ? " < > | <tab>
file={value}	(Required if vault type is CyberArk AIM and Cyber-ARK PIM Suite) Specify the name of the file in the secure digital safe where the password to be used for authentication should be stored. The file name can contain a maximum of 165 characters. The maximum length of a folder name plus a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a file name: \ / : * ? " < > | <tab>
Target Hosts	
ips={value}	(Required to create record) The IP address(es) for the Microsoft SharePoint targets you want to authenticate to. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid only when the networks feature is enabled) The network ID for the record.

Sample: List all Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list" "<qualys_base_url>/api/2.0/fo/auth/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/auth_records.dtd">
<AUTH_RECORDS_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-02-14T06:40:29Z</DATETIME>
        <AUTH_RECORDS>
            <AUTH_UNIX_IDS>
                <ID_SET>
                    <ID>63215</ID>
                    <ID>63239</ID>
                    <ID>65170</ID>
                    <ID>65172</ID>
                    <ID>66185</ID>
                </ID_SET>
            </AUTH_UNIX_IDS>
            <AUTH_VMWARE_IDS>
                <ID_SET>
                    <ID>63213</ID>
                    <ID>63235</ID>
                    <ID>63237</ID>
                    <ID>63241</ID>
                </ID_SET>
            </AUTH_VMWARE_IDS>
            <AUTH_POSTGRESQL_IDS>
                <ID_SET>
                    <ID>66387</ID>
                    <ID>66389</ID>
                    <ID>69602</ID>
                    <ID>72224</ID>
                </ID_SET>
            </AUTH_POSTGRESQL_IDS>
            <AUTH_ORACLE_HTTP_SERVER_IDS>
                <ID_SET>
                    <ID>66388</ID>
                </ID_SET>
            </AUTH_ORACLE_HTTP_SERVER_IDS>
            <AUTH_MICROSOFT_SHAREPOINT_IDS>
                <ID_SET>
```

```
                    <ID>72222</ID>
                </ID_SET>
            </AUTH_MICROSOFT_SHAREPOINT_IDS>
        </AUTH_RECORDS>
    </RESPONSE>
</AUTH_RECORDS_OUTPUT>
```

Sample - List Microsoft SharePoint Records with Basic Details

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=list&details=Basic"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/auth_microsoft_sharepoint_list_output.dtd">
    <AUTH_MICROSOFT_SHAREPOINT_LIST>
      <AUTH_MICROSOFT_SHAREPOINT>
        <ID>2372474</ID>
        <TITLE><![CDATA[SharePoint_WindowsAuth]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <IP_SET>
          <IP>10.10.10.13</IP>
        </IP_SET>
        <MSSQL>
          <DB_LOCAL><![CDATA[0]]></DB_LOCAL>

<WINDOWS_DOMAIN><![CDATA[sample.qualys.com]]></WINDOWS_DOMAIN>
          <KERBEROS><![CDATA[1]]></KERBEROS>
          <NTLMV2><![CDATA[1]]></NTLMV2>
        </MSSQL>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2020-03-10T18:47:26Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-03-10T18:47:26Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MICROSOFT_SHAREPOINT>
      <AUTH_MICROSOFT_SHAREPOINT>
        <ID>2372483</ID>
```

```
      <TITLE><![CDATA[SharePoint_DatabaseAuth]]></TITLE>
      <USERNAME><![CDATA[username]]></USERNAME>
      <IP_SET>
        <IP_RANGE>10.10.10.19-10.10.10.20</IP_RANGE>
      </IP_SET>
      <MSSQL>
        <DB_LOCAL><![CDATA[1]]></DB_LOCAL>
        <KERBEROS><![CDATA[1]]></KERBEROS>
        <NTLMV2><![CDATA[1]]></NTLMV2>
        <NTLMV1><![CDATA[1]]></NTLMV1>
      </MSSQL>
      <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
      <CREATED>
        <DATETIME>2020-03-10T20:53:37Z</DATETIME>
        <BY>joe_user</BY>
      </CREATED>
      <LAST_MODIFIED>
        <DATETIME>2020-03-10T20:53:37Z</DATETIME>
      </LAST_MODIFIED>
    </AUTH_MICROSOFT_SHAREPOINT>
```

Sample - List Microsoft SharePoint Records with All Details

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/auth_microsoft_sharepoint_list_output.dtd">
<AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-03-11T22:56:20Z</DATETIME>
    <AUTH_MICROSOFT_SHAREPOINT_LIST>
      <AUTH_MICROSOFT_SHAREPOINT>
        <ID>2372474</ID>
        <TITLE><![CDATA[SharePoint_WindowsAuth]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <IP_SET>
          <IP>10.10.10.13</IP>
        </IP_SET>
        <MSSQL>
```

```
          <DB_LOCAL><![CDATA[0]]></DB_LOCAL>

<WINDOWS_DOMAIN><![CDATA[sample.qualys.com]]></WINDOWS_DOMAIN>
          <KERBEROS><![CDATA[1]]></KERBEROS>
          <NTLMV2><![CDATA[1]]></NTLMV2>
        </MSSQL>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2020-03-10T18:47:26Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-03-10T18:47:26Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MICROSOFT_SHAREPOINT>
      <AUTH_MICROSOFT_SHAREPOINT>
        <ID>2372483</ID>
        <TITLE><![CDATA[SharePoint_DatabaseAuth]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <IP_SET>
          <IP_RANGE>10.10.10.19-10.10.10.20</IP_RANGE>
        </IP_SET>
        <MSSQL>
          <DB_LOCAL><![CDATA[1]]></DB_LOCAL>
          <KERBEROS><![CDATA[1]]></KERBEROS>
          <NTLMV2><![CDATA[1]]></NTLMV2>
          <NTLMV1><![CDATA[1]]></NTLMV1>
        </MSSQL>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2020-03-10T20:53:37Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-03-10T20:53:37Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MICROSOFT_SHAREPOINT>
      <AUTH_MICROSOFT_SHAREPOINT>
        <ID>2372484</ID>
        <TITLE><![CDATA[SharePoint123]]></TITLE>
        <USERNAME><![CDATA[userupdate]]></USERNAME>
        <IP_SET>
          <IP_RANGE>10.10.10.25-10.10.10.26</IP_RANGE>
        </IP_SET>
        <MSSQL>
          <DB_LOCAL><![CDATA[0]]></DB_LOCAL>
```

```
<WINDOWS_DOMAIN><![CDATA[sample2.qualys.com]]></WINDOWS_DOMAIN>
          <KERBEROS><![CDATA[1]]></KERBEROS>
          <NTLMV1><![CDATA[1]]></NTLMV1>
        </MSSQL>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2020-03-10T20:55:50Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-03-11T16:19:19Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MICROSOFT_SHAREPOINT>
    </AUTH_MICROSOFT_SHAREPOINT_LIST>
    <GLOSSARY>
      <USER_LIST>
        <USER>
          <USER_LOGIN>joe_user</USER_LOGIN>
          <FIRST_NAME>Joe</FIRST_NAME>
          <LAST_NAME>User</LAST_NAME>
        </USER>
      </USER_LIST>
    </GLOSSARY>
  </RESPONSE>
</AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT>
```

Sample - Create Microsoft SharePoint Record

API request with Microsoft Windows login (db_local=0):

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=create&title=SharePoint&ips=10.10.10.13&username=username&
password=<PASSWORD>&db_local=0&windows_domain=sample.qualys.com"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

API request with MS SQL Server database login (db_local=1):

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=create&title=SharePoint_withDatabase&ips=10.10.10.14&usern
ame=username&password=<PASSWORD>&db_local=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-02-13T07:31:33Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>72223</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Microsoft SharePoint Record

API request to update basic information:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=update&ids=10002&title=SharePoint2&username=newuser&passwo
rd=<newpassword>&comments=auth-updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

API request to update vault login and change to different vault:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=update&ids=10003&login_type=vault&vault_type=Thycotic+Secr
et+Server&vault_id=123&secret_name=secret-name"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-02-13T07:39:09Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>72223</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
```

```
</BATCH_RETURN>
```

Sample - Delete Microsoft SharePoint Records

API request for deleting single record:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=delete&ids=10000"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

API request for deleting multiple records:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: Curl' -d
"action=list&ids=10000,10001"
"https://qualysapi.qualys.com/api/2.0/fo/auth/microsoft_sharepoint
/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-02-13T07:40:06Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>72223</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “microsoft_sharepoint”

<platform API server>/api/2.0/auth_records.dtd

<platform API server>/api/2.0/fo/auth/microsoft_sharepoint/auth_microsoft_sharepoint_list_output.dtd

MongoDB Record

/api/2.0/fo/auth/mongodb/

[POST]

Create, update, list and delete MongoDB records for authenticated scans of MongoDB instances running on Unix. Vulnerability and compliance scans are supported (using VM, PC).

- Technologies supported: MongoDB 3.x

- For OS-level checks, make sure the IP addresses you define in your MongoDB records are also defined in Unix records.

- We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to MongoDB instances.

Requirement - You must configure authentication credentials on target hosts.

How it works - During scanning we'll authenticate to one or more instances on a single host using all MongoDB records in your account. For compliance scans, you can scan multiple MongoDB instances on a single host and port combination.

System created authentication records supported - You can allow the system to create MongoDB authentication records for auto discovered instances and scan them. This is supported for Unix installations only. To enable this feature, you must first create MongoDB System Record Templates using the is_template input parameter and specifying login credentials. See System created MongoDB records

Download Qualys User Guide - MongoDB Authentication (.pdf)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional) User defined comments. Maximum of 1999 characters.
is_template={**0**|1}	(Optional for create request, not valid for update request) By default, a new record is a regular MongoDB record. Specify 1 to create a MongoDB system record template.You must also specify login credentials, which are described below. See System created MongoDB records.

Parameter	Description
status={0|**1**}	(Optional) The record status, active or inactive. By default, a new record is set to active (1). Set to 0 for inactive record or 1 for active record. (This parameter applies to system created and user created MongoDB records. It cannot be specified for MongoDB system record templates.)
save_as_user_auth={**0**|1}	(Optional for update request, not valid for create request) Specify 1 to update a system created record and save it as a user created record. If another MongoDB record already exists with the same IP address and target configuration then an error will be returned. (This parameter applies only to system created MongoDB records. It cannot be specified for user created MongoDB records and it cannot be specified for MongoDB system record templates.)
ids={id1,id2,...}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
Target Hosts	
ips={value}	(Required to create record, optional to update record) Add IP addresses of the hosts you want to scan using this record. Overwrites (replaces) the IP address(es) in the IP list for an existing authentication record. The IPs you specify are added, and any existing IPs are removed. You may enter a combination of IPs and IP ranges.
add_ips={value}	(Optional to update record) Add IP address(es) to the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.
MongoDB	
unix_conf_file={value}	(Required for create request) The full path to the MongoDB configuration file on your Unix assets (IP addresses). The file must be in the same location on all assets for this record. Maximum 255 characters (ascii).
database_name={value}	(Required for create request) The username of the account to be used for authentication to the database. If password is specified this is the username of a MongoDB account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
port={value}	(Required for create request) The port where the database instance is running. Default is 27017.

Parameter	Description
ssl_verify={**0**|1}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
hosts={value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
Login credentials	
credential_type=**local**|external	(Optional) The credential type is local by default which means login credential type is local authentication. You need to set credential type to external for LDAP authentication option.
cleartext=**0**|1	(Optional) You must set credential_type to external to use cleartext parameter. The default value for cleartext is 0. You must set this parameter to 1 for successful MongoDB authentication for LDAP.
login_type={**basic**|vault|pkcert}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication) or pkcert (for certificate based authentication).
username={value}	(Required to create record when login_type=basic or login_type=vault) The username of the MongoDB account to be used for authentication. Maximum 100 characters (ascii).
password={value}	(Required to create record when login_type=basic) The password of the MongoDB account to be used for authentication. Maximum 100 characters (ascii).
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Database Secrets Engine in HashiCorp authentication records. Specify 1 to use Database Secrets Engine in the authentication records.
Vault	
vault_type={value}	(Required to create record when login_type=vault) The vault type to be used for authentication. See Vault Support matrix
vault_id={value}	(Required to create record when login_type=vault and you want to retrieve private key from vault) The vault ID where you want to retrieve the private key from. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition
private_key_vault_id={value}	(Required to create record when login_type=vault and you want to retrieve passphrase from vault) The vault ID where you want to retrieve the passphrase from. Certain vaults support this capability. See Vault Support matrix

Parameter	Description
passphrase_vault_id={value}	(For create request, required when login_type=vault and you want to retrieve passphrase from vault) The vault ID where you want to retrieve the passphrase from. Certain vaults support this capability. See Vault Support matrix
private_key={value}	(For create request, required when login_type=pkcert) The private key to be used for authentication. Certain vaults support this capability. See Vault Support matrix
passphrase={value}	(For create request, required when login_type=pkcert and passphrase_vault_id is not specified) The private key passphrase value of an encrypted private key. Maximum 255 characters (ascii). Certain vaults support this capability. See Vault Support matrix
certificate={value}	(For create request, optional when login_type=pkcert) The passphrase X.509 certificate content.
require_cert={**0**|1}	(Optional) Specify 1 to login with certificates/private keys along with login type Basic | vault. By default value will be 0

System created MongoDB records

When we auto discover MongoDB instances, we'll discover the target configuration for each instance but not the login credentials. We've introduced a new configuration called "MongoDB authentication record template" that you'll use to provide MongoDB login credentials for system created records. You'll create the system record template and then select it in the option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the scan.

Benefits

- We'll auto discover MongoDB instances on each scanned host and create authentication records for those instances. We support auto discovery and system record creation for MongoDB instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running MongoDB.

- When we create MongoDB authentication records for discovered instances, we'll insert the credentials from the MongoDB system record template you selected in the option profile.

- You can easily rotate MongoDB passwords. Simply edit the credentials in the MongoDB system record template and all MongoDB records linked to the template will be updated to use the new credentials with no additional scan or action by you.

- You can edit individual MongoDB system created records and save them as user created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.

How it works

Here's the basic flow for MongoDB instance discovery and auto record creation. Note - We support auto discovery and system record creation for MongoDB instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running MongoDB.

1) Create an MongoDB system record template and enter the login credentials you want to use for system created records.

2) Select the MongoDB system record template in the compliance option profile you want to use for discovery scans.

3) Launch your discovery scan. Your scan results will list the auto discovered instances.

4) List your MongoDB authentication records. For each system created record, you'll see the template associated with the record.

Sample - Create MongoDB record - basic login

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=API-mongodb-basic-login&username=joe_user&pas
sword=<PASSWORD>&ips=10.20.32.239&comments=mongo-basic-login&unix_
conf_path=/etc/mongod3.conf&port=28020&ssl_verify=0&database_name=
admin" "https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-12T22:43:27Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125709</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create MongoDB record, using SSL

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=API-mongo-basic-login-with-ssl-verify1_hosts&use
rname=mongo-
admin&password=<PASSWORD>&ips=10.20.32.239&comments=mongo-
basic-login-ssl_hosts&unix_conf_path=/opt/mongodb/&port=27018&ssl_ver
ify=1&hosts=abc123.s2012r2.lab.acme.com],abc123.s2008r2.lab.acme.com"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-12T22:45:06Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125710</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create MongoDB record, using vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=API-mongo-vault-CA_Access&ips=10.20.32.239&comme
nts=mongo-CA-Access-vault_login&unix_conf_path=/opt/mongodb4.conf/&po
rt=27010&login_type=vault&vault_type=CA Access
Control&vault_id=166657&end_point_name=name&end_point_type=type&end_p
oint_container=container&username=joe_user"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-12T22:46:47Z</DATETIME>
```

```
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125711</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create MongoDB Record for LDAP Authentication

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=Sample1&username=mlqa&password=<PASSWORD>&ips=10.20
.32.107&comments=Creating through API
v2.0&unix_conf_path=/etc/mongod3111.conf&port=28021&ssl_verify=0&database
_name=admin&credential_type=external&cleartext=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-09-08T06:15:39Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>3052106</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create MongoDB record - basic login and require_cert=1

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=mongo_auth_basic_cert&username=joe_user&passw
ord=<PASSWORD>&login_type=basic&ips=10.20.30.40&database_name=admi
n&port=27019&require_cert=1&unix_conf_path=/etc/mongod2.conf&ssl_v
erify=1&hosts=mlcent76mdb34.s2012r2.qualys.com'
--header 'X-Requested-With: qweb' \
```

```
--header 'Authorization: Basic <token>' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'certificate=-----BEGIN CERTIFICATE-----
MIIErDCCApSgAwIBAgIBIDANBgkqhkiG9w0BAQUFADCBljEbMBkGA1UEAwwSU2Nh
bm5lciBRQSBSb290IENBMRMwEQYDVQQIDApDYWxpZm9ybmlhMQswCQYDVQQGEwJV
UzEeMBwGCSqGSIb3DQEJARYPbWxxYUBxdWFseXMuY29tMRswGQYDVQQKDBJRdWFs
eXMgRW5naW5lZXJpbmcxGDAWBgNVBAsMD1NjYW5uZXIgUUEgVGVhbTAeFw0yMTA2
MTQyMTEwMDBaFw0yNDA2MTMyMTEwMDBaMIGMMR4wHAYDVQQDDBVtbGNlbnQ3Nm1k
YjM0X2NsaWVudDExEzARBgNVBAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMR4w
HAYJKoZIhvcNAQkBFg9tbHFhQHF1YWx5cy5jb20xFDASBgNVBAoMC1F1YWx5cyBJ
bmMuMRIwEAYDVQQLDAlNTFFBIFRlYW0wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCxPNX+jExoBJqbftSbOeMYdWgCP8o8YR+aqjS6ZqroX9i8dfFCsVc3
5ePxBDOUr5p/DivhvMWsBZsZp2qpSOAjj2vKQV4M7VNvR7h9mjQRpruLOPrCFFup
WWy+zSCzRskiYWhRGd8V5XWvaJhNytneBLsUX6l+1SAwFC+eD/M2oA4VhipAK612
sKTn7yUjYBTODjox+dumKpFTdoPfjaCO923K2fcMNrLUVYQNbibxygsQK6qFJnVl
XJ1LCSVyTBJLuOWrgBATrvcMh9Wv5U0XFRp1u6t2pqnUqkzRsa5jtGR3GBfR3lUu
1JUyo4Kx1QrDw2I3vkYFA/dVv2dTEUgBAgMBAAGjDTALMAkGA1UdEwQCMAAwDQYJ
KoZIhvcNAQEFBQADggIBAL5MYQ8XinuSInZYQgywYFWlhZJJOSEqD4B4DqDfset4
v/7OjDCDWYH8DeObWcHuJgHh1vADpHIYDjfJCPnAPBKgIquVz9QaLUgtV+u1fJDe
Hpxr6IACaizlV0IId6JmoSR+MR2LPig0mi7Du4r07vqUWBB8za4ZxDVtQNkcPI/k
8/Sgj+kyr8hF4up8kniTMEaD/7eZ7MNmYR1BFygcZ/ieYRfdWVMlOvYDxVT20tCK
V7OzI12wXy/J37xdm8BaIkkoJyKPBwP396c4BlIrC5bDvBGRH89VhNscWryhPz9l
CrNvhegnqC0sxi7b4KOEMH3NtbETRZT8IhLkzHZTF+SqxUNkqjD1jdnM3cq0Ab3d
TdB5Ul7B3IjwgtnNES6pxHaX//ycRvGo9v2rzJO8TCtsd0o21uaLXwJmqJ5qhFPz
iX92jYZqEWm3wSD2XMI8kolr4txNfzH9zwAcEGdtBqUlTJcrdOU8IUn3pqISqZkr
wWpiBeS5eU/YbnkhSz2l6bX1x0qaQWv8h16YusvBMjfb2jBWHkED/osRFA7F5f11
XBNipcTrie1iIDY758iDbFrwWaza/9cg0awluyOa560rkyhZTWxwoZkvUz/rnVE7
2UaXkwPxhWAHx3jzfcQca8GTIEVbzuDkg+jcwCoaRNI3IG3339PQE/eF50yiE1YM
-----END CERTIFICATE-----' \
--data-urlencode 'private_key=-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsTzV/oxMaASam37UmznjGHVoAj/KPGEfmqo0umaq6F/YvHXx
QrFXN+Xj8QQzlK+afw4r4bzFrAWbGadqqUjgI49rykFeDO1Tb0e4fZo0Eaa7izj6
whRbqVlsvs0gs0bJImFoURnfFeV1r2iYTcrZ3gS7FF+pftUgMBQvng/zNqAOFYYq
QCutdrCk5+8lI2AUzg46MfnbpiqRU3aD342gjvdtytn3DDay1FWEDW4m8coLECuq
hSZ1ZVydSwklckwSS7jlq4AQE673DIfVr+VNFxUadburdqap1KpM0bGuY7RkdxgX
0d5VLtSVMqOCsdUKw8NiN75GBQP3Vb9nUxFIAQIDAQABAoIBAQCKiPzTnKJUY9Td
WgOg2Vxyz8Jej7HqBBiJ8iSI1pscS17D4ISWFrwPyzeiOiB/RctDKLaQGdeAoFkd
ckjizT21TfN5AiMbg53Fy4+fTZsJeQP6zKzkarlC480mTnwS5W9t2imJyuke2l5k
nyL9G2O0MIpyYFvB8aDZM84MhHcc6CuRme3+VS9kFaIC7wNoEzUrGZt8CE1QDZh9
zKQsVLT5y7Hk+yiDLZ7BkgecFJ52J4xcYzIQhfrfIQp0UmCcKPslHrX3Xzens1GO
AyCkRIRfaI+NIwygrzVtwPTdKNOz+E4K5bmwwNUCdBjZi4DGPxZvobktD6FI7pjA
pHcWZL2BAoGBAOxAvhc5H/66MexOdBhtNRkueMHVWgeAnHYlcGvTjumRqbhipJIc
oVQHFcnFEXrP762dSo7QA2yg0SrhBD+U0iCkDKnzNQnDsXYftDSMNrhhEIznMUvX
JWn17yrXtROsq4oFpvSdJ33fZQHEy8K6aCOGRbAsWjAjAfb98acQHxe5AoGBAMAN
TisS8ZZShhEfKussVbcJYuIHqyVvA2TV3OetMt8tMiToNVOsRukV6Hnf9DFXOdBh
```

```
ddxFbGFJiaFDduzjjig8m53FCmmOtqnOxL5lxckx2ajxxGKfdKpSOG0OzDbxEKjF
uGX9VviOlpbt2JPuHF7qc850xf54z9QRu7OX+UaJAoGARKxFFScLv9WLsW7UnE0S
RDGX9G/57XhbApS7avxh7E7lEK3LvJUJ6AzvLmlUPWi3+LVh+MVKWYcdheNGgtzV
f5tv+u6xGheCPB3XGfcv6MR+NRb24160h2pvjPqKrh9g9YvTDgOoeRQ4nh0ARag9
oSXkl+MsjBWA+rSyS6eKAjECgYEAiRR2KPSaj8tTekEe50F75OvEMsV6eXulloG3
7X2IhBfEZOeBuLmM264Rg3xA1j8GOyB1ecXrt/0/SWXYKvm5bCrmgFQ2PGXrJ4U4
lRYbeKImVBpNLH/YTAHn2J/pT4X9eBm4psOPIlbUUeJu5hfdFDqQclqTQDGHVj1a
FrRw7tECgYBEuc85ghJunoV7hENuolP19+ppaiyH98q4Mc6vpkoEItuoKjWfH1Yr
98QtS58boBphSCNU4qL51dqnEAzCd0udYINxLawaosI3aaUOEGIUUa7IO7e7qUl8
Y4pb3owl0zwdpnyEgdSpuCW8N1Gnsiiur2fJ1NeAaHCF4cG3Se7bfw==
-----END RSA PRIVATE KEY-----'"
\"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2022-06-23T11:15:21Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>6298437</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List MongoDB records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb
_list_output.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-09-12T22:42:45Z</DATETIME>
```

```
    <AUTH_MONGODB_LIST>
      <AUTH_MONGODB>
        <ID>125693</ID>
        <TITLE><![CDATA[API-mongo-basic-login]]></TITLE>
        <USERNAME><![CDATA[mongo-admin-name]]></USERNAME>
        <DATABASE><![CDATA[db-admin-name]]></DATABASE>
        <PORT>28020</PORT>
<UNIX_CONFIGURATION_FILE><![CDATA[/opt/mongodb/updated]]></UNIX_CO
NFIGURATION_FILE>
        <IP_SET>
          <IP>10.20.32.239</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2017-09-12T20:22:09Z</DATETIME>
...
```

DTDs for auth type “mongodb”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/mongodb/auth_mongodb_list_output.dtd

MS Exchange Server

/api/2.0/fo/auth/ms_exchange/

[POST]

Create, update, list and delete MS Exchange Server authentication records. Compliance scans are supported (using PC).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - Create MS Exchange Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
```

```
"action=create&network_id=0&title=fordeltes&comments=editapicommen
t&ips=10.10.10.31"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-03-20T08:26:54Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>49029</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List MS Exchange Server records

Use the new MS Exchange Server Authentication Record List API (/api/2.0/fo/auth/ms_exchange/?action=list) to list MS Exchange Server records.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&details=Basic"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MS_EXCHANGE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/auth_ms_
exchange_list_output.dtd">
<AUTH_MS_EXCHANGE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-03-20T07:26:38Z</DATETIME>
        <AUTH_MS_EXCHANGE_LIST>
            <AUTH_MS_EXCHANGE>
                <ID>48050</ID>
                <TITLE>
                    <![CDATA[msexchange01]]>
```

```
                    </TITLE>
                    <IP_SET>
                        <IP>10.10.10.10</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2019-03-14T07:05:05Z</DATETIME>
                        <BY>quays_sp1</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2019-03-14T07:05:05Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[msexchange]]>
                    </COMMENTS>
                </AUTH_MS_EXCHANGE>
                ...
                <AUTH_MS_EXCHANGE>
                    <ID>49026</ID>
                    <TITLE>
                        <![CDATA[apicreate]]>
                    </TITLE>
                    <IP_SET>
                        <IP>10.10.10.13</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2019-03-19T11:46:23Z</DATETIME>
                        <BY>quays_sp1</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2019-03-19T11:56:57Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[editapicomment]]>
                    </COMMENTS>
                </AUTH_MS_EXCHANGE>
            </AUTH_MS_EXCHANGE_LIST>
        </RESPONSE>
    </AUTH_MS_EXCHANGE_LIST_OUTPUT>
```

DTDs for auth type “ms_exchange”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/ms_exchange/auth_ms_exchange_list_output.dtd

Sample: Update MS Exchange Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&ids=49029&title=forupdate&comments=editwapicomment&
ips=10.10.10.11"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-03-20T08:29:48Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>49029</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample: Delete MS Exchange Server record (single)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=delete&ids=49026"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-03-20T07:56:00Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>49026</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample: Delete MS Exchange Server records (bulk)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=delete&ids=49028,49029"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_exchange/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-03-20T08:31:35Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID_RANGE>49028-49029</ID_RANGE>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

MS SQL Record

/api/2.0/fo/auth/ms_sql/

[POST]

Create, update, list and delete MS SQL Server authentication records. Compliance scans are supported (using PC).

Requirement - You must configure authentication credentials on target hosts.

Download Qualys User Guide - MS SQL Server 2000 Authentication (.pdf)

Download Qualys User Guide - MS SQL Server 2005-2019 Authentication (.pdf)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional) User defined comments. Maximum 1999 characters.
Login credentials	
login_type={basic|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The user account to be used for authentication. May include 1-128 characters.
password={value}	(Required to create record, optional to update record) The password corresponding to the user account defined in the record for authentication. May include 1-128 characters.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix in the API user guide.
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory(AD) Secrets Engine in the authentication records.

Parameter	Description
vault_id={value}	(Required to create record, optional to update record). The vault ID from where you want to retrieve the password. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition
db_local={0|**1**}	(Optional to create or update record) Set to 1 when login credentials are for a MS SQL Server database account (for Windows or Unix). Set to 0 when login credentials are for a Microsoft Windows operating system account that is associated with a MS SQL Server database account. For create record, if the db_local parameter is unspecified, the flag is set to 1.
windows_domain={value}	(Required when db_local=0, otherwise invalid) The domain name where the login credentials are stored when the login credentials are for a Microsoft Windows operating system account that is associated with a MS SQL Server database account. The domain name may include 1-256 characters (ascii). For an update request when the credentials for the record are for a Microsoft Windows account (db_local=0) and you want to change the record to use credentials for a MS SQL Server account (db_local=1) note the following. You must set windows_domain='' (the empty string) to clear the current parameter setting.
auth_os_type={unix|windows}	(Optional when db_local=1) Specify "unix" when the OS type is Unix and "windows" when the OS type is Windows.
mssql_unix_insta_path={value}	(Optional when auth_os_type=unix) Specify the path to the MS SQL Server instance directory on Unix hosts. Sample value: /var/opt/mssql
mssql_unix_conf_path={value}	(Optional when auth_os_type=unix) Specify the path to the MS SQL Server configuration file on Unix hosts. Sample value: /var/opt/mssql/mssq.conf

Parameter	Description
instance={value}	(Optional to create or update record for Windows, Required to create record for Unix and Optional to update record for Unix) The name of the database instance to be scanned. This is the instance name assigned to the TCP/IP port. Important: This is not the host name that is assigned to the MS SQL Server instance name (see "MS SQL Server Instance Name" in the Qualys online help for information). The instance name may include a maximum of 128 characters (ascii). If the instance parameter is not specified for Windows, the instance name is set to "MSSQLSERVER". These parameters are mutually exclusive: instance and auto_discover_instances=1.
auto_discover_instances={**0**|1}	(Optional when auth_os_type=windows) Set auto_discover_instances=1 and we'll find all MS SQL Server instance names on each Windows host. Note that Windows authentication is required in order for us to auto discover instance names. Set up Windows authentication records for the hosts running MS SQL Servers. These parameters are mutually exclusive: instance and auto_discover_instances=1.
database={value}	(Optional to create or update record) The database name of the database to be scanned. The database name may contain a maximum of 128 characters. For a create request, if the database name is unspecified, the database name is set to "master".
auto_discover_databases={**0**|1}	(Optional to create or update record) Set auto_discover_databases=1 and we'll find all MS SQL Server database names on each host. These parameters are mutually exclusive: database and auto_discover_databases=1.
port={value}	(Required to create record, optional to update record) The port number assigned to the database instance to be scanned. To create a record you must specify one of these parameters: port or auto_discover_ports=1. These parameters are mutually exclusive.

Parameter	Description
auto_discover_ports={**0**|1}	Set auto_discover_ports=1 and for each host we'll find all ports MS SQL Server is running on. Note that Unix/Windows authentication is required for us to auto discover ports. Set up Unix/Windows authentication records for your hosts running MS SQL Server. To create a record you must specify one of these parameters: port or auto_discover_ports=1. These parameters are mutually exclusive.
Target Hosts	
ips={value}	You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. (Optional to update record) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed. For create request, it is required to specify either this parameter or member_domain parameter. For update request, this parameter and the add_ips or remove_ips or member_domain parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to add to the IP list for the authentication record. This parameter and the ips or member_domain parameter cannot be specified in the same request.
remove_ips={value}	(Optional for update request only) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips or member_domain parameter cannot be specified in the same request.
network_id={value}	(Optional and only valid when the networks feature is enabled) The network ID for the record.

Parameter	Description
member_domain={value}	(Optional and only valid for Windows) Defines the domain of the MS SQL server for the authentication record. For create request, it is required to specify either this parameter or ips or add_ips parameter. For update request, this parameter and the ips or add_ips or remove_ips parameter cannot be specified in the same request.
Protocols (Windows only)	
kerberos={0|**1**}	(Optional to create or update record) When not specified, Kerberos is enabled allowing the scanning engine to try Kerberos when negotiating authentication to target hosts. Specify kerberos=0 if you do not want Kerberos attempted.
ntlmv2={0|**1**}	(Optional to create or update record) When not specified, NTLMv2 is enabled allowing the scanning engine to try NTLMv2 when negotiating authentication to target hosts. Specify ntlmv2=0 if you do not want NTLMv2 attempted.
ntlmv1={**0**|1}	(Optional to create or update record) When not specified, NTLMv1 will not be attempted. Specify ntlmv1=1 to try NTMLv1 when negotiating authentication to target hosts.

Sample Create MS SQL Record for Unix

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&title=MSSQL_UNIX&username=root&password=<PASSWORD>&db_loc
al=1&ips=10.10.10.10&auto_discover_ports=1&auto_discover_databases=1&auth
_os_type=unix&instance=mssql&mssql_unix_conf_path=/var/opt/mssql/mssql.co
nf&mssql_unix_insta_path=/var/opt/mssql"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
 <RESPONSE>
   <DATETIME>2021-05-17T08:26:31Z</DATETIME>
   <BATCH_LIST>
     <BATCH>
       <TEXT>Successfully Created</TEXT>
       <ID_SET>
         <ID>103473</ID>
       </ID_SET>
     </BATCH>
   </BATCH_LIST>
 </RESPONSE>
</BATCH_RETURN>
```

Sample - List record for Windows using member domain

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&echo_request=1&ids=13907"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MS_SQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/auth_ms_sql_l
ist_output.dtd">
<AUTH_MS_SQL_LIST_OUTPUT>
    <REQUEST>
        <DATETIME>2017-09-20T05:34:37Z</DATETIME>
        <USER_LOGIN>user_john</USER_LOGIN>
        <RESOURCE>
           <qualys_base_url>/api/2.0/fo/auth/ms_sql/
        </RESOURCE>
        <PARAM_LIST>
```

```
            <PARAM>
              <KEY>action</KEY>
              <VALUE>list</VALUE>
            </PARAM>
            <PARAM>
              <KEY>echo_request</KEY>
              <VALUE>1</VALUE>
            </PARAM>
            <PARAM>
              <KEY>ids</KEY>
              <VALUE>13907</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2017-09-20T05:34:37Z</DATETIME>
        <AUTH_MS_SQL_LIST>
          <AUTH_MS_SQL>
            <ID>13907</ID>
            <TITLE><![CDATA[mssqlvt4]]></TITLE>
            <USERNAME><![CDATA[administrator]]></USERNAME>
            <NTLM_V2>1</NTLM_V2>
            <KERBEROS>1</KERBEROS>
            <INSTANCE><![CDATA[MSSQLSERVER]]></INSTANCE>
            <DATABASE><![CDATA[master]]></DATABASE>
            <PORT>8012</PORT>
            <DB_LOCAL>1</DB_LOCAL>

<MEMBER_DOMAIN><![CDATA[sitedomain.com]]></MEMBER_DOMAIN>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
                <DATETIME>2017-09-20T05:26:31Z</DATETIME>
                <BY>user_john</BY>
            </CREATED>
            <LAST_MODIFIED>
                <DATETIME>2017-09-20T05:26:31Z</DATETIME>
            </LAST_MODIFIED>
            <COMMENTS><![CDATA[authcreated]]></COMMENTS>
          </AUTH_MS_SQL>
        </AUTH_MS_SQL_LIST>
      </RESPONSE>
</AUTH_MS_SQL_LIST_OUTPUT>
```

Sample - Create record for Windows using member domain

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=mssqlvt1&username=administrator&password=<PAS
SWORD>&db_local=1&port=8012&member_domain=sitedomain.com&echo_requ
est=1&comments=aut hcreated&instance=MSSQLSERVER&database=master"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <REQUEST>
    <DATETIME>2018-03-20T05:26:31Z</DATETIME>
    <USER_LOGIN>user_john</USER_LOGIN>
    <RESOURCE>
       <qualys_base_url>/api/2.0/fo/auth/ms_sql/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>create</VALUE>
      </PARAM>
      <PARAM>
        <KEY>title</KEY>
        <VALUE>mssqlvt4</VALUE>
      </PARAM>
      <PARAM>
        <KEY>username</KEY>
        <VALUE>administrator</VALUE>
      </PARAM>
      <PARAM>
        <KEY>password</KEY>
        <VALUE>abc123</VALUE>
      </PARAM>
      <PARAM>
        <KEY>db_local</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>port</KEY>
        <VALUE>8012</VALUE>
      </PARAM>
      <PARAM>
        <KEY>member_domain</KEY>
```

```
        <VALUE>sitedomain.com</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>comments</KEY>
        <VALUE>authcreated</VALUE>
      </PARAM>
      <PARAM>
        <KEY>instance</KEY>
        <VALUE>MSSQLSERVER</VALUE>
      </PARAM>
      <PARAM>
        <KEY>database</KEY>
        <VALUE>master</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2018-03-20T05:26:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>13907</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update record for Windows using member domain

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&echo_request=1&ids=13907&member_domain=webdomain.co
m"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
```

```
<BATCH_RETURN>
  <REQUEST>
    <DATETIME>2018-03-20T05:37:13Z</DATETIME>
    <USER_LOGIN>user_john</USER_LOGIN>
    <RESOURCE><qualys_base_url>/api/2.0/fo/auth/ms_sql/
      </RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>update</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ids</KEY>
        <VALUE>13907</VALUE>
      </PARAM>
      <PARAM>
        <KEY>member_domain</KEY>
        <VALUE>webdomain.com</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2018-03-20T05:37:13Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET><ID>13907</ID>
         </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “ms_sql”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/ms_sql/auth_ms_sql_list_output.dtd

MySQL Record

For API version information, refer to API Version History section.

V 2.0| V 3.0

V 2.0

/api/2.0/fo/auth/mysql/

[POST]

Create, update, list and delete MySQL records for authenticated scans of MySQL Server instances. Vulnerability and compliance scans are supported (using VM, PC).

Requirement - You must configure authentication credentials on target hosts.

Download Qualys User Guide - MySQL Authentication (.zip)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
ssl_verify={**0**|1}	((Optional to create or update record, and valid for server that supports SSL) Specify 1 for a complete SSL certificate validation. - If unspecified (or ssl_verify=0), Qualys scanners authenticate with MySQL Servers that don't use SSL or MySQL servers that use SSL. However, in the SSL case, the server SSL certificate verification will be skipped. - If ssl_verify=1, the Qualys scanners will only send a login request after verifying that a connection the MySQL server uses SSL, the server SSL certificate is valid and matches the scanned host.

Parameter	Description
hosts={value}	(Optional to create or update record) A list of FQDNs for the hosts that correspond to all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
database={value}	(Required to create, optional to update record) The database name to authenticate to. Specify a valid MySQL database name.
port={value}	(Required to create, optional to update record) The port the database name is running on.
windows_config_file={value}	(Optional to create or update record) The path to the Windows MySQL config file. Access to this config file is required to run certain checks on Windows hosts.
	Note: You must specify either windows_config_file or unix_config_file depending on the host OS.
unix_config_file={value}	(Optional) Name of the client (Consultant type subscriptions).
	Note: You must specify either windows_config_file or unix_config_file depending on the host OS.
client_cert={value}	(Optional to create or update record) PEM-encoded X.509 certificate. Specify if certificate authentication is required by your server to establish an SSL connection.
client_key={value}	(Optional to create or update record) PEM-encoded RSA private key. Specify if certificate authentication is required by your server to establish an SSL connection.
Login credentials	
login_type={**basic**|vault}	(Optional) The login type is basic by default. Specify login_type=vault to use an authentication vault.
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a MySQL account. If login_type=vault is specified, this is the username of a vault account.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to MySQL server. Maximum 100 characters (ascii).
Vault	
vault_type={value}	(Required only when action=create and login_type=vault) The vault to be used for authentication. See Vault Support matrix.
vault_id={value}	(Required only when action=create and login_type=vault) The ID of the vault you want to use.

Parameter	Description
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips or member_domain parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - List MySQL record

You'll see vault information in the XML output when you list MySQL authentication records with vaults.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=284212"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/auth_mysql_lis
t_output.dtd">
<AUTH_MYSQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-07-17T17:09:18Z</DATETIME>
    <AUTH_MYSQL_LIST>
      <AUTH_MYSQL>
        <ID>284212</ID>
        <TITLE><![CDATA[api-Thycotic Secret Server_tss]]></TITLE>
```

```
        <USERNAME><![CDATA[test_tss]]></USERNAME>
        <DATABASE><![CDATA[mysql]]></DATABASE>
        <PORT>22</PORT>
        <HOSTS>
          <HOST><![CDATA[www.test.com]]></HOST>
        </HOSTS>
        <IP_SET>
          <IP>10.10.10.181</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vault]]></LOGIN_TYPE>
        <DIGITAL_VAULT>
          <DIGITAL_VAULT_ID><![CDATA[166638]]></DIGITAL_VAULT_ID>
          <DIGITAL_VAULT_TYPE><![CDATA[Thycotic Secret
Server]]></DIGITAL_VAULT_TYPE>
          <DIGITAL_VAULT_TITLE><![CDATA[3_Secret
Server]]></DIGITAL_VAULT_TITLE>
         <VAULT_SECRET_NAME><![CDATA[secret]]></VAULT_SECRET_NAME>
        </DIGITAL_VAULT>
        <SSL_VERIFY>true</SSL_VERIFY>
<WINDOWS_CONF_FILE><![CDATA[c:\mysql\myu.ini]]></WINDOWS_CONF_FILE
>
        <UNIX_CONF_FILE><![CDATA[]]></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-07-16T21:53:55Z</DATETIME>
          <BY>seenu_yn</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-07-16T21:55:05Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[test comments]]></COMMENTS>
      </AUTH_MYSQL>
    </AUTH_MYSQL_LIST>
  </RESPONSE>
</AUTH_MYSQL_LIST_OUTPUT>
```

Sample - Create new MySQL record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&title=NewMySQLRecord&username=USERNAME&password=<PA
SSWORD>&ips=10.10.31.84&echo_request=1&windows_config_file=c:\mysq
l\my.ini&port=22&database=mysql"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-07-27T17:02:23Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>291734</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create MySQL record, using vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&ips=10.10.10.189&username=USERNAME&title=api-
Cyberark-
vault_19&ssl_verify=1&login_type=vault&vault_type=CyberArk PIM
Suite&vault_id=166655&folder=folder&file=file&hosts=www.test1.com&
comments=test
comments&port=8080&database=mysqldb&windows_config_file=c:\mysql\m
yu.ini&unix_config_file=/etc/updated/my.ucnf"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-07-27T17:14:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>291735</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update MySQL record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=update&ids=137296922&password=<NEWPASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2018-01-23T17:14:28Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>137296922</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update vault details in MySQL record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=272380&ips=10.10.10.19&username=USERNAME&title=
NewMySQLRecord&ssl_verify=0&login_type=vault&vault_type=CyberArk
PIM
Suite&vault_id=248308&folder=folder&file=file&hosts=www.qualys.com
&comments=test comments updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-07-27T21:53:55Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>284212</ID>
        </ID_SET>
```

```
        </BATCH>
      </BATCH_LIST>
    </RESPONSE>
  </BATCH_RETURN>
```

DTDs for auth type “mysql”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/mysql/auth_mysql_list_output.dtd

V 3.0

/api/3.0/fo/auth/mysql/

[POST]

Create, update and list MySQL records for authenticated scans of MySQL Server instances. Vulnerability and compliance scans are supported (using VM, PC).

Requirement - You must configure authentication credentials on target hosts.

Download Qualys User Guide - MySQL Authentication (.zip)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.

Parameter	Description
ssl_verify={**0**|1}	((Optional to create or update record, and valid for server that supports SSL) Specify 1 for a complete SSL certificate validation. - If unspecified (or ssl_verify=0), Qualys scanners authenticate with MySQL Servers that don't use SSL or MySQL servers that use SSL. However, in the SSL case, the server SSL certificate verification will be skipped. - If ssl_verify=1, the Qualys scanners will only send a login request after verifying that a connection the MySQL server uses SSL, the server SSL certificate is valid and matches the scanned host.
hosts={value}	(Optional to create or update record) A list of FQDNs for the hosts that correspond to all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
database={value}	(Required to create, optional to update record) The database name to authenticate to. Specify a valid MySQL database name.
port={value}	(Required to create, optional to update record) The port the database name is running on.
windows_config_file={value}	(Optional to create or update record) The path to the Windows MySQL config file. Access to this config file is required to run certain checks on Windows hosts.
	Note: You must specify either windows_config_file or unix_config_file depending on the host OS.
unix_config_file={value}	(Optional) Name of the client (Consultant type subscriptions).
	Note: You must specify either windows_config_file or unix_config_file depending on the host OS.
client_cert={value}	(Optional to create or update record) PEM-encoded X.509 certificate. Specify if certificate authentication is required by your server to establish an SSL connection.
client_key={value}	(Optional to create or update record) PEM-encoded RSA private key. Specify if certificate authentication is required by your server to establish an SSL connection.
is_template{0|1}	(Optional for create request, not valid for update request) Specify to 1 to create a MySQL system record template. You must also specify login credentials.

Parameter	Description
save_as_user_auth={0|1}	(Optional for update request, not valid for create request) Specify 1 to update a system created record and save it as a user created record. If another MySQL record already exists with the same IP address and target configuration then an error is returned. (This parameter applies only to system created MySQL records. It cannot be specified for user created MySQL records and it cannot be specified for MySQL system record templates.)
is_system_created{0|1}	(Optional) By default, user created records and system created auth records are listed. Set to 0 to list only user created records, or set to 1 to list only system created records.
template_auth_id={value}	(Optional) Specify the template ID for MySQL system record template to only show MySQL records associated with the specified template.
template_auth_name={value}	(Optional) Specify the template name for MySQL system record template to only show MySQL records associated with the specified template.
status={0|1}	(Optional) By default, active and inactive auth records are listed. Set to 0 to list only inactive records or set to 1 to list only active records.
Login credentials	
login_type={**basic**|vault}	(Optional) The login type is basic by default. Specify login_type=vault to use an authentication vault.
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a MySQL account. If login_type=vault is specified, this is the username of a vault account.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to MySQL server. Maximum 100 characters (ascii).
Vault	
vault_type={value}	(Required only when action=create and login_type=vault) The vault to be used for authentication. See Vault Support matrix.
vault_id={value}	(Required only when action=create and login_type=vault) The ID of the vault you want to use.
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition.
Target Hosts	

Parameter	Description
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips or member_domain parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

Sample - List MySQL record template

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&ids=5158332"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM https://
https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/auth_mysql_list
_output.dtd>
    <AUTH_MYSQL_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-07-17T05:50:20Z</DATETIME>
            <AUTH_MYSQL_LIST>
                <AUTH_MYSQL>
                    <ID>5158332</ID>
                    <TITLE>
                        <![CDATA[Mysql_template_apiupdate]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[MysqlUserupdate]]>
                    </USERNAME>
                    <LOGIN_TYPE>
                        <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <CREATED>
```

```
                        <DATETIME>2024-07-17T05:40:21Z</DATETIME>
                        <BY>quay_sm</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2024-07-17T05:47:07Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                    <IS_TEMPLATE>1</IS_TEMPLATE>
                </AUTH_MYSQL>
            </AUTH_MYSQL_LIST>
        </RESPONSE>
    </AUTH_MYSQL_LIST_OUTPUT>
```

Sample - List MySQL record template with vault

You'll see vault information in the XML output when you list MySQL authentication records with vaults.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&ids=5158333"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM https://
https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/auth_mysql_list
_output.dtd>
    <AUTH_MYSQL_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-07-17T06:02:11Z</DATETIME>
            <AUTH_MYSQL_LIST>
                <AUTH_MYSQL>
                    <ID>5158333</ID>
                    <TITLE>
                        <![CDATA[Mysql_template_api_vaultupdate]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[MysqlUserupdate]]>
                    </USERNAME>
                    <LOGIN_TYPE>
                        <![CDATA[vault]]>
                    </LOGIN_TYPE>
                    <DIGITAL_VAULT>
                        <DIGITAL_VAULT_ID>
                            <![CDATA[1247724]]>
                        </DIGITAL_VAULT_ID>
                        <DIGITAL_VAULT_TYPE>
```

```
                        <![CDATA[Thycotic Secret Server]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                      <![CDATA[Thycotic Secret Server Vault]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_SECRET_NAME>
                        <![CDATA[secertpdate]]>
                    </VAULT_SECRET_NAME>
                </DIGITAL_VAULT>
                <CREATED>
                    <DATETIME>2024-07-17T05:57:49Z</DATETIME>
                    <BY>quay_sm</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2024-07-17T06:00:23Z</DATETIME>
                </LAST_MODIFIED>
                <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                <IS_ACTIVE>1</IS_ACTIVE>
                <IS_TEMPLATE>1</IS_TEMPLATE>
            </AUTH_MYSQL>
        </AUTH_MYSQL_LIST>
    </RESPONSE>
</AUTH_MYSQL_LIST_OUTPUT>
```

Sample: List MySQL all template

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&is_template=1"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM https://
https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/auth_mysql_list
_output.dtd>
    <AUTH_MYSQL_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-07-16T05:37:03Z</DATETIME>
            <AUTH_MYSQL_LIST>
                <AUTH_MYSQL>
                    <ID>5129495</ID>
                    <TITLE>
                        <![CDATA[Mysql template]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[qualys_scan]]>
                    </USERNAME>
                    <LOGIN_TYPE>
```

```
            <![CDATA[basic]]>
        </LOGIN_TYPE>
        <CREATED>
            <DATETIME>2024-07-09T10:34:25Z</DATETIME>
            <BY>quay_sm</BY>
        </CREATED>
        <LAST_MODIFIED>
            <DATETIME>2024-07-15T11:51:31Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
    </AUTH_MYSQL>
    <AUTH_MYSQL>
        <ID>5131010</ID>
        <TITLE>
            <![CDATA[mysql vaultcccc]]>
        </TITLE>
        <USERNAME>
            <![CDATA[recccccccccccccc]]>
        </USERNAME>
        <LOGIN_TYPE>
            <![CDATA[vault]]>
        </LOGIN_TYPE>
        <DIGITAL_VAULT>
            <DIGITAL_VAULT_ID>
                <![CDATA[1248749]]>
            </DIGITAL_VAULT_ID>
            <DIGITAL_VAULT_TYPE>
                <![CDATA[HashiCorp]]>
            </DIGITAL_VAULT_TYPE>
            <DIGITAL_VAULT_TITLE>
                <![CDATA[HashiCorp Vault]]>
            </DIGITAL_VAULT_TITLE>
            <VAULT_SECRET_KV_PATH>
                <![CDATA[path]]>
            </VAULT_SECRET_KV_PATH>
            <VAULT_SECRET_KV_NAME>
                <![CDATA[name]]>
            </VAULT_SECRET_KV_NAME>
            <VAULT_SECRET_KV_KEY>
                <![CDATA[key]]>
            </VAULT_SECRET_KV_KEY>
        </DIGITAL_VAULT>
        <CREATED>
            <DATETIME>2024-07-10T06:55:53Z</DATETIME>
            <BY>quay_sm</BY>
        </CREATED>
        <LAST_MODIFIED>
```

```
            <DATETIME>2024-07-12T09:48:02Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
    </AUTH_MYSQL>
    <AUTH_MYSQL>
        <ID>5144731</ID>
        <TITLE>
            <![CDATA[Mysql_template_api]]>
        </TITLE>
        <USERNAME>
            <![CDATA[MysqlUser]]>
        </USERNAME>
        <LOGIN_TYPE>
            <![CDATA[basic]]>
        </LOGIN_TYPE>
        <CREATED>
            <DATETIME>2024-07-15T05:53:48Z</DATETIME>
            <BY>quay_sm</BY>
        </CREATED>
        <LAST_MODIFIED>
            <DATETIME>2024-07-15T05:53:48Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
    </AUTH_MYSQL>
    <AUTH_MYSQL>
        <ID>5144751</ID>
        <TITLE>
            <![CDATA[M1_api]]>
        </TITLE>
        <USERNAME>
            <![CDATA[MysqlUser]]>
        </USERNAME>
        <LOGIN_TYPE>
            <![CDATA[basic]]>
        </LOGIN_TYPE>
        <CREATED>
            <DATETIME>2024-07-15T05:58:51Z</DATETIME>
            <BY>quay_sm</BY>
        </CREATED>
        <LAST_MODIFIED>
            <DATETIME>2024-07-15T05:58:51Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
```

```
                    </AUTH_MYSQL>
                    <AUTH_MYSQL>
                        <ID>5144986</ID>
                        <TITLE>
                            <![CDATA[test reader MYSQL sys record]]>
                        </TITLE>
                        <USERNAME>
                            <![CDATA[aef_at]]>
                        </USERNAME>
                        <LOGIN_TYPE>
                            <![CDATA[basic]]>
                        </LOGIN_TYPE>
                        <CREATED>
                            <DATETIME>2024-07-15T08:23:33Z</DATETIME>
                            <BY>quay_sm</BY>
                        </CREATED>
                        <LAST_MODIFIED>
                            <DATETIME>2024-07-15T08:23:33Z</DATETIME>
                        </LAST_MODIFIED>
                        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                        <IS_ACTIVE>1</IS_ACTIVE>
                        <IS_TEMPLATE>1</IS_TEMPLATE>
                    </AUTH_MYSQL>
                </AUTH_MYSQL_LIST>
            </RESPONSE>
        </AUTH_MYSQL_LIST_OUTPUT>
```

Sample - Create new MySQL record template

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=create&is_template=1&title=Mysql_template_api1&username=My
sqlUser&password=Password"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM https://
https://qualysapi.qualys.com/api/3.0/batch_return.dtd>
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-17T05:40:21Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>5158332</ID>
                    </ID_SET>
```

```
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Create MySQL record template using vault

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=create&is_template=1&title=Mysql_template_api_vault&userna
me=MysqlUser&login_type=vault&vault_type=Thycotic Secret
Server&vault_id=1247724&secret_name=secert"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
https://qualysapi.qualys.com/api/3.0/batch_return.dtd>
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-17T05:57:49Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>5158333</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update MySQL record template

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=update&title=Mysql_template_apiupdate&username=MysqlUserup
date&password=Passwordupdate&ids=5158332"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM https://
https://qualysapi.qualys.com/api/3.0/batch_return.dtd>
<BATCH_RETURN>
    <RESPONSE>
```

```
            <DATETIME>2018-01-23T17:14:28Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>137296922</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update vault details in MySQL record template

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=create&is_template=1&title=Mysql_template_api_vault&userna
me=MysqlUser&login_type=vault&vault_type=Thycotic Secret
Server&vault_id=1247724&secret_name=secert"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM https://
https://qualysapi.qualys.com/api/3.0/batch_return.dtd>
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-17T06:00:23Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>5158333</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample: Update MySQL system authentication record to save as user record

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d
"action=update&title=MySQLapi_edit_as_user&username=abc&password=1
23&database=dbaa&port=6766&ids=5140898&save_as_user_auth=1"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM https://
https://qualysapi.qualys.com/api/3.0/batch_return.dtd>
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2024-07-15T09:57:18Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>5140898</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample: List system created MySQL record

API Request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "Username:Password"
-d "action=list&ids=5145491"
"https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM https://
https://qualysapi.qualys.com/api/3.0/fo/auth/mysql/auth_mysql_list
_output.dtd>
    <AUTH_MYSQL_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-07-17T06:29:13Z</DATETIME>
            <AUTH_MYSQL_LIST>
                <AUTH_MYSQL>
                    <ID>5145491</ID>
                    <TITLE>
                       <![CDATA[MySQL [System Created] - 317088]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[qualys_scan]]>
                    </USERNAME>
                    <DATABASE>
                        <![CDATA[mysql]]>
                    </DATABASE>
                    <PORT>3306</PORT>
                    <IP_SET>
                        <IP>10.14.71.53</IP>
```

```
                        </IP_SET>
                        <LOGIN_TYPE>
                            <![CDATA[basic]]>
                        </LOGIN_TYPE>
                        <SSL_VERIFY>false</SSL_VERIFY>
                        <WINDOWS_CONF_FILE>
                            <![CDATA[]]>
                        </WINDOWS_CONF_FILE>
                        <UNIX_CONF_FILE>
                            <![CDATA[/etc/my.cnf]]>
                        </UNIX_CONF_FILE>
                        <NETWORK_ID>0</NETWORK_ID>
                        <CREATED>
                            <DATETIME>2024-07-15T12:23:15Z</DATETIME>
                        </CREATED>
                        <LAST_MODIFIED>
                            <DATETIME>2024-07-15T12:23:15Z</DATETIME>
                        </LAST_MODIFIED>
                        <IS_SYSTEM_CREATED>1</IS_SYSTEM_CREATED>
                        <IS_ACTIVE>1</IS_ACTIVE>
                        <IS_TEMPLATE>0</IS_TEMPLATE>
                        <TEMPLATE>
                            <ID>5129495</ID>
                            <TITLE>Mysql template</TITLE>
                        </TEMPLATE>
                        <COMMENTS>
                            <![CDATA[System created MySQL auth record
using scan data with history ID 2197119.]]>
                        </COMMENTS>
                    </AUTH_MYSQL>
                </AUTH_MYSQL_LIST>
            </RESPONSE>
        </AUTH_MYSQL_LIST_OUTPUT>
```

DTDs for auth type “mysql”

<platform API server>/api/3.0/batch_return.dtd

<platform API server>/api/3.0/fo/auth/mysql/auth_mysql_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/auth/mysql	Active	Active
/api/2.0/fo/auth/mysql	December 2025	December 2026

Neo4j Record

/api/2.0/fo/auth/neo4j/

[POST]

Create, update, list and delete Neo4j authentication records. Compliance scans are supported (using PC and SCA). User permissions for this API are the same as other authentication record APIs.

Requirement - You must configure authentication credentials on target hosts.

Download Qualys User Guide - Neo4j Authentication

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
ips={value}	(Required to create record) Enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.
add_ips={value}	(Optional and valid only to update record) Add IPs to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
database={value}	(Optional to create or update record) The database name of the Neo4j database to be scanned. The database name may contain a maximum of 255 multi-byte characters.
port={value}	(Required to create record, optional to update record) The port number assigned to the database instance to be scanned.
login_type={**basic**|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The username to be used for authentication to Neo4j.
password={value}	(Required to create record) When login_type=basic, specify the password to be used for authentication to Neo4j. Maximum 100 characters (ascii).

vault_id={value}	Required if login_type=vault The ID of the vault to be used to retrieve the password for login.
vault_type={value}	Required if login_type=vault The third party vault to be used to retrieve the password for login. Certain vaults support this capability.
ssl_verify={0|1}	(Optional to create or update record, and valid for server that supports SSL) Specify 1 for a complete SSL certificate validation. - If ssl_verify=0, the Qualys scanners authenticate with In Servers that don't use SSL or Neo4j servers that use SSL. However, in the SSL case, the server SSL certificate verification will be skipped. - If unspecified (or ssl_verify=1), the Qualys scanners will only send a login request after verifying that a connection to the Neo4j server uses SSL, the server SSL certificate is valid and matches the scanned host.
hosts={value}	(Required only when ssl_verify is enabled) A list of FQDNs for the hosts that correspond to all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
neo4j_version={value}	(Optional) Specifies the Neo4j version. Only Neo4j 3.x version is supported at this time. Valid value is "neo4j 3.x" (case insensitive). When unspecified, Neo4j 3.x is used.
unix_base_path={value}	(Optional) The base path for Neo4j on your Unix hosts. Sample value: /opt/neo4j-enterprise-3.5.16/ Instead of specifying the path information, you can choose to auto discover the base and configuration paths by specifying neo4j_auto_path=1.
unix_conf_path={value}	(Optional) The path to the Neo4j configuration file on your Unix hosts. Sample value: /opt/neo4j-enterprise-3.5.16/conf/neo4j.conf Note that the configuration file must be in the same location for all hosts (IPs) included in the record. Instead of specifying path information, you can choose to auto discover the base and configuration paths by specifying neo4j_auto_path=1.
neo4j_auto_path={**0**|1}	(Optional) When unspecified or neo4j_auto_path=0 (false), we will not use auto discovery to find the base and configuration paths for Neo4j on your Unix hosts. Use the unix_base_path and unix_conf_path input parameters to specify path information. When neo4j_auto_path=1 (true) we will auto discover the base and configuration paths for Neo4j on your Unix hosts.

Sample: Create Neo4j Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&title=neo4j-recordAuth
Record&username=root&password=<PASSWORD>&database=graph.db&port=7687&ips
=1.1.14&unix_conf_path=/opt/neo4j-enterprise-
3.5.16/conf/neo4j.conf&unix_base_path=/opt/neo4j-enterprise-
3.5.16/&neo4j_version=neo4j 3.x&neo4j_auto_path=0"
"https://qualysapi.qualys.com/api/2.0/fo/auth/neo4j/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-03-15T11:56:08Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>101430</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Update Neo4j Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&title=Neo4j Auth Record
&username=root&password=<PASSWORD>&database=graph.db&port=7689&ips=1.1.1
.1&ids=101430&unix_conf_path=/opt/neo4j-enterprise-
3.5.16/conf/neo4j.conf&unix_base_path=/opt/neo4j-enterprise-
3.5.16/&neo4j_version=neo4j 3.x&neo4j_auto_path=0"
"https://qualysapi.qualys.com/api/2.0/fo/auth/neo4j/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-03-15T11:56:08Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>101430</ID>
```

```
                </ID_SET>
              </BATCH>
          </BATCH_LIST>
      </RESPONSE>
</BATCH_RETURN>
```

Sample - List Neo4j Record

You'll see Neo4j record IDs in the output when you have Neo4j records in your account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/neo4j/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NEO4J_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/neo4j/auth_neo4j_list_outpu
t.dtd">
<AUTH_NEO4J_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-05-24T10:23:14Z</DATETIME>
    <AUTH_NEO4J_LIST>
      <AUTH_NEO4J>
        <ID>4815851</ID>
        <TITLE><![CDATA[Neo4j Sample]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <DATABASE><![CDATA[alpha]]></DATABASE>
        <PORT>123</PORT>
        <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.10</IP>
          <IP>10.10.10.20</IP>
        </IP_SET>
        <UNIX_CONF_PATH><![CDATA[/opt/neo4j-enterprise-
3.5.16/conf/neo4j.conf]]></UNIX_CONF_PATH>
        <UNIX_BASE_PATH><![CDATA[/opt/neo4j-enterprise-
3.5.16/]]></UNIX_BASE_PATH>
        <VERSION><![CDATA[Neo4j 3.x]]></VERSION>
        <AUTO_PATH><![CDATA[0]]></AUTO_PATH>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2021-05-24T10:46:38Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2021-05-24T10:48:36Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_NEO4J>
    </AUTH_NEO4J_LIST>
  </RESPONSE>
</AUTH_NEO4J_LIST_OUTPUT>
```

Sample: Delete Neo4j Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=delete&ids=4620768"
"https://qualysapi.qualys.com/api/2.0/fo/auth/neo4j/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-04-01T13:12:51Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4620768</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “neo4j”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/neo4j/auth_neo4j_list_output.dtd

Nginx Record

(api/2.0/fo/auth/nginx/)

[POST]

Create, update, list and delete Nginx authentication records. Compliance scans are supported (using PC and SCA). User permissions for this API are the same as other authentication record APIs.

Requirement - You must configure authentication credentials on target hosts.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
ips={value}	(Required to create record) Enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.
add_ips={value}	(Optional and valid only to update record) Add IPs to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
unix_bin_path={value}	(Optional) Absolute path of the Nginx binary file location.
unix_conf_path={value}	(Optional) The path to the Nginx configuration file on your Unix hosts.
unix_prefix_path	(Optional) The path to the Nginx configuration file on your Unix hosts.

Sample: Create Nginx Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&ips=1.2.3.4&
title=API_Nginx&unix_bin_path=/usr/local/nginx/sbin/nginx&unix_conf_path=
/usr/local/nginx/conf/nginx.conf
&unix_prefix_path=/usr/local/nginx"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
    <DATETIME>2021-08-13T11:36:30Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1157719</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Update Nginx Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&ids=229028&ips=10.10.10.10&title=Test
Nginx&unix_bin_path=/usr/local/nginx/sbin/nginx&unix_conf_path=/usr/local
/nginx/conf/nginx.conf&unix_prefix_path=/usr/local/nginx"
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-08-03T03:15:35Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>229028</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample: List the Nginx Records

You'll see Nginx record IDs in the output when you have Nginx records in your account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/nginx"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/auth_nginx_list_outpu
t.dtd">
<AUTH_NGINX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-08-02T13:57:09Z</DATETIME>
    <AUTH_NGINX_LIST>
           <AUTH_NGINX>
                <ID>228028</ID>
                <TITLE>
                    <![CDATA[Nginx second]]>
                </TITLE>
                <IP_SET>
                    <IP>10.11.12.13</IP>
                </IP_SET>
                <UNIX_BIN_PATH>
                    <![CDATA[/usr/local/nginx/sbin/nginx]]>
                </UNIX_BIN_PATH>
                <UNIX_CONF_PATH>
                    <![CDATA[/usr/local/nginx/conf/nginx.conf]]>
                </UNIX_CONF_PATH>
                <UNIX_PREFIX_PATH>
                    <![CDATA[/usr/local/nginx]]>
                </UNIX_PREFIX_PATH>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2021-07-29T06:15:12Z</DATETIME>
                    <BY>joe_user</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2021-07-29T07:20:17Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_NGINX>
        </AUTH_NGINX_LIST>
        <GLOSSARY>
            <USER_LIST>
                <USER>
                    <USER_LOGIN>joe_user</USER_LOGIN>
                    <FIRST_NAME>Joe</FIRST_NAME>
                    <LAST_NAME>User</LAST_NAME>
                </USER>
            </USER_LIST>
        </GLOSSARY>
    </RESPONSE>
</AUTH_NGINX_LIST_OUTPUT>
```

Sample: Delete Nginx Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=delete&ids=5146728,5146726"
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/nginx/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-08-27T11:38:07Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>5146726</ID>
          <ID>5146728</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “nginx”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/neo4j/auth_nginx_list_output.dtd

Oracle Record

/api/2.0/fo/auth/oracle/

[POST]

Create, update, list and delete Oracle records and Oracle system record templates for authenticated scans of Oracle instances. Vulnerability and compliance scans are supported (using VM, PC).

How it works - During scanning we'll authenticate to one or more instances on a single host using all Oracle records in your account. For compliance scans, you can scan multiple Oracle instances on a single host and port combination. Looking for more help? Search for "Oracle Use Cases" in Qualys online help.

System created authentication records supported - You can allow the system to create Oracle authentication records for auto discovered instances and scan them. This is supported for Unix installations only. To enable this feature, you must first create Oracle System Record Templates using the is_template input parameter and specifying login credentials. See System created Oracle records.

Requirement - You must configure login credentials on target hosts before scanning.

Download Qualys User Guide - Oracle Authentication for VM Scans (.zip)

Download Qualys User Guide - Oracle Authentication for Compliance Scans (.zip)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record, optional to update record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
is_template={**0**|1}	(Optional for create request, not valid for update request) By default, a new record is a regular Oracle record. Specify 1 to create an Oracle system record template. You must also specify login credentials, which are described below. See System created Oracle records.

Parameter	Description
status={0|**1**}	(Optional) The record status, active or inactive. By default, a new record is set to active (1). Set to 0 for inactive record or 1 for active record. (This parameter applies to system created and user created Oracle records. It cannot be specified for Oracle system record templates.)
save_as_user_auth={**0**|1}	(Optional for update request, not valid for create request) Specify 1 to update a system created record and save it as a user created record. If another Oracle record already exists with the same IP address and target configuration then an error will be returned. (This parameter applies only to system created Oracle records. It cannot be specified for user created Oracle records and it cannot be specified for Oracle system record templates.)
Login credentials	
login_type={basic|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The user account to be used for authentication to the Oracle database. The username may include 1-31 characters (ascii).
password={value}	(Required to create record, optional to update record) The password corresponding to the user account defined in the record for authentication. Maximum 100 characters (ascii).
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) or Database Secrets Engines in HashiCorp authentication records. Specify 1 to use Active Directory (AD) or Database Secrets Engines in the authentication records.
vault_id={value}	(Required to create record, optional to update record). The vault ID from where you want to retrieve the password. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See Vault Definition
sid={value}	(Optional to create or update record) The Oracle System ID (SID) that identifies the database instance to be authenticated to. To create a record sid or servicename is required. The parameters sid and servicename cannot be specified in the same request.

Parameter	Description
servicename={value}	(Optional to create or update record) The Oracle service name that identifies the database instance to be authenticated to. A maximum of 30 characters may be specified. The parameters sid and servicename cannot be specified in the same request.
port={value}	(Optional to create record) The port number that the Oracle database instance is running on. When not specified, the "All Ports" option is used and the scanning engine will authenticate to the database instance on each port that the Oracle service is detected on. Ports used for Oracle authentication These parameters are mutually exclusive: instance and auto_discover_instances=1.
is_cdb={**0**|1}	(Optional) Indicates whether the database is a Container Database (CDB). Specify 1 if the database is a CDB or 0 (the default) if the database is not a CDB. This setting is applied to compliance scans only. Identifying the Oracle database as CDB ensures the right compliance checks are performed for multitenant technologies. Also, when the database is a CDB, we auto-discover all Pluggable Databases (PDBs) within the container environment, and scan them for compliance. This saves you from having to create separate, additional Oracle records for each PDB instance.
pc_only={**0**|1}	(Optional to create record, valid when the compliance module is enabled) Specify 1 to perform compliance scans on multiple instances running on host and port combinations in this record. This parameter must be specified if this Oracle record has some host and port combination, which is already defined in another record. Note, however, when pc_only=1 is specified, the record will be used for compliance scans only. When not specified, the record will be used for vulnerability scans and compliance scans.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.

Parameter	Description
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
TCPS Configuration Parameters	Add TCPS configuration to Oracle authentication records.
ssl_verify={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
server_dn{value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
use_vault_passphrase={0|1}	(Optional) Set to 1 if you want to store Ewallet passphrase to vault.
cwallet,ewallet{value}	Specify Cwallets and Ewallets. Cwallets are certificates intended for storing binary contents of cwallet.sso file. SSO file format is an Oracle proprietary. Ewallets are certificates intended for storing binary contents of ewallet. p12 file. P12 file format is standard PKCS12.
passphrase{value}	Specify Ewallet passphrase.
OS Parameters Windows	OS Parameters are used for compliance scans only.
perform_windows_os_checks ={**0**|1}	(Optional) Specify 1 to perform OS-dependent compliance checks for the Oracle technology during Windows authenticated compliance scans. These checks are assigned to the control category "Databse Setttings" in the sub-category "DB OS-dependent Controls".
win_ora_home_name= {value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The Windows Oracle Home name. Example: OraHome1
win_ora_home_path= {value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The Windows Oracle Home path. Example: c:\Program Files\Oracle\10

Parameter	Description
win_init_ora_path={value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The pathname to the Windows init(SID).ora file. Example: c:\Program Files\oracle\dbs\initORA10.ora
win_spfile_ora_path={value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The pathname to the Windows spfile(SID).ora file. Example: c:\Program Files\oracle\network\admin\spfileORA10.ora
win_listener_ora_path={value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The pathname to the Window listener.ora file. Example: c:\Program Files\oracle\network\admin\listener.ora
win_sqlnet_ora_path={value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The pathname to the Windows sqlnet.ora file. Example: c:\Program Files\oracle\network\admin\sqlnet.ora
win_tnsnames_ora_path={value}	(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The pathname to the Windows tnsnames.ora file. Example: c:\ProgramFiles\oracle\network\admin\tnsnames.ora
OS Parameters Unix	OS Parameters are used for compliance scans only.
perform_unix_os_checks={**0**|1}	(Optional) Specify 1 to perform OS-dependent compliance checks for the Oracle technology during Unix authenticated compliance scans. These checks are assigned to the control category “Databse Setttings” in the sub-category “DB OS-dependent Controls”.
perform_unix_opatch_checks={**0**|1}	(Optional) Specify 1 to perform OPatch checks using the OPatch binary to return a list of all installed patches for the Oracle instance. In a case where perform_unix_os_checks=1 is specified and perform_unix_opatch_checks=0 is specified (or this parameter is not specified), the service checks for patch information from the Oracle database directly; information in the database may not be accurate so the list of installed patches returned by the service also may not be accurate.
unix_ora_home_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The Unix Oracle Home path. Example: /usr/opt/oracle/10

Parameter	Description
unix_init_ora_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix init(SID).ora file. Example: /usr/opt/oracle/dbs/initORA10.ora
unix_spfile_ora_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix spfile(SID).ora file. Example: /usr/opt/oracle/network/admin/spfileORA10.ora
unix_listener_ora_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix listener.ora file. Example: /usr/opt/oracle/network/admin/listener.ora
unix_sqlnet_ora_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix sqlnet.ora file. Example: /usr/opt/oracle/network/admin/sqlnet.ora
unix_tnsnames_ora_path={value}	(Required if perform_unix_os_checks=1 and/or perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix tnsnames.ora file. Example: /usr/opt/oracle/network/admin/tnsnames.ora
unix_invptrloc={value}	(Optional) if perform_unix_opatch_checks=1 is specified; otherwise invalid) The pathname to the Unix oraInst.loc file. Use this parameter to identify a custom inventory for patches. Example: /usr/opt/oracle/network/admin/oraInst.loc

Ports used for Oracle authentication

The “All Ports” option is used when the **`port`** parameter is not specified (the default). You may only create one Oracle record with this setting for each host. When All Ports is defined the scanning engine uses the credentials in the record to attempt authentication to the database instance (SID or service name) when a port-specific record does not exist. The scanning engine will authenticate to the database instance on each port the Oracle service is detected on.

A single port is used when the **`port`** parameter is specified (e.g. **`port=1521`**). The same port number cannot be entered in multiple Oracle records for the same host, unless the compliance module is enabled and **`pc_only=1`** is specified.

How it works - When the scanning engine detects an Oracle instance on a host, it first checks to see if you have an authentication record with the database instance and port specified. If you have a port-specific record, then it uses the credentials in that record to attempt authentication to the database instance. If a port-specific record does not exist

(or if authentication fails), then the scanning engine checks to see if you have an authentication record set to “All Ports” for the host and uses the credentials in that record to attempt authentication to the database instance.

System created Oracle records

When we auto discover Oracle instances, we’ll discover the target configuration for each instance but not the login credentials. We’ve introduced a new configuration called “Oracle System Record Template” that you’ll use to provide Oracle login credentials for system created records. You’ll create the system record template and then select it in the option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the scan.

Benefits

- We’ll auto discover Oracle instances on each scanned host and create authentication records for those instances. We support auto discovery and system record creation for Oracle instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running Oracle.

- When we create Oracle authentication records for discovered instances, we’ll insert the credentials from the Oracle system record template you selected in the option profile.

- You can easily rotate Oracle passwords. Simply edit the credentials in the Oracle system record template and all Oracle records linked to the template will be updated to use the new credentials with no additional scan or action by you.

- You can edit individual Oracle system created records and save them as user created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.

How it works

Here’s the basic flow for Oracle instance discovery and auto record creation. Note - We support auto discovery and system record creation for Oracle instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running Oracle.

1) Create an Oracle system record template and enter the login credentials you want to use for system created records.

2) Select the Oracle system record template in the compliance option profile you want to use for discovery scans.

Note: You can configure Oracle system record template for Multitenant Container Database. Select the "Is CDB" option to enable your Oracle database system created authentication records in Multitenant Container Database.

3) Launch your discovery scan. Your scan results will list the auto discovered instances.

4) List your Oracle authentication records. For each system created record, you’ll see the template associated with the record.

Sample create Oracle system record template

This sample creates an Oracle system record template by using is_template=1.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&is_template=1&title=OracleRecordTemplate&username=OracleUs
er&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T18:43:59Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2237956</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “oracle”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/oracle/auth_oracle_list_output.dtd

Oracle Listener Record

/api/2.0/fo/auth/oracle_listener/

[POST]

Create, update, list and delete Oracle Listener records for authenticated scans of Oracle Listener databases. Vulnerability scans are supported (using VM).

Oracle Listener records are used to connect to Oracle TNS Listeners in order to enumerate information about databases behind the Oracle Listeners. When authentication is successful and databases behind the Listener are discovered, the QID 19225 "Retrieved Oracle Database Name" is returned in the scan results. This is an information gathered check that lists the names of the databases discovered behind the Listener. This information is useful if you want to create Oracle authentication records on those databases and need the Oracle System IDs (SIDs).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record, optional to update record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
password={value}	(Required to create record, optional to update record) Specifies a password for authentication to target hosts. If more than one Listener is detected on the same host, then the same password is attempted on each Listener. Maximum 100 characters (ascii).

Parameter	Description
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	((Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

DTDs for auth type "oracle_listener"

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/oracle_listener/auth_oracle_listener_list_output.dtd

Oracle WebLogic Server Record

/api/2.0/fo/auth/oracle_weblogic/

[POST]

Create, update, list and delete Oracle WebLogic records for authenticated scans of Oracle WebLogic Server instances. Vulnerability and compliance scans are supported (using VM, PC).

What you'll need:

- We support these technologies: Oracle WebLogic Server 11g and Oracle WebLogic Server 12c

- Unix authentication is required so you'll need a Unix record for each host running an Oracle WebLogic Server

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required for update request; invalid for create request) The IDs of the Oracle WebLogic Server authentication records that you want to update. Multiple IDs are comma separated
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
installation_path={value}	(Required to create record, optional to update record) The directory where the Oracle WebLogic Server is installed (i.e. Home directory). Example: /u01/app/oracle/middleware
auto_discover={0|**1**}	(Optional) For a create request, we default to auto_discover=1, which means we will use auto discovery to find all domains for you. Specify auto_discover=0 and we will not auto discover domains. For an update request, we will keep the record's settings as is unless you overwrite them. auto_discover=0 must be specified with the domain parameter in the same request.

Parameter	Description
domain={value}	(Optional) A single Oracle WebLogic Server domain name. Example: website The domain parameter must be specified with auto_discover=0 in the same request.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create WebLogic record, no auto discover

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&installation_path=/u01/app/oracle&auto_discover=0&d
omain=www.qualys.com&ips=10.10.10.23&title=WEB_ORA_CREATE"
"<qualys_base_url>/api/2.0/fo/auth/oracle_weblogic/"
```

XML output:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
```

```
  <RESPONSE>
    <DATETIME>2018-03-10T13:30:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2707632279</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create WebLogic record, with auto discover

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&installation_path=/u01/app/oracle&auto_discover=1&i
ps=10.10.10.23&title=ABC_ORA"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_weblogic/"
```

XML output:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-10T13:42:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2707642279</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “oracle_weblogic”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/oracle_weblogic/
auth_oracle_weblogic_list_output.dtd

Palo Alto Firewall Record

/api/2.0/fo/auth/palo_alto_firewall/

[POST]

Create, update, list and delete Palo Alto Firewall records for authenticated scans of Palo Alto Firewall instances. Vulnerability and compliance scans are supported (using VM, PC).

Requirements:

- The user account you provide for authentication must either have the predefined role "Superuser (read-only)" or a custom role with these XML API privileges enabled: Configuration and Operational Requests.

- We use the PANOS XML API to retrieve system information from Palo Alto Firewall on port 443 so this port must be open.

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to Palo Alto Firewall instances.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a Palo Alto Firewall account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the Palo Alto Firewall account to be used for authentication. Maximum 100 characters (ascii).

Parameter	Description
login_type=vault	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Sample - Create Palo Alto Firewall record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=palo-
4&ips=10.10.10.10&login_type=basic&username=root&password=<PASSWORD>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-14T06:29:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
```

```
          <ID>125727</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Palo Alto Firewall record, using vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=palo-
4&ips=10.10.10.11&login_type=vault&username=root&vault_type=CyberArk
AIM&vault_id=16034&file=file&folder=folder"
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-16T06:22:01Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125726</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List Palo Alto Firewall records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/?
action=list&ids=125727"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_PALO_ALTO_FIREWALL_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/a
uth_palo_alto_firewall_list_output.dtd">
<AUTH_PALO_ALTO_FIREWALL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-09-13T06:30:32Z</DATETIME>
    <AUTH_PALO_ALTO_FIREWALL_LIST>
      <AUTH_PALO_ALTO_FIREWALL>
        <ID>125727</ID>
        <TITLE><![CDATA[palo-4]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2017-09-13T06:29:41Z</DATETIME>
...
```

DTDs for auth type “palo_alto_firewall”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/palo_alto_firewall/
auth_palo_alto_firewall_list_output.dtd

Pivotal Greenplum Record

/api/2.0/fo/auth/greenplum/

[POST]

List, create, update, and delete Pivotal Greenplum records for authenticated scans of Pivotal Greenplum 5.x and 6.x instances running on Unix. Compliance scans are supported (using PC).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
details={value}	(Optional) Default value is Basic. You can choose from None, Basic, and All.
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required only for update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Greenplum	
greenplum_unix_conf_file={value}	(Required for create request) The full path to the configuration file (postgresql.conf) on your Unix assets (IP addresses). The file must be in the same location on all assets for this record.
greenplum_db_name={value}	(Required for create request) The database instance you want to authenticate to.
port={value}	(Optional) The port where the database instance is running. Default is 5432.
ssl_verify={**0**|1}	(Optional) SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
hosts={value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
Login credentials	
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a Greenplum account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).

Parameter	Description
password={value}	(For create request, password or login_type=vault is required) The password of the Greenplum account to be used for authentication. Maximum 100 characters (ascii).
login_type={value}	(For create request, password or login_type=vault is required) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix.
Keys, Passphrase	
client_key_type={value}	(Optional) Client key type basic (default) or vault.
client_key={value}	(Optional if client_key_type=basic) Client key content, if private key not in vault.
client_key_vault_type={value}	(Required if client_key_type=vault) The third party vault to be used to retrieve the private key. Certain vaults support this capability. See Vault Support matrix.
client_key_vault_id={value}	(Required if client_key_type=vault) The ID of the vault to get the private key from.
passphrase_type={value}	(Optional) Passphrase type can be basic (default) or vault.
passphrase={value}	(Optional if passphrase_type=basic) The passphrase value.
client_cert={value}	(Optional if passphrase_type=basic) The passphrase certificate content.
passphrase_vault_type={value}	(Required if passphrase_type=vault) The vault where the private key passphrase is stored. For example: CA Access Control, CyberArk AIM, Thycotic Secret Server.
passphrase_vault_id={value}	(Required if passphrase_type=vault) The ID of the vault to get the passphrase from.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.

Parameter	Description
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid only when the networks feature is enabled) The network ID for the record.

Sample: List all record types

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl' -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/auth_records.dtd">
<AUTH_RECORDS_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-10-04T09:24:19Z</DATETIME>
    <AUTH_RECORDS>
      <AUTH_UNIX_IDS>
        <ID_SET>
          <ID>1029116</ID>
          <ID>1296290</ID>
          <ID_RANGE>1375563-1375564</ID_RANGE>
          <ID>1505926</ID>
        </ID_SET>
      </AUTH_UNIX_IDS>
      <AUTH_GREENPLUM_IDS>
        <ID_SET>
          <ID>1505929</ID>
        </ID_SET>
      </AUTH_GREENPLUM_IDS>
    </AUTH_RECORDS>
  </RESPONSE>
</AUTH_RECORDS_OUTPUT>
```

Sample - List Greenplum Records with All Details

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/greenplum/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_GREENPLUM_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/greenplum/auth_green
plum_list_output.dtd">
<AUTH_GREENPLUM_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-01-05T11:41:28Z</DATETIME>
        <AUTH_GREENPLUM_LIST>
            <AUTH_GREENPLUM>
                <ID>66186</ID>
                <TITLE>
                    <![CDATA[greenplum auth]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <DATABASE>
                    <![CDATA[postgres]]>
                </DATABASE>
                <PORT>5432</PORT>
                <SSL_VERIFY>
                    <![CDATA[0]]>
                </SSL_VERIFY>
                <IP_SET>
                    <IP>10.20.32.111</IP>
                </IP_SET>
                <UNIX_CONF_FILE>
                    <![CDATA[/usr/local/greenplum-db/master/gpseg-
1/postgresql.conf]]>
                </UNIX_CONF_FILE>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2019-12-31T10:51:10Z</DATETIME>
                    <BY>qualys_jd</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2019-12-31T10:51:10Z</DATETIME>
                </LAST_MODIFIED>
```

```
            </AUTH_GREENPLUM>
            <AUTH_GREENPLUM>
                <ID>66390</ID>
                <TITLE>
                    <![CDATA[my greenplum record]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <DATABASE>
                    <![CDATA[postgres]]>
                </DATABASE>
                <PORT>5432</PORT>
                <SSL_VERIFY>
                    <![CDATA[0]]>
                </SSL_VERIFY>
                <IP_SET>
                    <IP>10.10.10.1</IP>
                </IP_SET>
                <UNIX_CONF_FILE>
                  <![CDATA[ /var/lib/pgsql/data/postgresql.conf]]>
                </UNIX_CONF_FILE>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2020-01-05T09:14:54Z</DATETIME>
                    <BY>qualys_jd</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2020-01-05T09:14:54Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_GREENPLUM>
        </AUTH_GREENPLUM_LIST>
        <GLOSSARY>
            <USER_LIST>
                <USER>
                    <USER_LOGIN>qualys_jd</USER_LOGIN>
                    <FIRST_NAME>John</FIRST_NAME>
                    <LAST_NAME>Doe</LAST_NAME>
                </USER>
            </USER_LIST>
        </GLOSSARY>
    </RESPONSE>
</AUTH_GREENPLUM_LIST_OUTPUT>
```

Sample - Create Greenplum Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=create&title=my greenplum
record&ips=10.10.10.1&username=root&password=<PASSWORD>&greenplum_
db_name=postgres&port=5421&greenplum_unix_conf_path=/tmp/postgresq
l.conf"
"https://qualysapi.qualys.com/api/2.0/fo/auth/greenplum/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-01-05T12:04:32Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>66391</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Greenplum Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=update&ids=66391&title=my greenplum record&comments=new
comment"
"https://qualysapi.qualys.com/api/2.0/fo/auth/greenplum/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-01-05T12:09:25Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
```

```
                <ID_SET>
                    <ID>66391</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Greenplum Records

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=delete&ids=66391"
"https://qualysapi.qualys.com/api/2.0/fo/auth/greenplum/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-01-05T12:10:16Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>66391</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “greenplum”

<platform API server> /api/2.0/fo/auth/auth_records.dtd

<platform API server>/api/2.0/fo/auth/greenplum/auth_greenplum_list_output.dtd

PostgreSQL Record

/api/2.0/fo/auth/postgresql/

[POST]

Create, update, list and delete PostgreSQL records for authenticated scans of PostgreSQL 9.x, PostgreSQL 10.x, PostgreSQL 11.x and PostgreSQL 12.x instances running on Windows or Unix. Compliance scans are supported (using PC).

Requirement - You must configure login credentials on target hosts before scanning.

Qualys User Guide - PostreSQL Authentication (.zip)

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to PostgreSQL database instances.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
PostgreSQL	
pgsql_win_conf_path={value}	(Optional) The full path to the PostgreSQL configuration file on your Windows assets (IP addresses). The file must be in the same location on all assets for this record.
pgsql_unix_conf_path={value}	(Optional) The full path to the PostgreSQL configuration file on your Unix assets (IP addresses). The file must be in the same location on all assets for this record.
pgsql_db_name={value}	(Required for create request) The database instance you want to authenticate to.
port={value}	(Optional) The port where the database instance is running. Default is 5432.
hosts={value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.

Parameter	Description
ssl_verify={**0**|1}	(Optional) SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
Login credentials	
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a PostgreSQL account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(For create request, password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication. Maximum 100 characters (ascii).
login_type=vault	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Database Secrets Engine in HashiCorp authentication records. Specify 1 to use Database Secrets Engine in the authentication records.
Keys, Passphrase	
client_key_type={value}	(Optional) Client key type basic (default) or vault.
client_key={value}	(Optional if client_key_type=basic) Client key content, if private key not in vault.
client_key_vault_type={value}	(Required if client_key_type=vault) The third party vault to be used to retrieve the private key. Certain vaults support this capability. See Vault Support matrix
client_key_vault_id={value}	(Required if client_key_type=vault) The ID of the vault to get the private key from. Vault parameters: client_key_folder={value} and client_key_file={value} are required vault settings.
passphrase_type={value}	(Optional) Passphrase type can be basic (default) or vault.
passphrase={value}	(Optional if passphrase_type=basic) The passphrase value.
client_cert={value}	(Optional if passphrase_type=basic) The passphrase certificate content.
passphrase_vault_type={value}	(Required if passphrase_type=vault) The vault where the private key passphrase is stored. For example CA Access Control, CyberArk AIM, Thycotic Secret Server.
passphrase_vault_id={value}	(Required if passphrase_type=vault) The ID of the vault to get the passphrase from.

Parameter	Description
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create PostgreSQL Record on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=API_POSTGRE_2&username=root&password=<PASSWOR
D>&pgsql_db_name=presql&ips=10.10.10.35&pgsql_unix_conf_path=/etc&
network_id=4002"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-27T20:17:42Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
```

```
        <ID_SET>
          <ID>84307</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create PostgreSQL Record on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=create&title=api-windows-postgres&pgsql_win_conf_path=C:\Program
Files\PostgreSQL\11\data\postgresql.conf&pgsql_db_name=postgres&username=
qualys_scan&password=<PASSWORD>&ips=10.10.10.35"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql"
```

XML output:

```
<<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-01-28T10:55:39Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>72178</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update PostgreSQL Record on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=update&ids=84307&add_ips=10.10.10.40-10.10.10.42"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
```

```
  <RESPONSE>
    <DATETIME>2018-04-10T21:01:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update PostgreSQL Record on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=update&ids=72178&pgsql_win_conf_path=C:\Program
Files\PostgreSQL\11\data\postgresql11.conf"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-01-28T11:06:36Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>72178</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List PostgreSQL Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_POSTGRESQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/auth_post
gresql_list_output.dtd">
<AUTH_POSTGRESQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-04-24T22:01:50Z</DATETIME>
    <AUTH_POSTGRESQL_LIST>
      <AUTH_POSTGRESQL>
        <ID>79518</ID>
        <TITLE><![CDATA[PostgesSQL1]]></TITLE>
        <USERNAME><![CDATA[acme_as1]]></USERNAME>
        <DATABASE><![CDATA[mydb1]]></DATABASE>
        <PORT>5432</PORT>
        <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.45</IP>
        </IP_SET>
<WIN_CONF_FILE><![CDATA[C:\Program
Files\pgsql\data\postgresql.conf]]></WIN_CONF_FILE>
<UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]
></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-04-13T23:42:50Z</DATETIME>
          <BY>acme_as1</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-04-20T23:35:42Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[my comments]]></COMMENTS>
      </AUTH_POSTGRESQL>
      <AUTH_POSTGRESQL>
        <ID>82110</ID>
        <TITLE><![CDATA[POstgreSQL2]]></TITLE>
        <USERNAME><![CDATA[acme_as1]]></USERNAME>
        <DATABASE><![CDATA[mydb2]]></DATABASE>
        <PORT>5432</PORT>
        <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
        <HOSTS>
          <HOST><![CDATA[cent-31-107.ml2k8.qualys.com]]></HOST>
        </HOSTS>
        <IP_SET>
          <IP>10.20.31.107</IP>
        </IP_SET>
<WIN_CONF_FILE><![CDATA[C:\Program
```

```
Files\pgsql\data\postgresql.conf]]></WIN_CONF_FILE>
<UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]
></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-04-20T20:12:48Z</DATETIME>
          <BY>acme_as1</BY>
        </CREATED>
      ...
    </AUTH_POSTGRESQL_LIST>
  </RESPONSE>
</AUTH_POSTGRESQL_LIST_OUTPUT>
```

DTDs for auth type “postgresql”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/postgresql/auth_postgresql_list_output.dtd

SAP Hana Record

/api/2.0/fo/auth/sap_hana/

[POST]

SAP Hana authentication is supported for compliance scans (using PC or SCA). The SAP Hana API (api/2.0/fo/auth/sap_hana/) lets you list, create, update and delete SAP Hana authentication records. User permissions for this API are the same as other authentication record APIs.

Input Parameters

Use these parameters to create or update SAP Hana authentication records.

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
SAP Hana	
database={value}	(Required for create request) The name of the database you want to authenticate to.
port={value}	(Required for create request) The port the database is on.
unix_conf_path={value}	(Required for create request when this record will be used for scanning Unix hosts) The SAP Hana configuration path on Unix hosts (up to 255 multi-byte characters).
ssl_verify={**0**|1}	(Optional to create or update record) SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
hosts={value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
Login credentials	

Parameter	Description
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a SAP Hana account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(For create request, password or login_type=vault is required) The password of the SAP Hana account to be used for authentication. Maximum 100 characters (ascii).
password_encryption={**0**|1}	(Optional to create or update record) Enable this option when your database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail. When set to 1, password encryption is enabled in the record. When set to 0 (the default), password encryption is not enabled.
login_type={value}	(For create request, password or login_type=vault is required) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) for the targets you want to authenticate to. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid only when the networks feature is enabled) The network ID for the record.

Sample - Create SAP Hana Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=sap_hana_API&username=root&password=<PASSWORD>&data
base=sapDb&port=39013&ips=1.1.1.1&ssl_verify=1&hosts=test.domain.com&unix
_conf_path=/etc/saphana.conf&password_encryption=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sap_hana/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-01-12T14:39:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>4474043</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update SAP Hana Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=4474043&comments=update1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sap_hana/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-01-12T14:45:58Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>4474043</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List SAP Hana Records with All Details

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sap_hana/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SAP_HANA_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/sap_hana/auth_sap_hana_list
_output.dtd">
<AUTH_SAP_HANA_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-01-12T14:34:42Z</DATETIME>
    <AUTH_SAP_HANA_LIST>
      <AUTH_SAP_HANA>
        <ID>4474042</ID>
        <TITLE><![CDATA[SAP_HANA]]></TITLE>
        <USERNAME><![CDATA[SYSTEM]]></USERNAME>
        <DATABASE><![CDATA[SYSTEMDB]]></DATABASE>
        <PORT>39013</PORT>
        <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
        <HOSTS>
          <HOST><![CDATA[host.domain1]]></HOST>
        </HOSTS>
        <IP_SET>
          <IP>10.11.70.185</IP>
        </IP_SET>
        <UNIX_CONF_PATH><![CDATA[/etc/saphana.conf]]></UNIX_CONF_PATH>
        <PASSWORD_ENCRYPTION><![CDATA[1]]></PASSWORD_ENCRYPTION>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <CREATED>
          <DATETIME>2021-01-12T14:28:16Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2021-01-12T14:33:05Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[created successfully]]></COMMENTS>
      </AUTH_SAP_HANA>
    </AUTH_SAP_HANA_LIST>
    <GLOSSARY>
      <USER_LIST>
        <USER>
          <USER_LOGIN>joe_user</USER_LOGIN>
          <FIRST_NAME>Joe</FIRST_NAME>
          <LAST_NAME>User</LAST_NAME>
        </USER>
      </USER_LIST>
    </GLOSSARY>
  </RESPONSE>
</AUTH_SAP_HANA_LIST_OUTPUT>
```

Sample - Delete SAP Hana Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=delete&ids=4474043"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sap_hana/"
```

XML output:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-01-12T14:48:56Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4474043</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “sap hana”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/sap_hana/auth_sap_hana_list_output.dtd

SAP IQ Record

/api/2.0/fo/auth/sapiq/

[POST]

The SAP IQ API lets you list, create, update and delete SAP IQ authentication records for compliance scans (using PC). User permissions for this API are the same as other authentication record APIs.

Input Parameters

Use these parameters to create or update SAP IQ authentication records.

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
SAP IQ	
database={value}	(Required for create request) The name of the database you want to authenticate to.
port={value}	(Required for create request) The port the database is running on.
installation_dir={value}	(Required for create request when this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.
Login credentials	
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a SAP IQ account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(For create request, password or login_type=vault is required) The password of the SAP IQ account to be used for authentication. Maximum 100 characters (ascii).

Parameter	Description
password_encryption={**0**|1}	(Optional to create or update record) Enable this option when your database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail. When set to 1, password encryption is enabled in the record. When set to 0 (the default), password encryption is not enabled.
login_type={value}	(For create request, password or login_type=vault is required) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid only when the networks feature is enabled) The network ID for the record.

Sample - Create SAP IQ Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=create&title=sapiq&username=root&password=<PASSWORD>&database=sa
pDb&port=123&&ips=11.11.11.11"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-12-05T12:04:32Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>96171</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update SAP IQ Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=update&ids=4423386&installation_dir=/opt/sybase&comments=update_i
nst_dir"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-12-11T10:47:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>4423386</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List SAP IQ Records with All Details

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SAPIQ_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/auth_sapiq_list_outpu
t.dtd">
<AUTH_SAPIQ_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-12-11T18:02:56Z</DATETIME>
    <AUTH_SAPIQ_LIST>
      <AUTH_SAP_IQ>
        <ID>4423387</ID>
        <TITLE><![CDATA[sap_iq_api_2]]></TITLE>
        <USERNAME><![CDATA[dba]]></USERNAME>
        <IP_SET>
          <IP>10.11.70.54</IP>
        </IP_SET>
        <DATABASE><![CDATA[iqdemo]]></DATABASE>
        <PORT>2638</PORT>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-12-11T06:24:15Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-12-11T06:24:15Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_SAP_IQ>
      <AUTH_SAP_IQ>
        <ID>4423518</ID>
        <TITLE><![CDATA[sap_iq_api_3]]></TITLE>
        <USERNAME><![CDATA[dba]]></USERNAME>
        <IP_SET>
          <IP>10.11.70.52</IP>
        </IP_SET>
        <DATABASE><![CDATA[iqdemo]]></DATABASE>
        <PORT>2638</PORT>
        <INSTALLATION_DIR><![CDATA[test]]></INSTALLATION_DIR>
        <PASSWORD_ENCRYPTION><![CDATA[1]]></PASSWORD_ENCRYPTION>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-12-11T12:35:12Z</DATETIME>
          <BY>joe_user</BY>
      </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-12-11T12:35:12Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_SAP_IQ>
    </AUTH_SAPIQ_LIST>
    <GLOSSARY>
      <USER_LIST>
        <USER>
```

```
            <USER_LOGIN>joe_user</USER_LOGIN>
            <FIRST_NAME>Joe</FIRST_NAME>
            <LAST_NAME>User</LAST_NAME>
          </USER>
        </USER_LIST>
      </GLOSSARY>
    </RESPONSE>
</AUTH_SAPIQ_LIST_OUTPUT>
```

Sample - Delete SAP IQ Records

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=delete&ids=4423386"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-12-11T10:53:04Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4423386</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “sap iq”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/sapiq/auth_sapiq_list_output.dtd

SNMP Record

/api/2.0/fo/auth/snmp/

[POST]

Create, update, list and delete SNMP records for authenticated scans of SNMP enabled devices. Supported are vulnerability and compliance scans (using VM, PC). Supported versions are SNMPv1, SNMPv2 and SNMPv3.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
version={**v1**|v2c|v3}	(Optional to create or update record) Specifies the SNMP protocol version. For an update request, this parameter overwrites the existing SNMP version with a new version. A valid value is: v1 = SNMPv1 (the default) v2c = SNMPv2c v3 = SNMPv3
Login credentials	
community_strings={value}	(Optional and valid using SNMPv1 and SNMPv2c) The SNMP community strings to be used for authentication to target hosts. Multiple entries are comma separated. The service attempts authentication using several common default community strings. When community_strings is specified, the user-provided community strings are used for authentication before the default community strings.

Parameter	Description
username={value}	(Optional and valid using SNMPv3) The user account for authentication to target hosts. A maximum of 128 characters may be specified. These three parameters are used to specify authentication: username, password and auth_alg. If creating a record and authentication will be used, it is required that all three parameters are specified together. If updating a record to change the username, the username specified will replace the existing username in the record. If updating a record to remove authentication, specify an empty value for all three parameters.
password={value}	(Optional and valid using SNMPv3) The password for authentication to target hosts. Maximum of 128 characters.. These three parameters are used to specify authentication: username, password, and auth_alg. If creating a record and authentication will be used, it is required that all three parameters are specified together. If updating a record to change the password, the password specified will replace the existing password in the record. If updating a record to remove authentication, specify an empty value for all three parameters.
auth_alg={MD5|SHA1|SHA224|SHA256|SHA384|SHA512}	(Optional and valid using SNMPv3) The algorithm for authentication: MD5, SHA1, SHA224, SHA256.SHA384, and SHA512 This algorithm is used to safely prove to the SNMP server knowledge of the password without sending the password. These three parameters are used to specify authentication: username, password and auth_alg. If creating a record and authentication will be used, it is required that all three parameters are specified together. If updating a record to change the authentication algorithm, the algorithm specified will replace the existing algorithm in the record. If updating a record to remove authentication, specify an empty value for all three parameters.

Parameter	Description
encrypt_password={value}	(Optional and valid using SNMPv3) The password if privacy (data encryption) is to be used for SNMP communication. Maximum of 128 characters. These two parameters are used to specify privacy: encrypt_password and priv_alg. If creating a record and privacy will be used, it is required that both parameters are specified together. If updating a record to change the password, the password specified will replace the existing password in the record. If updating a record to remove privacy, specify an empty value for both parameters.
priv_alg={DES|AES}	(Optional and valid using SNMPv3) The algorithm to be used for privacy: DES or AES. This algorithm is used to encrypt and decrypt SNMP messages. These two parameters are used to specify privacy: encrypt_password and priv_alg. If creating a record and privacy will be used, it is required that both parameters are specified together. If updating a record to change the privacy algorithm, the algorithm specified will replace the existing algorithm in the record. If updating a record to remove privacy, specify an empty value for both parameters.
security_engine_id={value}	(Optional and valid using SNMPv3) The security engine ID when a security engine is part of the target host configuration. A valid ID is required. A maximum of 128 characters may be specified. If a security engine ID is part of the target host configuration, the parameter security_engine_id must be defined for the record in order for authentication to be successful. If the security engine ID is not defined (and is required by the target host for all SNMP requests), then the SNMP service may not be detected on the target host and authentication will fail.
context_engine_id={value}	(Optional and valid using SNMPv3) The context engine ID used in scoped PDUs when a context is part of the target host configuration. A valid ID is required. A maximum of 128 characters may be specified. If an SNMP context is part of the target host configuration, the parameters context_engine_id and/or context must be defined for the record in order for the scanning engine to retrieve context-sensitive information from the target host.

Parameter	Description
context={value}	(Optional and valid using SNMPv3) The context name used in scoped PDUs when a context is part of the target host configuration. A maximum of 128 characters may be specified. If an SNMP context is part of the target host configuration, the parameters context_engine_id and/or context must be defined for the record in order for the scanning engine to retrieve context-sensitive information from the target host.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create SNMP record, using SNMPv3

API request:

```
curl -H "X-Requested-With: Curl Sample" -d
"action=create&title=My+Record&version=v3&username=user&password=<
PASSWORD>&auth_alg=MD5&encrypt_password=<PASSWORD>&priv_alg=DES&se
curity_engine_id=0x80001F88805131F121BD9B194B&context_engine_id=0x
80001F88805131F121BD9B194B&context=bridge1&ips=10.10.10.2-
10.10.10.4"
-b "QualysSession=a3863e31b486417f81eea7f8881f3142; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/auth/snmp/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-02-27T06:22:01Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125726</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update an SNMP record

Change the user name and password for authentication and the target IPs.

```
curl -H "X-Requested-With: Curl Sample" -d
"action=update&ids=65319&username=user2&password=<PASSWORD>&ips=10
.10.10.5-10.10.10.6"
-b "QualysSession=a3863e31b486417f81eea7f8881f3142; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/auth/snmp/"
```

DTDs for auth type “snmp”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/snmp/auth_snmp_list_output.dtd

Sybase Record

For API version information, refer to the API Version History section.

V2.0 | V3.0

V2.0

/api/2.0/fo/auth/sybase/

[POST]

Create, update, list and delete Sybase records for authenticating to Sybase Adaptive Server Enterprise (ASE) instances. Sybase auth records are supported for VM & PC.

Requirement - You must configure login credentials on target hosts before scanning.

Download Qualys User Guide - Sybase Authentication (.zip)

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to Sybase database instances.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Sybase	
port={value}	(Required to create record) The port the Sybase database is on.
database={value}	(Optional to create and update record) The name of the Sybase database you want to authenticate to.

Parameter	Description
auto_discover_databases={**0**|1}	Specify auto_discover_databases=1 and we will find all Sybase database instances on the target host. This means you no longer have to create a separate Sybase record for each database name. Create one record with Auto Discover Databases enabled to authenticate to multiple databases on the same host. Note you must either enter a database name (with existing database parameter) OR use the Auto Discover option. When unspecified (auto_discover_databases=0), we will not auto discover database instances and look for the database name that you have entered in the database parameter.
installation_dir={value}	(Required for create request if this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a Sybase account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the Sybase account to be used for authentication. Maximum 100 characters (ascii).
password_encryption={**0**|1}	(Optional to create or update record) Enable this option when your Sybase database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail. When set to 1, password encryption is enabled in the Sybase record.When set to 0 (the default), password encryption is not enabled.
login_type=vault	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
Target Hosts	

Parameter	Description
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create Sybase Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=sybase_record&network_id=19015&username=acme_
ac12&password=<PASSWORD>&port=444&database=sybaseDB1&ips=10.10.24.
12,10.10.24.13,10.10.24.15&installation_dir=/dir123&comments=This%
20Sybase%20comments"
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-10T20:52:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
```

```
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Sybase Record, with vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=CYBER_ARK_DIGITAL_PIM_Vault_Sample&vault_id=1
39249&login_type=vault&vault_type=CyberArk%20PIM%20Suite&folder=Ro
ot&file=passwd_abc123&installation_dir=C://dir1/win/vault&username
=Syb_User&port=456&database=Syb_db_CyberArkSuite&ips=10.10.25.81-
10.10.25.82&comments=sybase_vault_comments"
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>88888</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Sybase Record to enable password encryption and auto discovery

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=sybase_record&network_id=19015&username=acme_
ac12&password=<PASSWORD>&password_encryption=1&ips=10.10.24.12&aut
o_discover_databases=1&port=444&installation_dir=/dir123&comments=
This%20
```

```
Sybase%20comments"
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-04-18T15:45:05Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>43025</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Sybase Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=update&ids=78782&add_ips=10.10.26.238&installation_dir=C:/
/user/dir"
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" >
file.xml
```

Sample - List Sybase records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list&details=All"
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" >
file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SYBASE_LIST_OUTPUT SYSTEM
"https://https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/auth_
sybase_list_output.dtd">
<AUTH_SYBASE_LIST_OUTPUT>
  <RESPONSE>
```

```
<DATETIME>2017-04-10T21:32:21Z</DATETIME>
<AUTH_SYBASE_LIST>
  <AUTH_SYBASE>
    <ID>78177</ID>
    <TITLE><![CDATA[api_syb_basic_2IPs_NW2]]></TITLE>
    <USERNAME><![CDATA[api_user1]]></USERNAME>
    <DATABASE><![CDATA[api_sybDB1]]></DATABASE>
    <PORT>444</PORT>
    <IP_SET>
      <IP_RANGE>10.10.24.12-10.10.24.13</IP_RANGE>
    </IP_SET>
    <NETWORK_ID>19019</NETWORK_ID>
    <CREATED>
      <DATETIME>2017-04-08T00:17:17Z</DATETIME>
      <BY>enter_ss</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2017-04-08T00:17:17Z</DATETIME>
    </LAST_MODIFIED>
  </AUTH_SYBASE>
  <AUTH_SYBASE>
    <ID>78186</ID>
    <TITLE><![CDATA[api_syb_basic_2IPs_Global]]></TITLE>
    <USERNAME><![CDATA[api_user1]]></USERNAME>
    <DATABASE><![CDATA[api_sybDB1]]></DATABASE>
    <PORT>444</PORT>
    <IP_SET>
      <IP_RANGE>10.10.24.12-10.10.24.13</IP_RANGE>
    </IP_SET>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
      <DATETIME>2017-04-08T01:10:04Z</DATETIME>
      <BY>enter_ss</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2017-04-08T01:10:04Z</DATETIME>
    </LAST_MODIFIED>
  </AUTH_SYBASE>
```

DTDs for auth type “sybase”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/sybase/auth_sybase_list_output.dtd

V3.0

/api/3.0/fo/auth/sybase/

[POST]

Create, update, list and delete Sybase records for authenticating to Sybase Adaptive Server Enterprise (ASE) instances. Sybase auth records are supported for VM & PC.

Requirement - You must configure login credentials on target hosts before scanning.

Download Qualys User Guide - Sybase Authentication (.zip)

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to Sybase database instances.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Sybase	
port={value}	(Required to create record) The port the Sybase database is on.
database={value}	(Optional to create and update record) The name of the Sybase database you want to authenticate to.
auto_discover_databases={**0**|1}	Specify auto_discover_databases=1 and we will find all Sybase database instances on the target host. This means you no longer have to create a separate Sybase record for each database name. Create one record with Auto Discover Databases enabled to authenticate to multiple databases on the same host. Note you must either enter a database name (with existing database parameter) OR use the Auto Discover option. When unspecified (auto_discover_databases=0), we will not auto discover database instances and look for the database name that you have entered in the database parameter.

Parameter	Description
installation_dir={value}	(Required for create request if this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.
ssl_verify={0|1}	(Optional) SSL verification. 1 - If set to 1, verify if the certificate of the server is valid and that it can be trusted. 0 - If set to 0, no verification is required for the server certificate validation.
hosts = {value}	(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If password is specified this is the username of a Sybase account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the Sybase account to be used for authentication. Maximum 100 characters (ascii).
password_encryption={0|1}	(Optional to create or update record) Enable this option when your Sybase database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail. When set to 1, password encryption is enabled in the Sybase record.When set to 0 (the default), password encryption is not enabled.
login_type=vault	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.

Parameter	Description
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - List Sybase Record

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u"johnd:PassW@123" -d
"action=list&ids=5555555"
"https://<qualys_base_url>/api/3.0/fo/auth/sybase/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SYBASE_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/auth/sybase/auth_sybase_list
_output.dtd">
<AUTH_SYBASE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2024-08-09T06:58:23Z</DATETIME>
        <AUTH_SYBASE_LIST>
            <AUTH_SYBASE>
                <ID>5555555</ID>
                <TITLE>
                    <![CDATA[sybase_auth_apiup]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[abcup]]>
                </USERNAME>
                <DATABASE>
                    <![CDATA[dbup]]>
                </DATABASE>
                <PORT>67</PORT>
                <INSTALLATION_DIR>
                    <![CDATA[/opt/update]]>
```

```
                    </INSTALLATION_DIR>
                    <SSL_VERIFY>true</SSL_VERIFY>
                    <HOSTS>
                        <HOST>
                            <![CDATA[agavaa]]>
                        </HOST>
                    </HOSTS>
                    <IP_SET>
                        <IP>1.1.1.1</IP>
                    </IP_SET>
                    <CREATED>
                        <DATETIME>2024-08-09T06:53:53Z</DATETIME>
                        <BY>jon_dre</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2024-08-09T06:56:43Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_SYBASE>
            </AUTH_SYBASE_LIST>
        </RESPONSE>
    </AUTH_SYBASE_LIST_OUTPUT>
```

Sample - Create Sybase Record

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "johnd:PassW@123" -
d
"action=create&title=sybase_auth_api&username=jon&password=passw@1
23&database=db&port=67&ips=1.1.1.1&ssl_verify=1&hosts=abc.com,qa&i
nstallation_dir=/opt"
"https://<qualys_base_url>/api/3.0/fo/auth/sybase/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2024-08-09T06:53:53Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>5555555</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Sybase Record

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "johnd:PassW@123" -
d
"action=update&title=sybase_auth_apiupdate&username=abcupdate&pass
word=123m&database=dbupdate&port=677&ids=5256516&ssl_verify=1&host
s=abc.com" "https://<qualys_base_url>/api/3.0/fo/auth/sybase/" >
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2024-08-05T06:13:55Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>5555555</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Sybase Record

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "johnd:PassW@123" -
d "action=delete&ids=5555555"
"https://<qualys_base_url>/api/3.0/fo/auth/sybase/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
```

```
            <DATETIME>2024-08-05T06:37:28Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Deleted</TEXT>
                    <ID_SET>
                        <ID>5555555</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

DTDs for auth type “sybase”

<platform API server>/api/3.0/batch_return.dtd

<platform API server>/api/3.0/fo/auth/sybase/auth_sybase_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/auth/sybase/	Active	Active
/api/2.0/fo/auth/sybase/	December 2025	December 2026

Tomcat Server Records

For API version information, refer to the API Version History Section

V2.0 | V3.0

V2.0

/api/2.0/fo/auth/tomcat/

[GET POST]

Create, update, list and delete Tomcat server records.

Supported Server

API URL	Supported Versions
/auth/tomcat/	Windows: Apache Tomcat 7.x, 8.x and 9.x Unix: Apache Tomcat 6.x, 7.x, 8.x and 9.x; VMware vFabric tc Server 2.9.x; Pivotal tc Server 3.x Vulnerability and Compliance scans are supported (using VM, PC)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete or list. See List Auth Records for type
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required for create) The title of the Server record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional)User defined notes about the Server record. The comments may include a maximum of 1999 characters (ascii); if comments have 2000 or more characters an error is returned and comments are not saved. Tags (such as <script>) cannot be included; if tags are included an error is returned and the request fails.
Application Server	

Parameter	Description
unix_installation_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record) The directory where the WebSphere application is installed.
unix_installation_dir={value}	(Required to create Tomcat Server record; valid only for this record) The directory where the tomcat server is installed. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_HOME) /opt/vmware/vfabric-tc-server-standard /opt/pivotal/pivotal-tc-server-standard
instance_path={value}	(Optional to create or update Tomcat Server record; valid only for this record) The directory where the tomcat server instance(s) are installed. You can specify a single tomcat instance (use with auto_discover_instances=0), or multiple instances (use with auto_discover_instances=1). Leave unspecified when the instance directory is the same as the installation directory or when your targets have different types of tomcat servers. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_BASE) /opt/vmware/vfabric-tc-server-standard/tc1 /opt/pivotal/pivotal-tc-server-standard/tc1
auto_discover_instances={0|1}	(Optional to create or update Tomcat Server record; valid only for this record) Specify auto_discover_instances=1 and we'll find all tomcat server instances for you. Applies to VMware vFabric and Pivotal when you've specified a directory with multiple instances or you did not specify an instance. When unspecified (auto_discover_instances=0), we will not auto discover instances. Applies to Apache Tomcat or when you've specified a single instance.
installation_path_windows	(Required to create Tomcat Server record on Windows; valid only for this record) The directory where the tomcat server is installed. Example: C:\tomcat\apache-tomcat-8.5.11

Parameter	Description
instance_path_windows	(Optional to create or update Tomcat Server record on UNIX; valid only for this record) The directory where the tomcat server instance(s) are installed. Example: C:\tomcat\apache-tomcat-8.5.11
service_name	(Optional) The Tomcat service name that identifies the server instance to be authenticated to.
Target Hosts	
ips={value}	(Required to create record) Add IP addresses of the hosts you want to scan using this record.
add_ips={value}	(Optional and valid only to update record) Add IP address(es) to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create Tomcat Server

API request:

```
curl
'<qualys_base_url>/api/2.0/fo/auth/tomcat/?action=create&installation_pat
h_windows=C:\tomcat\apache-tomcat-
8.5.11&instance_path_windows=C:\tomcat\apache-tomcat-
7.0.75&service_name=Tomcat7&ips=xx.xx.xx.xx&echo_request=1&title=API_TEST
_854_1786106317044' -X POST
-H 'Content-Type: application/json'
-H 'X-Requested-With: curl demo32'
-H 'Cache-Control: no-cache' -H 'Accept: */*'
-H 'Accept-Encoding: gzip, deflate, br'
-H 'Content-Length: 0' -u '<username>:<password>' --compressed -v
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <REQUEST>
            <DATETIME>2026-08-07T12:56:38Z</DATETIME>
            <USER_LOGIN>apaut_mm</USER_LOGIN>
            <RESOURCE>
                <qualys_base_url>/api/2.0/fo/auth/tomcat/
                </RESOURCE>
                <PARAM_LIST>
                    <PARAM>
```

```
                <KEY>action</KEY>
                <VALUE>create</VALUE>
            </PARAM>
            <PARAM>
                <KEY>installation_path_windows</KEY>
                <VALUE>C:\tomcat\apache-tomcat-8.5.11</VALUE>
            </PARAM>
            <PARAM>
                <KEY>instance_path_windows</KEY>
                <VALUE>C:\tomcat\apache-tomcat-7.0.75</VALUE>
            </PARAM>
            <PARAM>
                <KEY>service_name</KEY>
                <VALUE>Tomcat7</VALUE>
            </PARAM>
            <PARAM>
                <KEY>ips</KEY>
                <VALUE>xx.xx.xx.xx</VALUE>
            </PARAM>
            <PARAM>
                <KEY>echo_request</KEY>
                <VALUE>1</VALUE>
            </PARAM>
            <PARAM>
                <KEY>title</KEY>
                <VALUE>API_TEST_854_1786106317044</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2026-08-07T12:56:38Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>9535912</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <REQUEST>
            <DATETIME>2026-08-07T12:56:38Z</DATETIME>
            <USER_LOGIN>apaut_mm</USER_LOGIN>
            <RESOURCE>
                <qualys_base_url>/api/2.0/fo/auth/tomcat/
                </RESOURCE>
                <PARAM_LIST>
                    <PARAM>
                        <KEY>action</KEY>
```

```
                                <VALUE>create</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>installation_path_windows</KEY>
                                <VALUE>C:\tomcat\apache-tomcat-
8.5.11</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>instance_path_windows</KEY>
                                <VALUE>C:\tomcat\apache-tomcat-
7.0.75</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>service_name</KEY>
                                <VALUE>Tomcat7</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>ips</KEY>
                                <VALUE>xx.xx.xx.xx</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>echo_request</KEY>
                                <VALUE>1</VALUE>
                            </PARAM>
                            <PARAM>
                                <KEY>title</KEY>
                                <VALUE>API_TEST_854_1786106317044</VALUE>
                            </PARAM>
                        </PARAM_LIST>
                    </REQUEST>
                    <RESPONSE>
                        <DATETIME>2026-08-07T12:56:38Z</DATETIME>
                        <BATCH_LIST>
                            <BATCH>
                                <TEXT>Successfully Created</TEXT>
                                <ID_SET>
                                    <ID>9535912</ID>
                                </ID_SET>
                            </BATCH>
                        </BATCH_LIST>
                    </RESPONSE>
                </BATCH_RETURN>
```

Sample - Update Tomcat Server

API request:

```
curl '
<qualys_base_url>/api/2.0/fo/auth/tomcat/?action=update&installation_path
_windows=C:\tomcat\apache-tomcat-
8.5.12&instance_path_windows=C:\tomcat\apache-tomcat-
7.0.76&comments=Updated through API
v2.0&service_name=Tomcat8&ids=12868585' -X POST
-H 'Content-Type: application/json'
```

```
-H 'X-Requested-With: curl demo95'
-H 'Cache-Control: no-cache' -H 'Accept: */*'
-H 'Accept-Encoding: gzip, deflate, br'
-H 'Content-Length: 0' -u '
    <username>:<password>' --compressed -v
```

API Response

```
<<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/api/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2026-08-07T16:36:27Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>9535519</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - List Tomcat Server

API request:

```
curl '<qualys_base_url>/api/2.0/fo/auth/tomcat/?action=list&details=All'
-X POST
-H 'Content-Type: application/json'
-H 'X-Requested-With: curl demo344'
-H 'Cache-Control: no-cache' -H 'Accept: */*'
-H 'Accept-Encoding: gzip, deflate, br'
-H 'Content-Length: 0' -u '<username>:<password>' --compressed -v
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_TOMCAT_LIST_OUTPUT SYSTEM "
<qualys_base_url>/api/2.0/fo/auth/tomcat/auth_tomcat_list_output.dtd">
    <AUTH_TOMCAT_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-08-07T13:29:13Z</DATETIME>
            <AUTH_TOMCAT_LIST>
                <AUTH_TOMCAT>
                    <ID>9535519</ID>
                    <TITLE>
                        <![CDATA[API_TEST_4555_1786106317024]]>
                    </TITLE>
                    <IP_SET>
                        <IP>10.10.29.87</IP>
                    </IP_SET>
                    <INSTALLATION_PATH_WINDOWS>
                        <![CDATA[C:\tomcat\apache-tomcat-8.5.11]]>
```

```
                    </INSTALLATION_PATH_WINDOWS>
                    <CREATED>
                        <DATETIME>2026-08-07T12:41:36Z</DATETIME>
                        <BY>apaut_mm</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-08-07T12:41:36Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                </AUTH_TOMCAT>
                <AUTH_TOMCAT>
                    <ID>9535912</ID>
                    <TITLE>
                        <![CDATA[API_TEST_854_1786106317044]]>
                    </TITLE>
                    <IP_SET>
                        <IP>xx.xx.xx.xx</IP>
                    </IP_SET>
                    <INSTALLATION_PATH_WINDOWS>
                        <![CDATA[C:\tomcat\apache-tomcat-8.5.11]]>
                    </INSTALLATION_PATH_WINDOWS>
                    <INSTANCE_PATH_WINDOWS>
                        <![CDATA[C:\tomcat\apache-tomcat-7.0.75]]>
                    </INSTANCE_PATH_WINDOWS>
                    <SERVICE_NAME_WINDOWS>
                        <![CDATA[Tomcat7]]>
                    </SERVICE_NAME_WINDOWS>
                    <CREATED>
                        <DATETIME>2026-08-07T12:56:38Z</DATETIME>
                        <BY>apaut_mm</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-08-07T12:56:38Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                </AUTH_TOMCAT>
            </AUTH_TOMCAT_LIST>
        </RESPONSE>
    </AUTH_TOMCAT_LIST_OUTPUT>
```

Sample - Delete Tomcat Server

API request:

```
curl '<qualys_base_url>/api/2.0/fo/auth/tomcat/?action=delete&ids=3422' -
X POST
-H 'Content-Type: application/json'
-H 'X-Requested-With: curl demo32'
-H 'Cache-Control: no-cache' -H 'Accept: */*'
-H 'Accept-Encoding: gzip, deflate, br'
-H 'Content-Length: 0' -u '<username>:<password>' --compressed -v
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-08-07T17:39:17Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>9535519</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type "tomcat"

<platform API server>/api/2.0/fo/auth/tomcat./auth_tomcat_list_output.dtd

V3.0

api/3.0/fo/auth/tomcat/

[GET POST]

Create, update, list and delete Tomcat server records.

Supported Server

API URL	Supported Versions
/auth/tomcat/	Windows: Apache Tomcat 7.x, 8.x and 9.x Unix: Apache Tomcat 6.x, 7.x, 8.x and 9.x; VMware vFabric tc Server 2.9.x; Pivotal tc Server 3.x Vulnerability and Compliance scans are supported (using VM, PC)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete or list. See List Auth Records for type
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.

Parameter	Description
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required for create) The title of the Server record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional)User defined notes about the Server record. The comments may include a maximum of 1999 characters (ascii); if comments have 2000 or more characters an error is returned and comments are not saved. Tags (such as <script>) cannot be included; if tags are included an error is returned and the request fails.
Application Server	
unix_installation_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record) The directory where the WebSphere application is installed.
unix_installation_dir={value}	(Required to create Tomcat Server record; valid only for this record) The directory where the tomcat server is installed. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_HOME) /opt/vmware/vfabric-tc-server-standard /opt/pivotal/pivotal-tc-server-standard
instance_path={value}	(Optional to create or update Tomcat Server record; valid only for this record) The directory where the tomcat server instance(s) are installed. You can specify a single tomcat instance (use with auto_discover_instances=0), or multiple instances (use with auto_discover_instances=1). Leave unspecified when the instance directory is the same as the installation directory or when your targets have different types of tomcat servers. Examples: /opt/apache-tomcat-7.0.57 (e.g. $CATALINA_BASE) /opt/vmware/vfabric-tc-server-standard/tc1 /opt/pivotal/pivotal-tc-server-standard/tc1

Parameter	Description
auto_discover_instances={0|1}	(Optional to create or update Tomcat Server record; valid only for this record) Specify auto_discover_instances=1 and we'll find all tomcat server instances for you. Applies to VMware vFabric and Pivotal when you've specified a directory with multiple instances or you did not specify an instance. When unspecified (auto_discover_instances=0), we will not auto discover instances. Applies to Apache Tomcat or when you've specified a single instance.
installation_path_windows	(Required to create Tomcat Server record on Windows; valid only for this record) The directory where the tomcat server is installed. Example: C:\tomcat\apache-tomcat-8.5.11
instance_path_windows	(Optional to create or update Tomcat Server record on UNIX; valid only for this record) The directory where the tomcat server instance(s) are installed. Example: C:\tomcat\apache-tomcat-8.5.11
service_name	(Optional) The Tomcat service name that identifies the server instance to be authenticated to.
Target Hosts	
ips={value}	(Required to create record) Add IP addresses of the hosts you want to scan using this record.
add_ips={value}	(Optional and valid only to update record) Add IP address(es) to the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional and valid only to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Parameter	Description
asset_type={ips|asset_tags|ip_range_tag_rule}	(Optional) Indicates how assets will be defined in the record. Valid values are ips (the default), asset_tags, ip_range_tag_rule. When not specified, we will use asset_type=ips. ips - Specify this value to assign IP addresses/ranges to the record asset_tags - Specify this value to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. ip_range_tag_rule - Specify this value to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that do not already have the tag assigned.
tag_set_by={id|name}	(Optional when assetSpecify "id" (the default) to select a tag set by providing tag ids. Specify "name" to select a tag set by providing tag names._type=asset_tags or ip_range_tag_rule)
tags_include={tag1, tag2...}	(Required when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to include in the record. Hosts that match these tags will be included. You identify the tag set by providing tag names or IDs. Multiple entries are comma-separated. To specify tag names, you must also specify tag_set_by=name.
tags_exclude={tag1, tag2...}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to exclude in the record. Hosts that match these tags will be excluded. You identify the tag set by providing tag names or IDs. Multiple entries are comma-separated. To specify tag names, you must also specify tag_set_by=name.
tag_include_selector={any|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={any|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.

Sample - Create Tomcat Server with Asset tags (by Name)

API request:

```
ccurl --location --request POST '
<qualys_base_url>/api/3.0/fo/auth/tomcat/?action=create&instance_path=%2F
opt%2Fapach1e-tsomcat2-
api&auto_discover_instances=1&echo_request=1&installation_path=%2Fopt%2Fp
```

```
ivotal%2Fpivotal-t2c-server-standsard1-
api&title=API_TEST_2323_1779296368160&asset_type=asset_tags&tag_set_by=na
me&tags_include=Cloud%20Agent&tags_exclude=Cloud%20Agent' \
--header 'Content-Type: application/json' \
--header 'X-Requested-With: curl demo28' \
--header 'Cache-Control: no-cache' \
--header 'Accept: */*' \
--header 'Accept-Encoding: gzip, deflate, br' \
--header 'Content-Length: 0'
```

API Response

```
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/api/3.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2026-05-20T12:03:11Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>8904935</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update Tomcat Server with with IP Range Tage Rule IDs

API request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST <qualys_base_url>/api/3.0/fo/auth/tomcat/?action=update\
&ids=<AUTH_RECORD_ID>\
&asset_type=ip_range_tag_rule\
&tag_set_by=id\
&tags_include=401,402\
&tags_exclude=403"
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-22T10:23:42Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8927402</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
```

```
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Tomcat Server

API request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST "<qualys_base_url>/api/3.0/fo/auth/tomcat/?action=list"
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_TOMCAT_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/auth/tomcat/auth_tomcat_list_output.dtd">
<!-- This report was generated with an evaluation version of Qualys //-->
<AUTH_TOMCAT_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-22T13:20:54Z</DATETIME>
        <AUTH_TOMCAT_LIST>
            <AUTH_TOMCAT>
                <ID>8929417</ID>
                <TITLE>
                    <![CDATA[API_TEST_2323_1779296368160]]>
                </TITLE>
                <TAGS>
                    <TAG_TYPE>asset_tags</TAG_TYPE>
                    <TAGS_INCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>8214418</ID>
                            <NAME>Exc_1</NAME>
                        </TAG>
                    </TAGS_INCLUDE>
                    <TAGS_EXCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>7612812</ID>
                            <NAME>Cloud Agent</NAME>
                        </TAG>
                    </TAGS_EXCLUDE>
                </TAGS>
                <INSTALLATION_PATH>
                    <![CDATA[/opt/pivotal/pivotal-t2c-server-standsard1-
api]]>
                </INSTALLATION_PATH>
                <INSTANCE_PATH>
                    <![CDATA[/opt/apach1e-tsomcat2-api]]>
                </INSTANCE_PATH>
                <AUTO_DISCOVER_INSTANCES>1</AUTO_DISCOVER_INSTANCES>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2026-05-22T13:20:37Z</DATETIME>
                    <BY>mayur_aa</BY>
                </CREATED>
```

```
                    <LAST_MODIFIED>
                        <DATETIME>2026-05-22T13:20:37Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                </AUTH_TOMCAT>
            </AUTH_TOMCAT_LIST>
        </RESPONSE>
    </AUTH_TOMCAT_LIST_OUTPUT>
```

DTDs for auth type “tomcat”

<platform API server>/api/3.0/fo/auth/tomcat/auth_tomcat_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/auth/tomcat/	Active	Active
/api/2.0/fo/auth/tomcat/	December 2025	December 2026

Unix Record

For API version information, refer to the API Version History section

V2.0 | V3.0 | V4.0

V2.0

/api/2.0/fo/auth/unix/

[POST]

Create, update, list and delete Unix records for authenticated scans of hosts running on Unix, Cisco and Checkpoint Firewall. Vulnerability and compliance scans are supported on Unix and Cisco systems (using VM, PC). Compliance scans are supported on Checkpoint Firewall systems (using PC).

Download Qualys User Guide - Unix Authentication (pdf)

Input Parameters

Parameters: Request | Login credentials| Unix only | Target Hosts

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
sub_type={cisco|checkpoint_firewall}	(Required for hosts running on Cisco or Checkpoint Firewall) Choose cisco or checkpoint_firewall if you're scanning one of these system types.
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
port={value}	(Optional and valid for compliance scans only) Custom ports to be used to perform authenticated compliance assessment (control testing). Ports Used For Unix Compliance Scans
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).

Parameter	Description
password={value}	(To create record password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication when a vault will not be used. Maximum 100 characters (ascii).
login_type={**basic**|vault}	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
cleartext_password={**0**|1}	(Optional) When not specified, the scanning engine only uses strong password encryption for remote login. Specify 1 to allow your password to be transmitted in clear text when connecting to services which do not support strong password encryption. For more info, search for "Clear Text Password" in online help. For a create request, if cleartext_password=1, the password parameter is required. For an update request, if cleartext_password=1, and the record does not have a password set, then cleartext_password=1 is *silently ignored*.
skip_password={**0**|1}	(Optional and valid only for Unix record, i.e not supported for Cisco or Checkpoint Firewall sub-type) By default when only the required parameters are set (title, username, ips) the login account password is set to the empty password. You can set skip_password=1 if the login account does not have a password. When set it's not possible to set the empty password, another password using the "password" parameter, or password in a vault.
enable_password={value}	(Optional and valid only for Cisco sub-type) The password required for executing the "enable" command on the target hosts. Maximum 100 characters (ascii). Note: The pooled credentials feature is not supported if the "enable" command requires a password and it is specified using the enable_password parameter.
expert_password={value}	(Optional and valid only for Checkpoint Firewall sub-type) The password required for executing the "expert" command on the target hosts. Maximum 100 characters (ascii).

Parameter	Description
target_type={value}	(Optional) Specify the target type. You can choose from the following values: - A10 - HP_COMWARE - CISCO_ASA_WITH_FIREPOWE - auto (default)
Kerberos/GSSAPI authentication details, if it is enabled for the target host	
use_kerberos={0|1}	(Optional) Specify 1 to enable Kerberos authentication. By default, the value is set to 0.
realm_discovery={value}	(Mandatory, if 'use_kerberos=1') Specify the realm discovery method. The available values are manual, single, and DNS.
user_realm={value}	(Mandatory, if 'use_kerberos=1') Specify the name of the realm that a user belongs to.
service_realm={value}	(Mandatory, if 'use_kerberos=1') Specify the name of the realm that the service belongs to, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the "realm_discovery" parameter is set to "manual".
service_kdc={value}	(Optional) Specify the KDC that manages authentication for the service in its realm, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the "realm_discovery" parameter is set to "manual".
user_kdc={value}	(Optional) Specify the KDC (Key Distribution Center) that is responsible for authenticating users and issuing ticket-granting tickets (TGTs) for the realm.
krb5_password={value}	(Mandatory, if 'use_kerberos= 1') Enter the password to authenticate to the Kerberos Key Distribution Center (KDC).
krb5_login_type={value}	(Optional) Specify the type of login used to authenticate to the Kerberos Key Distribution Center (KDC). The available values are "basic" and "vault".
krb5_<vaultparameters>={value}	(Mandatory, if krb5_login_type =vault) If krb5_login_type is 'vault', then all vault parameter fields must be added with the prefix 'krb5_'. For example, krb5_vault_type, krb5_vault_id, etc. The vault-specific parameters depend on the vault type you have selected. See the "Vault Definition" section in the API user guide.

Parameter	Description
Unix only	
{XML File}	(Optional and valid only for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) XML file where you define private-key certificates and root delegations. These are defined using this DTD: <platform API server>/api/2.0/fo/auth/unix/unix_auth_params.dtd
use_agentless_tracking=[**0**|1}	((Optional and valid for Unix record only, i.e. not supported for Cisco or Checkpoint Firewall sub-type) Specify 1 to enable Agentless Tracking.
agentless_tracking_path={value}	(Required if use_agentless_tracking=1 for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) The pathname where you would like the service to store the host ID file on each host. This is required to enable Agentless Tracking for Unix.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Parameter	Description
Target Hosts with Tag Support	Note: Applicable only when you have Asset Tagging and Tag Support for Authentication Records enabled for your subscription.
asset_type={**ips**|asset_tags|ip_range_tag_rule}	(Optional) Indicates how assets will be defined in the record. Valid values are ips (the default), asset_tags, ip_range_tag_rule. When not specified, we'll use asset_type=ips ips - Specify this value to assign IP addresses/ranges to the record. asset_tags - Specify this value to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. ip_range_tag_rule - Specify this value to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that don't already have the tag assigned.
tag_set_by={**id**|name}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tags_include={tag1,tag2...}	(Required when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to include in the record. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tags_exclude={tag1,tag2,...}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to exclude from the record. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tag_include_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.

Parameter	Description
ips={value}	(Required to create record when asset_type=ips or asset_type is not specified) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record when asset_type=ips) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record when asset_type=ips) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record when asset_type=ips) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Ports Used For Unix Compliance Scans

The actual ports used for compliance scanning (Unix, Cisco, Checkpoint Firewall) depends on scan settings in 1) compliance option profile, and 2) Unix authentication record as indicated.

Compliance Option Profile	Authentication Record	Ports Scanned
Standard Scan	UI; Well Known Ports API: no "port" parameter	~ 1900 Ports (includes Ports 22, 23, 513)
Standard Scan	UI: Custom Ports API: "port" parameter	~ 1900 Ports + Custom Ports in record
Targeted Scan	UI: Well Known Ports API: no "port" parameter	Ports 22, 23 and 513 only
Targeted Scan	UI: Custom Ports API: "port" parameter	Custom Ports in record

Sample - Create Unix record, with password

Applies to record type Unix, Cisco and Checkpoint Firewall

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
```

```
"<qualys_base_url>/api/2.0/fo/auth/unix/?action=create&title=Unix&usernam
e=root&password=<PASSWORD>&ips=10.10.36.63"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12345</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix record, root delegation tools and vault

Applies to record type Unix only (not sub-types)

API request:

```
curl -H "X-Requested-With: curl" -H "Content-type:text/xml" -u
"USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?action=create&title=U
nix&vault&username=Qualys&ips=10.113.195.152&port=5857&login_type=vault&v
ault_type=LiebermanERPM&vault_id=10873203&auto_discover_system_name=0&sys
tem_name_single_host=a&custom_system_type=custom&system_type=custom"
--data-binary @add_params.xml
```

add_params.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS>
        <ROOT_TOOL>
            <STANDARD_TYPE type="pimsu"/>
            <PASSWORD_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[root]]></VAULT_USERNAME>
                    <VAULT_TYPE>Thycotic Secret Server</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
<SECRET_NAME><![CDATA[super_secret_name]]></SECRET_NAME>
                </DIGITAL_VAULT>
            </PASSWORD_INFO>
        </ROOT_TOOL>
        <ROOT_TOOL>
            <CUSTOM_TYPE><![CDATA[test]]></CUSTOM_TYPE>
            <PASSWORD_INFO type="basic">
                <PASSWORD><![CDATA[password]]></PASSWORD>
```

```
            </PASSWORD_INFO>
        </ROOT_TOOL>
    </ROOT_TOOLS>
    <PRIVATE_KEY_CERTIFICATES>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_TYPE>CyberArk AIM</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
                    <FOLDER><![CDATA[folder]]></FOLDER>
                    <FILE><![CDATA[file]]></FILE>
                </DIGITAL_VAULT>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic">
                <PASSPHRASE><![CDATA[passphrase]]></PASSPHRASE>
            </PASSPHRASE_INFO>
        </PRIVATE_KEY_CERTIFICATE>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,F9A653E2D12E019357B349B6EEE068B1
FiLfGHOc0rREmC0cBPsiyqqaitPNYTGeqKRmSBwGNrAzNTAcsKslsoY/WkMDW6QD
dLZNiGB0CFag94zyoMyCjyrdpayACAOWfH5w8VixxHF16Vxx5b6foLBE40FOYAIP
sdm1HvCfSFaN2dPf1Unb0erwjigjJNwYIV78529elE+2+dZIemi90ibh0R35NB60
TLeS3UUVezp/O9ZPLf0pqPPHnWgfW4GXp/SUpwojES9fCQE+BW4MMWHWu8XKtytt
....
-----END RSA PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[PASSPHRASE
USERNAME]]></VAULT_USERNAME>
                    <VAULT_TYPE>Quest Vault</VAULT_TYPE>
                    <VAULT_ID>35046922</VAULT_ID>
                  <SYSTEM_NAME><![CDATA[quest_system_name]]></SYSTEM_NAME>
                </DIGITAL_VAULT>
            </PASSPHRASE_INFO>
            <CERTIFICATE type="openssh">
                <![CDATA[ssh-rsa-cert-v01@openssh.com
AAAAHHNzaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgwR4bJSiBtJlOgCAQUF3yZ6Io2
WYfnBiOEsQ45RKbqLgAAAADAQABAAABAQC5sVLb7emh8/v2uHp6x1pN5R+MHQwz3A5M3GRKtu
uu1Njc/XYgqeWLMOJpbVtCVXwUcPgKt4Q0DmlGqc4uhZhzrdtpQGHrEivndNNLY9NQj7LozE7
x/sGiWdtmlucUh1teXMaBpM4aER9Y6uW5wv6ZylY7CAV9bcVz/ljlSypmjzkPjJ39AJq+QxZk
Iv+H4uh/T05LwHdilFrjWWwEoI8DV/DRIw3h8o4jhnj1QxBxyjad3efmFaejgRnY6cBW821gm
...
            </CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABCPiEUH5L3LZ
```

```
GInEw+h/m4+AAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQCpuwFVTYVmske0bd
FjSlYgsfvyCr7e5irIfoW7B8hNY0XJWyOEqZ5BzwPAEtzjua6m3vnqKPEQD1HyFdLse62JE7x
0jDXLr9bZ64THFpogERC/gI2aorrLKLxdr0K7u5wQUTm1L0xO7Y0hE9Bbi8ok++xTW+Ymf7Lb
VRLWVdN6kUBunIGow3W+tHIohPoUlw82QayZRa4iXpqpWVbh/9OMnb1raC
....
-----END OPENSSH PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
        </PRIVATE_KEY_CERTIFICATE>
    </PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12333</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with target type set to HP_COMWARE

Provide a target type while creating or updating the Unix (SSH2) authentication record.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?action=create&title=u
x-target-
type&username=root&ips=10.11.42.114&login_type=basic&password=<PASSWORD>&
target_type=HP_COMWARE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with Tags

In this sample, a new Unix record is created with asset_type=ip_range_tag_rule.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?action=create&title=u
nix&username=root&asset_type=ip_range_tag_rule&tags_include=7515612&tag_i
nclude_selector=all&tags_exclude=7514462&tag_exclude_selector=all"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-03-08T22:00:50Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>204020</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create unix auth record with Kerberos authentication details

API request:

```
curl --location --request POST
'https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?username=root&action=
create&ips=10.0.0.1&title=unix
krbsapi&use_kerberos=1&realm_discovery=manual&user_realm=realm.com&servic
e_realm=abc.com&service_kdc=kdc&user_kdc=kerbs&krb5_password=<PASSWORD>&k
rb5_login_type=basic'
--header 'X-Requested-With: portal'
--header 'Authorization: Basic <JWT token>'
```

API response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM"
https://qualysapi.qualys.com/api/2.0/fo/auth/unix/dtd/auth_list_output.dt
d">
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
```

```
<DATETIME>2023-02-13T04:08:26Z</DATETIME>
<AUTH_UNIX_LIST>
    <AUTH_UNIX>
        <ID>214497</ID>
        <TITLE>
            <![CDATA[krbs]]>
        </TITLE>
        <USERNAME>
            <![CDATA[root]]>
        </USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE>
            <![CDATA[Auto (default)]]>
        </TARGET_TYPE>
        <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
        <REALM_DISCOVERY>
            <![CDATA[manual]]>
        </REALM_DISCOVERY>
        <USER_REALM>
            <![CDATA[jsm.com]]>
        </USER_REALM>
        <USER_KDC>
            <![CDATA[kerbs.jsm.com]]>
        </USER_KDC>
        <SERVICE_REALM>
            <![CDATA[kerbs.jsm.com]]>
        </SERVICE_REALM>
        <SERVICE_KDC>
            <![CDATA[krb]]>
        </SERVICE_KDC>
        <IP_SET>
            <IP>0.0.0.0</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
            <DATETIME>2023-02-06T09:48:20Z</DATETIME>
            <BY>test_pq4</BY>
        </CREATED>
        <LAST_MODIFIED>
            <DATETIME>2023-02-06T12:30:33Z</DATETIME>
        </LAST_MODIFIED>
    </AUTH_UNIX>
    <AUTH_UNIX>
        <ID>214498</ID>
        <TITLE>
            <![CDATA[k1]]>
        </TITLE>
        <USERNAME>
            <![CDATA[root]]>
        </USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE>
```

```
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[manual]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[fwwqw]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[user]]>
                    </USER_KDC>
                    <SERVICE_REALM>
                        <![CDATA[s1sdd]]>
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[]]>
                    </SERVICE_KDC>
                    <KERBEROS_LOGIN_INFO type="vault">
                        <DIGITAL_VAULT>
                            <DIGITAL_VAULT_ID>
                                <![CDATA[55014]]>
                            </DIGITAL_VAULT_ID>
                            <DIGITAL_VAULT_TYPE>
                                <![CDATA[Quest Vault]]>
                            </DIGITAL_VAULT_TYPE>
                            <DIGITAL_VAULT_TITLE>
                                <![CDATA[quest]]>
                            </DIGITAL_VAULT_TITLE>
                            <VAULT_SYSTEM_NAME>
                                <![CDATA[fhk]]>
                            </VAULT_SYSTEM_NAME>
                        </DIGITAL_VAULT>
                    </KERBEROS_LOGIN_INFO>
                    <IP_SET>
                        <IP>0.0.0.0</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-02-06T12:54:00Z</DATETIME>
                        <BY>test_pq4</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2023-02-08T10:45:46Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
    </AUTH_UNIX_LIST_OUTPUT>
```

Sample - Update Unix auth record with target type CISCO_ASA_WITH_FIREPOWE

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
```

```
<qualys_base_url>/api/2.0/fo/auth/unix/?action=update&ids=149016&target_t
ype=CISCO_ASA_WITH_FIREPOWE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix auth record with to view updated target type

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?action=list&ids=149016
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/auth_unix_list_output.
dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-05-26T21:35:23Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>149016</ID>
                <TITLE>
                    <![CDATA[ux-target-type]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TARGET_TYPE>
                    <![CDATA[Cisco Adaptive Security Appliance with
FirePower]]>
                </TARGET_TYPE>
                <IP_SET>
                    <IP>10.11.42.114</IP>
                </IP_SET>
```

```
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
                        <BY>username</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
    </AUTH_UNIX_LIST_OUTPUT>
```

Sample - List Unix auth records

API request:

```
url -k -u agms_nb:Qatemp123# -s -S -H 'X-Requested-With:curl demo2' -d
"action=list" "<qualys_base_url>/api/2.0/fo/auth/unix/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/dtd/auth_list_output.d
td">
<AUTH_UNIX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-09-05T08:48:12Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>321277</ID>
        <TITLE><![CDATA[API_v2_END_TO_END_agms_nb_UNIX]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
          <ENABLED>0</ENABLED>
        </QUALYS_SHELL>
      </AUTH_UNIX>
 ...
<AUTH_UNIX>
        <ID>3382464</ID>
        <TITLE><![CDATA[unn]]></TITLE>
        <USERNAME><![CDATA[admin]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
```

```
<CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
<TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
<PRIVATE_KEY_CERTIFICATE_LIST>
  <PRIVATE_KEY_CERTIFICATE>
    <ID>2257361</ID>
    <PRIVATE_KEY_INFO type="basic">
      <PRIVATE_KEY type="pkcs8" />
    </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic" />
  </PRIVATE_KEY_CERTIFICATE>
  <PRIVATE_KEY_CERTIFICATE>
    <ID>2257360</ID>
    <PRIVATE_KEY_INFO type="basic">
      <PRIVATE_KEY type="pkcs8" />
    </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic" />
  </PRIVATE_KEY_CERTIFICATE>
  <PRIVATE_KEY_CERTIFICATE>
    <ID>2255896</ID>
    <PRIVATE_KEY_INFO type="basic">
      <PRIVATE_KEY type="pkcs8" />
    </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic" />
  </PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATE_LIST> <IP_SET>
  <IP>1.9.0.8</IP>
</IP_SET>
<NETWORK_ID>0</NETWORK_ID>
<CREATED>
  <DATETIME>2023-08-23T09:40:11Z</DATETIME>
  <BY>agms_nb</BY>
</CREATED>
<LAST_MODIFIED>
  <DATETIME>2023-08-24T10:04:07Z</DATETIME>
</LAST_MODIFIED>
<QUALYS_SHELL>
  <ENABLED>0</ENABLED>
</QUALYS_SHELL>
</AUTH_UNIX>
```

More Samples

Qualys API - Unix Authentication API samples (GitHub)

DTDs for auth type “unix”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/unix/auth_unix_list_output.dtd

For Unix type record type only, root delegation tools and private-key certificates are specified using the unix_auth_params.dtd here

<platform API server>/api/2.0/fo/auth/unix/unix_auth_params.dtd

V3.0

/api/3.0/fo/auth/unix/

[POST]

Create, update, list and delete Unix records for authenticated scans of hosts running on Unix, Cisco and Checkpoint Firewall. Vulnerability and compliance scans are supported on Unix and Cisco systems (using VM, PC). Compliance scans are supported on Checkpoint Firewall systems (using PC).

Download Qualys User Guide - Unix Authentication (pdf)

Input Parameters

Parameters: Request | Login credentials| Unix only | Target Hosts

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
sub_type={cisco|checkpoint_firewall}	(Required for hosts running on Cisco or Checkpoint Firewall) Choose cisco or checkpoint_firewall if you're scanning one of these system types.
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
port={value}	(Optional and valid for compliance scans only) Custom ports to be used to perform authenticated compliance assessment (control testing). Ports Used For Unix Compliance Scans
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication when a vault will not be used. Maximum 100 characters (ascii).
login_type={**basic**|vault}	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition

Parameter	Description
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
cleartext_password={**0**|1}	(Optional) When not specified, the scanning engine only uses strong password encryption for remote login. Specify 1 to allow your password to be transmitted in clear text when connecting to services which do not support strong password encryption. For more info, search for "Clear Text Password" in online help. For a create request, if cleartext_password=1, the password parameter is required. For an update request, if cleartext_password=1, and the record does not have a password set, then cleartext_password=1 is *silently ignored*.
skip_password={**0**|1}	(Optional and valid only for Unix record, i.e not supported for Cisco or Checkpoint Firewall sub-type) By default when only the required parameters are set (title, username, ips) the login account password is set to the empty password. You can set skip_password=1 if the login account does not have a password. When set it's not possible to set the empty password, another password using the "password" parameter, or password in a vault.
enable_password={value}	(Optional and valid only for Cisco sub-type) The password required for executing the "enable" command on the target hosts. Maximum 100 characters (ascii). Note: The pooled credentials feature is not supported if the "enable" command requires a password and it is specified using the enable_password parameter.
expert_password={value}	(Optional and valid only for Checkpoint Firewall sub-type) The password required for executing the "expert" command on the target hosts. Maximum 100 characters (ascii).
target_type={value}	(Optional) Specify the target type. You can choose from the following values: - A10 - HP_COMWARE - CISCO_ASA_WITH_FIREPOWE - auto (default)
Kerberos/GSSAPI authentication details, if it is enabled for the target host	
use_kerberos={0|1}	(Optional) Specify 1 to enable Kerberos authentication. By default, the value is set to 0.
realm_discovery={value}	(Mandatory, if 'use_kerberos=1') Specify the realm discovery method. The available values are manual, single, and DNS.

Parameter	Description
user_realm={value}	(Mandatory, if 'use_kerberos=1') Specify the name of the realm that a user belongs to.
service_realm={value}	(Mandatory, if 'use_kerberos=1') Specify the name of the realm that the service belongs to, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the "realm_discovery" parameter is set to "manual".
service_kdc={value}	(Optional) Specify the KDC that manages authentication for the service in its realm, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the "realm_discovery" parameter is set to "manual".
user_kdc={value}	(Optional) Specify the KDC (Key Distribution Center) that is responsible for authenticating users and issuing ticket-granting tickets (TGTs) for the realm.
krb5_password={value}	(Mandatory, if 'use_kerberos= 1') Enter the password to authenticate to the Kerberos Key Distribution Center (KDC).
krb5_login_type={value}	(Optional) Specify the type of login used to authenticate to the Kerberos Key Distribution Center (KDC). The available values are "basic" and "vault".
krb5_<vaultparameters>={value}	(Mandatory, if krb5_login_type =vault) If krb5_login_type is 'vault', then all vault parameter fields must be added with the prefix 'krb5_'. For example, krb5_vault_type, krb5_vault_id, etc. The vault-specific parameters depend on the vault type you have selected. See the "Vault Definition" section in the API user guide.
Unix only	
{XML File}	(Optional and valid only for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) XML file where you define private-key certificates and root delegations. These are defined using this DTD: <platform API server>/api/2.0/fo/auth/unix/unix_auth_params.dtd
use_agentless_tracking=[**0**|1}	((Optional and valid for Unix record only, i.e. not supported for Cisco or Checkpoint Firewall sub-type) Specify 1 to enable Agentless Tracking.

Parameter	Description
agentless_tracking_path={value}	(Required if use_agentless_tracking=1 for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) The pathname where you would like the service to store the host ID file on each host. This is required to enable Agentless Tracking for Unix.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Parameter	Description
Target Hosts with Tag Support	Note: Applicable only when you have Asset Tagging and Tag Support for Authentication Records enabled for your subscription.
asset_type={**ips**|asset_tags|ip_range_tag_rule}	(Optional) Indicates how assets will be defined in the record. Valid values are ips (the default), asset_tags, ip_range_tag_rule. When not specified, we'll use asset_type=ips ips - Specify this value to assign IP addresses/ranges to the record. asset_tags - Specify this value to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. ip_range_tag_rule - Specify this value to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that don't already have the tag assigned.
tag_set_by={**id**|name}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tags_include={tag1,tag2...}	(Required when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to include in the record. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tags_exclude={tag1,tag2,...}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to exclude from the record. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tag_include_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.

Parameter	Description
ips={value}	(Required to create record when asset_type=ips or asset_type is not specified) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record when asset_type=ips) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record when asset_type=ips) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record when asset_type=ips) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Ports Used For Unix Compliance Scans

The actual ports used for compliance scanning (Unix, Cisco, Checkpoint Firewall) depends on scan settings in 1) compliance option profile, and 2) Unix authentication record as indicated.

Compliance Option Profile	Authentication Record	Ports Scanned
Standard Scan	UI; Well Known Ports API: no "port" parameter	~ 1900 Ports (includes Ports 22, 23, 513)
Standard Scan	UI: Custom Ports API: "port" parameter	~ 1900 Ports + Custom Ports in record
Targeted Scan	UI: Well Known Ports API: no "port" parameter	Ports 22, 23 and 513 only
Targeted Scan	UI: Custom Ports API: "port" parameter	Custom Ports in record

Sample - Create Unix record, with password

Applies to record type Unix, Cisco and Checkpoint Firewall

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=Unix&usernam
e=root&password=<PASSWORD>&ips=10.10.36.63"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12345</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix record, root delegation tools and vault

Applies to record type Unix only (not sub-types)

API request:

```
curl -H "X-Requested-With: curl" -H "Content-type:text/xml" -u
"USERNAME:PASSWORD"
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=Unix&vault&u
sername=Qualys&ips=10.113.195.152&port=5857&login_type=vault&vault_type=L
iebermanERPM&vault_id=10873203&auto_discover_system_name=0&system_name_si
ngle_host=a&custom_system_type=custom&system_type=custom"
--data-binary @add_params.xml
```

add_params.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS>
        <ROOT_TOOL>
            <STANDARD_TYPE type="pimsu"/>
            <PASSWORD_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[root]]></VAULT_USERNAME>
                    <VAULT_TYPE>Thycotic Secret Server</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
<SECRET_NAME><![CDATA[super_secret_name]]></SECRET_NAME>
                </DIGITAL_VAULT>
            </PASSWORD_INFO>
```

```
        </ROOT_TOOL>
        <ROOT_TOOL>
            <CUSTOM_TYPE><![CDATA[test]]></CUSTOM_TYPE>
            <PASSWORD_INFO type="basic">
                <PASSWORD><![CDATA[password]]></PASSWORD>
            </PASSWORD_INFO>
        </ROOT_TOOL>
    </ROOT_TOOLS>
    <PRIVATE_KEY_CERTIFICATES>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_TYPE>CyberArk AIM</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
                    <FOLDER><![CDATA[folder]]></FOLDER>
                    <FILE><![CDATA[file]]></FILE>
                </DIGITAL_VAULT>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic">
                <PASSPHRASE><![CDATA[passphrase]]></PASSPHRASE>
            </PASSPHRASE_INFO>
        </PRIVATE_KEY_CERTIFICATE>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,F9A653E2D12E019357B349B6EEE068B1
FiLfGHOc0rREmC0cBPsiyqqaitPNYTGeqKRmSBwGNrAzNTAcsKslsoY/WkMDW6QD
dLZNiGB0CFag94zyoMyCjyrdpayACAOWfH5w8VixxHF16Vxx5b6foLBE40FOYAIP
sdm1HvCfSFaN2dPf1Unb0erwjigjJNwYIV78529elE+2+dZIemi90ibh0R35NB60
TLeS3UUVezp/O9ZPLf0pqPPHnWgfW4GXp/SUpwojES9fCQE+BW4MMWHWu8XKtytt
....
-----END RSA PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[PASSPHRASE
USERNAME]]></VAULT_USERNAME>
                    <VAULT_TYPE>Quest Vault</VAULT_TYPE>
                    <VAULT_ID>35046922</VAULT_ID>
                  <SYSTEM_NAME><![CDATA[quest_system_name]]></SYSTEM_NAME>
                </DIGITAL_VAULT>
            </PASSPHRASE_INFO>
            <CERTIFICATE type="openssh">
                <![CDATA[ssh-rsa-cert-v01@openssh.com
AAAAHHNzaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgwR4bJSiBtJlOgCAQUF3yZ6Io2
WYfnBiOEsQ45RKbqLgAAAADAQABAAABAQC5sVLb7emh8/v2uHp6x1pN5R+MHQwz3A5M3GRKtu
uu1Njc/XYgqeWLMOJpbVtCVXwUcPgKt4Q0DmlGqc4uhZhzrdtpQGHrEivndNNLY9NQj7LozE7
x/sGiWdtmlucUh1teXMaBpM4aER9Y6uW5wv6ZylY7CAV9bcVz/ljlSypmjzkPjJ39AJq+QxZk
Iv+H4uh/T05LwHdilFrjWWwEoI8DV/DRIw3h8o4jhnj1QxBxyjad3efmFaejgRnY6cBW821gm
...
            </CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE>
```

```
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABCPiEUH5L3LZ
GInEw+h/m4+AAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQCpuwFVTYVmske0bd
FjSlYgsfvyCr7e5irIfoW7B8hNY0XJWyOEqZ5BzwPAEtzjua6m3vnqKPEQD1HyFdLse62JE7x
0jDXLr9bZ64THFpogERC/gI2aorrLKLxdr0K7u5wQUTm1L0xO7Y0hE9Bbi8ok++xTW+Ymf7Lb
VRLWVdN6kUBunIGow3W+tHIohPoUlw82QayZRa4iXpqpWVbh/9OMnb1raC
....
-----END OPENSSH PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
        </PRIVATE_KEY_CERTIFICATE>
    </PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12333</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with target type set to HP_COMWARE

Provide a target type while creating or updating the Unix (SSH2) authentication record.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=ux-target-
type&username=root&ips=10.11.42.114&login_type=basic&password=<PASSWORD>&
target_type=HP_COMWARE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
```

```
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with Tags

In this sample, a new Unix record is created with asset_type=ip_range_tag_rule.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=unix&usern
ame=root&asset_type=ip_range_tag_rule&tags_include=7515612&tag_include_se
lector=all&tags_exclude=7514462&tag_exclude_selector=all"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-03-08T22:00:50Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>204020</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create unix auth record with Kerberos authentication details

API request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/auth/unix/?username=root&action=create&ip
s=10.0.0.1&title=unix
krbsapi&use_kerberos=1&realm_discovery=manual&user_realm=realm.com&servic
e_realm=abc.com&service_kdc=kdc&user_kdc=kerbs&krb5_password=<PASSWORD>&k
rb5_login_type=basic'
--header 'X-Requested-With: portal'
--header 'Authorization: Basic <JWT token>'
```

API response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM"
```

```
<qualys_base_url>/api/3.0/fo/auth/unix/dtd/auth_list_output.dtd">
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2023-02-13T04:08:26Z</DATETIME>
            <AUTH_UNIX_LIST>
                <AUTH_UNIX>
                    <ID>214497</ID>
                    <TITLE>
                        <![CDATA[krbs]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[manual]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[jsm.com]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[kerbs.jsm.com]]>
                    </USER_KDC>
                    <SERVICE_REALM>
                        <![CDATA[kerbs.jsm.com]]>
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[krb]]>
                    </SERVICE_KDC>
                    <IP_SET>
                        <IP>0.0.0.0</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-02-06T09:48:20Z</DATETIME>
                        <BY>test_pq4</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2023-02-06T12:30:33Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
                <AUTH_UNIX>
                    <ID>214498</ID>
                    <TITLE>
                        <![CDATA[k1]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
```

```
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[manual]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[fwwqw]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[user]]>
                    </USER_KDC>
                    <SERVICE_REALM>
                        <![CDATA[s1sdd]]>
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[]]>
                    </SERVICE_KDC>
                    <KERBEROS_LOGIN_INFO type="vault">
                        <DIGITAL_VAULT>
                            <DIGITAL_VAULT_ID>
                                <![CDATA[55014]]>
                            </DIGITAL_VAULT_ID>
                            <DIGITAL_VAULT_TYPE>
                                <![CDATA[Quest Vault]]>
                            </DIGITAL_VAULT_TYPE>
                            <DIGITAL_VAULT_TITLE>
                                <![CDATA[quest]]>
                            </DIGITAL_VAULT_TITLE>
                            <VAULT_SYSTEM_NAME>
                                <![CDATA[fhk]]>
                            </VAULT_SYSTEM_NAME>
                        </DIGITAL_VAULT>
                    </KERBEROS_LOGIN_INFO>
                    <IP_SET>
                        <IP>0.0.0.0</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-02-06T12:54:00Z</DATETIME>
                        <BY>test_pq4</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2023-02-08T10:45:46Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Update Unix auth record with target type CISCO_ASA_WITH_FIREPOWE

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
<qualys_base_url>/api/3.0/fo/auth/unix/?action=update&ids=149016&target_t
ype=CISCO_ASA_WITH_FIREPOWE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix auth record with to view updated target type

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/api/3.0/fo/auth/unix/?action=list&ids=149016
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/3.0/fo/auth/unix/auth_unix_list_output.
dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-05-26T21:35:23Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>149016</ID>
                <TITLE>
                    <![CDATA[ux-target-type]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TARGET_TYPE>
                    <![CDATA[Cisco Adaptive Security Appliance with
FirePower]]>
```

```
                    </TARGET_TYPE>
                    <IP_SET>
                        <IP>10.11.42.114</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
                        <BY>username</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
    </AUTH_UNIX_LIST_OUTPUT>
```

Sample - List Unix auth records

API request:

```
url -k -u <username>:<password> -s -S -H 'X-Requested-With:curl demo2' -d
"action=list" "https://qualysapi.qualys.com/api/3.0/fo/auth/unix/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/3.0/fo/auth/unix/dtd/auth_list_output.d
td">
<AUTH_UNIX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-09-05T08:48:12Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>321277</ID>
        <TITLE><![CDATA[API_v2_END_TO_END_agms_nb_UNIX]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
          <ENABLED>0</ENABLED>
        </QUALYS_SHELL>
      </AUTH_UNIX>
 ...
<AUTH_UNIX>
```

```
    <ID>3382464</ID>
    <TITLE><![CDATA[unn]]></TITLE>
    <USERNAME><![CDATA[admin]]></USERNAME>
    <SKIP_PASSWORD>0</SKIP_PASSWORD>
    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
    <TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
    <PRIVATE_KEY_CERTIFICATE_LIST>
      <PRIVATE_KEY_CERTIFICATE>
        <ID>2257361</ID>
        <PRIVATE_KEY_INFO type="basic">
          <PRIVATE_KEY type="pkcs8" />
        </PRIVATE_KEY_INFO>
        <PASSPHRASE_INFO type="basic" />
      </PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_CERTIFICATE>
        <ID>2257360</ID>
        <PRIVATE_KEY_INFO type="basic">
          <PRIVATE_KEY type="pkcs8" />
        </PRIVATE_KEY_INFO>
        <PASSPHRASE_INFO type="basic" />
      </PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_CERTIFICATE>
        <ID>2255896</ID>
        <PRIVATE_KEY_INFO type="basic">
          <PRIVATE_KEY type="pkcs8" />
        </PRIVATE_KEY_INFO>
        <PASSPHRASE_INFO type="basic" />
      </PRIVATE_KEY_CERTIFICATE>
    </PRIVATE_KEY_CERTIFICATE_LIST> <IP_SET>
      <IP>1.9.0.8</IP>
    </IP_SET>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
      <DATETIME>2023-08-23T09:40:11Z</DATETIME>
      <BY>agms_nb</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2023-08-24T10:04:07Z</DATETIME>
    </LAST_MODIFIED>
    <QUALYS_SHELL>
      <ENABLED>0</ENABLED>
    </QUALYS_SHELL>
  </AUTH_UNIX>
```

Sample - Create Unix record with resource ID

API request:

```
curl --location --request
POST'<qualys_base_url>/api/2.0/fo/auth/unix/?action=create&title=Unix&use
rname=root&ips=10.113.197.129&login_type=vault&vault_type=Hitachi
IDPAM&vault_id=1358956&resource_id=123' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic XXXXXXXXXXXX'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"
<qualys_base_url>/api/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2023-11-30T10:18:03Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>3804148</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update Unix record with resource ID

API request:

```
curl --location --request
POST'<qualys_base_url>/api/2.0/fo/auth/unix/?action=update&ids=3804148&lo
gin_type=vault&vault_type=Hitachi
IDPAM&vault_id=1358956&resource_id=1234' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic XXXXXXXXXXXX'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"
<qualys_base_url>/api/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2023-11-30T10:19:57Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>3804148</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - List Unix record with resource ID

API request:

```
curl --location --request
GET'<qualys_base_url>/api/2.0/fo/auth/unix/?action=list&ids=3804148' \--
header 'X-Requested-With: curl' \--header 'Authorization: Basic
XXXXXXXXXXXX'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"
<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2023-11-30T10:22:26Z</DATETIME>
            <AUTH_UNIX_LIST>
                <AUTH_UNIX>
                    <ID>3804148</ID>
                    <TITLE>
                        <![CDATA[Unix]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <IP_SET>
                        <IP>10.113.197.129</IP>
                    </IP_SET>
                    <LOGIN_TYPE>
                        <![CDATA[vault]]>
                    </LOGIN_TYPE>
                    <DIGITAL_VAULT>
                        <DIGITAL_VAULT_ID>
                            <![CDATA[1358956]]>
                        </DIGITAL_VAULT_ID>
                        <DIGITAL_VAULT_TYPE>
                            <![CDATA[Hitachi ID PAM]]>
                        </DIGITAL_VAULT_TYPE>
                        <DIGITAL_VAULT_TITLE>
                            <![CDATA[mob hitachi]]>
                        </DIGITAL_VAULT_TITLE>
                        <VAULT_RESOURCE_ID>

<![CDATA[1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb2]]>
                        </VAULT_RESOURCE_ID>
                    </DIGITAL_VAULT>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-11-30T10:18:03Z</DATETIME>
                        <BY>appe_rm</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2023-11-30T10:19:57Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
```

```
        </AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create with Asset Tags (by Name) - Cisco

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=Cisco&port=42&asset
_type=ip_range_tag_rule&tag_set_by=name&tags_include=Exc_1&tags_exclude=Exc_2&pa
ssword=test&username=test&sub_type=cisco&port=22' \
--header 'X-Requested-With: abcd' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-20T12:03:11Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8904935</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update with IP Range Tag Rule IDs - Cisco

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=update&ids=<AUTH_RECORD_ID>&sub_
type=cisco&asset_type=ip_range_tag_rule&tag_set_by=id&tags_include=201,202&tags_
exclude=203"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-22T10:23:42Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
```

```
                <ID_SET>
                    <ID>8927402</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Cisco

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST "<qualys_base_url>/api/3.0/fo/auth/unix/?action=list"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
<!-- This report was generated with an evaluation version of Qualys -->
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-22T12:29:55Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8926408</ID>
                <TITLE>
                    <![CDATA[API_TEST_AUTOMATION_476349994]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[API_RNDM_476384383]]>
                </USERNAME>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TAGS>
                    <TAG_TYPE>asset_tags</TAG_TYPE>
                    <TAGS_INCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>7612812</ID>
                            <NAME>Cloud Agent</NAME>
                        </TAG>
                    </TAGS_INCLUDE>
                    <TAGS_EXCLUDE>
                        <SELECTOR>any</SELECTOR>
                    </TAGS_EXCLUDE>
                </TAGS>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2026-05-22T04:38:17Z</DATETIME>
```

```
                    <BY>mayur_aa</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2026-05-22T12:28:04Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_UNIX>
        </AUTH_UNIX_LIST>
    </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create with Asset Tags (by name) - Checkpoint Firewall

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/auth/unix/?action=create&title=cicso_auth&port=42&
asset_type=asset_tags&tag_set_by=name&tags_include=Exc_1&tags_exclude=Exc_2&pass
word=test&username=test&sub_type=checkpoint_firewall&port=22' \
--header 'X-Requested-With: abcd' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-20T12:03:11Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8904935</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update with IP Range Tag Rule IDs - Checkpoint Firewall

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST
"<qualys_base_url>/api/3.0/fo/auth/unix/?action=update&ids=<AUTH_RECORD_ID>&sub_
type=checkpoint_firewall&asset_type=ip_range_tag_rule&tag_set_by=id&tags_include
=101,102&tags_exclude=103"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-22T10:23:42Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8927402</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Checkpoint Firewall

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST "<qualys_base_url>/api/3.0/fo/auth/unix/?action=list"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
<!-- This report was generated with an evaluation version of Qualys -->
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-22T12:29:55Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8926408</ID>
                <TITLE>
                    <![CDATA[API_TEST_AUTOMATION_476349994]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[API_RNDM_476384383]]>
                </USERNAME>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TAGS>
                    <TAG_TYPE>asset_tags</TAG_TYPE>
                    <TAGS_INCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>7612812</ID>
                            <NAME>Cloud Agent</NAME>
                        </TAG>
```

```
                    </TAGS_INCLUDE>
                    <TAGS_EXCLUDE>
                        <SELECTOR>any</SELECTOR>
                    </TAGS_EXCLUDE>
                </TAGS>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2026-05-22T04:38:17Z</DATETIME>
                    <BY>mayur_aa</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2026-05-22T12:28:04Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_UNIX>
        </AUTH_UNIX_LIST>
    </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/3.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=create' \
--data-urlencode 'title=Postman_Unix' \
--data-urlencode 'ips=1.1.1.2' \
--data-urlencode 'username=root' \
--data-urlencode 'login_type=vault' \
--data-urlencode 'vault_id=2304704' \
--data-urlencode 'vault_type=One Identity Safeguard' \
--data-urlencode 'vault_app_name=<vault_app_name>' \
--data-urlencode 'vault_asset_name=<vault_asset_name>' \
--data-urlencode 'vault_appkey=<vault_assetkey>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-27T07:29:29Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8975403</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/3.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=update' \
--data-urlencode 'ids=8975403' \
--data-urlencode 'add_ips=1.1.1.3' \
--data-urlencode 'vault_type=One Identity Safeguard' \
--data-urlencode 'vault_id=2304704' \
--data-urlencode 'vault_app_name=<vault_app_name>' \
--data-urlencode 'vault_asset_name=<vault_asset_name>' \
--data-urlencode 'vault_appkey=<vault_assetkey>' \
--data-urlencode 'login_type=vault'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-27T07:30:18Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8975403</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/3.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=list' \
--data-urlencode 'ids=8975403'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/auth/unix/dtd/auth_list_output.dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-26T13:07:17Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8975403</ID>
                <TITLE>
                    <![CDATA[Postman_Unix]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TARGET_TYPE>
                    <![CDATA[Auto (default)]]>
                </TARGET_TYPE>
                <IP_SET>
                    <IP>1.1.1.2</IP>
                </IP_SET>
                <LOGIN_TYPE>
                    <![CDATA[vault]]>
                </LOGIN_TYPE>
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[2304704]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[One Identity Safeguard]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                        <![CDATA[One_Identity_vault]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_APP_NAME>
                        <![CDATA[amit]]>
                    </VAULT_APP_NAME>
                    <VAULT_ASSET_NAME>
                        <![CDATA[rahul]]>
                    </VAULT_ASSET_NAME>
                    <VAULT_APPKEY>
                        <![CDATA[saket]]>
                    </VAULT_APPKEY>
                </DIGITAL_VAULT>
                <CREATED>
```

```
                <DATETIME>2026-05-26T13:06:55Z</DATETIME>
                <BY>vsh_sm</BY>
            </CREATED>
            <LAST_MODIFIED>
                <DATETIME>2026-05-26T13:06:55Z</DATETIME>
            </LAST_MODIFIED>
        </AUTH_UNIX>
    </AUTH_UNIX_LIST>
</RESPONSE>
   </AUTH_UNIX_LIST_OUTPUT>
```

More Samples

Qualys API - Unix Authentication API samples (GitHub)

DTDs for auth type "unix"

<platform API server>/api/3.0/batch_return.dtd

<platform API server>/api/3.0/fo/auth/unix/auth_unix_list_output.dtd

For Unix type record type only, root delegation tools and private-key certificates are specified using the unix_auth_params.dtd here

<platform API server>/api/3.0/fo/auth/unix/unix_auth_params.dtd

V4.0

/api/4.0/fo/auth/unix/

[POST]

Create, update, list and delete Unix records for authenticated scans of hosts running on Unix, Cisco and Checkpoint Firewall. Vulnerability and compliance scans are supported on Unix and Cisco systems (using VM, PC). Compliance scans are supported on Checkpoint Firewall systems (using PC).

Download Qualys User Guide - Unix Authentication (pdf)

Input Parameters

Parameters: Request | Login credentials| Unix only | Target Hosts

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
sub_type={cisco|checkpoint_firewall}	(Required for hosts running on Cisco or Checkpoint Firewall) Choose cisco or checkpoint_firewall if you're scanning one of these system types.
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.

Parameter	Description
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
port={value}	(Optional and valid for compliance scans only) Custom ports to be used to perform authenticated compliance assessment (control testing). Ports Used For Unix Compliance Scans
Login credentials	
username={value}	(Required to create record, optional to update record) The username of the account to be used for authentication. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication when a vault will not be used. Maximum 100 characters (ascii).
login_type={**basic**|vault}	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
cleartext_password={**0**|1}	(Optional) When not specified, the scanning engine only uses strong password encryption for remote login. Specify 1 to allow your password to be transmitted in clear text when connecting to services which do not support strong password encryption. For more info, search for “Clear Text Password” in online help. For a create request, if cleartext_password=1, the password parameter is required. For an update request, if cleartext_password=1, and the record does not have a password set, then cleartext_password=1 is *silently ignored*.
skip_password={**0**|1}	(Optional and valid only for Unix record, i.e not supported for Cisco or Checkpoint Firewall sub-type) By default when only the required parameters are set (title, username, ips) the login account password is set to the empty password. You can set skip_password=1 if the login account does not have a password. When set it’s not possible to set the empty password, another password using the “password” parameter, or password in a vault.

Parameter	Description
enable_password={value}	(Optional and valid only for Cisco sub-type) The password required for executing the “enable” command on the target hosts. Maximum 100 characters (ascii). Note: The pooled credentials feature is not supported if the “enable” command requires a password and it is specified using the enable_password parameter.
expert_password={value}	(Optional and valid only for Checkpoint Firewall sub-type) The password required for executing the “expert” command on the target hosts. Maximum 100 characters (ascii).
target_type={value}	(Optional) Specify the target type. You can choose from the following values: - A10 - HP_COMWARE - CISCO_ASA_WITH_FIREPOWE - auto (default)
Kerberos/GSSAPI authentication details, if it is enabled for the target host	
use_kerberos={0|1}	(Optional) Specify 1 to enable Kerberos authentication. By default, the value is set to 0.
realm_discovery={value}	(Mandatory, if ‘use_kerberos=1’) Specify the realm discovery method. The available values are manual, single, and DNS.
user_realm={value}	(Mandatory, if ‘use_kerberos=1’) Specify the name of the realm that a user belongs to.
service_realm={value}	(Mandatory, if ‘use_kerberos=1’) Specify the name of the realm that the service belongs to, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the “realm_discovery” parameter is set to “manual”.
service_kdc={value}	(Optional) Specify the KDC that manages authentication for the service in its realm, when a user wants to access a service that is part of a different realm. **Note**: This parameter is valid only if the “realm_discovery” parameter is set to “manual”.
user_kdc={value}	(Optional) Specify the KDC (Key Distribution Center) that is responsible for authenticating users and issuing ticket-granting tickets (TGTs) for the realm.
krb5_password={value}	(Mandatory, if ‘use_kerberos= 1’) Enter the password to authenticate to the Kerberos Key Distribution Center (KDC).
krb5_login_type={value}	(Optional) Specify the type of login used to authenticate to the Kerberos Key Distribution Center (KDC). The available values are “basic” and “vault”.

Parameter	Description
krb5_<vaultparameters>={value}	(Mandatory, if krb5_login_type =vault) If krb5_login_type is 'vault', then all vault parameter fields must be added with the prefix 'krb5_'. For example, krb5_vault_type, krb5_vault_id, etc. The vault-specific parameters depend on the vault type you have selected. See the “Vault Definition” section in the API user guide.
Unix only	
{XML File}	(Optional and valid only for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) XML file where you define private-key certificates and root delegations. These are defined using this DTD: <platform API server>/api/2.0/fo/auth/unix/unix_auth_params.dtd
use_agentless_tracking=[**0**|1}	((Optional and valid for Unix record only, i.e. not supported for Cisco or Checkpoint Firewall sub-type) Specify 1 to enable Agentless Tracking.
agentless_tracking_path={value}	(Required if use_agentless_tracking=1 for Unix record, i.e. not supported for Cisco or Checkpoint Firewall sub-type) The pathname where you would like the service to store the host ID file on each host. This is required to enable Agentless Tracking for Unix.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record’s credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Parameter	Description
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.
Target Hosts with Tag Support	Note: Applicable only when you have Asset Tagging and Tag Support for Authentication Records enabled for your subscription.
asset_type={**ips**|asset_tags|ip_range_tag_rule}	(Optional) Indicates how assets will be defined in the record. Valid values are ips (the default), asset_tags, ip_range_tag_rule. When not specified, we'll use asset_type=ips ips - Specify this value to assign IP addresses/ranges to the record. asset_tags - Specify this value to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. ip_range_tag_rule - Specify this value to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that don't already have the tag assigned.
tag_set_by={**id**|name}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tags_include={tag1,tag2...}	(Required when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to include in the record. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tags_exclude={tag1,tag2,...}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to exclude from the record. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.

Parameter	Description
tag_include_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
ips={value}	(Required to create record when asset_type=ips or asset_type is not specified) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record when asset_type=ips) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record when asset_type=ips) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record when asset_type=ips) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Ports Used For Unix Compliance Scans

The actual ports used for compliance scanning (Unix, Cisco, Checkpoint Firewall) depends on scan settings in 1) compliance option profile, and 2) Unix authentication record as indicated.

Compliance Option Profile	Authentication Record	Ports Scanned
Standard Scan	UI; Well Known Ports API: no "port" parameter	~ 1900 Ports (includes Ports 22, 23, 513)
Standard Scan	UI: Custom Ports API: "port" parameter	~ 1900 Ports + Custom Ports in record

Compliance Option Profile	Authentication Record	Ports Scanned
Targeted Scan	UI: Well Known Ports API: no “port” parameter	Ports 22, 23 and 513 only
Targeted Scan	UI: Custom Ports API: “port” parameter	Custom Ports in record

Sample - Create Unix record, with password

Applies to record type Unix, Cisco and Checkpoint Firewall

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"<qualys_base_url>/api/4.0/fo/auth/unix/?action=create&title=Unix&usernam
e=root&password=<PASSWORD>&ips=10.10.36.63"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12345</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix record, root delegation tools and vault

Applies to record type Unix only (not sub-types)

API request:

```
curl -H "X-Requested-With: curl" -H "Content-type:text/xml" -u
"USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/4.0/fo/auth/unix/?action=create&title=U
nix&vault&username=Qualys&ips=10.113.195.152&port=5857&login_type=vault&v
ault_type=LiebermanERPM&vault_id=10873203&auto_discover_system_name=0&sys
tem_name_single_host=a&custom_system_type=custom&system_type=custom"
--data-binary @add_params.xml
```

add_params.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS>
```

```
        <ROOT_TOOL>
            <STANDARD_TYPE type="pimsu"/>
            <PASSWORD_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[root]]></VAULT_USERNAME>
                    <VAULT_TYPE>Thycotic Secret Server</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
<SECRET_NAME><![CDATA[super_secret_name]]></SECRET_NAME>
                </DIGITAL_VAULT>
            </PASSWORD_INFO>
        </ROOT_TOOL>
        <ROOT_TOOL>
            <CUSTOM_TYPE><![CDATA[test]]></CUSTOM_TYPE>
            <PASSWORD_INFO type="basic">
                <PASSWORD><![CDATA[password]]></PASSWORD>
            </PASSWORD_INFO>
        </ROOT_TOOL>
    </ROOT_TOOLS>
    <PRIVATE_KEY_CERTIFICATES>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_TYPE>CyberArk AIM</VAULT_TYPE>
                    <VAULT_ID>25026922</VAULT_ID>
                    <FOLDER><![CDATA[folder]]></FOLDER>
                    <FILE><![CDATA[file]]></FILE>
                </DIGITAL_VAULT>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic">
                <PASSPHRASE><![CDATA[passphrase]]></PASSPHRASE>
            </PASSPHRASE_INFO>
        </PRIVATE_KEY_CERTIFICATE>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,F9A653E2D12E019357B349B6EEE068B1
FiLfGHOc0rREmC0cBPsiyqqaitPNYTGeqKRmSBwGNrAzNTAcsKslsoY/WkMDW6QD
dLZNiGB0CFag94zyoMyCjyrdpayACAOWfH5w8VixxHF16Vxx5b6foLBE40FOYAIP
sdm1HvCfSFaN2dPf1Unb0erwjigjJNwYIV78529elE+2+dZIemi90ibh0R35NB60
TLeS3UUVezp/O9ZPLf0pqPPHnWgfW4GXp/SUpwojES9fCQE+BW4MMWHWu8XKtytt
....
-----END RSA PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_USERNAME><![CDATA[PASSPHRASE
USERNAME]]></VAULT_USERNAME>
                    <VAULT_TYPE>Quest Vault</VAULT_TYPE>
                    <VAULT_ID>35046922</VAULT_ID>
                 <SYSTEM_NAME><![CDATA[quest_system_name]]></SYSTEM_NAME>
                </DIGITAL_VAULT>
            </PASSPHRASE_INFO>
```

```
            <CERTIFICATE type="openssh">
                <![CDATA[ssh-rsa-cert-v01@openssh.com
AAAAHHNzaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgwR4bJSiBtJlOgCAQUF3yZ6Io2
WYfnBiOEsQ45RKbqLgAAAADAQABAAABAQC5sVLb7emh8/v2uHp6x1pN5R+MHQwz3A5M3GRKtu
uu1Njc/XYgqeWLMOJpbVtCVXwUcPgKt4Q0DmlGqc4uhZhzrdtpQGHrEivndNNLY9NQj7LozE7
x/sGiWdtmlucUh1teXMaBpM4aER9Y6uW5wv6ZylY7CAV9bcVz/ljlSypmjzkPjJ39AJq+QxZk
Iv+H4uh/T05LwHdilFrjWWwEoI8DV/DRIw3h8o4jhnj1QxBxyjad3efmFaejgRnY6cBW821gm
...
            </CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE>
        <PRIVATE_KEY_CERTIFICATE>
            <PRIVATE_KEY_INFO type="basic">
                <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABCPiEUH5L3LZ
GInEw+h/m4+AAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQCpuwFVTYVmske0bd
FjSlYgsfvyCr7e5irIfoW7B8hNY0XJWyOEqZ5BzwPAEtzjua6m3vnqKPEQD1HyFdLse62JE7x
0jDXLr9bZ64THFpogERC/gI2aorrLKLxdr0K7u5wQUTm1L0xO7Y0hE9Bbi8ok++xTW+Ymf7Lb
VRLWVdN6kUBunIGow3W+tHIohPoUlw82QayZRa4iXpqpWVbh/9OMnb1raC
....
-----END OPENSSH PRIVATE KEY-----]]></PRIVATE_KEY>
            </PRIVATE_KEY_INFO>
        </PRIVATE_KEY_CERTIFICATE>
    </PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-18T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>12333</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with target type set to HP_COMWARE

Provide a target type while creating or updating the Unix (SSH2) authentication record.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/4.0/fo/auth/unix/?action=create&title=u
x-target-
type&username=root&ips=10.11.42.114&login_type=basic&password=<PASSWORD>&
```

```
target_type=HP_COMWARE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Unix Record with Tags

In this sample, a new Unix record is created with asset_type=ip_range_tag_rule.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/4.0/fo/auth/unix/?action=create&title=u
nix&username=root&asset_type=ip_range_tag_rule&tags_include=7515612&tag_i
nclude_selector=all&tags_exclude=7514462&tag_exclude_selector=all"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-03-08T22:00:50Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>204020</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Create unix auth record with Kerberos authentication details

API request:

```
curl --location --request POST
```

```
'https://qualysapi.qualys.com/api/4.0/fo/auth/unix/?username=root&action=
create&ips=10.0.0.1&title=unix
krbsapi&use_kerberos=1&realm_discovery=manual&user_realm=realm.com&servic
e_realm=abc.com&service_kdc=kdc&user_kdc=kerbs&krb5_password=<PASSWORD>&k
rb5_login_type=basic'
--header 'X-Requested-With: portal'
--header 'Authorization: Basic <JWT token>'
```

API response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM"
https://qualysapi.qualys.com/api/4.0/fo/auth/unix/dtd/auth_list_output.dt
d">
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2023-02-13T04:08:26Z</DATETIME>
            <AUTH_UNIX_LIST>
                <AUTH_UNIX>
                    <ID>214497</ID>
                    <TITLE>
                        <![CDATA[krbs]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[manual]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[jsm.com]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[kerbs.jsm.com]]>
                    </USER_KDC>
                    <SERVICE_REALM>
                        <![CDATA[kerbs.jsm.com]]>
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[krb]]>
                    </SERVICE_KDC>
                    <IP_SET>
                        <IP>0.0.0.0</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2023-02-06T09:48:20Z</DATETIME>
                        <BY>test_pq4</BY>
```

```
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2023-02-06T12:30:33Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_UNIX>
<AUTH_UNIX>
    <ID>214498</ID>
    <TITLE>
        <![CDATA[k1]]>
    </TITLE>
    <USERNAME>
        <![CDATA[root]]>
    </USERNAME>
    <SKIP_PASSWORD>0</SKIP_PASSWORD>
    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
    <TARGET_TYPE>
        <![CDATA[Auto (default)]]>
    </TARGET_TYPE>
    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
    <REALM_DISCOVERY>
        <![CDATA[manual]]>
    </REALM_DISCOVERY>
    <USER_REALM>
        <![CDATA[fwwqw]]>
    </USER_REALM>
    <USER_KDC>
        <![CDATA[user]]>
    </USER_KDC>
    <SERVICE_REALM>
        <![CDATA[s1sdd]]>
    </SERVICE_REALM>
    <SERVICE_KDC>
        <![CDATA[]]>
    </SERVICE_KDC>
    <KERBEROS_LOGIN_INFO type="vault">
        <DIGITAL_VAULT>
            <DIGITAL_VAULT_ID>
                <![CDATA[55014]]>
            </DIGITAL_VAULT_ID>
            <DIGITAL_VAULT_TYPE>
                <![CDATA[Quest Vault]]>
            </DIGITAL_VAULT_TYPE>
            <DIGITAL_VAULT_TITLE>
                <![CDATA[quest]]>
            </DIGITAL_VAULT_TITLE>
            <VAULT_SYSTEM_NAME>
                <![CDATA[fhk]]>
            </VAULT_SYSTEM_NAME>
        </DIGITAL_VAULT>
    </KERBEROS_LOGIN_INFO>
    <IP_SET>
        <IP>0.0.0.0</IP>
    </IP_SET>
    <NETWORK_ID>0</NETWORK_ID>
```

```
                        <CREATED>
                            <DATETIME>2023-02-06T12:54:00Z</DATETIME>
                            <BY>test_pq4</BY>
                        </CREATED>
                        <LAST_MODIFIED>
                            <DATETIME>2023-02-08T10:45:46Z</DATETIME>
                        </LAST_MODIFIED>
                    </AUTH_UNIX>
                </AUTH_UNIX_LIST>
            </RESPONSE>
        </AUTH_UNIX_LIST_OUTPUT>
```

Sample - Update Unix auth record with target type CISCO_ASA_WITH_FIREPOWE

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
<qualys_base_url>/api/4.0/fo/auth/unix/?action=update&ids=149016&target_t
ype=CISCO_ASA_WITH_FIREPOWE
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>149016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix auth record with to view updated target type

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/api/4.0/fo/auth/unix/?action=list&ids=149016
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/4.0/fo/auth/unix/auth_unix_list_output.
dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-05-26T21:35:23Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
```

```
                    <ID>149016</ID>
                    <TITLE>
                        <![CDATA[ux-target-type]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Cisco Adaptive Security Appliance with
FirePower]]>
                    </TARGET_TYPE>
                    <IP_SET>
                        <IP>10.11.42.114</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2020-05-26T21:17:17Z</DATETIME>
                        <BY>username</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-05-26T21:34:18Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - List Unix auth records

API request:

```
url -k -u agms_nb:Qatemp123# -s -S -H 'X-Requested-With:curl demo2' -d
"action=list" "<qualys_base_url>/api/4.0/fo/auth/unix/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/4.0/fo/auth/unix/dtd/auth_list_output.d
td">
<AUTH_UNIX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-09-05T08:48:12Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>321277</ID>
        <TITLE><![CDATA[API_v2_END_TO_END_agms_nb_UNIX]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
```

```
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-15T08:48:06Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
          <ENABLED>0</ENABLED>
        </QUALYS_SHELL>
      </AUTH_UNIX>
 ...
<AUTH_UNIX>
        <ID>3382464</ID>
        <TITLE><![CDATA[unn]]></TITLE>
        <USERNAME><![CDATA[admin]]></USERNAME>
        <SKIP_PASSWORD>0</SKIP_PASSWORD>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
        <PRIVATE_KEY_CERTIFICATE_LIST>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2257361</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2257360</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2255896</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE_LIST> <IP_SET>
          <IP>1.9.0.8</IP>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2023-08-23T09:40:11Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2023-08-24T10:04:07Z</DATETIME>
        </LAST_MODIFIED>
        <QUALYS_SHELL>
          <ENABLED>0</ENABLED>
        </QUALYS_SHELL>
```

```
</AUTH_UNIX>
```

Sample - Create Unix record with resource ID

API request:

```
curl --location --request
POST'<qualys_base_url>/api/2.0/fo/auth/unix/?action=create&title=Unix&use
rname=root&ips=10.113.197.129&login_type=vault&vault_type=Hitachi
IDPAM&vault_id=1358956&resource_id=123' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic XXXXXXXXXXXX'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"
<qualys_base_url>/api/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2023-11-30T10:18:03Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>3804148</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update Unix record with resource ID

API request:

```
curl --location --request
POST'<qualys_base_url>/api/2.0/fo/auth/unix/?action=update&ids=3804148&lo
gin_type=vault&vault_type=Hitachi
IDPAM&vault_id=1358956&resource_id=1234' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic XXXXXXXXXXXX'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"
<qualys_base_url>/api/2.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2023-11-30T10:19:57Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
                    <ID_SET>
                        <ID>3804148</ID>
                    </ID_SET>
                </BATCH>
```

```
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - List Unix record with resource ID

API request:

```
curl --location --request
GET'<qualys_base_url>/api/2.0/fo/auth/unix/?action=list&ids=3804148' \--
header 'X-Requested-With: curl' \--header 'Authorization: Basic
XXXXXXXXXXXX'
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"
<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2023-11-30T10:22:26Z</DATETIME>
            <AUTH_UNIX_LIST>
                <AUTH_UNIX>
                    <ID>3804148</ID>
                    <TITLE>
                        <![CDATA[Unix]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <IP_SET>
                        <IP>10.113.197.129</IP>
                    </IP_SET>
                    <LOGIN_TYPE>
                        <![CDATA[vault]]>
                    </LOGIN_TYPE>
                    <DIGITAL_VAULT>
                        <DIGITAL_VAULT_ID>
                            <![CDATA[1358956]]>
                        </DIGITAL_VAULT_ID>
                        <DIGITAL_VAULT_TYPE>
                            <![CDATA[Hitachi ID PAM]]>
                        </DIGITAL_VAULT_TYPE>
                        <DIGITAL_VAULT_TITLE>
                            <![CDATA[mob hitachi]]>
                        </DIGITAL_VAULT_TITLE>
                        <VAULT_RESOURCE_ID>

<![CDATA[1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
   aaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb2]]>
                        </VAULT_RESOURCE_ID>
```

```
                        </DIGITAL_VAULT>
                        <NETWORK_ID>0</NETWORK_ID>
                        <CREATED>
                            <DATETIME>2023-11-30T10:18:03Z</DATETIME>
                            <BY>appe_rm</BY>
                        </CREATED>
                        <LAST_MODIFIED>
                            <DATETIME>2023-11-30T10:19:57Z</DATETIME>
                        </LAST_MODIFIED>
                    </AUTH_UNIX>
                </AUTH_UNIX_LIST>
            </RESPONSE>
        </AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create with Asset Tags (by Name) - Cisco

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/auth/unix/?action=create&title=Cisco&port=42&asset
_type=ip_range_tag_rule&tag_set_by=name&tags_include=Exc_1&tags_exclude=Exc_2&pa
ssword=test&username=test&sub_type=cisco&port=22' \
--header 'X-Requested-With: abcd' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-20T12:03:11Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8904935</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
       </BATCH_RETURN>
```

Sample - Update with IP Range Tag Rule IDs - Cisco

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST
"<qualys_base_url>/api/4.0/fo/auth/unix/?action=update&ids=<AUTH_RECORD_ID>&sub_
type=cisco&asset_type=ip_range_tag_rule&tag_set_by=id&tags_include=201,202&tags_
exclude=203"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-22T10:23:42Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8927402</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Cisco

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST "<qualys_base_url>/api/4.0/fo/auth/unix/?action=list"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
<!-- This report was generated with an evaluation version of Qualys -->
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-22T12:29:55Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8926408</ID>
                <TITLE>
                    <![CDATA[API_TEST_AUTOMATION_476349994]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[API_RNDM_476384383]]>
                </USERNAME>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TAGS>
                    <TAG_TYPE>asset_tags</TAG_TYPE>
                    <TAGS_INCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>7612812</ID>
```

```
                        <NAME>Cloud Agent</NAME>
                    </TAG>
                </TAGS_INCLUDE>
                <TAGS_EXCLUDE>
                    <SELECTOR>any</SELECTOR>
                </TAGS_EXCLUDE>
            </TAGS>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
                <DATETIME>2026-05-22T04:38:17Z</DATETIME>
                <BY>mayur_aa</BY>
            </CREATED>
            <LAST_MODIFIED>
                <DATETIME>2026-05-22T12:28:04Z</DATETIME>
            </LAST_MODIFIED>
        </AUTH_UNIX>
    </AUTH_UNIX_LIST>
</RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create with Asset Tags (by name) - Checkpoint Firewall

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/4.0/fo/auth/unix/?action=create&title=cicso_auth&port=42&
asset_type=asset_tags&tag_set_by=name&tags_include=Exc_1&tags_exclude=Exc_2&pass
word=test&username=test&sub_type=checkpoint_firewall&port=22' \
--header 'X-Requested-With: abcd' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-20T12:03:11Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8904935</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update with IP Range Tag Rule IDs - Checkpoint Firewall

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST
"<qualys_base_url>/api/4.0/fo/auth/unix/?action=update&ids=<AUTH_RECORD_ID>&sub_
type=checkpoint_firewall&asset_type=ip_range_tag_rule&tag_set_by=id&tags_include
=101,102&tags_exclude=103"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-22T10:23:42Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8927402</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Checkpoint Firewall

API Request:

```
curl -u "USER:PASSWORD" \
  -H "X-Requested-With: curl" \
  -X POST "<qualys_base_url>/api/4.0/fo/auth/unix/?action=list"
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/unix/dtd/auth_list_output.dtd">
<!-- This report was generated with an evaluation version of Qualys -->
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-22T12:29:55Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8926408</ID>
                <TITLE>
                    <![CDATA[API_TEST_AUTOMATION_476349994]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[API_RNDM_476384383]]>
```

```
                </USERNAME>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TAGS>
                    <TAG_TYPE>asset_tags</TAG_TYPE>
                    <TAGS_INCLUDE>
                        <SELECTOR>any</SELECTOR>
                        <TAG>
                            <ID>7612812</ID>
                            <NAME>Cloud Agent</NAME>
                        </TAG>
                    </TAGS_INCLUDE>
                    <TAGS_EXCLUDE>
                        <SELECTOR>any</SELECTOR>
                    </TAGS_EXCLUDE>
                </TAGS>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2026-05-22T04:38:17Z</DATETIME>
                    <BY>mayur_aa</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2026-05-22T12:28:04Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_UNIX>
        </AUTH_UNIX_LIST>
    </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/4.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=create' \
--data-urlencode 'title=Postman_Unix' \
--data-urlencode 'ips=1.1.1.2' \
--data-urlencode 'username=root' \
--data-urlencode 'login_type=vault' \
--data-urlencode 'vault_id=2304704' \
--data-urlencode 'vault_type=One Identity Safeguard' \
--data-urlencode 'vault_app_name=<vault_app_name>' \
--data-urlencode 'vault_asset_name=<vault_asset_name>' \
--data-urlencode 'vault_appkey=<vault_assetkey>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
```

```
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-27T07:29:29Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>8975403</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/4.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=update' \
--data-urlencode 'ids=8975403' \
--data-urlencode 'add_ips=1.1.1.3' \
--data-urlencode 'vault_type=One Identity Safeguard' \
--data-urlencode 'vault_id=2304704' \
--data-urlencode 'vault_app_name=<vault_app_name>' \
--data-urlencode 'vault_asset_name=<vault_asset_name>' \
--data-urlencode 'vault_appkey=<vault_assetkey>' \
--data-urlencode 'login_type=vault'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/4.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-05-27T07:30:18Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>8975403</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix Authentication Record with One Identity Safeguard vault

API Request:

```
curl --location '<qualys_base_url>/api/4.0/fo/auth/unix/' \
--header 'X-Requested-With: Qualys Postman Collection' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic dnNoX3NtOlF1YWx5c0A3ODk=' \
--data-urlencode 'action=list' \
--data-urlencode 'ids=8975403'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/auth/unix/dtd/auth_list_output.dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-05-26T13:07:17Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>8975403</ID>
                <TITLE>
                    <![CDATA[Postman_Unix]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <TARGET_TYPE>
                    <![CDATA[Auto (default)]]>
                </TARGET_TYPE>
                <IP_SET>
                    <IP>1.1.1.2</IP>
                </IP_SET>
                <LOGIN_TYPE>
                    <![CDATA[vault]]>
                </LOGIN_TYPE>
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[2304704]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[One Identity Safeguard]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                        <![CDATA[One_Identity_vault]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_APP_NAME>
                        <![CDATA[amit]]>
```

```
                    </VAULT_APP_NAME>
                    <VAULT_ASSET_NAME>
                        <![CDATA[rahul]]>
                    </VAULT_ASSET_NAME>
                    <VAULT_APPKEY>
                        <![CDATA[saket]]>
                    </VAULT_APPKEY>
                </DIGITAL_VAULT>
                <CREATED>
                    <DATETIME>2026-05-26T13:06:55Z</DATETIME>
                    <BY>vsh_sm</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2026-05-26T13:06:55Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_UNIX>
        </AUTH_UNIX_LIST>
    </RESPONSE>
       </AUTH_UNIX_LIST_OUTPUT>
```

Sample - Create Unix Authentication record with with root delegtion AD

API request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/auth/unix/?action=create&title=Unix_HashiCor
p_AD_RootDelegation&username=<username>&password=<password>&ips=xx.xx.xx.
xx\
--header 'X-Requested-With: curl demo' \
--header 'Content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
                <UNIX_AUTH_PARAMS>
                    <ROOT_TOOLS>
                        <ROOT_TOOL>
                            <STANDARD_TYPE type="sudo"/>
                            <PASSWORD_INFO type="vault">
                                <DIGITAL_VAULT>
                                    <VAULT_TYPE>HashiCorp</VAULT_TYPE>
                                    <VAULT_ID>2468704</VAULT_ID>

<SECRET_KV_PATH>unix/hosts</SECRET_KV_PATH>

<SECRET_KV_NAME>account_name</SECRET_KV_NAME>
                                        <USE_AD_HASHICORP>1</USE_AD_HASHICORP>
                                </DIGITAL_VAULT>
                            </PASSWORD_INFO>
                        </ROOT_TOOL>
                    </ROOT_TOOLS>
                </UNIX_AUTH_PARAMS>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/api/4.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2026-07-21T02:25:54Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>9439474</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update Unix Authentication record with with root delegtion AD

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/auth/unix/?action=update&ids=12839871&usern
ame=<username>&password=<password>\
--header 'X-Requested-With: curl demo' \
--header 'Content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
--data '
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS>
        <ROOT_TOOL>
            <STANDARD_TYPE type="sudo"/>
            <PASSWORD_INFO type="vault">
                <DIGITAL_VAULT>
                    <VAULT_TYPE>HashiCorp</VAULT_TYPE>
                    <VAULT_ID>5306952</VAULT_ID>
                    <SECRET_KV_PATH>unix/hosts</SECRET_KV_PATH>
                    <SECRET_KV_NAME>updatedname</SECRET_KV_NAME>
                    <USE_AD_HASHICORP>1</USE_AD_HASHICORP>
                </DIGITAL_VAULT>
            </PASSWORD_INFO>
        </ROOT_TOOL>
    </ROOT_TOOLS>
</UNIX_AUTH_PARAMS>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/api/4.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2026-07-21T02:40:52Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Updated</TEXT>
```

```
                    <ID_SET>
                        <ID>9439474</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - List Unix Authentication record with with root delegtion AD

API request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/auth/unix/?action=list' \
--header 'X-Requested-With: curl demo' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM "
<qualys_base_url>/api/4.0/fo/auth/unix/dtd/auth_list_output.dtd">
    <!-- This report was generated with an evaluation version of Qualys
//-->
    <AUTH_UNIX_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-07-21T02:43:57Z</DATETIME>
            <AUTH_UNIX_LIST>
                <AUTH_UNIX>
                    <ID>8679211</ID>
                    <TITLE>
                        <![CDATA[test_auth_unix_CyberArkAIMvault]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[admin]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <PORT>2222</PORT>
                    <IP_SET>
                        <IP>xxx.xx.xx.xx </IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2026-04-28T19:18:39Z</DATETIME>
                        <BY>scan_at</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-04-28T19:18:39Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[creating auth profile for automation
user1]]>
```

```
            </COMMENTS>
        </AUTH_UNIX>
        <AUTH_UNIX>
            <ID>8972423</ID>
            <TITLE>
                <![CDATA[test_auth_unix]]>
            </TITLE>
            <USERNAME>
                <![CDATA[admin]]>
            </USERNAME>
            <SKIP_PASSWORD>0</SKIP_PASSWORD>
            <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
            <TARGET_TYPE>
                <![CDATA[Auto (default)]]>
            </TARGET_TYPE>
            <ROOT_TOOL_INFO_LIST>
                <ROOT_TOOL_INFO>
                    <ID>3829135</ID>
                    <ROOT_TOOL>Sudo</ROOT_TOOL>
                    <PASSWORD_INFO type="basic" />
                </ROOT_TOOL_INFO>
            </ROOT_TOOL_INFO_LIST>
            <PORT>2222</PORT>
            <IP_SET>
                <IP>172.xx.xx.xx </IP>
            </IP_SET>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
                <DATETIME>2026-05-26T20:31:57Z</DATETIME>
                <BY>scan_su</BY>
            </CREATED>
            <LAST_MODIFIED>
                <DATETIME>2026-05-26T20:31:57Z</DATETIME>
            </LAST_MODIFIED>
            <COMMENTS>
                <![CDATA[creating auth profile for automation
user]]>
            </COMMENTS>
        </AUTH_UNIX>
        <AUTH_UNIX>
            <ID>9006410</ID>
            <TITLE>
                <![CDATA[test_auth_unix_Kerberos_IP_DNSRealm]]>
            </TITLE>
            <USERNAME>
                <![CDATA[admin]]>
            </USERNAME>
            <SKIP_PASSWORD>0</SKIP_PASSWORD>
            <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
            <TARGET_TYPE>
                <![CDATA[Auto (default)]]>
            </TARGET_TYPE>
            <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
            <REALM_DISCOVERY>
```

```
                        <![CDATA[dns]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[test]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[testtest]]>
                    </USER_KDC>
                    <ROOT_TOOL_INFO_LIST>
                        <ROOT_TOOL_INFO>
                            <ID>3839139</ID>
                            <ROOT_TOOL>Sudo</ROOT_TOOL>
                            <PASSWORD_INFO type="basic" />
                        </ROOT_TOOL_INFO>
                    </ROOT_TOOL_INFO_LIST>
                    <PORT>2222</PORT>
                    <IP_SET>
                        <IP>xxx.xx.xx.xx</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2026-05-29T19:27:14Z</DATETIME>
                        <BY>scan_at</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-05-29T19:27:14Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[creating auth profile for automation
user1]]>
                    </COMMENTS>
                </AUTH_UNIX>
                <AUTH_UNIX>
                    <ID>9339403</ID>
                    <TITLE>
                        <![CDATA[test_auth_unix_Kerberos_IP]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[admin]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[manual]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[test]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[testtest]]>
```

```
                    </USER_KDC>
                    <SERVICE_REALM>
                        <![CDATA[test]]>
                    </SERVICE_REALM>
                    <SERVICE_KDC>
                        <![CDATA[test]]>
                    </SERVICE_KDC>
                    <ROOT_TOOL_INFO_LIST>
                        <ROOT_TOOL_INFO>
                            <ID>3916136</ID>
                            <ROOT_TOOL>Sudo</ROOT_TOOL>
                            <PASSWORD_INFO type="basic" />
                        </ROOT_TOOL_INFO>
                    </ROOT_TOOL_INFO_LIST>
                    <PORT>2222</PORT>
                    <IP_SET>
                        <IP>xxx.xx.xx.xx</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2026-06-30T19:18:08Z</DATETIME>
                        <BY>scan_at</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-06-30T19:18:08Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[creating auth profile for automation
user1]]>
                    </COMMENTS>
                </AUTH_UNIX>
                <AUTH_UNIX>
                    <ID>9362189</ID>
                    <TITLE>
                       <![CDATA[test_auth_unix_Kerberos_IP_singleRealm]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[admin]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <KERBEROS_AUTHENTICATION>1</KERBEROS_AUTHENTICATION>
                    <REALM_DISCOVERY>
                        <![CDATA[single]]>
                    </REALM_DISCOVERY>
                    <USER_REALM>
                        <![CDATA[test]]>
                    </USER_REALM>
                    <USER_KDC>
                        <![CDATA[testtest]]>
                    </USER_KDC>
```

```
                    <ROOT_TOOL_INFO_LIST>
                        <ROOT_TOOL_INFO>
                            <ID>3925254</ID>
                            <ROOT_TOOL>Sudo</ROOT_TOOL>
                            <PASSWORD_INFO type="basic" />
                        </ROOT_TOOL_INFO>
                    </ROOT_TOOL_INFO_LIST>
                    <PORT>2222</PORT>
                    <IP_SET>
                        <IP>172.xx.xx.xx</IP>
                    </IP_SET>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2026-07-03T19:19:03Z</DATETIME>
                        <BY>scan_at</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-07-03T19:19:03Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[creating auth profile for automation
user1]]>
                    </COMMENTS>
                </AUTH_UNIX>
                <AUTH_UNIX>
                    <ID>9439474</ID>
                    <TITLE>
                        <![CDATA[Unix_HashiCorp_AD_RootDelegation]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[qualys]]>
                    </USERNAME>
                    <SKIP_PASSWORD>0</SKIP_PASSWORD>
                    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                    <TARGET_TYPE>
                        <![CDATA[Auto (default)]]>
                    </TARGET_TYPE>
                    <ROOT_TOOL_INFO_LIST>
                        <ROOT_TOOL_INFO>
                            <ID>3945137</ID>
                            <ROOT_TOOL>Sudo</ROOT_TOOL>
                            <PASSWORD_INFO type="vault">
                                <DIGITAL_VAULT>
                                    <DIGITAL_VAULT_ID>
                                        <![CDATA[2468704]]>
                                    </DIGITAL_VAULT_ID>
                                    <DIGITAL_VAULT_TYPE>
                                        <![CDATA[HashiCorp]]>
                                    </DIGITAL_VAULT_TYPE>
                                    <DIGITAL_VAULT_TITLE>
                                      <![CDATA[HashiCorp_Vault_AD_Test]]>
                                    </DIGITAL_VAULT_TITLE>
                                    <VAULT_SECRET_KV_PATH>
                                        <![CDATA[unix/hosts]]>
```

```
                    </VAULT_SECRET_KV_PATH>
                    <VAULT_SECRET_KV_NAME>
                        <![CDATA[updated-root-account]]>
                    </VAULT_SECRET_KV_NAME>
                    <VAULT_USE_AD_HASHICORP>
                        <![CDATA[1]]>
                    </VAULT_USE_AD_HASHICORP>
                </DIGITAL_VAULT>
            </PASSWORD_INFO>
        </ROOT_TOOL_INFO>
    </ROOT_TOOL_INFO_LIST>
    <IP_SET>
        <IP>xx.xx.xx.xx</IP>
    </IP_SET>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
        <DATETIME>2026-07-21T02:25:54Z</DATETIME>
        <BY>scan_at</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2026-07-21T02:40:52Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_UNIX>
<AUTH_UNIX>
    <ID>9439475</ID>
    <TITLE>
        <![CDATA[Unix_HashiCorp_AD_RootDelegation1]]>
    </TITLE>
    <USERNAME>
        <![CDATA[qualys]]>
    </USERNAME>
    <SKIP_PASSWORD>0</SKIP_PASSWORD>
    <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
    <TARGET_TYPE>
        <![CDATA[Auto (default)]]>
    </TARGET_TYPE>
    <ROOT_TOOL_INFO_LIST>
        <ROOT_TOOL_INFO>
            <ID>3945136</ID>
            <ROOT_TOOL>Sudo</ROOT_TOOL>
            <PASSWORD_INFO type="vault">
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[2468704]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[HashiCorp]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                      <![CDATA[HashiCorp_Vault_AD_Test]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_SECRET_KV_PATH>
                        <![CDATA[unix/hosts]]>
                    </VAULT_SECRET_KV_PATH>
```

```
                                <VAULT_SECRET_KV_NAME>
                                    <![CDATA[root-account]]>
                                </VAULT_SECRET_KV_NAME>
                                <VAULT_USE_AD_HASHICORP>
                                    <![CDATA[1]]>
                                </VAULT_USE_AD_HASHICORP>
                            </DIGITAL_VAULT>
                        </PASSWORD_INFO>
                    </ROOT_TOOL_INFO>
                </ROOT_TOOL_INFO_LIST>
                <IP_SET>
                    <IP>xx.xx.xx.xx</IP>
                </IP_SET>
                <LOGIN_TYPE>
                    <![CDATA[vault]]>
                </LOGIN_TYPE>
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[2468704]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[HashiCorp]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                        <![CDATA[HashiCorp_Vault_AD_Test]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_SECRET_KV_PATH>
                        <![CDATA[unix/hosts]]>
                    </VAULT_SECRET_KV_PATH>
                    <VAULT_SECRET_KV_NAME>
                        <![CDATA[login-account]]>
                    </VAULT_SECRET_KV_NAME>
                    <VAULT_SECRET_KV_KEY>
                        <![CDATA[password]]>
                    </VAULT_SECRET_KV_KEY>
                    <VAULT_USE_AD_HASHICORP>
                        <![CDATA[0]]>
                    </VAULT_USE_AD_HASHICORP>
                </DIGITAL_VAULT>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2026-07-21T02:32:11Z</DATETIME>
                    <BY>scan_at</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2026-07-21T02:32:11Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_UNIX>
        </AUTH_UNIX_LIST>
    </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

Sample - Delete Unix Authentication record with with root delegtion AD

API request:

```
curl --location --request POST '
<qualys_base_url>/api/4.0/fo/auth/unix/?action=delete&ids=9439475' \
--header 'X-Requested-With: curl demo' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM "
<qualys_base_url>/api/4.0/batch_return.dtd">
    <BATCH_RETURN>
        <RESPONSE>
            <DATETIME>2026-07-21T02:49:33Z</DATETIME>
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Deleted</TEXT>
                    <ID_SET>
                        <ID>9439475</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

More Samples

Qualys API - Unix Authentication API samples (GitHub)

DTDs for auth type “unix”

<platform API server>/api/4.0/batch_return.dtd

<platform API server>/api/4.0/fo/auth/unix/auth_unix_list_output.dtd

For Unix type record type only, root delegation tools and private-key certificates are specified using the unix_auth_params.dtd here

<platform API server>/api/4.0/fo/auth/unix/unix_auth_params.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/auth/sybase/	Active	Active
/api/3.0/fo/auth/sybase/	February 2027	August 2027
/api/2.0/fo/auth/sybase/	December 2025	December 2026

Network SSH Record

/api/2.0/fo/auth/network_ssh/

[POST]

Network SSH authentication is supported for vulnerability and compliance scans. The new Network SSH API (/api/2.0/fo/auth/network_ssh/) lets you list, create, update and delete Network SSH authentication records. This authentication supports SSH2 format.

Network SSH authentication record can be used in place of the Cisco and Checkpoint Firewall authentication records. This authentication record has all the same functionality as the Cisco and Checkpoint Firewall records and additional support for target_type field similar to Unix authentication record.

Network SSH authentication records support for password and password2 fields with vaults. This password2 field is similar to expert_password field (for Checkpoint Firewall sub-type) and enable_password field (for Cisco sub-type).

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
id={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
port={value}	(Optional) The port the database name is running on.
target_type={value}	(Optional) Specify the target type.
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a Network SSH account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(Optional) The password of the Network SSH account to be used for authentication. Maximum 100 characters (ascii).

Parameter	Description
cleartext_password={0|1}	(Optional) When not specified, the scanning engine only uses strong password encryption for remote login. Specify 1 to allow your password to be transmitted in clear text when connecting to services which do not support strong password encryption. For more info, search for "Clear Text Password" in online help. For a create request, if cleartext_password=1, the password parameter is required. For an update request, if cleartext_password=1, and the record does not have a password set, then cleartext_password=1 is *silently ignored*.
password2={value}	(Optional) This password2 field is similar to existing expert_password field (for Checkpoint Firewall sub-type) and enable_password field (for Cisco sub-type). For Checkpoint Firewall: The password required for executing the "expert" command on the target hosts. The password may include 1-31 characters (ascii). For Cisco: The password required for executing the "enable" command on the target hosts. The password may include 1-31 characters (ascii).
login_type={value}	(Optional) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See "Vault Definition" in the API user guide.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See Vault Support matrix in the API user guide.
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) Secrets Engine in HashiCorp authentication records. Specify 1 to use Active Directory (AD) Secrets Engine in the authentication records.
p2_login_type={value}	(Optional) p2 Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See "Vault Definition" in the API user guide.

Parameter	Description
p2_<vault parameters>={value}	(Optional) If p2_login_type is vault then all vault parameter fields must be added with prefix 'p2_' For example, p2_vault_type, p2_vault_id. Vault specific parameters required depend on the vault type you've selected. See “Vault Definition” in the API user guide.
ips={value}	(Required to create record) The IP address(es) for the targets you want to authenticate to. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. An IP added to the Network SSH authentication record cannot added in Unix, Cisco or Checkpoint authentication records. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
{XML File}	(Optional) XML file where you define private-key certificates. These are defined using this DTD: <platform API server>/api/2.0/fo/auth/network_ssh/network_ssh_auth_params.dtd

Sample - Create Network SSH Authentication Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/auth/network_ssh/?action=
create&username=abc&title=a11&ips=10.10.110.12&password=<PASSWORD>
&port=270,17,122&cleartext_password=1&target_type=A10&password2=12
34"
```

API request using xml file:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"<qualys_base_url>/api/2.0/fo/auth/network_ssh/?action=create&user
name=abc&title=new%201&ips=10.10.110.12&password=<PASSWORD>&commen
ts=new%20auth%20record&port=270,17,122&cleartext_password=1&target
_type=A10&p2_login_type=vault&p2_vault_type=Thycotic%20Secret%20Se
rver&p2_vault_id=41014&p2_secret_name=sc_name&password2=1234&login
_type=vault&vault_type=Thycotic%20Secret%20Server&vault_id=41014&s
ecret_name=bder&details=All"
--data-binary @add_params.xml
```

Content of add_params.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<NETWORK_SSH_AUTH_PARAMS>
<PRIVATE_KEY_CERTIFICATES>
<PRIVATE_KEY_CERTIFICATE>
<PRIVATE_KEY_INFO type="vault">
<DIGITAL_VAULT>
<VAULT_TYPE>CA PAM</VAULT_TYPE>
<VAULT_ID>41022</VAULT_ID>
<VAULT_DEVICE_NAME>hq_device</VAULT_DEVICE_NAME>
<VAULT_APP_NAME>APP_NAME</VAULT_APP_NAME>
</DIGITAL_VAULT>
</PRIVATE_KEY_INFO>
<PASSPHRASE_INFO type="vault">
<DIGITAL_VAULT>
<VAULT_TYPE>CA PAM</VAULT_TYPE>
<VAULT_ID>41022</VAULT_ID>
<VAULT_DEVICE_NAME>hq_device</VAULT_DEVICE_NAME>
<VAULT_APP_NAME>APP_NAME</VAULT_APP_NAME>
</DIGITAL_VAULT>
</PASSPHRASE_INFO>
</PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATES>
</NETWORK_SSH_AUTH_PARAMS>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-04-21T06:34:05Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>102451</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Network SSH Authentication Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/auth/network_ssh/?username=abc&p
assword2=1234&action=update&ids=102419"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-04-21T06:37:07Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>102419</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Network SSH Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=delete&ids=4474043"
"https://qualysapi.qualys.com/api/2.0/fo/auth/network_ssh/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-01-12T14:48:56Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>4474043</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
```

```
</BATCH_RETURN>
```

Sample - List Network SSH Records

API request:

```
curl -k -u agms_nb:Qatemp123# -s -S -H 'X-Requested-With:curl
demo2' -d "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/network_ssh/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NETWORK_SSH_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/network_ssh/dtd/auth
_list_output.dtd">
<AUTH_NETWORK_SSH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-09-05T08:44:22Z</DATETIME>
    <AUTH_NETWORK_SSH_LIST>
      <AUTH_NETWORK_SSH>
        <ID>3441133</ID>
        <TITLE><![CDATA[API_Unix_Auth_Unix_21]]></TITLE>
        <USERNAME><![CDATA[Qualys]]></USERNAME>
        <IP_SET>
          <IP>10.10.10.10</IP>
        </IP_SET>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <TARGET_TYPE><![CDATA[Auto (default)]]></TARGET_TYPE>
        <PRIVATE_KEY_CERTIFICATE_LIST>
          <PRIVATE_KEY_CERTIFICATE>
            <ID>2274448</ID>
            <PRIVATE_KEY_INFO type="basic">
              <PRIVATE_KEY type="pkcs8" />
            </PRIVATE_KEY_INFO>
            <PASSPHRASE_INFO type="basic" />
          </PRIVATE_KEY_CERTIFICATE>
        </PRIVATE_KEY_CERTIFICATE_LIST>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2023-09-04T15:43:07Z</DATETIME>
          <BY>agms_nb</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2023-09-04T15:43:07Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_NETWORK_SSH>
```

```
    </AUTH_NETWORK_SSH_LIST>
  </RESPONSE>
</AUTH_NETWORK_SSH_LIST_OUTPUT>
```

DTDs for auth type “network_ssh”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/network_ssh/dtd/auth_list_output.dtd

Private-key certificates are specified using the network_ssh_auth_params.dtd here

<platform API server>/api/2.0/fo/auth/network_ssh/network_ssh_auth_params.dtd

VMware Record

/api/2.0/fo/auth/vmware/

[POST]

Create, update, list and delete VMware records for authenticating to vSphere components running vSphere v4.x and 5.x. Vulnerability and compliance scans are supported (using VM, PC).

How it works - The VMware record allows for connections to the vSphere API for vSphere 5.x and 4.x. The vSphere API is a SOAP API used by all vSphere components, including VMware ESXi, VMware ESX, VMware vCenter Server, and the VMware vCenter Server Appliance. By default, the API connection occurs over an encrypted SSL web services connection on port 443.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Login credentials	
username={value}	(Required to create record, optional to update record) The user name for a VMware account. A maximum of 13 characters (ascii) may be specified.
password={value}	(To create record password or login_type=vault is required) The password for a VMware account. Maximum 100 characters (ascii).
login_type={**basic**|vault|vcenter}	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition Set to “vcenter” to scan ESXi hosts through vCenter. The VMware record will include your ESXi IP addresses. You also need a vCenter authentication record with the vCenter IP addresses that map to your ESXi hosts.

Parameter	Description
port={value}	(Optional) The service communicates with ESXi web services on port 443 and another port can be configured. When unspecified, port 443 is used.
hosts={value}	(Optional) A list of FQDNs for the hosts that correspond to all ESXi host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed. Multiple hosts are comma separated.
ssl_verify={value}	(Optional) Specify “all” for a complete SSL certificate validation. Specify “skip” if the host SSL certificate is self-signed or uses an SSL certificate signed by a custom root CA. Specify “none” for no SSL verification.
is_disconnect={**0**|1}	(Optional) Specify 0 (the default) if the ESXi hosts are not disconnected. Specify 1 if the ESXi hosts are disconnected and you don’t want to send any traffic to the ESXi hosts. Note: is_disconnect=1 is only valid when login_type=vcenter
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record’s credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request. **Note**: If you set “is_disconnect=1” and add IPs that are already associated with a Unix record, the VMware ESXi record is not created or updated. Instead, an error is returned in the response. You must remove the IPs from the non-applicable record to resolve the error.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Parameter	Description
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.

Sample - Create VMware record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&title=NewVMwareRecordWithAPI&username=USERNAME&pass
word=<PASSWORD>&ips=10.10.10.2-10.10.10.4"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/" >
apiOutputCreateVMwareRecord.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-02-13T21:16:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>30486</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update VMware record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=update&ids=1344232&is_disconnect=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version=""1.0"" encoding=""UTF-8"" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-03T12:19:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1344232</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List VMware record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X "POST" -
d "action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version=""1.0"" encoding=""UTF-8"" ?>
<!DOCTYPE AUTH_VMWARE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/auth_vmware_l
ist_output.dtd">
<AUTH_VMWARE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-11-22T07:32:21Z</DATETIME>
    <AUTH_VMWARE_LIST>
      <AUTH_VMWARE>
        <ID>409187</ID>
        <TITLE><![CDATA[VMware_Basic]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <PORT>443</PORT>
        <SSL_VERIFY><![CDATA[skip]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
```

```
      <DATETIME>2020-01-23T07:55:13Z</DATETIME>
      <BY>joe_user</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2020-01-23T07:55:13Z</DATETIME>
    </LAST_MODIFIED>
  </AUTH_VMWARE>
  <AUTH_VMWARE>
    <ID>1344231</ID>
    <TITLE><![CDATA[VMware_Disconnected_Disabled]]></TITLE>
    <PORT>443</PORT>
    <IP_SET>
      <IP>10.11.12.13</IP>
    </IP_SET>
    <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
    <DISCONNECTED_ESXI>0</DISCONNECTED_ESXI>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
      <DATETIME>2021-11-03T12:09:53Z</DATETIME>
      <BY>joe_user</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2021-11-10T13:11:23Z</DATETIME>
    </LAST_MODIFIED>
  </AUTH_VMWARE>
  <AUTH_VMWARE>
    <ID>1344232</ID>
    <TITLE><![CDATA[VMware_Disconnected_Enabled]]></TITLE>
    <PORT>443</PORT>
    <IP_SET>
      <IP>8.9.10.11</IP>
    </IP_SET>
    <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
    <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
      <DATETIME>2021-11-03T12:16:36Z</DATETIME>
      <BY>joe_user</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2021-11-10T13:10:17Z</DATETIME>
    </LAST_MODIFIED>
  </AUTH_VMWARE>
</AUTH_VMWARE_LIST>
<GLOSSARY>
```

```
        <USER_LIST>
          <USER>
            <USER_LOGIN>joe_user</USER_LOGIN>
            <FIRST_NAME>Joe</FIRST_NAME>
            <LAST_NAME>User</LAST_NAME>
          </USER>
        </USER_LIST>
      </GLOSSARY>
    </RESPONSE>
  </AUTH_VMWARE_LIST_OUTPUT>
```

DTDs for auth type “vmware”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/vmware/auth_vmware_list_output.dtd

VMware NSX Record

For API version information, refer to the API Version History section.

V2.0 | V3.0

V2.0

/api/2.0/fo/auth/nsx/

[POST]

Create, update, list, and delete VMware NSX records for authenticated scans of VMware NSX environments. This capability allows you to securely authenticate to NSX managed components using VMware NSX credentials, enabling authenticated vulnerability and compliance assessments of supported NSX services and appliances.

This simplifies secure access to NSX environments, improves assessment accuracy through authenticated scanning, and reduces operational overhead when managing credentials at scale.

This supports both VM and PA.

Both basic and vault based authentication are supported. Vault based authentication is

supported only for HashiCorp Vault. For the Vault based authentication, see Vault Support matrix for the supported vaults.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET).
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Login credentials	
username={value}	(Required to create record, optional to update record) The username to be used for authentication to NSX.
password={value}	The password to be used for authentication to NSX.

Parameter	Description
login_type={**basic**|vault|vcenter}	The login type is basic by default. You can choose vault (for vault based authentication). Set to vault if a third party vault is used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition
port={value}	(Optional) The port number that the NSX instance is running on.
hosts={value}	(Optional) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
ssl_verify_with_host={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
Target Hosts	
ips={value}	(Required to create record) IPs to be added to your NSX record. You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed
vault_id={value}	(Required if login_type=vault). The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability.

Sample - Create NSX record

API request:

```
curl --location '
/api/2.0/fo/auth/nsx/index.php?action=create&title=1234NSXkk235&ips=10.xx
x.xxx.xxx&username=root&password=Password%40456&port=443' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=create'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:32:56Z</DATETIME>
        <BATCH_LIST>
```

```
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update NSX record

API request:

```
curl --location '
/api/2.0/fo/auth/nsx/index.php?action=update%20&username=root&password=Pa
ssword%40456&ids=11629987' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=update'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:37:10Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete NSX record

API request:

```
curl --location '
/api/2.0/fo/auth/nsx/index.php?action=delete&ids=11629987' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=delete'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
```

```
"<qualys_base_url>/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:41:22Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List NSX record

API request:

```
curl --location --request GET '
/api/2.0/fo/auth/nsx/index.php?action=list' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=list'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NSX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/auth/nsx/auth_nsx_list_output.dtd">
<AUTH_NSX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-12-11T10:31:18Z</DATETIME>
        <AUTH_NSX_LIST>
            <AUTH_NSX>
                <ID>11500969</ID>
                <TITLE>
                    <![CDATA[nsx_auth]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[admin]]>
                </USERNAME>
                <SSL_VERIFY>
                    <![CDATA[0]]>
                </SSL_VERIFY>
                <IP_SET>
                    <IP>10.xxx.xxx.xxx</IP>
                </IP_SET>
                <PORT>
                    <![CDATA[443]]>
                </PORT>
                <SSL_VERIFY_WITH_HOST>
                    <![CDATA[0]]>
```

```
    </SSL_VERIFY_WITH_HOST>
    <HOSTS>
        <![CDATA[www.google.com]]>
    </HOSTS>
    <LOGIN_TYPE>
        <![CDATA[basic]]>
    </LOGIN_TYPE>
    <CREATED>
        <DATETIME>2025-11-28T07:48:06Z</DATETIME>
        <BY>username</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2025-12-10T06:45:07Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_NSX>
<AUTH_NSX>
    <ID>11541079</ID>
    <TITLE>
        <![CDATA[mob_api12345]]>
    </TITLE>
    <USERNAME>
        <![CDATA[root]]>
    </USERNAME>
    <IP_SET>
        <IP>111.xx.xx.xx</IP>
    </IP_SET>
    <PORT>
        <![CDATA[443]]>
    </PORT>
    <LOGIN_TYPE>
        <![CDATA[basic]]>
    </LOGIN_TYPE>
    <CREATED>
        <DATETIME>2025-12-04T05:49:51Z</DATETIME>
        <BY>username</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2025-12-04T05:49:51Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_NSX>
<AUTH_NSX>
    <ID>11541968</ID>
    <TITLE>
        <![CDATA[1234NSX6]]>
    </TITLE>
    <USERNAME>
        <![CDATA[root]]>
    </USERNAME>
    <IP_SET>
        <IP>10.xxx.xxx.xxx</IP>
    </IP_SET>
    <PORT>
        <![CDATA[445]]>
    </PORT>
```

```
                    <LOGIN_TYPE>
                        <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <CREATED>
                        <DATETIME>2025-12-04T06:42:32Z</DATETIME>
                        <BY>vmspxtb</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2025-12-04T08:50:33Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_NSX>
                <AUTH_NSX>
                    <ID>11542967</ID>
                    <TITLE>
                        <![CDATA[1234NSXkk23]]>
                    </TITLE>
                    <USERNAME>
                        <![CDATA[root]]>
                    </USERNAME>
                    <IP_SET>
                        <IP>10.xxx.xxx.xxx</IP>
                    </IP_SET>
                    <PORT>
                        <![CDATA[443]]>
                    </PORT>
                    <LOGIN_TYPE>
                        <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <CREATED>
                        <DATETIME>2025-12-04T09:11:25Z</DATETIME>
                        <BY>vmspxtb</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2025-12-04T09:11:25Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_NSX>
            </AUTH_NSX_LIST>
        </RESPONSE>
    </AUTH_NSX_LIST_OUTPUT>
```

DTDs for auth type “NSX”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>

/api/2.0/fo/auth/nsx/auth_nsx_list_output.dtd

V3.0

/api/3.0/fo/auth/nsx/

[POST]

Create, update, list, and delete VMware NSX records for authenticated scans of VMware NSX environments. This capability allows you to securely authenticate to NSX managed components using VMware NSX credentials, enabling authenticated vulnerability and compliance assessments of supported NSX services and appliances.

This simplifies secure access to NSX environments, improves assessment accuracy through authenticated scanning, and reduces operational overhead when managing credentials at scale.

This supports both VM and PA.

Both basic and vault based authentication are supported. Vault based authentication is

supported only for HashiCorp Vault. For the Vault based authentication, see Vault Support matrix for the supported vaults.

You can use Active Directory (AD) support with HashiCorp Vault when you create, update, list, and delete VMware NSX authentication records for authenticated scans of VMware NSX environments. This enables you to securely retrieve AD credentials from Vault.

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET).
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
Login credentials	
username={value}	(Required to create record, optional to update record) The username to be used for authentication to NSX.
password={value}	The password to be used for authentication to NSX.
login_type={**basic**|vault|vcenter}	The login type is basic by default. You can choose vault (for vault based authentication). Set to vault if a third party vault is used to retrieve the password. Vault parameters need to be provided in the record. See Vault Definition
port={value}	(Optional) The port number that the NSX instance is running on.
hosts={value}	(Optional) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.

Parameter	Description
ssl_verify_with_host={0|1}	(Optional) SSL verification. Set to 1 if you want to verify the server's certificate is valid and trusted.
Target Hosts	
ips={value}	(Required to create record) IPs to be added to your NSX record. You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated. Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed
vault_id={value}	(Required if login_type=vault). The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability.
use_ad_hashicorp={0|1}	(Required) Specify 1 to enable the Active Directory when the HashiCorp Vault is selected.

Sample - Create NSX record

API request:

```
curl --location '
/api/3.0/fo/auth/nsx/index.php?action=create&title=1234NSXkk235&ips=10.xx
x.xxx.xxx&username=root&password=Password%40456&port=443' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=create'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:32:56Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update NSX record

API request:

```
curl --location '
/api/3.0/fo/auth/nsx/index.php?action=update%20&username=root&password=Pa
ssword%40456&ids=11629987' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=update'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:37:10Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete NSX record

API request:

```
curl --location '
/api/3.0/fo/auth/nsx/index.php?action=delete&ids=11629987' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=delete'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2025-12-11T10:41:22Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>11629987</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List NSX record

API request:

```
curl --location --request GET '
/api/3.0/fo/auth/nsx/index.php?action=list' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=list'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NSX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/auth/nsx/auth_nsx_list_output.dtd">
<AUTH_NSX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-12-11T10:31:18Z</DATETIME>
        <AUTH_NSX_LIST>
            <AUTH_NSX>
                <ID>11500969</ID>
                <TITLE>
                    <![CDATA[nsx_auth]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[admin]]>
                </USERNAME>
                <SSL_VERIFY>
                    <![CDATA[0]]>
                </SSL_VERIFY>
                <IP_SET>
                    <IP>10.xxx.xxx.xxx</IP>
                </IP_SET>
                <PORT>
                    <![CDATA[443]]>
                </PORT>
                <SSL_VERIFY_WITH_HOST>
                    <![CDATA[0]]>
                </SSL_VERIFY_WITH_HOST>
                <HOSTS>
                    <![CDATA[www.google.com]]>
                </HOSTS>
                <LOGIN_TYPE>
                    <![CDATA[basic]]>
                </LOGIN_TYPE>
                <CREATED>
                    <DATETIME>2025-11-28T07:48:06Z</DATETIME>
                    <BY>username</BY>
                </CREATED>
```

```
    <LAST_MODIFIED>
        <DATETIME>2025-12-10T06:45:07Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_NSX>
<AUTH_NSX>
    <ID>11541079</ID>
    <TITLE>
        <![CDATA[mob_api12345]]>
    </TITLE>
    <USERNAME>
        <![CDATA[root]]>
    </USERNAME>
    <IP_SET>
        <IP>111.xx.xx.xx</IP>
    </IP_SET>
    <PORT>
        <![CDATA[443]]>
    </PORT>
    <LOGIN_TYPE>
        <![CDATA[basic]]>
    </LOGIN_TYPE>
    <CREATED>
        <DATETIME>2025-12-04T05:49:51Z</DATETIME>
        <BY>username</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2025-12-04T05:49:51Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_NSX>
<AUTH_NSX>
    <ID>11541968</ID>
    <TITLE>
        <![CDATA[1234NSX6]]>
    </TITLE>
    <USERNAME>
        <![CDATA[root]]>
    </USERNAME>
    <IP_SET>
        <IP>10.xxx.xxx.xxx</IP>
    </IP_SET>
    <PORT>
        <![CDATA[445]]>
    </PORT>
    <LOGIN_TYPE>
        <![CDATA[basic]]>
    </LOGIN_TYPE>
    <CREATED>
        <DATETIME>2025-12-04T06:42:32Z</DATETIME>
        <BY>vmspxtb</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2025-12-04T08:50:33Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_NSX>
```

```
            <AUTH_NSX>
                <ID>11542967</ID>
                <TITLE>
                    <![CDATA[1234NSXkk23]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <IP_SET>
                    <IP>10.xxx.xxx.xxx</IP>
                </IP_SET>
                <PORT>
                    <![CDATA[443]]>
                </PORT>
                <LOGIN_TYPE>
                    <![CDATA[basic]]>
                </LOGIN_TYPE>
                <CREATED>
                    <DATETIME>2025-12-04T09:11:25Z</DATETIME>
                    <BY>vmspxtb</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2025-12-04T09:11:25Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_NSX>
        </AUTH_NSX_LIST>
    </RESPONSE>
</AUTH_NSX_LIST_OUTPUT>
```

Sample - Create a NSX record with AD enabled

API request:

```
curl --location ' /api/3.0/fo/auth/nsx/index.php' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer ' \
--data-urlencode 'action=create' \
--data-urlencode 'title=API NSX1211' \
--data-urlencode 'username=nsxuser' \
--data-urlencode 'ips=10.xxx.xxx.xxx' \
--data-urlencode 'port=443' \
--data-urlencode 'ssl_verify_with_host=1' \
--data-urlencode 'hosts=aa.aa' \
--data-urlencode 'login_type=vault' \
--data-urlencode 'vault_type=HashiCorp' \
--data-urlencode 'vault_id=4980801' \
--data-urlencode 'secret_kv_name=Test' \
--data-urlencode 'use_ad_hashicorp=1'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
```

```
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-07T06:09:35Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>12426426</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update NSX record with AD enabled

API request:

```
curl --location ' /api/3.0/fo/auth/nsx/index.php' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer ' \
--data-urlencode 'action=update' \
--data-urlencode 'login_type=vault' \
--data-urlencode 'vault_type=HashiCorp' \
--data-urlencode 'vault_id=4980801' \
--data-urlencode 'secret_kv_name=Test' \
--data-urlencode 'use_ad_hashicorp=1' \
--data-urlencode 'ids=12427803' \
--data-urlencode 'secret_kv_key=566'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-07T10:15:27Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>12427803</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List NSX record with AD enabled

API request:

```
curl --location '
/api/3.0/fo/auth/nsx/index.php?action=list&ids=12426322' \
```

```
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer ' \
--data-urlencode 'action=list
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_NSX_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/auth/nsx/auth_nsx_list_output.dtd">
<AUTH_NSX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-04-07T06:09:03Z</DATETIME>
        <AUTH_NSX_LIST>
            <AUTH_NSX>
                <ID>12426322</ID>
                <TITLE>
                    <![CDATA[NSX_AD ]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <IP_SET>
                    <IP>10.xxx.xxx.xxx</IP>
                </IP_SET>
                <PORT>
                    <![CDATA[443]]>
                </PORT>
                <SSL_VERIFY_WITH_HOST>
                    <![CDATA[0]]>
                </SSL_VERIFY_WITH_HOST>
                <LOGIN_TYPE>
                    <![CDATA[vault]]>
                </LOGIN_TYPE>
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[4980801]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[HashiCorp]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                        <![CDATA[Nutanix_HashiCorp]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_SECRET_KV_PATH>
                        <![CDATA[/tmp]]>
                    </VAULT_SECRET_KV_PATH>
                    <VAULT_SECRET_KV_NAME>
                        <![CDATA[adnsx]]>
                    </VAULT_SECRET_KV_NAME>
                    <VAULT_USE_AD_HASHICORP>
                        <![CDATA[1]]>
                    </VAULT_USE_AD_HASHICORP>
                </DIGITAL_VAULT>
```

```
                    <CREATED>
                        <DATETIME>2026-04-07T05:25:48Z</DATETIME>
                        <BY>vmspxtb</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2026-04-07T05:25:48Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_NSX>
            </AUTH_NSX_LIST>
        </RESPONSE>
    </AUTH_NSX_LIST_OUTPUT>
```

Sample - Delete NSX record with AD enabled

API request:

```
curl --location '
/api/3.0/fo/auth/nsx/index.php?action=delete&ids=12426426' \
--header 'X-Requested-With: curl demo2' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer  ' \
--data-urlencode 'action=list'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"<qualys_base_url>/api/3.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-07T06:29:43Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>12426426</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

DTDs for auth type “NSX”

<platform API server>/api/3.0/batch_return.dtd

<platform API server>

/api/3.0/fo/auth/nsx/auth_nsx_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/auth/nsx/	Active	Active
/api/2.0/fo/auth/nsx/	November 2026	May 2027

Windows Record

/api/2.0/fo/auth/windows/

[POST]

Create, update, list and delete Windows records for authenticating to Windows systems. Vulnerability and Compliance scans are supported (using VM, PC).

Download Qualys User Guide - Windows Authentication (.pdf)

Input Parameters

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
use_agentless_tracking=[**0**|1}	(Optional to create or update record) Specify 1 to enable Agentless Tracking.
Login credentials	
username={value}	(Required to create record, optional to update record) The username for the Windows account to be used for authentication on target hosts. The username may include 1-31 characters (ascii).
password={value}	(To create record password or login_type=vault is required) The password of the Windows account to be used for authentication. Maximum 100 characters (ascii).
login_type={**basic**|vault}	(To create record password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters need to be provided in the record. See Vault Definition
use_ad_hashicorp{0|1}	(Optional) Use to manage the utilization of Active Directory (AD) or Database Secrets Engines in HashiCorp authentication records. Specify 1 to use Active Directory (AD) or Database Secrets Engines in the authentication records.

Parameter	Description
windows_ad_domain={value}	(Optional) The Windows Active Directory domain name for domain level authentication. When specified, we'll use an Active Directory forest to authenticate to hosts in a certain domain within the framework. You'll need to enter a Fully Qualified Domain Name (FQDN). See Windows Domains This parameter and the windows_domain parameter cannot be specified in the same request. This parameter and the ips parameter cannot be specified in the same request.
windows_domain={value}	(Optional) The Windows NetBIOS domain name for domain level authentication. See Windows Domains This parameter and the windows_ad_domain parameter cannot be specified in the same request. When the ips parameter is also specified, the domain type is NetBIOS, User-Selected IPs. We'll use NetBIOS to authenticate to the IPs in the domain configuration. When the ips parameter is not specified, the domain type is NetBIOS, Service-Selected IPs. We'll use NetBIOS to authenticate to hosts in the domain using credentials stored on the domain.
ntlm={0|**1**}	(Optional) When not specified, NTLM authentication is enabled allowing the scanning engine to try the NTLM authentication protocol when negotiating authentication to target hosts. Specify ntlm=0 if you do not want the NTLM authentication protocol attempted for the hosts defined in the Windows record. This may be the case if the target hosts are running a version of Windows that supports a more secure authentication protocol like Kerberos. When NTLM authentication is disabled, it will not be attempted even if other methods like NTLMSSP and Kerberos fail.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.

Parameter	Description
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid when the networks feature is enabled) The network ID for the record.
Target Hosts with Tag Support	Note: Applicable only when you have Asset Tagging and Tag Support for Authentication Records enabled for your subscription.
asset_type={**ips**|asset_tags|ip_range_tag_rule}	(Optional) Indicates how assets will be defined in the record. Valid values are ips (the default), asset_tags, ip_range_tag_rule. When not specified, we'll use asset_type=ips ips - Specify this value to assign IP addresses/ranges to the record. asset_tags - Specify this value to add tags to the record for the assets you want included. IP addresses with the selected tags already assigned will be associated with the record. ip_range_tag_rule - Specify this value to add tags that have IP address ranges defined in the tag rule. All IP addresses defined in the tag rule will be associated with the record, including IPs that don't already have the tag assigned.
tag_set_by={**id**|name}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tags_include={tag1,tag2...}	(Required when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to include in the record. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.

Parameter	Description
tags_exclude={tag1,tag2,...}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Specify a tag set to exclude from the record. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. To specify tag names, you must also specify tag_set_by=name.
tag_include_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when asset_type=asset_tags or ip_range_tag_rule) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
ips={value}	(Required to create record when asset_type=ips or asset_type is not specified) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record when asset_type=ips) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record when asset_type=ips) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record when asset_type=ips) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.

Parameter	Description
Protocols	
For Windows domain level authentication, all three authentication protocols are supported. Kerberos and NTLMv2 are enabled by default in new records. If NTLM was enabled in a record prior to this release, then NTLMv1 is enabled. For Windows local host level authentication, NTLMv2 and NTLMv1 protocols are supported. NTLMv2 is enabled by default in new records. If NTLM was enabled in a record prior to this release, then NTLMv1 is enabled.	
kerberos={0|**1**}	(Optional) When not specified, Kerberos is enabled allowing the scanning engine to try Kerberos when negotiating authentication to target hosts. Specify kerberos=0 if you do not want Kerberos attempted. Kerberos is supported for domain authentication only. When kerberos=1 you must define a domain name for Windows Active Directory (windows_ad_domain) or NetBIOS (windows_domain) for the record.
ntlmv2={0|**1**}	(Optional) When not specified for a new record, NTLMv2 is enabled allowing the scanning engine to try NTLMv2 when negotiating authentication to target hosts. Specify ntlmv2=0 if you do not want NTLMv2 attempted.
ntlm={**0**|1}	(Optional) When not specified, NTLMv1 will not be attempted. Specify ntlm=1 to allow the scanning engine to try NTMLv1 when negotiating authentication to target hosts.
SMB signing	
SMB Signing option is disabled by default, meaning SMB signing is not required. This is the recommended setting. When disabled, we can authenticate to any Windows version regardless of how SMB signing is configured on the target. You are not protected, however, against man-in-the-middle (MITM) attacks.	
require_smb_signing={**0**|1}	(Optional) Set to 0 (default) when SMB signing is not required. Set value to 1 to require SMB signing. Should I require SMB signing? The answer is No in most cases. If you enable this option in your record, we will require each Windows target to support SMB signing. If SMB signing is disabled on a target host, authentication will fail and the host will not be scanned. This option protects against MITM attacks but we won't be able to authenticate to some hosts.
minimum_smb_version={value}	(Optional) The minimum SMB protocol version. Valid values are: 1, 2.0.2, 2.1, 3.0, 3.0.2, 3.1.1, and “” (empty string means no version set).

Windows Domains

- Supported domain types: Active Directory, NetBIOS User-Selected IPs, NetBIOS Service-Selected IPs.

- Authentication is performed at the local host level when a domain name is not defined for Active Directory (windows_ad_domain) or NetBIOS (windows_domain).

- Once a Windows record is saved, you cannot change the domain type from Active Directory to NetBIOS or from NetBIOS to Active Directory.

Sample - Create Windows Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=API_v2_utwrx_mp_Windows&username=User&passwor
d=<PASSWORD>&ips=10.10.10.200"
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/" >
apiOutputCreatewindowsRecord.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/batch_return
.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-13T21:16:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>30486</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Windows Record with Tags

In this sample, a new Windows record is created with asset_type=asset_tags.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/?action=crea
te&title=windows&username=root&asset_type=asset_tags&tags_include=
ag1&tag_include_selector=all&tags_exclude=ag20&tag_set_by=name&tag
_exclude_selector=all"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2021-03-11T00:45:31Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>204027</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List windows records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&ids=1310338&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_WINDOWS_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/auth_windows
_list_output.dtd">
<AUTH_WINDOWS_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2018-04-30T09:29:45Z</DATETIME>
   <AUTH_WINDOWS_LIST>
     <AUTH_WINDOWS>
       <ID>1310338</ID>
       <TITLE><![CDATA[Windows_Record_1]]></TITLE>
       <USERNAME><![CDATA[acme_jd]]></USERNAME>
       <IP_SET>
         <IP>10.10.10.202</IP>
       </IP_SET>
       <CREATED>
         <DATETIME>2018-04-30T09:28:00Z</DATETIME>
```

```
          <BY>acme_jd</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-04-30T09:28:43Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[My comments on Windows Record
1]]></COMMENTS>
      </AUTH_WINDOWS>
    </AUTH_WINDOWS_LIST>
    <GLOSSARY>
      <USER_LIST>
        <USER>
          <USER_LOGIN>acme_jd</USER_LOGIN>
          <FIRST_NAME>John</FIRST_NAME>
          <LAST_NAME>Doe</LAST_NAME>
        </USER>
      </USER_LIST>
    </GLOSSARY>
  </RESPONSE>
</AUTH_WINDOWS_LIST_OUTPUT>
```

DTDs for auth type “windows”

<platform API server>/api/2.0/batch_return.dtd

<platform API server>/api/2.0/fo/auth/windows/auth_windows_list_output.dtd

Oracle HTTP Server Record

/api/2.0/fo/auth/oracle_http_server/

[POST]

Create, update, list and delete Oracle HTTP Server records for authenticating to Unix and Windows systems. Vulnerability and Compliance scans are supported (using VM, PC). User permissions for this API are the same as other authentication record APIs. Note that the API supports authentication record creation only for Oracle Server installed on respective OS - Unix or Windows.

Input parameters

Parameter	Description
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
ids={value}	(Required to update or delete record) Record Oracle HTTP type auth record IDs to update. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
Unix Configuration	
unix_home_path={value}	(Required to create or update record if Unix working mode is selected) The root directory path for Oracle HTTP Server. Maximum of 255 characters.
unix_domain_path={value}	(Required to create or update record if Unix working mode is selected for Oracle HTTP Server 12c and higher) Absolute path to the top level directory where domains are configured. Maximum of 255 characters.
unix_inst_path={value}	(Required to create or update record if Unix working mode is selected for Oracle HTTP Server 11g) Absolute path to the top level directory where instances are configured. Maximum of 255 characters.

Parameter	Description
unix_inst_name={value}	(Optional) The Oracle HTTP server instance name. Maximum of 4000 characters.
Windows Configuration	
windows_home_path={value}	(Required to create or update record if Windows working mode is selected) The home directory path. Maximum of 255 characters.
windows_domain_path={value}	(Required to create or update record if Windows working mode is selected for Oracle HTTP Server 12c and higher) Absolute path to the top level directory where domains are configured. Maximum of 255 characters.
windows_inst_path={value}	(Required to create or update record if Windows working mode is selected for Oracle HTTP Server 11g) Absolute path to the top level directory where instances are configured. Maximum of 255 characters.
windows_inst_name={value}	(Optional) The Oracle HTTP server instance name. Maximum of 4000 characters.

Sample - Create Oracle HTTP Server 11g Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Unix
server_11&unix_home_path=/opt/Oracle/Middleware/Oracle_WT1&unix_in
st_path=/opt/Oracle/Middleware/Oracle_WT1/instances/instance1&unix
_inst_name=ohs1&ips=10.11.70.24"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T05:51:21Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530246</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 11g Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Windows_server_11&windows_home_pa
th=C:\Middleware\Oracle_WT1&windows_inst_path=C:\Middleware\Oracle
_WT1\instances\instance1&windows_inst_name=ohs1&ips=10.11.70.193"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T05:50:01Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530243</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 12c Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Unix
server_12&unix_home_path=/opt/Oracle/Middleware/Oracle_Home&unix_d
omain_path=/opt/Oracle/Middleware/Oracle_Home/user_projects/domain
s/base_domain&windows_inst_name=ohs1&ips=10.11.70.68"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T05:45:50Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
```

```
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530234</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 12c Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Windows
server_12&windows_home_path=C:\Oracle\Middleware\Oracle_Home&windo
ws_domain_path=C:\Oracle\Middleware\Oracle_Home\user_projects\doma
ins\base_domain&windows_inst_path=C:\Oracle\Middleware\Oracle_Home
\instances\instance1&windows_inst_name=ohs1&ips=10.11.70.84"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T05:48:55Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530241</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 11g Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530246&unix_home_path=/opt/Oracle/Middleware/O
racle_WT1&unix_inst_path=/opt/Oracle/Middleware/Oracle_WT1/instanc
es/instance1&unix_inst_name=ohs1&ips=10.11.70.24&comments=ohs unix
```

```
auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T06:01:38Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530246</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 11g Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530243&windows_home_path=C:\Middleware\Oracle_
WT1&windows_inst_path=C:\Middleware\Oracle_WT1\instances\instance1
&windows_inst_name=ohs1&ips=10.11.70.193&comments=ohs wind auth
record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T06:05:43Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530243</ID>
        </ID_SET>
      </BATCH>
```

```
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 12c Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530234&unix_home_path=/opt/Oracle/Middleware/O
racle_Home&unix_domain_path=/opt/Oracle/Middleware/Oracle_Home/use
r_projects/domains/base_domain&windows_inst_name=ohs1&ips=10.11.70
.68&comments=ohs unix auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T06:14:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530234</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 12c Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530241&windows_home_path=C:\Oracle\Middleware\
Oracle_Home&windows_domain_path=C:\Oracle\Middleware\Oracle_Home\u
ser_projects\domains\base_domain&windows_inst_path=C:\Oracle\Middl
eware\Oracle_Home\instances\instance1&windows_inst_name=ohs1&ips=1
0.11.70.84&comments=ohs wind auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-15T06:11:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530241</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List Oracle HTTP Server Records with Basic Details

API request:

```
curl -S -H 'X-Requested-With:curl demo2' -u "USERNAME:PASSWORD" -d
"action=list&details=Basic&ids=1505927"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"

XML output:
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/a
uth_oracle_http_server_list_output.dtd">
<AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-10-04T07:28:22Z</DATETIME>
    <AUTH_ORACLE_HTTP_SERVER_LIST>
      <AUTH_ORACLE_HTTP_SERVER>
        <ID>1505927</ID>
        <TITLE><![CDATA[Oracle_HTTP_Unix server]]></TITLE>
        <IP_SET>
          <IP>10.11.70.24</IP>
        </IP_SET>

        <UNIX>

<HOME_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1]]></HOME_PAT
H>
          <DOMAIN_PATH><![CDATA[]]></DOMAIN_PATH>

<INST_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1/instances/in
```

```
stance1]]></INST_PATH>
          <INST_NAME><![CDATA[ohs1]]></INST_NAME>
        </UNIX>
        <CREATED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
          <BY> john_doe</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_ORACLE_HTTP_SERVER>
    </AUTH_ORACLE_HTTP_SERVER_LIST>
  </RESPONSE>
</AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
```

Sample - List Oracle HTTP Server Records with All Details

API request:

```
curl -S -H 'X-Requested-With:curl demo2' -u "USERNAME:PASSWORD" -d
"action=list&details=All&ids=1505927"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/a
uth_oracle_http_server_list_output.dtd">
<AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-10-04T07:29:33Z</DATETIME>
    <AUTH_ORACLE_HTTP_SERVER_LIST>
      <AUTH_ORACLE_HTTP_SERVER>
        <ID>1505927</ID>
        <TITLE><![CDATA[Oracle_HTTP_Unix server]]></TITLE>
        <IP_SET>
          <IP>10.11.70.24</IP>
        </IP_SET>
        <UNIX>

<HOME_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1]]></HOME_PAT
H>
          <DOMAIN_PATH><![CDATA[]]></DOMAIN_PATH>

<INST_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1/instances/in
stance1]]></INST_PATH>
```

```
            <INST_NAME><![CDATA[ohs1]]></INST_NAME>
          </UNIX>
          <CREATED>
            <DATETIME>2019-10-03T12:24:04Z</DATETIME>
            <BY> john_doe</BY>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2019-10-03T12:24:04Z</DATETIME>
          </LAST_MODIFIED>
        </AUTH_ORACLE_HTTP_SERVER>
      </AUTH_ORACLE_HTTP_SERVER_LIST>
      <GLOSSARY>
        <USER_LIST>
          <USER>
            <USER_LOGIN> john_doe</USER_LOGIN>
            <FIRST_NAME>John</FIRST_NAME>
            <LAST_NAME>Doe</LAST_NAME>
          </USER>
        </USER_LIST>
      </GLOSSARY>
    </RESPONSE>
</AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
```

Sample - Delete Oracle HTTP Server Record(s)

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=delete&ids=1507609"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-10-04T09:19:50Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>1507609</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
```

```
    </RESPONSE>
  </BATCH_RETURN>
```

DTDs for auth type “oracle_http_server”

<platform API server>/api/2.0/fo/auth/auth_records.dtd

<platform API server>/api/2.0/fo/auth/oracle_http_server/auth_oracle_http_server_list_output.dtd

vCenter - ESXi Mapping Records

/api/2.0/fo/auth/vcenter/vcenter_mapping/

[POST]

Input Parameters

The following table shows input parameters used for listing, importing and purging vCenter - ESXi mapping data.

Parameter	Description
echo_request={0|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
action={action}	(Required) One action (list, import or purge) required for the request.
id_min={value}	(Optional to list) Used to filter the XML output to show only vulnerabilities that have a QID number greater than or equal to a QID number you specify.
id_max={value}	(Optional to list) Used to filter the XML output to show only vulnerabilities that have a QID number less than or equal to a QID number you specify.
output_format={XML|**CSV**}	(Optional to list) Specifies the format of the mapping list output. When not specified, the output format is CSV. A valid value is XML or CSV.
truncation_limit={value}	(Optional to list) Specifies the maximum number records listed per request.
vcenter_ip={value}	(Optional to list) Specifies the IP address of the vCenter.
esxi_ip={value}	(Optional to list) Specifies the IP address of the ESXi server.
network_id={1|**0**}	(Optional) By default, the parameter is set to 0. If this parameter is not provided, it will be Global Default Network.
csv_data={value}	(Required to import and purge) The CSV data file containing the vCenter - ESXi mapping records that you want to add/purge. This parameter or xml_data must be specified. The parameters csv_data and xml_data cannot be specified in the same request.
xml_data={value}	(Required to import and purge) The XML data file containing the vCenter - ESXi mapping records that you want to add/purge. This parameter or csv_data must be specified. The parameters csv_data and xml_data cannot be specified in the same request.

Sample - List vCenter - ESXi Mapping in CSV Format

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/?ac
tion=list"
```

OR

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/?ac
tion=list&output_format=csv"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
vCenter IP,ESXi IP,Mapping Data Source
"11.11.11.11","30.30.30.23","File"
"10.10.10.10","10.10.10.12","File"
----END_RESPONSE_BODY_CSV
----BEGIN_RESPONSE_FOOTER_CSV
"Status Message"
"Finished"
----END_RESPONSE_FOOTER_CSV
```

Sample - List vCenter - ESXi Mapping in XML Format

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/?ac
tion=list&output_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VCENTER_ESXI_MAP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/vce
nter_esxi_map_list_output.dtd">
<VCENTER_ESXI_MAP_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-05-22T16:49:40Z</DATETIME>
        <VCENTER_ESXI_MAP_LIST>
            <VCENTER_ESXI_MAP>
                <VCENTER_IP>11.11.11.11</VCENTER_IP>
                <ESXI_IP>30.30.30.23</ESXI_IP>
                <MAPPING_DATA_SOURCE>File</MAPPING_DATA_SOURCE>
            </VCENTER_ESXI_MAP>
            <VCENTER_ESXI_MAP>
                <VCENTER_IP>10.10.10.10</VCENTER_IP>
                <ESXI_IP>10.10.10.12</ESXI_IP>
                <MAPPING_DATA_SOURCE>File</MAPPING_DATA_SOURCE>
            </VCENTER_ESXI_MAP>
        </VCENTER_ESXI_MAP_LIST>
    </RESPONSE>
</VCENTER_ESXI_MAP_LIST_OUTPUT>
```

DTD for vCenter - ESXi Mapping

<platform API server>/api/2.0/fo/auth/vcenter/vcenter_mapping/vcenter_esxi_map_list_output.dtd

Sample - Import vCenter - ESXi Mapping

You'll be able to import vCenter - ESXi mapping in the CSV and XML format. You can provide CSV or XML data in API call or in the file.

CSV Data in API Call

Following is the sample API request when you want to import mapping using CSV data in API call.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' --data-binary
"action=import&csv_data=vCenter IP,ESXi
IP%0A10.10.10.10,10.10.10.11%0A10.10.10.10,10.10.10.12"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

XML Data in API Call

Following is the sample API request when you want to import mapping using XML data in API call.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' --data-binary
"action=import&xml_data=<VCENTER_ESXI_MAP_LIST><VCENTER_ESXI_MAP><VCENTER
_IP>11.11.11.11</VCENTER_IP><ESXI_IP>22.22.22.22</ESXI_IP></VCENTER_ESXI_
MAP><VCENTER_ESXI_MAP><VCENTER_IP>11.11.11.12</VCENTER_IP><ESXI_IP>22.22.
22.23</ESXI_IP></VCENTER_ESXI_MAP></VCENTER_ESXI_MAP_LIST>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

CSV Data in File

Following is the sample API request when you want to import the mapping using a file containing CSV data. In the sample request, **add.csv** is a CSV data file.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-with: curl' --data-binary
"@add.csv"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

Sample content of **add.csv** file:

```
action=import&csv_data=
vCenter IP,ESXi IP
10.10.10.10,20.20.20.20
10.10.10.10,20.20.20.21
10.10.10.10,20.20.20.22
11.11.11.11,30.30.30.23
12.12.12.12,40.40.40.24
```

XML Data in File

Following is the sample API request when you want to import the mapping using a file containing XML data. In the sample request, **add.xml** is a XML data file.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-with: curl' --data-binary
"@add.xml"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

Sample content of **add.xml** file:

```
action=import&xml_data=
<?xml version="1.0" encoding="UTF-8" ?>
<VCENTER_ESXI_MAP_LIST>
    <VCENTER_ESXI_MAP>
        <VCENTER_IP>10.10.10.10</VCENTER_IP>
        <ESXI_IP>20.20.20.21</ESXI_IP>
    </VCENTER_ESXI_MAP>
    <VCENTER_ESXI_MAP>
        <VCENTER_IP>10.10.10.10</VCENTER_IP>
        <ESXI_IP>20.20.20.22</ESXI_IP>
    </VCENTER_ESXI_MAP>
</VCENTER_ESXI_MAP_LIST>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-05-07T10:57:23Z</DATETIME>
    <TEXT>Successfully imported 2 records</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Purge vCenter - ESXi Mapping

You'll be able to purge vCenter - ESXi mapping in the CSV and XML format. You can provide CSV or XML data in API call or in the file.

CSV Data in API Call

Following is the sample API request when you want to purge mapping using CSV data in API call.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' --data-binary
"action=purge&csv_data=vCenter IP,ESXi
IP%0A10.10.10.10,10.10.10.11%0A10.10.10.10,10.10.10.12"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

XML Data in API Call

Following is the sample API request when you want to purge mapping using XML data in API call.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' --data-binary
"action=purge&xml_data=<VCENTER_ESXI_MAP_LIST><VCENTER_ESXI_MAP><VCENTER_
IP>11.11.11.11</VCENTER_IP><ESXI_IP>22.22.22.22</ESXI_IP></VCENTER_ESXI_M
AP><VCENTER_ESXI_MAP><VCENTER_IP>11.11.11.12</VCENTER_IP><ESXI_IP>22.22.2
2.23</ESXI_IP></VCENTER_ESXI_MAP></VCENTER_ESXI_MAP_LIST>"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

CSV Data in File

Following is the sample API request when you want to purge the mapping using a file containing CSV data. In the sample request, **purge.csv** is a CSV data file.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-with: curl' --data-binary
"@purge.csv"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

Sample content of **purge.csv** file:

```
action=purge&csv_data=
vCenter IP,ESXi IP
10.10.10.10,20.20.20.20
10.10.10.10,20.20.20.21
10.10.10.10,20.20.20.22
11.11.11.11,30.30.30.23
12.12.12.12,40.40.40.24
```

XML Data in File

Following is the sample API request when you want to purge the mapping using a file containing XML data. In the sample request, **purge.xml** is a XML data file.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-with: curl' --data-binary
"@purge.xml"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/vcenter_mapping/"
```

Sample content of **purge.xml** file:

```
action=purge&xml_data=
<?xml version="1.0" encoding="UTF-8" ?>
<VCENTER_ESXI_MAP_LIST>
    <VCENTER_ESXI_MAP>
        <VCENTER_IP>10.10.10.10</VCENTER_IP>
        <ESXI_IP>20.20.20.21</ESXI_IP>
    </VCENTER_ESXI_MAP>
    <VCENTER_ESXI_MAP>
```

```
            <VCENTER_IP>10.10.10.10</VCENTER_IP>
            <ESXI_IP>20.20.20.22</ESXI_IP>
        </VCENTER_ESXI_MAP>
    </VCENTER_ESXI_MAP_LIST>
```

XML output:

```
    <?xml version="1.0" encoding="UTF-8" ?>
    <!DOCTYPE SIMPLE_RETURN SYSTEM
    "https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
    <SIMPLE_RETURN>
      <RESPONSE>
        <DATETIME>2020-05-07T10:57:23Z</DATETIME>
        <TEXT>Successfully purged 2 records</TEXT>
      </RESPONSE>
</SIMPLE_RETURN>
```

Vault Support

Set up and manage integration with third party password vaults, an option for authenticated scanning (e.g. trusted scanning).

Vault summary	
Vault Support matrix	View supported vaults by OS and supported features (i.e. password, key passphrase, private key
Vault settings	
Vault Definition	Use Authentication API (/api/2.0/fo/auth/*) to add vault definition in authentication records
List Vaults	Use Vault API (/api/2.0/fo/vault) to list vault records
Manage Vaults	Use Vault API (/api/2.0/fo/vault) to create, edit, and delete vault records

Vault Support matrix

Supported vaults by authentication type (OS/technology) and capability (password, private key, key passphrase, root delegation tool password). Use the vault name as shown when providing vault name using the Qualys API (i.e. vault_type=Quest Vault).

Vaults can be defined as part of authentication records using the Authentication API (/api/2.0/fo/auth/*) except as noted below. Some vaults can be defined using the Vault API (/api/2.0/fo/vault).

password	private key	key passphrase	root delegation passwd
Azure MS SQL (compliance scans only)			
ARCON PAM Azure Key **(UI support only)** BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			

password	private key	key passphrase	root delegation passwd
Apache Cassandra (compliance scans only)			
CyberArk AIM Thycotic Secret Server HashiCorp Azure Key			
Cisco			
ARCON PAM Azure Key CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Thycotic Secret Server			
Checkpoint Firewall (compliance scans only)			
ARCON PAM Azure Key CyberArk AIM CyberArk PIM Suite Thycotic Secret Server			
IBM DB2			
ARCON PAM CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			
Infoblox			
Azure Key CyberArk PIM Suite HashiCorp BeyondTrust PBPS Thycotic Secret Server Wallix AdminBastion (WAB)			
MariaDB (compliance scans only)			

password	private key	key passphrase	root delegation passwd
ARCON PAM Azure Key BeyondTrust PBPS CyberArk AIM CyberArk PIM Suite HashiCorp Quest Vault Thycotic Secret Server			
MongoDB			
ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Quest Vault Thycotic Secret Server	Azure Key BeyondTrust PBPS CyberArk AIM HashiCorp Thycotic Secret Server	Azure Key CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	
MS SharePoint (compliance scans only)			
ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			
MS SQL (compliance scans only)			
Arcon PAM Azure Key BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			

password	private key	key passphrase	root delegation passwd
MySQL			
ARCON PAM Azure Key BeyondTrust PBPS CyberArk AIM CyberArk PIM Suite HashiCorp Quest Vault Thycotic Secret Server			
Neo4j			
ARCON PAM Vault Azure Key BeyondTrust PBPS CyberArk AIM CyberArk PIM Suite HashiCorp Thycotic Secret Server			
Oracle			
ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			
Oracle Listener			
(UI support only) BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
Palo Alto Firewall			

password	private key	key passphrase	root delegation passwd
Azure Key BeyondTrust PBPS CyberArk AIM CyberArk PIM Suite Quest Vault Thycotic Secret Server			
Pivotal Greenplum			
ARCON PAM CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Quest Vault Thycotic Secret Server	Azure Key BeyondTrust PBPS CA PAM CyberArk AIM HashiCorp Thycotic Secret Server	Azure Key CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	
PostgreSQL (compliance scans only)			
ARCON PAM CA Access Control CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Quest Vault Thycotic Secret Server	Azure Key BeyondTrust PBPS CA PAM CyberArk AIM HashiCorp Thycotic Secret Server	Azure Key CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	
SAP Hana (compliance scans only)			
ARCON PAM Azure Key BeyondTrust PBPS CyberArk AIM CyberArk PIM Suite HashiCorp Thycotic Secret Server			

password	private key	key passphrase	root delegation passwd
SAP IQ (compliance scans only)			
Arcon PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitachi ID PAM Liberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion			
Sybase (compliance scans only)			
ARCON PAM CyberArk AIM CyberArk PIM Suite HashiCorp Lieberman ERPM Quest Vault Thycotic Secret Server			
Unix			
ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion	ARCON PAM Azure Key BeyondTrust PBPS CA PAM CyberArk AIM HashiCorp Thycotic Secret Server Wallix AdminBastion	Azure Key CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion

password	private key	key passphrase	root delegation passwd
VMware			
BeyondTrust PBPS CA Access Control CyberArk AIM CyberArk PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
Windows			
ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitatchi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion			
HTTP			
CyberArk PIM Suite CyberArk AIM Thycotic Secret Server Quest Vault CA Access Control Hitachi ID PAM Lieberman ERPM BeyondTrust PBPS HashiCorp Azure Key Arcon PAM			

Vault Definition

Various record types support adding vault definition as part of authentication record settings. When supported these parameters are used to provide the vault definition in record settings.

Parameter	Description
login_type={**basic**|vault}	(Required only when you want to create or update vault information) Set login_type=vault, to add vault information. By default, the parameter is set to basic.
vault_id={value}	(Required only when action=create and login_type=vault) A vault ID.
	For Windows, vault_id and password parameters are mutually exclusive and cannot be specified in the same request.
	For Unix, vault_id and password, cleartext_password parameters are mutually exclusive and cannot be specified in the same request.
vault_type={value}	(Required only when action=create and login_type=vault. Also, required when updating details for HashiCorp and Wallix Authentication Vaults. Want to know what vaults support what technologies and capabilities? See Vault Support matrix Choose one: Arcon PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitachi ID PAM (no parameters specific to this vault type.) Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion (WAB)
ARCON PAM	
vault_service_type={value}	(Required if vault type is ARCON PAM) Specify a vault service type for authenticating to the vault and launching the scan on the host. This value is validated against the predefined list of service types.
Azure Key	
ak_secret_name={value}	(Required if vault type is Azure Key) The secret name assigned to the secret stored in the vault.
BeyondTrust PBPS	

Parameter	Description
system_name={value}	(Optional if vault type is BeyondTrust PBPS) The managed system name (also known as asset name). When not specified, we'll attempt to auto-discover the system name at scan time.
account_name={value}	(Optional if vault type is BeyondTrust PBPS) The account name. When not specified, we'll try the username specified in the authentication record.
CA Access Control	
end_point_name={value}	(Required if vault type is CA Access Control) The End-Point name identifies a managed system, either a target for local accounts or a domain controller for domain accounts. An End-Point name is a user-defined value within your installation of CA Access Control Enterprise Management. The End-Point name entered in this record must match a pre-defined name exactly.
end_point_type={value}	(Required if vault type is CA Access Control) The End-Point type represents the method of access to the End-Point system. CA Access Control Enterprise Management uses pre-defined values for various methods and the End-Point type value must match a pre-defined value exactly. Examples: "Windows Agentless" (for Windows accounts) and "SSH Device" (for Unix via SSH).
end_point_container={value}	(Required if vault type is CA Access Control) The End-Point container stores configuration values. CA Access Control Enterprise Management uses pre-defined values for various methods and the End-Point container value must match a pre-defined value exactly. Examples: "Accounts" (for Windows accounts) and "SSH Accounts" (for Unix via SSH).
CA PAM	
vault_app_name={value}	(Required) Application name as defined in the vault configuration for accessing a specific device.

Parameter	Description

vault_device_name={value}	(Optional) Specify the target device name defined in the vault configuration for which you want to retrieve the credentials.
	
	You can use one or more variables when defining the device name in order to match several targets that use the same naming convention.
	${ip} // The IP address of the target, i.e. 10.20.30.40.
	${ip_dash} // The IP address of the target with dashes instead of dots, i.e. 10-20-30-40.
	${dnshost} // The DNS host name of the target, i.e. host.domain.
	${host} // The host name of the target, i.e. host before .domain.
	${nbhost} // (Windows only) The NetBIOS host name of the target in upper-case, i.e.HOST_ABC.
	
	Example, device-unix-${ip} will match these 3 devices: device-unix-10.50.60.70, device-unix-10.50.60.88 and device-unix-10.30.10.12.
	
	Note: You must specify “vault_device_name” or “vault_device_host”, but not both.

vault_device_host={value}	(Optional) Specify the target device address defined in the vault configuration for which you want to retrieve the credentials. You can use one or more variables when defining the device host in order to match several targets that use the same naming convention. ${ip} - The IP address of the target, i.e. 10.20.30.40. ${ip_dash} - The IP with dashes, i.e. 10-20-30-40. ${dnshost} - DNS hostname of the target, i.e. host.domain. ${host} - Hostname of the target, i.e. host before .domain. ${nbhost} - (Windows only) The NetBIOS name of the target in upper-case, i.e. HOST_ABC. For example, ${host}-${ip_dash} will match these 3 devices: host40-10-20-30-40, host80-10-50-60-70 and host12-10-30-10-12. Note: You must specify “vault_device_name” or “vault_device_host”, but not both.

Parameter	Description
CyberArk AIM	
folder={value}	(Required if vault type is CyberArk AIM) Specify the name of the folder in the secure digital safe where the password to be used for authentication should be stored. The folder name can contain a maximum of 169 characters. Entering a trailing /, as in folder/, is optional (when specified, the service removes the trailing / and does not save it in the folder name). The maximum length of a folder name with a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a folder name: / : * ? " < > | <tab> You can use one or more variables when defining the folder name in order to match several targets that use the same naming convention. ${ip} - The IP address of the target, i.e. 10.20.30.40. ${ip_dash} - The IP with dashes, i.e. 10-20-30-40. ${dnshost} - DNS hostname of the target, i.e. host.domain. ${host} - Hostname of the target, i.e. host before .domain. ${nbhost} - (Windows only) The NetBIOS name of the target in upper-case, i.e. HOST_ABC. For example, ${host}-${ip_dash} will match these 3 targets: host40-10-20-30-40, host80-10-50-60-70 and host12-10-30-10-12.
file={value}	(Required if vault type is CyberArk AIM) Specify the name of the file in the secure digital safe where the password to be used for authentication should be stored. The file name can contain a maximum of 165 characters. The maximum length of a folder name plus a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a file name: \ / : * ? " < > | <tab> You can use one or more variables when defining the file name in order to match several targets that use the same naming convention. ${ip} - The IP address of the target, i.e. 10.20.30.40. ${ip_dash} - The IP with dashes, i.e. 10-20-30-40. ${dnshost} - DNS hostname of the target, i.e. host.domain. ${host} - Hostname of the target, i.e. host before .domain. ${nbhost} - (Windows only) The NetBIOS name of the target in upper-case, i.e. HOST_ABC. For example, ${host}-${ip_dash} will match these 3 targets: host40-10-20-30-40, host80-10-50-60-70 and host12-10-30-10-12.

Parameter	Description
CyberArk PIM Suite	
folder={value}	(Required if vault type is CyberArk PIM Suite) Specify the name of the folder in the secure digital safe where the password to be used for authentication should be stored. The folder name can contain a maximum of 169 characters. Entering a trailing /, as in folder/, is optional (when specified, the service removes the trailing / and does not save it in the folder name). The maximum length of a folder name with a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a folder name: / : * ? " < > | <tab>
file={value}	(Required if vault type is CyberArk PIM Suite) Specify the name of the file in the secure digital safe where the password to be used for authentication should be stored. The file name can contain a maximum of 165 characters. The maximum length of a folder name plus a file name is 170 characters (the leading and/or trailing space in the input value will be removed). These special characters cannot be included in a file name: \ / : * ? " < > | <tab>
HashiCorp	
secret_kv_path={value}	(Optional if vault type is HashiCorp) The path of the secret engine. The default is “secret/data”. For a custom path, please provide path in the format "path/to/secret/data". Note that we only support Key-Value Secret Engine version 2 to retrieve secrets from the HashiCorp Vault.
secret_kv_name={value}	(Required when updating details for HashiCorp Authentication Vaults) The secret name which stores key-value pairs.
secret_kv_key={value}	Required when updating details for HashiCorp Authentication Vaults. The key name for identifying a specific key-value pair. **Note**: This field does not appear while using Database Secrets Engine or Active Directory (AD) Secrets Engine while creating or updating HashiCorp authentication records (Oracle, Windows, HTTP, MS SQL, Network SSH, and Unix record).
Hitachi ID PAM	
resource_id	(Optional) specify resource id for a Hitachi ID PAM authentication record.

Parameter	Description
Lieberman ERPM	
auto_discover_system_name={0|1}	(Required if vault type is Lieberman ERPM) Specify 1 to enable auto discovery of the system name and 0 to disable auto discovery. Each system in your ERPM environment has a system name and this is needed in order to retrieve the password for authentication. Use auto discovery to allow the service to find the system name for you at scan time. The service uses information known about each host (like the IP address and FQDN) to query ERPM for the system name. Auto discovery is the only option available when your record includes multiple IPs.
system_name_single_host={value}	(Required if vault type is Lieberman ERPM) Specify the system name that is needed to retrieve password for authentication.
	To specify system_name_single_host, ensure that auto discovery of system name is disabled (auto_discover_system_name=0). If auto discovery of system name is enabled (auto_discover_system_name=1), specifying system_name_single_host is invalid.
system_type={value}	(Required if vault type is Lieberman ERPM) A valid value is one of the following system type: auto, windows, unix, oracle, mssq, ldap, cisco, custom
custom_system_type={value}	(Required if vault type is Lieberman ERPM) Specify the custom system type name.
	custom_system_type is valid only when system_type=custom.
Quest Vault	
system_name={value}	(Required if vault type is Quest Vault) Specify the system name. During a scan we'll perform a search for the system name and then retrieve the password. A single exact match of the system name must be found in order for authentication to be successful.
Thycotic Secret Server	
secret_name={value}	(Required if vault type is Thycotic Secret Server) Specify the secret name that contains the password to be used for authentication. The scanning engine will perform a search for the secret name and then get the password from the secret returned by the search. A single exact match of the secret name must be found in order for authentication to be successful. The secret name may contain a maximum of 256 characters, and must not contain multibyte characters.
Wallix AdminBastion (WAB)	
authorization_name={value}	(Required if vault type is Wallix AdminBastion (WAB)) Specify the name of the authorization that enables secret retrieval from a group of targets.

Parameter	Description
target_name={value}	(Required if vault type is Wallix AdminBastion (WAB)) Specify the name of the target device using one of these formats: user@global_WABdomain user@local_WABdomain@device where user is the user with access to the target, global_WABdomain is a domain name in a domain controller, local_WABdomain is a local domain, device is the device you want to scan Use one or more variables in the target name to match several targets that use the same naming convention. ${ip} - The IP address of the target, i.e. 10.20.30.40. ${ip_dash} - The IP with dashes, i.e. 10-20-30-40. ${dnshost} - DNS hostname of the target, i.e. host.domain. ${host} - Hostname of the target, i.e. host before .domain. ${nbhost} - (Windows only) The NetBIOS name of the target in upper-case, i.e. HOST_ABC. For example, the target name user@local_WABdomain@${ip} will match these 3 devices: 10.50.60.70, 10.50.60.88 and 10.30.10.12.
secret_kv_name={value}	(Required when updating details for Wallix Authentication Vaults) The secret name which stores key-value pairs.
secret_kv_key={value}	Required when updating details for Wallix Authentication Vaults. The key name for identifying a specific key-value pair.

List Vaults

The Authentication Vault API (resource **/api/2.0/fo/vault/**) allows you to list authentication vaults in your account. Use the parameter "action=list" to list the vaults

Permissions: Managers, Unit Managers and Scanners can view vaults and their settings.

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: curl" -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/vault/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VAULT_LIST_OUTPUT SYSTEM

"https://qualysapi.qualys.com/api/2.0/fo/vault/vault_output.dtd">
<AUTH_VAULT_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2014-09-12T13:55:57Z</DATETIME>
        <STATUS>Success</STATUS>
        <COUNT>13</COUNT>
        <AUTH_VAULTS>
            <AUTH_VAULT>
                <TITLE>
                    <![CDATA[added failover ip]]>
                </TITLE>
                <VAULT_TYPE>
                    <![CDATA[CyberArk PIM Suite]]>
                </VAULT_TYPE>
                <LAST_MODIFIED>
                    <DATETIME>2014-02-13T12:05:21Z</DATETIME>
                    <BY>quays_rn1</BY>
                </LAST_MODIFIED>
                <ID>1421</ID>
            </AUTH_VAULT>
            <AUTH_VAULT>
                <TITLE>
                    <![CDATA[added failover ip1]]>
                </TITLE>
                <VAULT_TYPE>
                    <![CDATA[CyberArk PIM Suite]]>
                </VAULT_TYPE>
                <LAST_MODIFIED>
                    <DATETIME>2014-02-19T06:43:44Z</DATETIME>
                    <BY>quays_rn1</BY>
                </LAST_MODIFIED>
```

```
            <ID>1441</ID>
        </AUTH_VAULT>
        <AUTH_VAULT>
            <TITLE>
                <![CDATA[Blue]]>
            </TITLE>
            <VAULT_TYPE>
                <![CDATA[CA Access Control]]>
            </VAULT_TYPE>
            <LAST_MODIFIED>
                <DATETIME>2013-09-21T05:26:32Z</DATETIME>
                <BY>quays_rn1</BY>
            </LAST_MODIFIED>
            <ID>1406</ID>
        </AUTH_VAULT>
    </AUTH_VAULTS>
  </RESPONSE>
</AUTH_VAULT_LIST_OUTPUT>
```

Parameters:

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Set to 1 to show (echo) the request's input parameters (names and value) in the XML output.
title={value}	(Optional) Include vaults matching this title.
type={value}	(Optional) Include a certain vault type only. A valid value is: ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion (WAB)
modified={date}	(Optional) Include vaults modified on or after a certain date/time, in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT).

Parameter	Description
orderby={value}	(Optional) Sort the vaults list by certain data. One of: “id”, “title”, “system_name”, “last_modified”, “last_modified_by”. A date must be specified in YYYYMM-DD[THH:MM:SSZ] format (UTC/GMT).
sortorder={asc|desc}	(Optional) The sort order, used when the request includes the orderby parameter. One of: asc (for ascending order) or desc (for descending order).
limit={value}	(Optional) The maximum number of vault records processed for the request, starting at the record number specified by the offset parameter. These parameters must be specified together: limit and offset. Limit value must always be greater than “0”. If you specify a value 0 for the parameter, the request will fail. When not specified, default limit is set to 1,000 vault records. You can specify a value less than or greater than the default.
offset={value}	(Optional) The starting vault record number, used only when the request includes the limit parameter.

More sample requests:

1) List all vaults, order vaults by system name

```
curl -H "X-Requested-With:API" -u "USERNAME:PASSWD" -d
"action=list&orderby=system_name"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/?"
```

2) List all vaults, order vaults by title in descending order

```
curl -H "X-Requested-With:API" -u "USERNAME:PASSWD" -d
"action=list&sortorder=desc&title"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/?"
```

3) List only 9th and 10th vault records

```
curl -H "X-Requested-With:API" -u "USERNAME:PASSWD" -d
"action=list&limit=2&offset=9"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/?"
```

Manage Vaults

The Authentication Vault API (resource **/api/2.0/fo/vault**) allows you to manage authentication vaults (create, update, delete) as separate configurations.

Permissions: Managers can perform all functions (create, update, delete). Unit Managers can perform these functions if they are granted the permission "Create/edit authentication records/vaults".

Create a new vault

Parameters:

Parameter	Description
action=create	(Required)
title={value}	(Required) The vault title.
type={value}	(Required) The vault type. A valid value is: ARCON PAM Azure Key BeyondTrust PBPS CA Access Control CA PAM CyberArk AIM CyberArk PIM Suite HashiCorp Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server Wallix AdminBastion (WAB)
comments={value}	(Optional) User defined comments.
{vault settings}	"Tell me about vault settings"

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&type=CyberArk AIM&title=New-CyberArk-
AIM&appid=CyberArk007&safe=Vaultsafe&url=https://afco.com&ssl_veri
fy=1&
cert=-----BEGIN+CERTIFICATE-----
%0D%0AMIIDXzCCAkcCAQEwDQYJKoZIwdjELMAkGA1UEBhM%0D%0A-----
END+CERTIFICATE
-----&private_key_pwd=password&private_key=-----
BEGIN+RSA+PRIVATE+KEY-----
%0D%0AMIIEowIBAAKCAQEAmbSGAPwS662q5SsJ2XA2mVvKOfXa%2%0D%0A-----
END+RSA+PRIVATE+KEY-----"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2016-09-02T06:10:02Z</DATETIME>
    <TEXT>Success</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>7004</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update vault settings

Parameters:

Parameter	Description
action=update	(Required)
id={value}	(Required) A vault ID.
title={value}	(Optional) A new title to replace the existing title.
comments={value}	(Optional) User defined comments.
{vault settings}	"Tell me about vault settings"

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: curl" -X "POST" -d
"id=14836922&server_address=10.10.10.10"
"https://qualysapi.qualys.com/api/2.0/fo/vault/?action=update"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2014-09-12T14:13:28Z</DATETIME>
        <TEXT>Success</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
```

```
                <VALUE>14836922</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

View vault settings

Parameter	Description
action=view	(Required)
id={value}	(Required) A vault ID.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=view&id=7004"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VAULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/vault/vault_view.dtd">
<VAULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2016-09-08T06:38:28Z</DATETIME>
    <VAULT_QUEST>
      <TITLE><![CDATA[New CyberArk AIM Vault]]></TITLE>
      <COMMENTS><![CDATA[]]></COMMENTS>
      <VAULT_TYPE><![CDATA[CyberArk AIM]]></VAULT_TYPE>
      <CREATED_ON>2016-09-07T07:09:34Z</CREATED_ON>
      <OWNER>user_john</OWNER>
      <LAST_MODIFIED>
        <DATETIME>2016-09-08T06:37:49Z</DATETIME>
        <BY>user_john</BY>
      </LAST_MODIFIED>
      <APPID><![CDATA[735435]]></APPID>
      <URL><![CDATA[https://afco.com]]></URL>
      <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
      <SAFE><![CDATA[56908456904]]></SAFE>
      <ID>7004</ID>
    </VAULT_QUEST>
  </RESPONSE>
</VAULT_OUTPUT>
```

Delete a vault

Parameter	Description
action=view	(Required)
id={value}	(Required) A vault ID.

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: curl" -d
"id=43463"
"https://qualysapi.qualys.com/api/2.0/fo/vault/?action=delete"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2014-09-12T14:13:28Z</DATETIME>
        <TEXT>Success</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>Status</KEY>
                <VALUE>Deleted</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Tell me about vault settings

The vault settings differ per vault type.

ARCON PAM	
url={value}	(Required to create and optional to update vault) The HTTP or HTTPS URL to access the ARCON PAM Vault API. The HTTPS URL is required if the ssl_verify parameter is set 1.
ssl_verify={0|**1**}	(Required to create and optional to update vault) When set to 1 (the default), our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
username={value}	(Required to create and optional to update vault) A username required to access the vault.
password={value}	(Required to create and optional to update vault) A password required to access the vault.

Azure Key	
url={value}	(Required to create and optional to update vault) The HTTP or HTTPS URL to access the Azure key Vault HTTP API. The HTTPS URL is required if the ssl_verify parameter is set 1.
app_id={value}	(Required to create and optional to update vault) The application ID associated with the application created in the Azure Key Vault.
ssl_verify={0|**1**}	(Required to create and optional to update vault) When set to 1 (the default), our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
certificate={value}	(Required to create and optional to update vault) The client certificate for authentication. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----). For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.
private_key={value}	(Required to create and optional to update vault) The private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----).
passphrase={value}	(Optional) The private key passphrase is required if the private key is encrypted.
BeyondTrust PBPS	
appkey={value}	(Required for new vault) The application key (alpha-numeric string) for the BeyondTrust PBPS web services API. The maximum length is 128 bytes. A leading and/or trailing space or periods in the input value will be removed.
url={value}	(Required for new vault) The HTTP or HTTPS URL to access the BeyondTrust PBPS web services API.
ssl_verify={1|0}	(Optional) When set to 1, our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
username={value}	(Required for new vault) The user account that can call the BeyondTrust PBPS web services API. The maximum length is 64 characters. This special character cannot be included: @
password={value}	(Optional) Specify a user password when required by the Application API Key configuration in BeyondTrust.

cert={value}	(Optional) Provide an X.509 client certificate with your private key when required by the Application API Key configuration in BeyondTrust. The certificate must be trusted by the PBPS web server. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).
	For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.
private_key={value}	(Optional) Specify the private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----).
	For a create/update request, if the private_key parameter is specified, then the cert parameter must also be specified.
private_key_pwd={value}	(Optional) Specify a password for your private key if it's encrypted.
CA Access Control	
ca_url={value}	(Required for new vault) The HTTP or HTTPS URL of the CA Access Control web services, an API interface to your CA Access Control Enterprise Management installation. Note that the web services URL is different from the web management URL. Sample web services URL: http://caac126u-32-235.caac125.domain.com:18080/iam/TEWS6/ac Sample web management URL: http://caac126p-33-166.caac125.domain.com:18080/iam/ac/
ca_api_username={value}	(Required for new vault) The name of a user that is granted GetAccountPassword API permissions.
ca_ssl_verify={1|0}	(Required for new vault) When set to 1, our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0 our service will not verify the certificate of the web server.
ca_web_username={value}	(Optional) The web user name used to access Basic Authentication of the CA Access Control web server.
ca_web_password={value}	(Optional) The web password used to access Basic Authentication of the CA Access Control web server.
CA PAM	
ssl_verify={0|**1**}	(Required to create and optional to update vault) The user account that can call the CA PAM Vault HTTP API.

url={value}	(Required to create and optional to update vault) The HTTP or HTTPS URL to access the CA PAM Vault HTTP API.
apikey_name={value}	(Required to create and optional to update vault) The user account that can call the CA PAM Vault HTTP API.
apikey={value}	(Required to create and optional to update vault) The password for the user account that can call the CA PAM Vault HTTP API.
CyberArk AIM	
appid={value}	(Required) Application ID string defined by the customer. The application ID acts as an authenticator for our scanner to call CCP web services API. The maximum length of an application ID name is 128 bytes and the first 28 characters must be unique (leading and/or trailing space or periods in the input value will be removed). These restricted words cannot be included in a application ID: Users, Addresses, Areas, XUserRules, unknown, Locations, Safes, Schedule, VaultCategories, Builtin. These special characters cannot be included in a application ID: \ / : * ? " < > | \t \r \n \x1F.
safe={value}	(Required) The name of the digital password safe. The safe name can contain a maximum of 28 characters (leading and/or trailing space in the input value will be removed). These special characters cannot be included in a safe name: \ / : * ? " < > | \t \r \n \x1F
url={value}	(Required) The HTTP or HTTPS URL over SSL protocols to access CyberArk's CCP web services.
ssl_verify={1|0}	(Required) When set to 1, our service will verify the CCP SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0 our service will not verify the certificate of the web server.
cert={value}	(Optional) You must include an X.509 certificate with your private key. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).
	For a create/update request, if the certificate parameter is specified, then the private_key parameter must also be specified.
private_key={value}	(Optional) Specify private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----).
	For a create/update request, if the private_key parameter is specified, then the certificate parameter must also be specified.
private_key_pwd={value}	(Optional) Specify a password for the encrypted private_key.

CyberArk PIM Suite	
server_address={value}	(Required for new vault) The IP address of the vault server that stores system login credentials to be used.
port={value}	(Optional) The port the vault server is running on. The port must be in the range 1025 to 65535. For a new vault the port is set to 1858 by default, if the port parameter is not specified.
safe={value}	(Required for new vault) The name of the digital password safe. The safe name can contain a maximum of 28 characters (leading and/or trailing space in the input value will be removed). These special characters cannot be included in a safe name: \ / : * ? " < > . |
username={value}	(Required for new vault) The username for an account with access to your CyberArk PIM Suite environment.
password={value}	(Required for new vault) The password for an account with access to your CyberArk PIM Suite environment.
HashiCorp	
url={value}	(Required) The HTTP or HTTPS URL to access the HashiCorp Vault HTTP API.
api_version{value}	(Optional) The HashiCorp Vault HTTP API version. This is v1 by default, which is the only supported version.
ssl_verify={0|1}	(Required to create and optional to update vault) When set to 1 (the default), our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
auth_type={value}	(Required to create vault, optional to update vault) HashiCorp Vault API supports three authentication types. First choose any one of the authentication method you want to use (Username/Password, Cert or App Role) and then provide login credentials for authenticating to the vault server via the HashiCorp Vault HTTP API. Valid authentication values for API are: userpass, cert and approle.
`auth_type={userpass}`	Choose this authentication method to authenticate to the vault server with a username and password combination. auth_type= {userpass} supports 3 parameters: path, username, password.
path={value}	(Optional) The path for the Username/Password authentication method. The default path is auth/userpass but you can specify a custom path like auth/my-path.
username={value}	(Required to create and update vault) The user account that can access the vault server.
password={value}	(Required to create and update vault) The password for the user account.

auth_type={cert}	Choose the this authentication method to authenticate to the vault server using SSL/TLS client certificates which are either signed by a CA (Certificate Authority) or self-signed. CA certificates are associated with a role name. auth_type= {cert} supports 5 parameters: path, role_name, cert, private_key, passphrase..
path={value}	(Optional) The path for the Cert authentication method. The default path is auth/cert but you can specify a custom path like auth/my-path.
role_name={value}	(Required to create and update vault) The role associated with the CA certificate.
cert={value}	(Required to create and update vault) The client certificate for authentication. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----). For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.
private_key={value}	(Required to create and update vault) The private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----).
passphrase{value}	(Optional) The private key passphrase, if the private key is encrypted.
auth_type={approle}	Choose the App Role authentication method to authenticate to the vault server with a vault-defined role. auth_type= {approle} supports 3 parameters: path, role_id, secret_id.
path={value}	(Optional) The path for the App Role authentication method. The default path is auth/approle but you can specify a custom path like auth/my-path.
role_id={value}	(Required to create and update vault) The role ID of the App Role you want to use for authentication.
secret_id={value}	(Optional) The secret ID of the App Role you want to use for authentication.
Hitachi ID PAM	
url={value}	(Required for new vault) The HTTP or HTTPS URL of the Hitachi ID PAM webservices.

username={value}	(Required for new vault) The username (ID) for the Hitachi ID PAM user account. To allow Qualys scanners to connect using this account, this user must have the following settings under Administrator information in the Hitachi ID Management Suite: 1) the privilege “OTP IDAPI caller” and 2) the value entered in the “IP address with CIDR bitmask” field must include the Qualys scanner IP addresses.
password={value}	(Required for new vault) The password for the Hitachi ID PAM user account.
ssl_verify={1|0}	(Required for new vault) When set to 1, our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0 our service will not verify the certificate of the web server.
Lieberman ERPM	
url={value}	(Required for new vault) The HTTP or HTTPS URL of the Lieberman ERPM server.
domain={value}	(Optional) A domain name if your Lieberman ERPM server is part of a domain.
username={value}	(Required for new vault) The username for the Lieberman ERPM server account.
password={value}	(Required) The password for the Lieberman ERPM server account.
ssl_verify={1|0}	(Required for new vault) When set to 1, our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0 our service will not verify the certificate of the web server.
Quest Vault	
server_address={value}	(Required for new vault) The IP address of the vault server, Quest One Privileged Password Manager.
port={value}	(Optional) The listing port of the vault server. For a new vault the port is set to 22 by default, if the port parameter is not specified.
username={value}	(Required for new vault) The username to be used for SSH authentication. We recommend you create a dedicated user account for Qualys scanning. Using Quest/Dell 2.4 or higher, enter the key for the API user account you've created for use with our service. We support both API and CLI keys but recommend use of an API key.
access_key={value}	(Required for new vault) The DSA private key in PEM format for SSH authentication.
Thycotic Secret Server	
url={value}	(Required for new vault) The HTTP or HTTPS URL of the Secret Server webservices. The URL may contain a maximum of 256 characters, and must not contain multibyte characters.

username={value}	(Required for new vault) The username for a Secret Server user. This user must have access to the secret names to be used for authentication.
password={value}	(Required for new vault) The password for a Secret Server user.
domain={value}	(Optional) Specify a fully qualified domain name if Secret Server is integrated with Active Directory. The domain may contain a maximum of 128 characters, and must not contain any multibyte characters.
Wallix AdminBastion (WAB)	
url={value}	(Required for new vault) The HTTP or HTTPS URL to access the WAB web services API.
ssl_verify={0|1}	(Optional) When set to 1 (the default), our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
username={value}	(Required for new vault) The user account that can call the WAB web services API.
password={value}	(Optional) The password for the user account that can call the WAB web services API. For a new vault, you must specify password or appkey. Both parameters cannot be specified in the same request.
appkey={value}	(Optional) Your WAB REST API key (alpha-numeric value) for connecting to the WAB web services API. - Do not include leading or trailing periods or spaces. - These characters are not allowed: \\ / : * ? " < > | - UTF-8 multibyte characters are not allowed. For a new vault, you must specify password or appkey. Both parameters cannot be specified in the same request.

Assets

Manage the host assets you want to scan (internal and external facing) for vulnerabilities and compliance.

IP List | Add IPs | Update IPs

Host List | Host Update

Host List Detection | Host List Detection - Normalized Data| Host List Detection - Best Practices | Host List Detection - Use Cases

Excluded Host List | Excluded Hosts Change History | Manage Excluded Hosts

Virtual Host List | Manage Virtual Hosts

Restricted IPs List | Manage Restricted IPs

Asset Group List | Manage Asset Groups

Purge Hosts

Patch List

IP List

/api/2.0/fo/asset/ip/?action=list

[GET] [POST]

List IP addresses in the user account. By default, all hosts in the user account are included. Optional input parameters support filtering the list by IP addresses and host tracking method.

Permissions - Managers and Auditors view all assets in the subscription, Unit Managers view assets in their own business unit, Scanners and Readers view assets in their own account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required) A flag used to make an IP list request.
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. A host IP range is specified with a hyphen (for example, 10.10.10.44-10.10.10.90).
network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) A non-Manager user can use this parameter to restrict the request to IP addresses in a certain custom network ID. For a Manager user, the output will be the same regardless of the network_id specified in the request because all IPs are part of all networks automatically and Managers have access to all IPs in all networks. Specify network_id along with tracking_method to filter the results.
tracking_method={value}	(Optional) Show only IP addresses/ranges which have a certain tracking method. Valid values: IP, DNS, NETBIOS.

Parameter	Description
compliance_enabled={0|1}	(Optional) Specifying this parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list IP addresses in the user's account assigned to the Policy Compliance module. Specify 0 to list IPs which are not assigned to the Policy Compliance module. An error is returned if a user specifies this parameter, and the user's account does not have compliance management privileges to view the requested list. This may be due to the user's role and/or account settings as indicated below. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If the user does not have this permission and sets this parameter to 1, an error is returned. An Auditor user cannot make a request to view vulnerability management IP addresses. If an Auditor sets this parameter to 0, an error is returned.
certview_enabled={0|1}	(Optional) Set to 1 to list IP addresses in the user's account assigned to the Certificate View module. Specify 0 to list IPs that are not assigned to the Certificate View module. Note - This option will be supported when Certificate View GA is released and is enabled for your account.

Filter the output by module

Only interested in seeing IP addresses for VM, PC or CertView? Your request must include the compliance_enabled and certview_enabled parameters as described below.

To return only VM IP addresses, specify compliance_enabled=0 and certview_enabled=0.

To return only PC IP addresses, specify compliance_enabled=1 and certview_enabled=0.

To return only CertView IP addresses, specify compliance_enabled=0 and certview_enabled=1.

To return both PC and CertView IP addresses, specify compliance_enabled=1 and certview_enabled=1.

Sample - List Host IPs

API request:

```
curl -H "X-Requested-With: Curl Sample" -b
"QualysSession=71e6cda2a35d2cd404cddaf305ea0208;
path=/api; secure"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/?action=list"
```

XML output:

```
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/
ip_list_output.dtd">

<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-05-21T13:32:17Z</DATETIME>
    <IP_SET>
      <IP>123.123.45.0</IP>
      <IP_RANGE>123.124.45.0-123.124.45.255</IP_RANGE>
      <IP_RANGE>123.124.46.0-123.124.46.255</IP_RANGE>
      <IP_RANGE>123.124.47.0-123.124.47.255</IP_RANGE>
      <IP_RANGE>123.124.48.0-123.124.48.255</IP_RANGE>
    </IP_SET>
  </RESPONSE>
</IP_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/asset/ip/ip_list_output.dtd

Add IPs

/api/2.0/fo/asset/ip/?action=add

[POST]

Add IP addresses to the user's subscription. Once added they are available for scanning and reporting.

Permissions - A Manager has permissions to add IP addresses. A Unit Manager can add IP addresses when the “Add assets” permission is enabled in their account. Users with other roles (Scanner, Reader, Auditor) do not have permissions to add IP addresses.

Input Parameters

Parameter	Description
action=add	(Required) Add new IPs.
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
enable_vm={0|1}	(Required) Specify 1 to add IP addresses to the user's account assigned to the VM module. **Note:** Specifying this parameter is supported only when the VM module is enabled for the user account.
enable_pc={0|1}	(Required) Specify 1 to add IP addresses to the user's account assigned to the PC module. **Note:** Specifying this parameter is supported only when the PC module is enabled for the user account.
enable_sca={0|1}	(Required) Specify 1 to add IP addresses to the user's account assigned to the SCA module. **Note:** Specifying this parameter is supported only when the SCA module is enabled for the user account.
ips={value} -or- {POSTed CSV raw data}	(Required) The hosts you want to add to the subscription. IPs must be specified by using the “ips” parameter (using the POST method) or by uploading CSV raw data (using the POST method). To upload CSV raw data, specify --data-binary <data>. How to specify IP addresses. One or more IPs/ranges may be specified. Multiple IPs/ranges are comma separated. An IP range is specified with a hyphen (for example, 10.10.30.1-10.10.30.50). CIDR notation is supported.
tracking_method={value}	(Optional) The tracking method is set to IP for IP address by default. To use another tracking method specify DNS or NETBIOS.

Parameter	Description
enable_vm={**0**|1} enable_pc={**0**|1}	(Required) You must enable the hosts for the VM app (enable_vm=1) or the PC app (enable_pc=1) or both apps.
owner={value}	(Optional) The owner of the host asset(s). The owner must be a Manager or a Unit Manager. A valid Unit Manager must have the "Add assets" permission and sufficient remaining IPs (maximum number of IPs that can be added to the Unit Manager's business unit).
ud1={value} ud2={value} ud3={value}	(Optional) Values for user-defined fields 1, 2 and 3. You can specify a maximum of 128 characters (ascii) for each field value.
comment={value}	(Optional) User-defined comments.
ag_title={value}	(Required if the request is being made by a Unit Manager; otherwise invalid) The title of an asset group in the Unit Manager's business unit that the host(s) will be added to.
enable_certview={**0**|1}	(Optional) Set to 1 to add IPs to your CertView license. By default IPs are not added to your CertView license. This option will be supported when CertView GA is released and is enabled for your account.

Sample - Add IPs using POSTED data

API request:

```
curl -H "X-Requested-With: Curl" -H "Content-Type:text/csv"
-u "USERNAME:PASSWORD" --data-binary @ips_list.csv
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/?action=add&enab
le_vm=1&enable_pc=1&tracking_method=IP&owner=quays_es1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
  <!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
 <SIMPLE_RETURN>
    <RESPONSE>
      <DATETIME>2018-08-07T01:21:03Z</DATETIME>
      <TEXT>IPs successfully added to Vulnerability
Management/Compliance Management</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Add IPs using "ips" parameter

API request:

```
curl -H "X-Requested-With: demo" -u "USERNAME:PASSWORD" -X "POST"
-d "action=add&enable_vm=1&enable_pc=1&ips=10.10.10.1,10.10.10.10-
```

```
10.10.10.20,10.10.10.200"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Update IPs

/api/2.0/fo/asset/ip/?action=update

[POST]

Update IP addresses in the user's subscription.

Good to Know

- Host attributes you can update include tracking method (IP, DNS, NETBIOS), owner, user-defined fields (ud1, ud2, ud3), and comments.

- You cannot update an IP to use tracking method EC2 or AGENT. Also, if an IP is already tracked by EC2 or AGENT, you cannot change the tracking method to something else. We will skip the tracking method update in these cases.

- You can update multiple IPs/ranges in the same request. The host attribute changes will apply to all IPs included in the action.

- When the Network Support feature is enabled, you can update IPs in a custom network or in the Global Default Network. Only one network ID can be specified per update request. When a network ID is not specified in the request, we default to a value of 0 for Global Default Network.

Note: If Cloud (EC2, Azure, or GCP) or QAgent tracked hosts (IPs) are executed along with IP, DNS, or NETBios tracked hosts (IPs) for changing the tracking method, the Cloud or QAgent hosts will remain unchanged (Tracking method for cloud and Qagent hosts will not be changed).

Permissions

Managers have permission to update any IP, in any network. Sub-users (who have permission to update IPs) can update IPs for networks in their user scope. A Unit Manager can update IPs in asset groups assigned to their business unit. Users with other roles (Scanner, Reader, Auditor) do not have permission to update IP addresses.

Input Parameters

Parameter	Description
action=update	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.

Parameter	Description
ips={value} -or- {POSTed CSV raw data}	(Required) The hosts within the subscription you want to update. IPs must be specified by using the "ips" parameter (using the POST method) or by uploading CSV raw data (using the POST method). To upload CSV raw data, specify --data-binary <data>. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.30.1-10.10.30.50). CIDR notation is supported.
network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network by specifying the network ID. When unspecified, we default to "0" for Global Default Network.
tracking_method={value}	(Optional) To change to another tracking method specify IP for IP address, DNS or NETBIOS. You cannot change the tracking method to EC2 or AGENT. If an IP is already tracked by EC2 or AGENT, you cannot change the tracking method to something else.
host_dns={value}	(Optional) The DNS hostname for the IP you want to update. A single IP must be specified in the same request and the IP will only be updated if it matches the hostname specified.
host_netbios={value}	(Optional) The NetBIOS hostname for the IP you want to update. A single IP must be specified in the same request and the IP will only be updated if it matches the hostname specified.
owner={value}	(Optional) The owner of the host asset(s). The owner must be a Manager. Another user (Unit Manager, Scanner, Reader) can be the owner if the IP address is in the user's account.
ud1={value} ud2={value} ud3={value}	(Optional) Values for user-defined fields 1, 2 and 3. You can specify a maximum of 128 characters (ascii) for each field value.
comment={value}	(Optional) User-defined comments.

Sample - Add IPs and assign tracking method

API request:

```
curl -H "X-Requested-With: demo" -u "USERNAME:PASSWORD" -X "POST"
-d "action=update&ips=10.10.10.200,10.10.23.40&tracking_method=
DNS" "https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-07T17:27:36Z</DATETIME>
    <TEXT>IPs successfully updated</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update IP with matching NetBIOS name

IP 10.10.26.167 has multiple entries so we're specifying the NetBIOS hostname in the request to identify which entry to update.

API request:

```
curl -H "X-Requested-With: demo" -u "USERNAME:PASSWORD" -X "POST"
-d "action=update&ips=10.10.26.167&host_netbios=ORA10105-WIN-
25&&comment=mycomment"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

Sample - Update IPs in custom network

(Applicable when the Network Support feature is enabled.) In this sample, network ID 2222 is specified in the request. The tracking method will be changed for the specified IPs in this network only.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=update&network_id=2222&ips=10.10.10.200,10.10.23.40&tracki
ng_method=DNS" "https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

Sample - Network ID is not in user's scope

(Applicable when the Network Support feature is enabled.) In this sample, the sub-user is trying to update an IP address in a network that is not in their scope.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=update&network_id=55555&ips=10.10.10.10&comment=mycomment"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-10-14T17:27:36Z</DATETIME>
```

```
    <CODE>1905</CODE>
    <TEXT>parameter network_id has invalid value: 55555 (No such
network ID or not in user scope)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Duplicate host error

For the request below we're updating IP 10.10.25.224. The duplicate host warning is returned because there are 2 asset records for IP 10.10.25.224.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X POST -d
"action=update&ips=10.10.25.224&tracking_method=IP"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DUPLICATE_HOSTS_ERROR_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/duplicate_hosts_
error.dtd">
<DUPLICATE_HOSTS_ERROR_OUTPUT>
  <RESPONSE>
    <CODE>1982</CODE>
    <DATETIME>2018-03-16T04:54:15Z</DATETIME>
    <WARNING>
     <TEXT>You cannot change the tracking method for the following
host using the API since there are multiple scan data entries. This
can happen when the host is resolved to different hostnames in
different scan tasks. You'll need to change the tracking method
using the UI. Use the URL to log into your account, edit the host
and select another tracking method. At the prompt click Apply to
save the most recent scan data and purge the other scan
data.</TEXT>
      <DUPLICATE_HOSTS>
        <DUPLICATE_HOST>
          <IP>10.10.25.224</IP>
          <DNS_HOSTNAME>ora10105-win-25-
224.qualys.com</DNS_HOSTNAME>
          <NETBIOS_HOSTNAME>ORA10105-WIN-25</NETBIOS_HOSTNAME>
          <LAST_SCANDATE>09/09/2016 at 13:35:29
(GMT)</LAST_SCANDATE>
          <TRACKING>DNS</TRACKING>
        </DUPLICATE_HOST>
      </DUPLICATE_HOSTS>
<URL><![CDATA[https://qualysguard.qualys.com/fo/tools/ip_assets.ph
p]]></URL>
```

```
      </WARNING>
    </RESPONSE>
</DUPLICATE_HOSTS_ERROR_OUTPUT>
```

DTD for duplicate host error

<platform API server>/api/2.0/fo/asset/ip/duplicate_hosts_error.dtd"

Host List

For API version information, refer to API Version History section.

V2.0| V3.0 |V4.0 | V5.0 | V6.0

V2.0

/api/2.0/fo/asset/host/?action=list

[GET] [POST]

Download a list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided. Hosts in the XML output are sorted by host ID in ascending order.

The output of the Host List API is paginated. By default, a maximum of 1,000 host records are returned per request. You can customize the page size (i.e. the number of host records) by using the parameter "truncation_limit=10000" for instance. In this case the results will be return with pages of 10,000 host records.

The Host List API also shows the TruRisk score for each asset record in the API output and allows users to filter the output based on the TruRisk score .

The TruRisk score is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

TruRisk score has a range from 0 to 1000:

- Severe (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

The API output also displays the updated Asset Criticality Score (ACS), which may differ from the score shown in the Vulnerabilities and Assets tabs, as those scores are only updated after a vulnerability scan.

Permissions - Managers view all scanned hosts in subscription. Auditors view all scanned compliance hosts in subscription. Unit Managers view scanned hosts in user's business unit. Scanners and Readers view scanned hosts in user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR and PC. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

For Unit Managers, Scanners, and Readers to view compliance hosts, the "Manage compliance" permission must be granted in the user's account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)A flag used to make a host list request.
os_hostname={**0**|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
details={**Basic**|Basic/AGs | All|All/AGs | None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None. Basic - (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system. Basic/AGs - Show basic host information plus asset group information. Asset group information includes the asset group ID and title. All - Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates. All/AGs - Show all host information plus asset group information. Asset group information includes the asset group ID and title. None - Show only the host ID.

Parameter	Description
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter. For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php PCRE syntax: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php
truncation_limit={value}	(Optional) Specify the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more host records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. See example: Sample - Record Limit Exceeded Warning You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is downloaded.

Parameter	Description
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value. A valid host ID is required.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.

Parameter	Description
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Use this parameter to filter the scanned hosts list to show either: 1) a list of scanned compliance hosts, or 2) a list of scanned vulnerability management hosts. Specify 1 to list scanned compliance hosts in the user's account. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module. A user can specify 0 only when the user has compliance management privileges. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If this permission is not enabled and the user makes a request with this parameter set to 0, the request fails with an error (unknown parameter).
Date Filters	
no_vm_scan_since={date}	(Optional) Show hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - An Auditor cannot specify this parameter.
no_compliance_scan_since ={date}	(Optional) Show compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_scan_since={date}	(Optional) Show hosts that were last scanned for vulnerabilities since a certain date and time (optional). Hosts that were the target of a vulnerability scan since the date/time will be shown. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: An Auditor cannot specify this parameter.

Parameter	Description
compliance_scan_since={date}	(Optional) Show hosts that were last scanned for compliance since a certain date and time (optional). Hosts that were the target of a compliance scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
vm_scan_date_before={date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.

Parameter	Description
vm_auth_scan_date_before ={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_auth_scan_date_after= {date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
scap_scan_since={date}	(Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
no_scap_scan_since={date}	(Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
Asset Tags	
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify **1** if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names.
tag_include_selector= {**any**|all}	(Optional when use_tags=1) Select “any” (the default) to include hosts that match at least one of the selected tags. Select “all” to include hosts that match all of the selected tags.
tag_exclude_selector= {**any**|all}	(Optional when use_tags=1) Select “any” (the default) to exclude hosts that match at least one of the selected tags. Select “all” to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

Parameter	Description
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.
Asset Risk Score (ARS)	**Note**: The ARS parameters will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification. You must start using the new TruRisk parameters mentioned below.
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.
TruRisk Score	
show_trurisk={0|1}	(Optional) Specify 1 to show the TruRisk value in the output. Specify 0 if you do not want to show the TruRisk value.
trurisk_min={value}	(Optional) Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.

Parameter	Description
trurisk_max={value}	(Optional) Show only detection records with an TruRisk value less than or equal to the TruRisk max value specified. trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_trurisk_factors={0|1}	(Optional) Specify 1 to show TruRisk contributing factors associated with each asset record in the output. Specify 0 if you do not want to show TruRisk contributing factors.
EC2/Azure/GCP metadata	
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance). If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter.

Sample - Regular expression strings for matching OS names

API request:

```
curl --location --request POST
'https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&complian
```

```
ce_enabled=1&os_pattern=%5EWindows.*2%24' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: /' \
--header 'Content-Length: 0' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-10T05:07:38Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>66942</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[2k3sp2-25-12]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[2k3.patch.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[2K3SP2-25-12]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2016-11-15T07:39:22Z</FIRST_FOUND_DATE>
            </HOST>
 </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List assets

API request:

```
curl --location --request GET
'https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&show_ass
et_id=1&host_metadata=all&details=All
--header 'X-Requested-With: curl'
```

```
--header 'Authorization: <token>'
```

XML output:

```
...
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-04-25T03:52:05Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>32229</ID>
                <ASSET_ID>454545</ASSET_ID>
                <IP>10.14.28.129</IP>
                <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                <DNS>
                    <![CDATA[pt-w1122h2u]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pt-w1122h2u]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PT-W1122H2U]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows Microsoft Windows 11 Enterprise
10.0.22621 Build 22621]]>
                </OS>
                <QG_HOSTID>
                    <![CDATA[c6656ff6-c4c3-40df-81b4-fffe361acf02]]>
                </QG_HOSTID>
                <FIRST_FOUND_DATE>2023-03-15T07:22:33Z</FIRST_FOUND_DATE>
                <LAST_BOOT>2023-03-15T07:22:33Z</LAST_BOOT>
               <SERIAL_NUMBER><![CDATA[hmhC53tK52oWfsv3]]></SERIAL_NUMBER>
                <HARDWARE_UUID><![CDATA[08b829fb-ff42-8e41-a2ae-
1269ffc6872b]]></HARDWARE_UUID>
                <LAST_ACTIVITY>2023-03-15T07:22:33Z</LAST_ACTIVITY>
                <AGENT_STATUS><![CDATA[Inventory Scan
Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[GCP]]></CLOUD_AGENT_RUNNING_ON>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
...
```

Sample - List assets based on scan end date, scan processed date

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&truncati
on_limit=10&details=All
/AGs&vm_scan_date_before=2017-09-
14T06:32:15Z&vm_auth_scan_date_before=2017-09-
14T06:32:15Z&vm_scan_date_after=2016-05-
12T06:32:15Z&vm_auth_scan_date_after=2016-05-
12T06:32:15Z&vm_processed_before=2017-09&scap_scan_since=2018-08-29
-14T06:33:24Z&vm_processed_after=2016-09-12T06:33:24Z"-12T06:33:24Z"
```

Sample - List assets with specific TruRisk score

API request:

```
curl --location
'https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&ips=10.1
15.126.190&show_trurisk=1&trurisk_min=1&trurisk_max=1000&show_trurisk_fac
tors=1'
--header 'X-Requested-With: curl demo2'
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-06-21T06:46:04Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1800139</ID>
        <IP>10.115.126.190</IP>
        <ASSET_RISK_SCORE>680</ASSET_RISK_SCORE>
        <TRURISK_SCORE>680</TRURISK_SCORE>
        <ASSET_CRITICALITY_SCORE>4</ASSET_CRITICALITY_SCORE>
        <TRURISK_SCORE_FACTORS>
          <TRURISK_SCORE_FORMULA>4 *
{(1.0*95*(14^0.01))+(0.6*74*(31^0.01))+(0.4*47*(73^0.01))+(0.2*33*(66^0.
01))}</TRURISK_SCORE_FORMULA>
          <VULN_COUNT qds_severity="1">0</VULN_COUNT>
          <VULN_COUNT qds_severity="2">66</VULN_COUNT>
          <VULN_COUNT qds_severity="3">73</VULN_COUNT>
          <VULN_COUNT qds_severity="4">31</VULN_COUNT>
          <VULN_COUNT qds_severity="5">14</VULN_COUNT>
        </TRURISK_SCORE_FACTORS>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>0</NETWORK_ID>
        <DNS><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ca1]]></HOSTNAME>
          <DOMAIN><![CDATA[rdlab.in03.qualys.com.abc123]]></DOMAIN>
          <FQDN><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></FQDN>
```

```
        </DNS_DATA>
        <NETBIOS><![CDATA[SYS_10_115_126_190]]></NETBIOS>
        <OS><![CDATA[CentOS Linux 7.5.1804]]></OS>
        <QG_HOSTID><![CDATA[6fc281d4-40e2-4145-bcaa-
753f3f0d57d7]]></QG_HOSTID>
        <LAST_BOOT>2022-05-27T18:18:43Z</LAST_BOOT>
       <SERIAL_NUMBER><![CDATA[VMware-56 4d 99 7a 19 f5 a6 94-b5 f0 07 68
7c 9a e5 b5]]></SERIAL_NUMBER>
        <HARDWARE_UUID><![CDATA[564D997A-19F5-A694-B5F0-
07687C9AE5B5]]></HARDWARE_UUID>
        <FIRST_FOUND_DATE>2021-07-28T08:37:55Z</FIRST_FOUND_DATE>
        <LAST_ACTIVITY>2023-06-21T06:15:43Z</LAST_ACTIVITY>
        <AGENT_STATUS><![CDATA[Inventory Scan Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[QAGENT]]></CLOUD_AGENT_RUNNING_ON>
      </HOST>
      ...
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List scanned assets with certain EC2 metadata

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,ac
countId,instanceId"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/host_list_output.dtd"
>
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-15T09:50:46Z</DATETIME>
    <HOST_LIST>
       <HOST>
       <ID>135151</ID>
       <IP>10.97.5.247</IP>
       <TRACKING_METHOD>EC2</TRACKING_METHOD>
       <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>
       <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>
       <OS><![CDATA[Amazon Linux 2016.09]]></OS>
       <METADATA>
         <EC2>
           <ATTRIBUTE>
             <NAME><![CDATA[latest/dynamic/instance-
              identity/document/region]]></NAME>
             <LAST_STATUS>Success</LAST_STATUS>
             <VALUE><![CDATA[us-east-1]]></VALUE>
             <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
             <LAST_ERROR_DATE></LAST_ERROR_DATE>
```

```
            <LAST_ERROR><![CDATA[]]></LAST_ERROR>
          </ATTRIBUTE>
          <ATTRIBUTE>
            <NAME><![CDATA[latest/dynamic/instance-
             identity/document/accountId]]></NAME>
            <LAST_STATUS>Success</LAST_STATUS>
            <VALUE><![CDATA[205767712438]]></VALUE>
            <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
            <LAST_ERROR_DATE></LAST_ERROR_DATE>
            <LAST_ERROR><![CDATA[]]></LAST_ERROR>
          </ATTRIBUTE>
        </EC2>
      </METADATA>
      <LAST_VULN_SCAN_DATETIME>2017-03-
       21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
      <LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
      <LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
      <LAST_VM_AUTH_SCANNED_DATE>2017-03-
       21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
      <LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
      <LAST_COMPLIANCE_SCAN_DATETIME>2017-03-
       21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
    </HOST>
  </HOST_LIST>
 </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - Record Limit Exceeded Warning

In this case 1,000 host records are included in the XML output and the Warning message (shown below) indicates the URL you need to use to request the next 1,000 host records.

```
<RESPONSE>
...
   <WARNING>
            <CODE>1980</CODE>
            <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>
            <URL>

<![CDATA[https://qualysapi.p01.eng.sjc01.qualys.com/api/2.0/fo/asset/host
/?action=list&details=None&truncation_limit=100&id_min=145359]]>
            </URL>
        </WARNING>
    </RESPONSE>
...
```

DTD

<platform API server>/api/2.0/fo/asset/host/dtd/list/output.dtd

V3.0

api/3.0/fo/asset/host/?action=list

[GET] [POST]

Download a list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided. Hosts in the XML output are sorted by host ID in ascending order.

The output of the Host List API is paginated. By default, a maximum of 1,000 host records are returned per request. You can customize the page size (i.e. the number of host records) by using the parameter "truncation_limit=10000" for instance. In this case the results will be return with pages of 10,000 host records.

The Host List API also shows the TruRisk score for each asset record in the API output and allows users to filter the output based on the TruRisk score .

The TruRisk score is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

TruRisk score has a range from 0 to 1000:

- Severe (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

The API output also displays the updated Asset Criticality Score (ACS), which may differ from the score shown in the Vulnerabilities and Assets tabs, as those scores are only updated after a vulnerability scan.

Permissions - Managers view all scanned hosts in subscription. Auditors view all scanned compliance hosts in subscription. Unit Managers view scanned hosts in user's business unit. Scanners and Readers view scanned hosts in user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR and PC. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

For Unit Managers, Scanners, and Readers to view compliance hosts, the "Manage compliance" permission must be granted in the user's account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)A flag used to make a host list request.
os_hostname={**0**|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.

Parameter	Description
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
details={**Basic**|Basic/AGs | All|All/AGs | None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None. Basic - (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system. Basic/AGs - Show basic host information plus asset group information. Asset group information includes the asset group ID and title. All - Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates. All/AGs - Show all host information plus asset group information. Asset group information includes the asset group ID and title. None - Show only the host ID.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Refer to Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter. For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php PCRE syntax: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Parameter	Description
truncation_limit={value}	(Optional) Specify the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more host records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. See example: Sample - Record Limit Exceeded Warning You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is downloaded.
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value. A valid host ID is required.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.

Parameter	Description
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Use this parameter to filter the scanned hosts list to show either: 1) a list of scanned compliance hosts, or 2) a list of scanned vulnerability management hosts. Specify 1 to list scanned compliance hosts in the user's account. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module. A user can specify 0 only when the user has compliance management privileges. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If this permission is not enabled and the user makes a request with this parameter set to 0, the request fails with an error (unknown parameter).
Date Filters	
no_vm_scan_since={date}	(Optional) Show hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - An Auditor cannot specify this parameter.
no_compliance_scan_since ={date}	(Optional) Show compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_scan_since={date}	(Optional) Show hosts that were last scanned for vulnerabilities since a certain date and time (optional). Hosts that were the target of a vulnerability scan since the date/time will be shown. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: An Auditor cannot specify this parameter.

Parameter	Description
compliance_scan_since={date}	(Optional) Show hosts that were last scanned for compliance since a certain date and time (optional). Hosts that were the target of a compliance scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
vm_scan_date_before={date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.

Parameter	Description
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
pc_auth_success_date_before={date}	(Optional) Show hosts with a successful compliance scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
pc_auth_success_date_after={date}	(Optional) Show hosts with a successful compliance scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
scap_scan_since={date}	(Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
no_scap_scan_since={date}	(Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.

Parameter	Description
Asset Tags	
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify **1** if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.
Asset Risk Score (ARS)	**Note**: The ARS parameters will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification. You must start using the new TruRisk parameters mentioned below.
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.

Parameter	Description
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.
TruRisk Score	
show_trurisk={0|1}	(Optional) Specify 1 to show the TruRisk value in the output. Specify 0 if you do not want to show the TruRisk value.
trurisk_min={value}	(Optional) Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
trurisk_max={value}	(Optional) Show only detection records with an TruRisk value less than or equal to the TruRisk max value specified. trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_trurisk_factors={0|1}	(Optional) Specify 1 to show TruRisk contributing factors associated with each asset record in the output. Specify 0 if you do not want to show TruRisk contributing factors.
EC2/Azure/GCP metadata	
host_metadata={value}	(Optional) Specify “all” to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.

Parameter	Description
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter.

Sample regular expression strings for matching OS names

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/3.0/fo/asset/host/?action=list&compliance_
enabled=1&os_pattern=%5EWindows.*2%24' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
 <HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T07:36:40Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>66942</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[2k3sp2-25-12]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[2k3.patch.ad.vuln.qa.qualys.com]]>
```

```
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[2K3SP2-25-12]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2016-11-15T07:39:22Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>66950</ID>
                <IP>11.11.11.1</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[pci-2k3sp2-25-9]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pci-2k3sp2-25-9]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PCI-2K3SP2-25-9]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141141</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[com-sql-24-68.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[com-sql-24-68]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[com-sql-24-
```

```
68.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[COM-SQL-24-68]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141142</ID>
                <IP>11.11.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[win2k3r2-64bit.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[win2k3r2-64bit]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[win2k3r2-
64bit.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[WIN2K3R2-64BIT]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:10:49Z</FIRST_FOUND_DATE>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List assets

API request:

```
curl --location --request GET
'<qualys_base_url>/api/3.0/fo/asset/host/?action=list&show_asset_id=1&hos
t_metadata=all&details=All
--header 'X-Requested-With: curl'
--header 'Authorization: <token>'
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-17T07:16:54Z</datetime>
    <host_list>
      <host>
        <id>1295154</id>
        <asset_id>5856721</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>JUNOS 15.1R6-S2.1</os>
        <first_found_date>2020-08-18T07:08:12Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
      <host>
        <id>1295155</id>
        <asset_id>5856524</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <netbios>COM-XP-64-32-93</netbios>
        <first_found_date>2020-08-18T07:08:14Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
....
      <host>
        <id>6162135</id>
        <asset_id>47773653</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:35Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-17T07:15:35Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
17T06:46:48Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-17T06:48:56Z</pc_auth_success_date>
      </host>
      <host>
```

```
        <id>6171463</id>
        <asset_id>47817089</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 8.6</os>
        <first_found_date>2024-09-16T17:55:07Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
16T17:30:19Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T17:55:08Z</pc_auth_success_date>
      </host>
    </host_list>
    <glossary>
      <user_list>
        <user>
          <user_login>username</user_login>
          <first_name>xxxx</first_name>
          <last_name>yyyy</last_name>
        </user>
      </user_list>
    </glossary>
  </response>
</host_list_output>
```

Sample - List assets based on scan end date, scan processed date

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://<qualys_base_url>/api/3.0/fo/asset/host/?action=list&truncation_
limit=10&details=All
/AGs&vm_scan_date_before=2017-09-
14T06:32:15Z&vm_auth_scan_date_before=2017-09-
14T06:32:15Z&vm_scan_date_after=2016-05-
12T06:32:15Z&vm_auth_scan_date_after=2016-05-
12T06:32:15Z&vm_processed_before=2017-09&scap_scan_since=2018-08-29
-14T06:33:24Z&vm_processed_after=2016-09-12T06:33:24Z"-12T06:33:24Z"
```

Sample - List assets with specific TruRisk score

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/asset/host/?action=list&ips=10.115.126.190&
show_trurisk=1&trurisk_min=1&trurisk_max=1000&show_trurisk_factors=1'
--header 'X-Requested-With: curl demo2'
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-06-21T06:46:04Z</DATETIME>
    <HOST_LIST>
      <HOST>
```

```
        <ID>1800139</ID>
        <IP>11.111.111.111</IP>
        <ASSET_RISK_SCORE>680</ASSET_RISK_SCORE>
        <TRURISK_SCORE>680</TRURISK_SCORE>
        <ASSET_CRITICALITY_SCORE>4</ASSET_CRITICALITY_SCORE>
        <TRURISK_SCORE_FACTORS>
          <TRURISK_SCORE_FORMULA>4 *
{(1.0*95*(14^0.01))+(0.6*74*(31^0.01))+(0.4*47*(73^0.01))+(0.2*33*(66^0.
01))}</TRURISK_SCORE_FORMULA>
          <VULN_COUNT qds_severity="1">0</VULN_COUNT>
          <VULN_COUNT qds_severity="2">66</VULN_COUNT>
          <VULN_COUNT qds_severity="3">73</VULN_COUNT>
          <VULN_COUNT qds_severity="4">31</VULN_COUNT>
          <VULN_COUNT qds_severity="5">14</VULN_COUNT>
        </TRURISK_SCORE_FACTORS>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>0</NETWORK_ID>
        <DNS><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ca1]]></HOSTNAME>
          <DOMAIN><![CDATA[rdlab.in03.qualys.com.abc123]]></DOMAIN>
          <FQDN><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[SYS_10_115_126_190]]></NETBIOS>
        <OS><![CDATA[CentOS Linux 7.5.1804]]></OS>
        <QG_HOSTID><![CDATA[6fc281d4-40e2-4145-bcaa-
753f3f0d57d7]]></QG_HOSTID>
        <LAST_BOOT>2022-05-27T18:18:43Z</LAST_BOOT>
       <SERIAL_NUMBER><![CDATA[VMware-56 4d 99 7a 19 f5 a6 94-b5 f0 07 68
7c 9a e5 b5]]></SERIAL_NUMBER>
        <HARDWARE_UUID><![CDATA[564D997A-19F5-A694-B5F0-
07687C9AE5B5]]></HARDWARE_UUID>
        <FIRST_FOUND_DATE>2021-07-28T08:37:55Z</FIRST_FOUND_DATE>
        <LAST_ACTIVITY>2023-06-21T06:15:43Z</LAST_ACTIVITY>
        <AGENT_STATUS><![CDATA[Inventory Scan Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[QAGENT]]></CLOUD_AGENT_RUNNING_ON>
      </HOST>
      ...
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List scanned assets with certain EC2 metadata

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,ac
countId,instanceId"
"https://<qualys_base_url>/api/3.0/fo/asset/host/"
```

XML output:

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
```

```
"https://<qualys_base_url>/api/3.0/fo/asset/host/host_list_output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-15T09:50:46Z</DATETIME>
    <HOST_LIST>
       <HOST>
       <ID>135151</ID>
       <IP>11.11.1.111</IP>
       <TRACKING_METHOD>EC2</TRACKING_METHOD>
       <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>
       <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>
       <OS><![CDATA[Amazon Linux 2016.09]]></OS>
       <METADATA>
         <EC2>
           <ATTRIBUTE>
             <NAME><![CDATA[latest/dynamic/instance-
              identity/document/region]]></NAME>
             <LAST_STATUS>Success</LAST_STATUS>
             <VALUE><![CDATA[us-east-1]]></VALUE>
             <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
             <LAST_ERROR_DATE></LAST_ERROR_DATE>
             <LAST_ERROR><![CDATA[]]></LAST_ERROR>
           </ATTRIBUTE>
           <ATTRIBUTE>
             <NAME><![CDATA[latest/dynamic/instance-
              identity/document/accountId]]></NAME>
             <LAST_STATUS>Success</LAST_STATUS>
             <VALUE><![CDATA[205767712438]]></VALUE>
             <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
             <LAST_ERROR_DATE></LAST_ERROR_DATE>
             <LAST_ERROR><![CDATA[]]></LAST_ERROR>
           </ATTRIBUTE>
         </EC2>
       </METADATA>
       <LAST_VULN_SCAN_DATETIME>2017-03-
        21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
       <LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
       <LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
       <LAST_VM_AUTH_SCANNED_DATE>2017-03-
        21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
       <LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
       <LAST_COMPLIANCE_SCAN_DATETIME>2017-03-
        21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
     </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - Record Limit Exceeded Warning

In this case 1,000 host records are included in the XML output and the Warning message (shown below) indicates the URL you need to use to request the next 1,000 host records.

```
<RESPONSE>
        ...
```

```
        <WARNING>
            <CODE>1980</CODE>
            <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>
            <URL>

<![CDATA[https://qualysapi.p01.eng.sjc01.qualys.com/api/3.0/fo/asset/host
/?action=list&details=None&truncation_limit=100&id_min=145359]]>
            </URL>
        </WARNING>
    </RESPONSE>
...
```

Sample - Display the hosts that have completed the compliance scan before the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&pc_auth_success_date_before=2022-06-06&details=All"
"https://<qualys_base_url>/api/3.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T10:58:10Z</datetime>
    <host_list>
      <host>
        <id>2584392</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>compaix6lpr01</dns>
        <dns_data>
          <hostname>compaix6lpr01</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>AIX 6.1.0.0</os>
        <qg_hostid>2f06cf12-c127-4cfa-93c1-2fe3b9a1cdec</qg_hostid>
        <last_boot>2022-04-01T18:03:47Z</last_boot>
        <first_found_date>2022-04-27T09:51:52Z</first_found_date>
        <last_activity>2022-05-11T05:36:34Z</last_activity>
        <agent_status>Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
11T06:52:31Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-11T06:39:13Z</pc_auth_success_date>
      </host>
      <host>
        <id>2588281</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
```

```
        <dns>tomcat10.rdlab.in03.qualys.com</dns>
        <dns_data>
          <hostname>tomcat10</hostname>
          <domain>rdlab.in03.qualys.com</domain>
          <fqdn>tomcat10.rdlab.in03.qualys.com</fqdn>
        </dns_data>
        <os>CentOS Linux 7.5.1804 (Core) 7.5.1804</os>
        <qg_hostid>4400c88b-95ba-435d-94f2-8dfc1a1ebe38</qg_hostid>
        <last_boot>2022-01-14T05:41:41Z</last_boot>
        <hardware_uuid>422af3eb-59b3-d7c4-aa71-
dd20780e4c0a</hardware_uuid>
        <first_found_date>2022-04-29T07:16:12Z</first_found_date>
        <last_activity>2022-05-17T09:08:13Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
17T00:12:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-17T00:15:23Z</pc_auth_success_date>
      </host>
      <host>
        <id>2612147</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>comwls14c</dns>
        <dns_data>
          <hostname>comwls14c</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.8.2003 (Core) 7.8.2003</os>
        <qg_hostid>6020ae3c-cefa-4540-8690-aa9c23cdfd2d</qg_hostid>
        <last_boot>2021-06-15T06:52:48Z</last_boot>
        <hardware_uuid>420cf117-1fcb-0325-1d67-
def7b2161823</hardware_uuid>
        <first_found_date>2022-05-05T11:48:45Z</first_found_date>
        <last_activity>2022-05-09T04:49:16Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
09T00:19:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-09T00:38:21Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

Sample - Display the hosts that have completed the compliance scan after the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "username:password" -d
"action=list&pc_auth_success_date_after=2024-08-26&details=All"
"https://<qualys_base_url>/api/3.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T11:07:45Z</datetime>
    <host_list>
      <host>
        <id>5583053</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>nileshcentous7_9</dns>
        <dns_data>
          <hostname>nileshcentous7_9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.9.2009</os>
        <qg_hostid>694b795c-39b2-4e15-b5d1-2015888ecd76</qg_hostid>
        <last_boot>2022-12-08T12:20:16Z</last_boot>
       <serial_number>VMware-42 13 0c f3 66 e0 b6 17-18 37 0c 69 bd 6d b5
2d</serial_number>
        <hardware_uuid>f30c1342-e066-17b6-1837-
0c69bd6db52d</hardware_uuid>
        <first_found_date>2024-06-11T04:52:09Z</first_found_date>
        <last_activity>2024-09-16T10:53:53Z</last_activity>
        <agent_status>PC Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
11T07:13:49Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T07:14:45Z</pc_auth_success_date>
      </host>
      <host>
        <id>5953668</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
        <os>Windows Microsoft Windows Server 2022 Datacenter 10.0.20348
Build 20348</os>
        <qg_hostid>660e9f09-03a8-0004-0046-0050568cb2b6</qg_hostid>
        <last_boot>2024-07-11T16:13:07Z</last_boot>
       <serial_number>VMware-42 0c 7e 00 c9 37 08 c4-1f 5c b3 f4 8b 19 02
fe</serial_number>
        <hardware_uuid>007E0C42-37C9-C408-1F5C-
B3F48B1902FE</hardware_uuid>
        <first_found_date>2024-08-05T08:40:14Z</first_found_date>
        <last_activity>2024-09-16T05:51:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
```

```
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
16T08:21:17Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T08:24:54Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964522</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
       <os>Windows Server 2022 Datacenter 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:34Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:16:35Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964524</id>
        <ip>11.11.111.11</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-dc01.veda.local</dns>
        <dns_data>
          <hostname>win-dc01</hostname>
          <domain>veda.local</domain>
          <fqdn>win-dc01.veda.local</fqdn>
        </dns_data>
        <netbios>WIN-DC01</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:59Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:18:01Z</pc_auth_success_date>
      </host>
      <host>
        <id>5985791</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Red Hat Enterprise Linux 9.0</os>
        <qg_hostid>2c4b95d3-51e1-4457-8049-979e80b06527</qg_hostid>
        <first_found_date>2024-08-12T11:17:54Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:42:27Z</pc_auth_success_date>
      </host>
      <host>
        <id>6130324</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
```

```
        <os>Oracle Enterprise Linux 9.0</os>
        <first_found_date>2024-09-06T10:55:16Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:42:36Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:03:22Z</pc_auth_success_date>
      </host>
      <host>
        <id>6143865</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-cr35vneg5h9</dns>
        <dns_data>
          <hostname>win-cr35vneg5h9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <netbios>WIN-CR35VNEG5H9</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-09-10T04:06:38Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:47:04Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:04:32Z</pc_auth_success_date>
      </host>
      <host>
        <id>6144034</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>orac23cvm.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>orac23cvm</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>orac23cvm.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 9.0</os>
        <qg_hostid>a2126498-3b97-4d0c-883c-28615acbf0fb</qg_hostid>
        <last_boot>2024-09-13T08:46:06Z</last_boot>
       <serial_number>VMware-42 2e ce a2 1e 23 43 8b-9c d5 82 50 b6 f3 48
9d</serial_number>
        <hardware_uuid>a2ce2e42-231e-8b43-9cd5-
8250b6f3489d</hardware_uuid>
        <first_found_date>2024-09-10T05:31:09Z</first_found_date>
        <last_activity>2024-09-16T10:46:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T15:07:12Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T15:12:17Z</pc_auth_success_date>
      </host>
      <host>
        <id>6149368</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <os>Alibaba Cloud Linux 3</os>
        <first_found_date>2024-09-10T21:53:40Z</first_found_date>
```

```
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:02:33Z</pc_auth_success_date>
      </host>
      <host>
        <id>6162135</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:42Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-16T10:47:42Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T14:16:06Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T14:18:16Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

DTD

<platform API server>/api/3.0/fo/asset/host/dtd/list/output.dtd

V4.0

api/4.0/fo/asset/host/?action=list

[GET] [POST]

Download a list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided. Hosts in the XML output are sorted by host ID in ascending order.

The output of the Host List API is paginated. By default, a maximum of 1,000 host records are returned per request. You can customize the page size (i.e. the number of host records) by using the parameter "truncation_limit=10000" for instance. In this case the results will be return with pages of 10,000 host records.

The Host List API also shows the TruRisk score for each asset record in the API output and allows users to filter the output based on the TruRisk score .

The TruRisk score is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

TruRisk score has a range from 0 to 1000:

- Severe (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

The API output also displays the updated Asset Criticality Score (ACS), which may differ from the score shown in the Vulnerabilities and Assets tabs, as those scores are only updated after a vulnerability scan.

Permissions - Managers view all scanned hosts in subscription. Auditors view all scanned compliance hosts in subscription. Unit Managers view scanned hosts in user's business unit. Scanners and Readers view scanned hosts in user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR and PC. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

For Unit Managers, Scanners, and Readers to view compliance hosts, the "Manage compliance" permission must be granted in the user's account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)A flag used to make a host list request.
os_hostname={**0**|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.

Parameter	Description
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
details={**Basic**|Basic/AGs | All|All/AGs | None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None. Basic - (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system. Basic/AGs - Show basic host information plus asset group information. Asset group information includes the asset group ID and title. All - Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates. All/AGs - Show all host information plus asset group information. Asset group information includes the asset group ID and title. None - Show only the host ID.

Parameter	Description
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Refer to Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter. For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php PCRE syntax: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php
truncation_limit={value}	(Optional) Specify the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more host records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. See example: Sample - Record Limit Exceeded Warning You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is downloaded.

Parameter	Description
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value. A valid host ID is required.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.

Parameter	Description
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Use this parameter to filter the scanned hosts list to show either: 1) a list of scanned compliance hosts, or 2) a list of scanned vulnerability management hosts. Specify 1 to list scanned compliance hosts in the user's account. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module. A user can specify 0 only when the user has compliance management privileges. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If this permission is not enabled and the user makes a request with this parameter set to 0, the request fails with an error (unknown parameter).
cloud_agent_activationkey={0|1}	(Optional) Specify 1, to have two tags AGENT_ACTIVATION_KEY and AGENT_ACTIVATION_TITLE in the response for appropriate assets.
Date Filters	
no_vm_scan_since={date}	(Optional) Show hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - An Auditor cannot specify this parameter.
no_compliance_scan_since={date}	(Optional) Show compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_scan_since={date}	(Optional) Show hosts that were last scanned for vulnerabilities since a certain date and time (optional). Hosts that were the target of a vulnerability scan since the date/time will be shown. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: An Auditor cannot specify this parameter.

Parameter	Description
compliance_scan_since={date}	(Optional) Show hosts that were last scanned for compliance since a certain date and time (optional). Hosts that were the target of a compliance scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
vm_scan_date_before={date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.

Parameter	Description
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
pc_auth_success_date_before={date}	(Optional) Show hosts with a successful compliance scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
pc_auth_success_date_after={date}	(Optional) Show hosts with a successful compliance scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
scap_scan_since={date}	(Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
no_scap_scan_since={date}	(Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.

Parameter	Description
Asset Tags	
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify **1** if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.
Asset Risk Score (ARS)	**Note**: The ARS parameters will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification. You must start using the new TruRisk parameters mentioned below.
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.

Parameter	Description
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.
TruRisk Score	
show_trurisk={0|1}	(Optional) Specify 1 to show the TruRisk value in the output. Specify 0 if you do not want to show the TruRisk value.
trurisk_min={value}	(Optional) Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
trurisk_max={value}	(Optional) Show only detection records with an TruRisk value less than or equal to the TruRisk max value specified. trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_trurisk_factors={0|1}	(Optional) Specify 1 to show TruRisk contributing factors associated with each asset record in the output. Specify 0 if you do not want to show TruRisk contributing factors.
EC2/Azure/GCP metadata	
host_metadata={value}	(Optional) Specify “all” to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.

Parameter	Description
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter.

Sample - Regular expression strings for matching OS names

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/4.0/fo/asset/host/?action=list&compliance_
enabled=1&os_pattern=%5EWindows.*2%24&cloud_agent_activationkey=0' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T07:34:37Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>66942</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[2k3sp2-25-12]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[2k3.patch.ad.vuln.qa.qualys.com]]>
```

```
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[2K3SP2-25-12]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2016-11-15T07:39:22Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>66950</ID>
                <IP>11.11.11.1</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[pci-2k3sp2-25-9]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pci-2k3sp2-25-9]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PCI-2K3SP2-25-9]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141141</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[com-sql-24-68.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[com-sql-24-68]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[com-sql-24-
```

```
68.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[COM-SQL-24-68]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141142</ID>
                <IP>11.11.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[win2k3r2-64bit.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[win2k3r2-64bit]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[win2k3r2-
64bit.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[WIN2K3R2-64BIT]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:10:49Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141146</ID>
                <IP>11.11.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[vstasp2u-26-106]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[vstasp2u-26-106]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
```

```
                    <NETBIOS>
                        <![CDATA[VSTASP2U-26-106]]>
                    </NETBIOS>
                    <OS>
                        <![CDATA[Windows Vista Enterprise Service Pack 2]]>
                    </OS>
                    <FIRST_FOUND_DATE>2017-11-07T09:11:25Z</FIRST_FOUND_DATE>
                </HOST>
                <HOST>
                    <ID>141159</ID>
                    <IP>11.11.11.11</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[was-2k3-30-58]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[was-2k3-30-58]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[WAS-2K3-30-58]]>
                    </NETBIOS>
                    <OS>
                        <![CDATA[Windows 2003 Service Pack 2]]>
                    </OS>
                    <FIRST_FOUND_DATE>2017-11-07T09:13:35Z</FIRST_FOUND_DATE>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_OUTPUT>
```

Sample - List assets

API request:

```
curl --location --request GET
'<qualys_base_url>/api/4.0/fo/asset/host/?action=list&show_asset_id=1&hos
t_metadata=all&details=All
--header 'X-Requested-With: curl'
--header 'Authorization: <token>'
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-17T07:16:54Z</datetime>
    <host_list>
      <host>
        <id>1295154</id>
```

```
        <asset_id>5856721</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>JUNOS 15.1R6-S2.1</os>
        <first_found_date>2020-08-18T07:08:12Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
      <host>
        <id>1295155</id>
        <asset_id>5856524</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <netbios>COM-XP-64-32-93</netbios>
        <first_found_date>2020-08-18T07:08:14Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
....
      <host>
        <id>6162135</id>
        <asset_id>47773653</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:35Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-17T07:15:35Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
17T06:46:48Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-17T06:48:56Z</pc_auth_success_date>
      </host>
      <host>
        <id>6171463</id>
        <asset_id>47817089</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 8.6</os>
        <first_found_date>2024-09-16T17:55:07Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
16T17:30:19Z</last_compliance_scan_datetime>
```

```
          <pc_auth_success_date>2024-09-16T17:55:08Z</pc_auth_success_date>
        </host>
      </host_list>
      <glossary>
        <user_list>
          <user>
            <user_login>username</user_login>
            <first_name>xxxx</first_name>
            <last_name>yyyy</last_name>
          </user>
        </user_list>
      </glossary>
    </response>
</host_list_output>
```

Sample - List assets based on scan end date, scan processed date

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://<qualys_base_url>/api/4.0/fo/asset/host/?action=list&truncation_
limit=10&details=All
/AGs&vm_scan_date_before=2017-09-
14T06:32:15Z&vm_auth_scan_date_before=2017-09-
14T06:32:15Z&vm_scan_date_after=2016-05-
12T06:32:15Z&vm_auth_scan_date_after=2016-05-
12T06:32:15Z&vm_processed_before=2017-09&scap_scan_since=2018-08-29
-14T06:33:24Z&vm_processed_after=2016-09-12T06:33:24Z"-12T06:33:24Z"
```

Sample - List assets with specific TruRisk score

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/?action=list&ips=10.115.126.190&
show_trurisk=1&trurisk_min=1&trurisk_max=1000&show_trurisk_factors=1'
--header 'X-Requested-With: curl demo2'
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-06-21T06:46:04Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1800139</ID>
        <IP>11.111.111.111</IP>
        <ASSET_RISK_SCORE>680</ASSET_RISK_SCORE>
        <TRURISK_SCORE>680</TRURISK_SCORE>
        <ASSET_CRITICALITY_SCORE>4</ASSET_CRITICALITY_SCORE>
        <TRURISK_SCORE_FACTORS>
          <TRURISK_SCORE_FORMULA>4 *
{(1.0*95*(14^0.01))+(0.6*74*(31^0.01))+(0.4*47*(73^0.01))+(0.2*33*(66^0.
```

```
01))}</TRURISK_SCORE_FORMULA>
          <VULN_COUNT qds_severity="1">0</VULN_COUNT>
          <VULN_COUNT qds_severity="2">66</VULN_COUNT>
          <VULN_COUNT qds_severity="3">73</VULN_COUNT>
          <VULN_COUNT qds_severity="4">31</VULN_COUNT>
          <VULN_COUNT qds_severity="5">14</VULN_COUNT>
        </TRURISK_SCORE_FACTORS>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>0</NETWORK_ID>
        <DNS><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ca1]]></HOSTNAME>
          <DOMAIN><![CDATA[rdlab.in03.qualys.com.abc123]]></DOMAIN>
          <FQDN><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[SYS_10_115_126_190]]></NETBIOS>
        <OS><![CDATA[CentOS Linux 7.5.1804]]></OS>
        <QG_HOSTID><![CDATA[6fc281d4-40e2-4145-bcaa-
753f3f0d57d7]]></QG_HOSTID>
        <LAST_BOOT>2022-05-27T18:18:43Z</LAST_BOOT>
       <SERIAL_NUMBER><![CDATA[VMware-56 4d 99 7a 19 f5 a6 94-b5 f0 07 68
7c 9a e5 b5]]></SERIAL_NUMBER>
        <HARDWARE_UUID><![CDATA[564D997A-19F5-A694-B5F0-
07687C9AE5B5]]></HARDWARE_UUID>
        <FIRST_FOUND_DATE>2021-07-28T08:37:55Z</FIRST_FOUND_DATE>
        <LAST_ACTIVITY>2023-06-21T06:15:43Z</LAST_ACTIVITY>
        <AGENT_STATUS><![CDATA[Inventory Scan Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[QAGENT]]></CLOUD_AGENT_RUNNING_ON>
      </HOST>
      ...
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List scanned assets with certain EC2 metadata

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,ac
countId,instanceId"
"https://<qualys_base_url>/api/4.0/fo/asset/host/"
```

XML output:

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/asset/host/host_list_output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-15T09:50:46Z</DATETIME>
    <HOST_LIST>
       <HOST>
       <ID>135151</ID>
       <IP>11.11.1.111</IP>
```

```
        <TRACKING_METHOD>EC2</TRACKING_METHOD>
        <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>
        <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>
        <OS><![CDATA[Amazon Linux 2016.09]]></OS>
        <METADATA>
          <EC2>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/region]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[us-east-1]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/accountId]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[205767712438]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
          </EC2>
        </METADATA>
        <LAST_VULN_SCAN_DATETIME>2017-03-
         21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
        <LAST_VM_AUTH_SCANNED_DATE>2017-03-
         21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
        <LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
        <LAST_COMPLIANCE_SCAN_DATETIME>2017-03-
         21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - Record Limit Exceeded Warning

In this case 1,000 host records are included in the XML output and the Warning message (shown below) indicates the URL you need to use to request the next 1,000 host records.

```
<RESPONSE>
    ...
        <WARNING>
            <CODE>1980</CODE>
           <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>
            <URL>

<![CDATA[https://qualysapi.p01.eng.sjc01.qualys.com/api/4.0/fo/asset/host
/?action=list&details=None&truncation_limit=100&cloud_agent_activationkey
```

```
=0&id_min=145359]]>
            </URL>
        </WARNING>
    </RESPONSE>
...
```

Sample - Display the hosts that have completed the compliance scan before the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&pc_auth_success_date_before=2022-06-06&details=All"
"https://<qualys_base_url>/api/4.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T10:58:10Z</datetime>
    <host_list>
      <host>
        <id>2584392</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>compaix6lpr01</dns>
        <dns_data>
          <hostname>compaix6lpr01</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>AIX 6.1.0.0</os>
        <qg_hostid>2f06cf12-c127-4cfa-93c1-2fe3b9a1cdec</qg_hostid>
        <last_boot>2022-04-01T18:03:47Z</last_boot>
        <first_found_date>2022-04-27T09:51:52Z</first_found_date>
        <last_activity>2022-05-11T05:36:34Z</last_activity>
        <agent_status>Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
11T06:52:31Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-11T06:39:13Z</pc_auth_success_date>
      </host>
      <host>
        <id>2588281</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>tomcat10.rdlab.in03.qualys.com</dns>
        <dns_data>
          <hostname>tomcat10</hostname>
          <domain>rdlab.in03.qualys.com</domain>
          <fqdn>tomcat10.rdlab.in03.qualys.com</fqdn>
        </dns_data>
```

```
        <os>CentOS Linux 7.5.1804 (Core) 7.5.1804</os>
        <qg_hostid>4400c88b-95ba-435d-94f2-8dfc1a1ebe38</qg_hostid>
        <last_boot>2022-01-14T05:41:41Z</last_boot>
        <hardware_uuid>422af3eb-59b3-d7c4-aa71-
dd20780e4c0a</hardware_uuid>
        <first_found_date>2022-04-29T07:16:12Z</first_found_date>
        <last_activity>2022-05-17T09:08:13Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
17T00:12:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-17T00:15:23Z</pc_auth_success_date>
      </host>
      <host>
        <id>2612147</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>comwls14c</dns>
        <dns_data>
          <hostname>comwls14c</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.8.2003 (Core) 7.8.2003</os>
        <qg_hostid>6020ae3c-cefa-4540-8690-aa9c23cdfd2d</qg_hostid>
        <last_boot>2021-06-15T06:52:48Z</last_boot>
        <hardware_uuid>420cf117-1fcb-0325-1d67-
def7b2161823</hardware_uuid>
        <first_found_date>2022-05-05T11:48:45Z</first_found_date>
        <last_activity>2022-05-09T04:49:16Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
09T00:19:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-09T00:38:21Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

Sample - Display the hosts that have completed the compliance scan after the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "username:password" -d
"action=list&pc_auth_success_date_after=2024-08-26&details=All"
"https://<qualys_base_url>/api/4.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
```

```
    <datetime>2024-09-16T11:07:45Z</datetime>
    <host_list>
      <host>
        <id>5583053</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>nileshcentous7_9</dns>
        <dns_data>
          <hostname>nileshcentous7_9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.9.2009</os>
        <qg_hostid>694b795c-39b2-4e15-b5d1-2015888ecd76</qg_hostid>
        <last_boot>2022-12-08T12:20:16Z</last_boot>
       <serial_number>VMware-42 13 0c f3 66 e0 b6 17-18 37 0c 69 bd 6d b5
2d</serial_number>
        <hardware_uuid>f30c1342-e066-17b6-1837-
0c69bd6db52d</hardware_uuid>
        <first_found_date>2024-06-11T04:52:09Z</first_found_date>
        <last_activity>2024-09-16T10:53:53Z</last_activity>
        <agent_status>PC Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
11T07:13:49Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T07:14:45Z</pc_auth_success_date>
      </host>
      <host>
        <id>5953668</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
        <os>Windows Microsoft Windows Server 2022 Datacenter 10.0.20348
Build 20348</os>
        <qg_hostid>660e9f09-03a8-0004-0046-0050568cb2b6</qg_hostid>
        <last_boot>2024-07-11T16:13:07Z</last_boot>
       <serial_number>VMware-42 0c 7e 00 c9 37 08 c4-1f 5c b3 f4 8b 19 02
fe</serial_number>
        <hardware_uuid>007E0C42-37C9-C408-1F5C-
B3F48B1902FE</hardware_uuid>
        <first_found_date>2024-08-05T08:40:14Z</first_found_date>
        <last_activity>2024-09-16T05:51:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
16T08:21:17Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T08:24:54Z</pc_auth_success_date>
      </host>
```

```
      <host>
        <id>5964522</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
       <os>Windows Server 2022 Datacenter 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:34Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:16:35Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964524</id>
        <ip>11.11.111.11</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-dc01.veda.local</dns>
        <dns_data>
          <hostname>win-dc01</hostname>
          <domain>veda.local</domain>
          <fqdn>win-dc01.veda.local</fqdn>
        </dns_data>
        <netbios>WIN-DC01</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:59Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:18:01Z</pc_auth_success_date>
      </host>
      <host>
        <id>5985791</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Red Hat Enterprise Linux 9.0</os>
        <qg_hostid>2c4b95d3-51e1-4457-8049-979e80b06527</qg_hostid>
        <first_found_date>2024-08-12T11:17:54Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:42:27Z</pc_auth_success_date>
      </host>
      <host>
        <id>6130324</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 9.0</os>
        <first_found_date>2024-09-06T10:55:16Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:42:36Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:03:22Z</pc_auth_success_date>
```

```
      </host>
      <host>
        <id>6143865</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-cr35vneg5h9</dns>
        <dns_data>
          <hostname>win-cr35vneg5h9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <netbios>WIN-CR35VNEG5H9</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-09-10T04:06:38Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:47:04Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:04:32Z</pc_auth_success_date>
      </host>
      <host>
        <id>6144034</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>orac23cvm.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>orac23cvm</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>orac23cvm.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 9.0</os>
        <qg_hostid>a2126498-3b97-4d0c-883c-28615acbf0fb</qg_hostid>
        <last_boot>2024-09-13T08:46:06Z</last_boot>
       <serial_number>VMware-42 2e ce a2 1e 23 43 8b-9c d5 82 50 b6 f3 48
9d</serial_number>
        <hardware_uuid>a2ce2e42-231e-8b43-9cd5-
8250b6f3489d</hardware_uuid>
        <first_found_date>2024-09-10T05:31:09Z</first_found_date>
        <last_activity>2024-09-16T10:46:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T15:07:12Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T15:12:17Z</pc_auth_success_date>
      </host>
      <host>
        <id>6149368</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <os>Alibaba Cloud Linux 3</os>
        <first_found_date>2024-09-10T21:53:40Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:02:33Z</pc_auth_success_date>
      </host>
      <host>
```

```
            <id>6162135</id>
            <ip>11.11.11.11</ip>
            <tracking_method>Cloud Agent</tracking_method>
            <dns>singlestore_test.comp.rdlab.qualys.com</dns>
            <dns_data>
              <hostname>singlestore_test</hostname>
              <domain>comp.rdlab.qualys.com</domain>
              <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
            </dns_data>
            <os>Oracle Enterprise Linux 8.6</os>
            <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
            <last_boot>2024-09-16T09:16:42Z</last_boot>
           <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
    0a</serial_number>
            <hardware_uuid>034c2e42-e6e3-c1ba-5366-
    da59f960c40a</hardware_uuid>
            <first_found_date>2024-09-13T09:37:09Z</first_found_date>
            <last_activity>2024-09-16T10:47:42Z</last_activity>
            <agent_status>Inventory Scan Complete</agent_status>
            <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
            <last_compliance_scan_datetime>2024-09-
    13T14:16:06Z</last_compliance_scan_datetime>
            <pc_auth_success_date>2024-09-13T14:18:16Z</pc_auth_success_date>
          </host>
        </host_list>
      </response>
</host_list_output>
```

Sample - Display the Activation Key and Activation Title associated with the agent assets

API Request:

```
curl
"<qualys_base_url>/api/4.0/fo/asset/host/?ips=11.111.11.111,11.111.11.111
&action=list&details=All&cloud_agent_activationkey=1" -X POST -b
"QualysSession=ae630e1f345b6503324a93d52b3a69de" -H "Content-Type:
application/x-www-form-urlencoded" -H "X-Requested-With: curl demo2" -H
"Accept: /" -H "Content-Length: 0" --compressed -k -v
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/4.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-12-20T07:41:21Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>5962587</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[centos7-dns-11-111.rdlab.com]]>
                    </DNS>
```

```
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[centos7-hostname-11-111]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[rdlab.com]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[CentOS Linux 7.9.2009]]>
                    </OS>
                    <QG_HOSTID>
                        <![CDATA[b4192ceb-de61-4884-b392-55135e14ce25]]>
                    </QG_HOSTID>
                    <LAST_BOOT>2024-06-07T04:33:55Z</LAST_BOOT>
                    <SERIAL_NUMBER>
                        <![CDATA[VMware-42 2a 6c b2 02 2c 46 38-fb 92 8d
5f 02 44 b4 ac]]>
                    </SERIAL_NUMBER>
                    <HARDWARE_UUID>
                        <![CDATA[b26c2a42-2c02-3846-fb92-8d5f0244b4ac]]>
                    </HARDWARE_UUID>
                    <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                    <LAST_ACTIVITY>2024-08-12T10:20:55Z</LAST_ACTIVITY>
                    <AGENT_STATUS>
                        <![CDATA[Inventory Scan Complete]]>
                    </AGENT_STATUS>
                    <CLOUD_AGENT_RUNNING_ON>
                        <![CDATA[QAGENT]]>
                    </CLOUD_AGENT_RUNNING_ON>
                    <AGENT_ACTIVATION_TITLE>
                        <![CDATA[title_Activation_key]]>
                    </AGENT_ACTIVATION_TITLE>
                    <AGENT_ACTIVATION_KEY>
                        <![CDATA[e5decf50-c20a-4782-8e9e-b6a712261a4d]]>
                    </AGENT_ACTIVATION_KEY>
                    <LAST_VULN_SCAN_DATETIME>2024-08-
13T03:41:08Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_SCANNED_DATE>
                    <LAST_VM_AUTH_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_AUTH_SCANNED_DATE>
                    <LAST_COMPLIANCE_SCAN_DATETIME>2024-08-
12T18:33:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
                </HOST>
                <HOST>
                    <ID>5962589</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
```

```
                    <DNS>
                        <![CDATA[centos7-dns-11-111.rdlab.com]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[centos7-hostname-11-111]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[rdlab.com]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[CentOS Linux 7.9.2009]]>
                    </OS>
                    <QG_HOSTID>
                        <![CDATA[0714edfe-8a72-44d9-98eb-95401672b235]]>
                    </QG_HOSTID>
                    <LAST_BOOT>2024-06-07T04:45:05Z</LAST_BOOT>
                    <SERIAL_NUMBER>
                        <![CDATA[VMware-42 2a 60 7f 5c 9d 67 71-4b 17 71
35 9b 73 28 d4]]>
                    </SERIAL_NUMBER>
                    <HARDWARE_UUID>
                        <![CDATA[7f602a42-9d5c-7167-4b17-71359b7328d4]]>
                    </HARDWARE_UUID>
                    <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                    <LAST_ACTIVITY>2024-09-19T12:05:05Z</LAST_ACTIVITY>
                    <AGENT_STATUS>
                        <![CDATA[Inventory Scan Complete]]>
                    </AGENT_STATUS>
                    <CLOUD_AGENT_RUNNING_ON>
                        <![CDATA[QAGENT]]>
                    </CLOUD_AGENT_RUNNING_ON>
                    <AGENT_ACTIVATION_KEY>
                        <![CDATA[fcce41e6-446e-4818-bf3e-4b3e3860574b]]>
                    </AGENT_ACTIVATION_KEY>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
19T09:54:48Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_SCANNED_DATE>
                    <LAST_VM_AUTH_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_AUTH_SCANNED_DATE>
                    <LAST_COMPLIANCE_SCAN_DATETIME>2024-09-
19T04:25:11Z</LAST_COMPLIANCE_SCAN_DATETIME>
                </HOST>
                <HOST>
                    <ID>6060439</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
```

```
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:32Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:32Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>519</LAST_VM_SCANNED_DURATION>
                </HOST>
                <HOST>
                    <ID>6060639</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:58Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:58Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>544</LAST_VM_SCANNED_DURATION>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_OUTPUT>
```

DTD

<platform API server>/api/4.0/fo/asset/host/dtd/list/output.dtd

V5.0

api/5.0/fo/asset/host/?action=list

[GET] [POST]

Download a list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided. Hosts in the XML output are sorted by host ID in ascending order.

The output of the Host List API is paginated. By default, a maximum of 1,000 host records are returned per request. You can customize the page size (i.e. the number of host records) by using the parameter "truncation_limit=10000" for instance. In this case the results will be return with pages of 10,000 host records.

The Host List API also shows the TruRisk score for each asset record in the API output and allows users to filter the output based on the TruRisk score .

The TruRisk score is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

TruRisk score has a range from 0 to 1000:

- Severe (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

The API output also displays the updated Asset Criticality Score (ACS), which may differ from the score shown in the Vulnerabilities and Assets tabs, as those scores are only updated after a vulnerability scan.

Permissions - Managers view all scanned hosts in subscription. Auditors view all scanned compliance hosts in subscription. Unit Managers view scanned hosts in user's business unit. Scanners and Readers view scanned hosts in user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR and PC. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

For Unit Managers, Scanners, and Readers to view compliance hosts, the "Manage compliance" permission must be granted in the user's account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)A flag used to make a host list request.
os_hostname={**0**|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.

Parameter	Description
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
details={**Basic**|Basic/AGs | All|All/AGs | None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None. Basic - (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system. Basic/AGs - Show basic host information plus asset group information. Asset group information includes the asset group ID and title. All - Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates. All/AGs - Show all host information plus asset group information. Asset group information includes the asset group ID and title. None - Show only the host ID.

Parameter	Description
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Refer to Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter. For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php PCRE syntax: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php
truncation_limit={value}	(Optional) Specify the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more host records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. See example: Sample - Record Limit Exceeded Warning You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is downloaded.

Parameter	Description
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value. A valid host ID is required.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.

Parameter	Description
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Use this parameter to filter the scanned hosts list to show either: 1) a list of scanned compliance hosts, or 2) a list of scanned vulnerability management hosts. Specify 1 to list scanned compliance hosts in the user's account. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module. A user can specify 0 only when the user has compliance management privileges. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If this permission is not enabled and the user makes a request with this parameter set to 0, the request fails with an error (unknown parameter).
cloud_agent_activationkey={0|1}	(Optional) Specify 1, to have two tags AGENT_ACTIVATION_KEY and AGENT_ACTIVATION_TITLE in the response for appropriate assets.
Date Filters	
no_vm_scan_since={date}	(Optional) Show hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - An Auditor cannot specify this parameter.
no_compliance_scan_since={date}	(Optional) Show compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_scan_since={date}	(Optional) Show hosts that were last scanned for vulnerabilities since a certain date and time (optional). Hosts that were the target of a vulnerability scan since the date/time will be shown. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: An Auditor cannot specify this parameter.

Parameter	Description
compliance_scan_since={date}	(Optional) Show hosts that were last scanned for compliance since a certain date and time (optional). Hosts that were the target of a compliance scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
vm_scan_date_before={date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.

Parameter	Description
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
pc_auth_success_date_before={date}	(Optional) Show hosts with a successful compliance scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
pc_auth_success_date_after={date}	(Optional) Show hosts with a successful compliance scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
scap_scan_since={date}	(Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
no_scap_scan_since={date}	(Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.

Parameter	Description
Asset Tags	
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify **1** if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.
Asset Risk Score (ARS)	**Note**: The ARS parameters will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification. You must start using the new TruRisk parameters mentioned below.
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.

Parameter	Description
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.
TruRisk Score	
show_trurisk={0|1}	(Optional) Specify 1 to show the TruRisk value in the output. Specify 0 if you do not want to show the TruRisk value.
trurisk_min={value}	(Optional) Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
trurisk_max={value}	(Optional) Show only detection records with an TruRisk value less than or equal to the TruRisk max value specified. trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_trurisk_factors={0|1}	(Optional) Specify 1 to show TruRisk contributing factors associated with each asset record in the output. Specify 0 if you do not want to show TruRisk contributing factors.
EC2/Azure/GCP metadata	
host_metadata={value}	(Optional) Specify “all” to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.

Parameter	Description
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter.

Sample - Regular expression strings for matching OS names

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/5.0/fo/asset/host/?action=list&compliance_
enabled=1&os_pattern=%5EWindows.*2%24&cloud_agent_activationkey=0' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T07:34:37Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>66942</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[2k3sp2-25-12]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[2k3.patch.ad.vuln.qa.qualys.com]]>
```

```
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[2K3SP2-25-12]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2016-11-15T07:39:22Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>66950</ID>
                <IP>11.11.11.1</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[pci-2k3sp2-25-9]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pci-2k3sp2-25-9]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PCI-2K3SP2-25-9]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141141</ID>
                <IP>11.11.11.11</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[com-sql-24-68.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[com-sql-24-68]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[com-sql-24-
```

```
68.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[COM-SQL-24-68]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141142</ID>
                <IP>11.11.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[win2k3r2-64bit.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[win2k3r2-64bit]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[win2k3r2-
64bit.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[WIN2K3R2-64BIT]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:10:49Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141146</ID>
                <IP>11.11.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[vstasp2u-26-106]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[vstasp2u-26-106]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
```

```
                    <NETBIOS>
                        <![CDATA[VSTASP2U-26-106]]>
                    </NETBIOS>
                    <OS>
                        <![CDATA[Windows Vista Enterprise Service Pack 2]]>
                    </OS>
                    <FIRST_FOUND_DATE>2017-11-07T09:11:25Z</FIRST_FOUND_DATE>
                </HOST>
                <HOST>
                    <ID>141159</ID>
                    <IP>11.11.11.11</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[was-2k3-30-58]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[was-2k3-30-58]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[WAS-2K3-30-58]]>
                    </NETBIOS>
                    <OS>
                        <![CDATA[Windows 2003 Service Pack 2]]>
                    </OS>
                    <FIRST_FOUND_DATE>2017-11-07T09:13:35Z</FIRST_FOUND_DATE>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_OUTPUT>
```

Sample - List assets

API request:

```
curl --location --request GET
'<qualys_base_url>/api/5.0/fo/asset/host/?action=list&show_asset_id=1&hos
t_metadata=all&details=All
--header 'X-Requested-With: curl'
--header 'Authorization: <token>'
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-17T07:16:54Z</datetime>
    <host_list>
      <host>
        <id>1295154</id>
```

```
        <asset_id>5856721</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>JUNOS 15.1R6-S2.1</os>
        <first_found_date>2020-08-18T07:08:12Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
      <host>
        <id>1295155</id>
        <asset_id>5856524</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <netbios>COM-XP-64-32-93</netbios>
        <first_found_date>2020-08-18T07:08:14Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
....
      <host>
        <id>6162135</id>
        <asset_id>47773653</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:35Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-17T07:15:35Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
17T06:46:48Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-17T06:48:56Z</pc_auth_success_date>
      </host>
      <host>
        <id>6171463</id>
        <asset_id>47817089</asset_id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 8.6</os>
        <first_found_date>2024-09-16T17:55:07Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
16T17:30:19Z</last_compliance_scan_datetime>
```

```
          <pc_auth_success_date>2024-09-16T17:55:08Z</pc_auth_success_date>
        </host>
      </host_list>
      <glossary>
        <user_list>
          <user>
            <user_login>username</user_login>
            <first_name>xxxx</first_name>
            <last_name>yyyy</last_name>
          </user>
        </user_list>
      </glossary>
    </response>
</host_list_output>
```

Sample - List assets based on scan end date, scan processed date

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"<qualys_base_url>/api/5.0/fo/asset/host/?action=list&truncation_limit=10
&details=All
/AGs&vm_scan_date_before=2017-09-
14T06:32:15Z&vm_auth_scan_date_before=2017-09-
14T06:32:15Z&vm_scan_date_after=2016-05-
12T06:32:15Z&vm_auth_scan_date_after=2016-05-
12T06:32:15Z&vm_processed_before=2017-09&scap_scan_since=2018-08-29
-14T06:33:24Z&vm_processed_after=2016-09-12T06:33:24Z"-12T06:33:24Z"
```

Sample - List assets with specific TruRisk score

API request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/?action=list&ips=10.115.126.190&
show_trurisk=1&trurisk_min=1&trurisk_max=1000&show_trurisk_factors=1'
--header 'X-Requested-With: curl demo2'
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-06-21T06:46:04Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1800139</ID>
        <IP>11.111.111.111</IP>
        <ASSET_RISK_SCORE>680</ASSET_RISK_SCORE>
        <TRURISK_SCORE>680</TRURISK_SCORE>
        <ASSET_CRITICALITY_SCORE>4</ASSET_CRITICALITY_SCORE>
        <TRURISK_SCORE_FACTORS>
          <TRURISK_SCORE_FORMULA>4 *
{(1.0*95*(14^0.01))+(0.6*74*(31^0.01))+(0.4*47*(73^0.01))+(0.2*33*(66^0.
```

```
01))}</TRURISK_SCORE_FORMULA>
          <VULN_COUNT qds_severity="1">0</VULN_COUNT>
          <VULN_COUNT qds_severity="2">66</VULN_COUNT>
          <VULN_COUNT qds_severity="3">73</VULN_COUNT>
          <VULN_COUNT qds_severity="4">31</VULN_COUNT>
          <VULN_COUNT qds_severity="5">14</VULN_COUNT>
        </TRURISK_SCORE_FACTORS>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>0</NETWORK_ID>
        <DNS><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ca1]]></HOSTNAME>
          <DOMAIN><![CDATA[rdlab.in03.qualys.com.abc123]]></DOMAIN>
          <FQDN><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[SYS_10_115_126_190]]></NETBIOS>
        <OS><![CDATA[CentOS Linux 7.5.1804]]></OS>
        <QG_HOSTID><![CDATA[6fc281d4-40e2-4145-bcaa-
753f3f0d57d7]]></QG_HOSTID>
        <LAST_BOOT>2022-05-27T18:18:43Z</LAST_BOOT>
       <SERIAL_NUMBER><![CDATA[VMware-56 4d 99 7a 19 f5 a6 94-b5 f0 07 68
7c 9a e5 b5]]></SERIAL_NUMBER>
        <HARDWARE_UUID><![CDATA[564D997A-19F5-A694-B5F0-
07687C9AE5B5]]></HARDWARE_UUID>
        <FIRST_FOUND_DATE>2021-07-28T08:37:55Z</FIRST_FOUND_DATE>
        <LAST_ACTIVITY>2023-06-21T06:15:43Z</LAST_ACTIVITY>
        <AGENT_STATUS><![CDATA[Inventory Scan Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[QAGENT]]></CLOUD_AGENT_RUNNING_ON>
      </HOST>
      ...
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List scanned assets with certain EC2 metadata

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,ac
countId,instanceId"
"<qualys_base_url>/api/5.0/fo/asset/host/"
```

XML output:

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/host_list_output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-15T09:50:46Z</DATETIME>
    <HOST_LIST>
       <HOST>
       <ID>135151</ID>
       <IP>11.11.1.111</IP>
```

```
        <TRACKING_METHOD>EC2</TRACKING_METHOD>
        <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>
        <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>
        <OS><![CDATA[Amazon Linux 2016.09]]></OS>
        <METADATA>
          <EC2>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/region]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[us-east-1]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/accountId]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[205767712438]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
          </EC2>
        </METADATA>
        <LAST_VULN_SCAN_DATETIME>2017-03-
         21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
        <LAST_VM_AUTH_SCANNED_DATE>2017-03-
         21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
        <LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
        <LAST_COMPLIANCE_SCAN_DATETIME>2017-03-
         21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - Record Limit Exceeded Warning

In this case 1,000 host records are included in the XML output and the Warning message (shown below) indicates the URL you need to use to request the next 1,000 host records.

```
<RESPONSE>
    ...
        <WARNING>
            <CODE>1980</CODE>
           <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>
            <URL>

<![CDATA[https://qualysapi.p01.eng.sjc01.qualys.com/api/4.0/fo/asset/host
/?action=list&details=None&truncation_limit=100&cloud_agent_activationkey
```

```
=0&id_min=145359]]>
            </URL>
        </WARNING>
    </RESPONSE>
...
```

Sample - Display the hosts that have completed the compliance scan before the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&pc_auth_success_date_before=2022-06-06&details=All"
"<qualys_base_url>/api/5.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T10:58:10Z</datetime>
    <host_list>
      <host>
        <id>2584392</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>compaix6lpr01</dns>
        <dns_data>
          <hostname>compaix6lpr01</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>AIX 6.1.0.0</os>
        <qg_hostid>2f06cf12-c127-4cfa-93c1-2fe3b9a1cdec</qg_hostid>
        <last_boot>2022-04-01T18:03:47Z</last_boot>
        <first_found_date>2022-04-27T09:51:52Z</first_found_date>
        <last_activity>2022-05-11T05:36:34Z</last_activity>
        <agent_status>Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
11T06:52:31Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-11T06:39:13Z</pc_auth_success_date>
      </host>
      <host>
        <id>2588281</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>tomcat10.rdlab.in03.qualys.com</dns>
        <dns_data>
          <hostname>tomcat10</hostname>
          <domain>rdlab.in03.qualys.com</domain>
          <fqdn>tomcat10.rdlab.in03.qualys.com</fqdn>
        </dns_data>
```

```
        <os>CentOS Linux 7.5.1804 (Core) 7.5.1804</os>
        <qg_hostid>4400c88b-95ba-435d-94f2-8dfc1a1ebe38</qg_hostid>
        <last_boot>2022-01-14T05:41:41Z</last_boot>
        <hardware_uuid>422af3eb-59b3-d7c4-aa71-
dd20780e4c0a</hardware_uuid>
        <first_found_date>2022-04-29T07:16:12Z</first_found_date>
        <last_activity>2022-05-17T09:08:13Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
17T00:12:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-17T00:15:23Z</pc_auth_success_date>
      </host>
      <host>
        <id>2612147</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>comwls14c</dns>
        <dns_data>
          <hostname>comwls14c</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.8.2003 (Core) 7.8.2003</os>
        <qg_hostid>6020ae3c-cefa-4540-8690-aa9c23cdfd2d</qg_hostid>
        <last_boot>2021-06-15T06:52:48Z</last_boot>
        <hardware_uuid>420cf117-1fcb-0325-1d67-
def7b2161823</hardware_uuid>
        <first_found_date>2022-05-05T11:48:45Z</first_found_date>
        <last_activity>2022-05-09T04:49:16Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
09T00:19:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-09T00:38:21Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

Sample - Display the hosts that have completed the compliance scan after the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "<username>:<password>" -d
"action=list&pc_auth_success_date_after=2024-08-26&details=All"
"<qualys_base_url>/api/5.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
```

```
    <datetime>2024-09-16T11:07:45Z</datetime>
    <host_list>
      <host>
        <id>5583053</id>
        <ip>11.111.111.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>nileshcentous7_9</dns>
        <dns_data>
          <hostname>nileshcentous7_9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.9.2009</os>
        <qg_hostid>694b795c-39b2-4e15-b5d1-2015888ecd76</qg_hostid>
        <last_boot>2022-12-08T12:20:16Z</last_boot>
       <serial_number>VMware-42 13 0c f3 66 e0 b6 17-18 37 0c 69 bd 6d b5
2d</serial_number>
        <hardware_uuid>f30c1342-e066-17b6-1837-
0c69bd6db52d</hardware_uuid>
        <first_found_date>2024-06-11T04:52:09Z</first_found_date>
        <last_activity>2024-09-16T10:53:53Z</last_activity>
        <agent_status>PC Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
11T07:13:49Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T07:14:45Z</pc_auth_success_date>
      </host>
      <host>
        <id>5953668</id>
        <ip>11.11.11.111</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
        <os>Windows Microsoft Windows Server 2022 Datacenter 10.0.20348
Build 20348</os>
        <qg_hostid>660e9f09-03a8-0004-0046-0050568cb2b6</qg_hostid>
        <last_boot>2024-07-11T16:13:07Z</last_boot>
       <serial_number>VMware-42 0c 7e 00 c9 37 08 c4-1f 5c b3 f4 8b 19 02
fe</serial_number>
        <hardware_uuid>007E0C42-37C9-C408-1F5C-
B3F48B1902FE</hardware_uuid>
        <first_found_date>2024-08-05T08:40:14Z</first_found_date>
        <last_activity>2024-09-16T05:51:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
16T08:21:17Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T08:24:54Z</pc_auth_success_date>
      </host>
```

```
      <host>
        <id>5964522</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
       <os>Windows Server 2022 Datacenter 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:34Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:16:35Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964524</id>
        <ip>11.11.111.11</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-dc01.veda.local</dns>
        <dns_data>
          <hostname>win-dc01</hostname>
          <domain>veda.local</domain>
          <fqdn>win-dc01.veda.local</fqdn>
        </dns_data>
        <netbios>WIN-DC01</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:59Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:18:01Z</pc_auth_success_date>
      </host>
      <host>
        <id>5985791</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Red Hat Enterprise Linux 9.0</os>
        <qg_hostid>2c4b95d3-51e1-4457-8049-979e80b06527</qg_hostid>
        <first_found_date>2024-08-12T11:17:54Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:42:27Z</pc_auth_success_date>
      </host>
      <host>
        <id>6130324</id>
        <ip>11.11.11.11</ip>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 9.0</os>
        <first_found_date>2024-09-06T10:55:16Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:42:36Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:03:22Z</pc_auth_success_date>
```

```
      </host>
      <host>
        <id>6143865</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <dns>win-cr35vneg5h9</dns>
        <dns_data>
          <hostname>win-cr35vneg5h9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <netbios>WIN-CR35VNEG5H9</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-09-10T04:06:38Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:47:04Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:04:32Z</pc_auth_success_date>
      </host>
      <host>
        <id>6144034</id>
        <ip>11.11.11.11</ip>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>orac23cvm.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>orac23cvm</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>orac23cvm.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 9.0</os>
        <qg_hostid>a2126498-3b97-4d0c-883c-28615acbf0fb</qg_hostid>
        <last_boot>2024-09-13T08:46:06Z</last_boot>
       <serial_number>VMware-42 2e ce a2 1e 23 43 8b-9c d5 82 50 b6 f3 48
9d</serial_number>
        <hardware_uuid>a2ce2e42-231e-8b43-9cd5-
8250b6f3489d</hardware_uuid>
        <first_found_date>2024-09-10T05:31:09Z</first_found_date>
        <last_activity>2024-09-16T10:46:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T15:07:12Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T15:12:17Z</pc_auth_success_date>
      </host>
      <host>
        <id>6149368</id>
        <ip>11.11.11.111</ip>
        <tracking_method>IP</tracking_method>
        <os>Alibaba Cloud Linux 3</os>
        <first_found_date>2024-09-10T21:53:40Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:02:33Z</pc_auth_success_date>
      </host>
      <host>
```

```
            <id>6162135</id>
            <ip>11.11.11.11</ip>
            <tracking_method>Cloud Agent</tracking_method>
            <dns>singlestore_test.comp.rdlab.qualys.com</dns>
            <dns_data>
              <hostname>singlestore_test</hostname>
              <domain>comp.rdlab.qualys.com</domain>
              <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
            </dns_data>
            <os>Oracle Enterprise Linux 8.6</os>
            <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
            <last_boot>2024-09-16T09:16:42Z</last_boot>
           <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
    0a</serial_number>
            <hardware_uuid>034c2e42-e6e3-c1ba-5366-
    da59f960c40a</hardware_uuid>
            <first_found_date>2024-09-13T09:37:09Z</first_found_date>
            <last_activity>2024-09-16T10:47:42Z</last_activity>
            <agent_status>Inventory Scan Complete</agent_status>
            <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
            <last_compliance_scan_datetime>2024-09-
    13T14:16:06Z</last_compliance_scan_datetime>
            <pc_auth_success_date>2024-09-13T14:18:16Z</pc_auth_success_date>
          </host>
        </host_list>
      </response>
</host_list_output>
```

Sample - Display the Activation Key and Activation Title associated with the agent assets

API Request:

```
curl
"<qualys_base_url>/api/5.0/fo/asset/host/?ips=11.111.11.111,11.111.11.111
&action=list&details=All&cloud_agent_activationkey=1" -X POST -b
"QualysSession=ae630e1f345b6503324a93d52b3a69de" -H "Content-Type:
application/x-www-form-urlencoded" -H "X-Requested-With: curl demo2" -H
"Accept: /" -H "Content-Length: 0" --compressed -v
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-12-20T07:41:21Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>5962587</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[centos7-dns-11-111.rdlab.com]]>
                    </DNS>
```

```
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[centos7-hostname-11-111]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[rdlab.com]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[CentOS Linux 7.9.2009]]>
                    </OS>
                    <QG_HOSTID>
                        <![CDATA[b4192ceb-de61-4884-b392-55135e14ce25]]>
                    </QG_HOSTID>
                    <LAST_BOOT>2024-06-07T04:33:55Z</LAST_BOOT>
                    <SERIAL_NUMBER>
                        <![CDATA[VMware-42 2a 6c b2 02 2c 46 38-fb 92 8d
5f 02 44 b4 ac]]>
                    </SERIAL_NUMBER>
                    <HARDWARE_UUID>
                        <![CDATA[b26c2a42-2c02-3846-fb92-8d5f0244b4ac]]>
                    </HARDWARE_UUID>
                    <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                    <LAST_ACTIVITY>2024-08-12T10:20:55Z</LAST_ACTIVITY>
                    <AGENT_STATUS>
                        <![CDATA[Inventory Scan Complete]]>
                    </AGENT_STATUS>
                    <CLOUD_AGENT_RUNNING_ON>
                        <![CDATA[QAGENT]]>
                    </CLOUD_AGENT_RUNNING_ON>
                    <AGENT_ACTIVATION_TITLE>
                        <![CDATA[title_Activation_key]]>
                    </AGENT_ACTIVATION_TITLE>
                    <AGENT_ACTIVATION_KEY>
                        <![CDATA[e5decf50-c20a-4782-8e9e-b6a712261a4d]]>
                    </AGENT_ACTIVATION_KEY>
                    <LAST_VULN_SCAN_DATETIME>2024-08-
13T03:41:08Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_SCANNED_DATE>
                    <LAST_VM_AUTH_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_AUTH_SCANNED_DATE>
                    <LAST_COMPLIANCE_SCAN_DATETIME>2024-08-
12T18:33:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
                </HOST>
                <HOST>
                    <ID>5962589</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
```

```
                    <DNS>
                        <![CDATA[centos7-dns-11-111.rdlab.com]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[centos7-hostname-11-111]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[rdlab.com]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[CentOS Linux 7.9.2009]]>
                    </OS>
                    <QG_HOSTID>
                        <![CDATA[0714edfe-8a72-44d9-98eb-95401672b235]]>
                    </QG_HOSTID>
                    <LAST_BOOT>2024-06-07T04:45:05Z</LAST_BOOT>
                    <SERIAL_NUMBER>
                        <![CDATA[VMware-42 2a 60 7f 5c 9d 67 71-4b 17 71
35 9b 73 28 d4]]>
                    </SERIAL_NUMBER>
                    <HARDWARE_UUID>
                        <![CDATA[7f602a42-9d5c-7167-4b17-71359b7328d4]]>
                    </HARDWARE_UUID>
                    <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                    <LAST_ACTIVITY>2024-09-19T12:05:05Z</LAST_ACTIVITY>
                    <AGENT_STATUS>
                        <![CDATA[Inventory Scan Complete]]>
                    </AGENT_STATUS>
                    <CLOUD_AGENT_RUNNING_ON>
                        <![CDATA[QAGENT]]>
                    </CLOUD_AGENT_RUNNING_ON>
                    <AGENT_ACTIVATION_KEY>
                        <![CDATA[fcce41e6-446e-4818-bf3e-4b3e3860574b]]>
                    </AGENT_ACTIVATION_KEY>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
19T09:54:48Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_SCANNED_DATE>
                    <LAST_VM_AUTH_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_AUTH_SCANNED_DATE>
                    <LAST_COMPLIANCE_SCAN_DATETIME>2024-09-
19T04:25:11Z</LAST_COMPLIANCE_SCAN_DATETIME>
                </HOST>
                <HOST>
                    <ID>6060439</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
```

```
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:32Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:32Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>519</LAST_VM_SCANNED_DURATION>
                </HOST>
                <HOST>
                    <ID>6060639</ID>
                    <IP>11.111.11.111</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:58Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:58Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>544</LAST_VM_SCANNED_DURATION>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_OUTPUT>
```

Sample - Display the VM authentication insufficient privilege status

API Request:

```
curl --location 'https://
<qualys_base_url>/api/5.0/fo/asset/host/?action=list&details=All&truncati
on_limit=0&ids=5811143' \
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/5.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2025-04-21T11:58:09Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>5811143</ID>
                    <IP>10.xx.xx.xx</IP>
```

```
                        <TRACKING_METHOD>DNS</TRACKING_METHOD>
                        <NETWORK_ID>0</NETWORK_ID>
                        <DNS>
                            <![CDATA[w2k3r2-2.vuln.qa.qualys.com]]>
                        </DNS>
                        <DNS_DATA>
                            <HOSTNAME>
                                <![CDATA[w2k3r2-2]]>
                            </HOSTNAME>
                            <DOMAIN>
                                <![CDATA[vuln.qa.qualys.com]]>
                            </DOMAIN>
                            <FQDN>
                                <![CDATA[w2k3r2-2.vuln.qa.qualys.com]]>
                            </FQDN>
                        </DNS_DATA>
                        <OS>
                            <![CDATA[Red Hat Linux 7.3]]>
                        </OS>
                        <FIRST_FOUND_DATE>2024-07-
02T09:52:57Z</FIRST_FOUND_DATE>
                        <LAST_VULN_SCAN_DATETIME>2025-04-
09T05:33:21Z</LAST_VULN_SCAN_DATETIME>
                        <LAST_VM_SCANNED_DATE>2025-04-
09T05:33:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>59</LAST_VM_SCANNED_DURATION>
                        <LAST_VM_AUTH_SCANNED_DATE>2025-04-
09T05:33:21Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>59</LAST_VM_AUTH_SCANNED_DURATION>

<VM_AUTH_INSUFFICIENT_PRIVILEGE>Yes</VM_AUTH_INSUFFICIENT_PRIVILEGE>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_OUTPUT>
```

DTD

<platform API server>/api/5.0/fo/asset/host/dtd/list/output.dtd

V6.0

api/6.0/fo/asset/host/?action=list

[GET] [POST]

Download a list of scanned hosts in the user's account. By default, all scanned hosts in the user account are included and basic information about each host is provided. Hosts in the XML output are sorted by host ID in ascending order.

The output of the Host List API is paginated. By default, a maximum of 1,000 host records are returned per request. You can customize the page size (i.e. the number of host records) by using the parameter "truncation_limit=10000" for instance. In this case the results will be return with pages of 10,000 host records.

The Host List API also shows the TruRisk score for each asset record in the API output and allows users to filter the output based on the TruRisk score .

The TruRisk score is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

TruRisk score has a range from 0 to 1000:

- Severe (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

The API output also displays the updated Asset Criticality Score (ACS), which may differ from the score shown in the Vulnerabilities and Assets tabs, as those scores are only updated after a vulnerability scan.

Permissions - Managers view all scanned hosts in subscription. Auditors view all scanned compliance hosts in subscription. Unit Managers view scanned hosts in user's business unit. Scanners and Readers view scanned hosts in user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR and PC. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

For Unit Managers, Scanners, and Readers to view compliance hosts, the "Manage compliance" permission must be granted in the user's account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)A flag used to make a host list request.
os_hostname={**0**|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.

Parameter	Description
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
details={**Basic**|Basic/AGs | All|All/AGs | None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None. Basic - (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system. Basic/AGs - Show basic host information plus asset group information. Asset group information includes the asset group ID and title. All - Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates. All/AGs - Show all host information plus asset group information. Asset group information includes the asset group ID and title. None - Show only the host ID.

Parameter	Description
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Refer to Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter. For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php PCRE syntax: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php
truncation_limit={value}	(Optional) Specify the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more host records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. See example: Sample - Record Limit Exceeded Warning You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is downloaded.

Parameter	Description
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value. A valid host ID is required.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.

Parameter	Description
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Use this parameter to filter the scanned hosts list to show either: 1) a list of scanned compliance hosts, or 2) a list of scanned vulnerability management hosts. Specify 1 to list scanned compliance hosts in the user's account. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module. A user can specify 0 only when the user has compliance management privileges. For a Unit Manager, Scanner or Reader, the "Manage compliance" permission must be enabled in the user account. If this permission is not enabled and the user makes a request with this parameter set to 0, the request fails with an error (unknown parameter).
cloud_agent_activationkey={0|1}	(Optional) Specify 1, to have two tags AGENT_ACTIVATION_KEY and AGENT_ACTIVATION_TITLE in the response for appropriate assets.
Date Filters	
no_vm_scan_since={date}	(Optional) Show hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - An Auditor cannot specify this parameter.
no_compliance_scan_since ={date}	(Optional) Show compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". Permissions - A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_scan_since={date}	(Optional) Show hosts that were last scanned for vulnerabilities since a certain date and time (optional). Hosts that were the target of a vulnerability scan since the date/time will be shown. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: An Auditor cannot specify this parameter.

Parameter	Description
compliance_scan_since={date}	(Optional) Show hosts that were last scanned for compliance since a certain date and time (optional). Hosts that were the target of a compliance scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Date/time is specified in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT). Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
vm_scan_date_before={date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z". Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.

Parameter	Description
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
pc_auth_success_date_before={date}	(Optional) Show hosts with a successful compliance scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data on or before the specified date, meaning that the specified date itself is included in the search query.
pc_auth_success_date_after={date}	(Optional) Show hosts with a successful compliance scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”. Note: When a date is provided without a specific time, the query includes the data after the specified date, meaning that the specified date is excluded from the search query.
scap_scan_since={date}	(Optional) Show hosts that were last scanned for SCAP since a certain date and time. Hosts that were the target of a SCAP scan since the date/time will be shown. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.
no_scap_scan_since={date}	(Optional) Show hosts not scanned for SCAP since a certain date and time. This parameter is invalid for an Express Lite user. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”.

Parameter	Description
Asset Tags	
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify **1** if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.
Asset Risk Score (ARS)	**Note**: The ARS parameters will be retained for the next few releases. However, there will be a future update where these parameters will be removed with advance notification. You must start using the new TruRisk parameters mentioned below.
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.

Parameter	Description
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.
TruRisk Score	
show_trurisk={0|1}	(Optional) Specify 1 to show the TruRisk value in the output. Specify 0 if you do not want to show the TruRisk value.
trurisk_min={value}	(Optional) Show only asset records with a TruRisk value greater than or equal to the TruRisk min value specified. trurisk_min can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
trurisk_max={value}	(Optional) Show only detection records with an TruRisk value less than or equal to the TruRisk max value specified. trurisk_max can only be specified when show_trurisk=1. When trurisk_min and trurisk_max are specified in the same request, the trurisk_min value must be less than the trurisk_max value.
show_trurisk_factors={0|1}	(Optional) Specify 1 to show TruRisk contributing factors associated with each asset record in the output. Specify 0 if you do not want to show TruRisk contributing factors.
EC2/Azure/GCP metadata	
host_metadata={value}	(Optional) Specify “all” to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.

Parameter	Description
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Note: If a host has a missing or null value for Information Gathered (IG) processed date or vulnerability processed date, it will be excluded when using the vm_processed_before parameter in the Host List API. To include these hosts in the results, use the vm_scan_date_before parameter.

Sample - Regular expression strings for matching OS names

API request:

```
curl --location --request POST
'https://<qualys_base_url>/api/6.0/fo/asset/host/?action=list&compliance_
enabled=1&os_pattern=%5EWindows.*2%24&cloud_agent_activationkey=0' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-Requested-With: curl demo2' \
--header 'Accept: */*' \
--header 'Content-Length: 0' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-01-09T07:34:37Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>66942</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[2k3sp2-25-12]]>
                    </HOSTNAME>
```

```
                    <DOMAIN>
                        <![CDATA[2k3.patch.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[2k3sp2-25-
12.2k3.patch.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[2K3SP2-25-12]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2016-11-15T07:39:22Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>66950</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[pci-2k3sp2-25-9]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[pci-2k3sp2-25-9]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[PCI-2K3SP2-25-9]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141141</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[com-sql-24-68.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[com-sql-24-68]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
```

```
                    <FQDN>
                        <![CDATA[com-sql-24-
68.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[COM-SQL-24-68]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2018-01-26T23:48:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141142</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[win2k3r2-64bit.lab.ad.vuln.qa.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[win2k3r2-64bit]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[lab.ad.vuln.qa.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[win2k3r2-
64bit.lab.ad.vuln.qa.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[WIN2K3R2-64BIT]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 R2 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:10:49Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141146</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[vstasp2u-26-106]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[vstasp2u-26-106]]>
                    </HOSTNAME>
                    <DOMAIN />
```

```
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[VSTASP2U-26-106]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows Vista Enterprise Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:11:25Z</FIRST_FOUND_DATE>
            </HOST>
            <HOST>
                <ID>141159</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[was-2k3-30-58]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[was-2k3-30-58]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[WAS-2K3-30-58]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows 2003 Service Pack 2]]>
                </OS>
                <FIRST_FOUND_DATE>2017-11-07T09:13:35Z</FIRST_FOUND_DATE>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List assets

API request:

```
curl --location --request GET
'<qualys_base_url>/api/6.0/fo/asset/host/?action=list&show_asset_id=1&hos
t_metadata=all&details=All
--header 'X-Requested-With: curl'
--header 'Authorization: <token>'
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-17T07:16:54Z</datetime>
    <host_list>
      <host>
```

```
        <id>1295154</id>
        <asset_id>5856721</asset_id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <os>JUNOS 15.1R6-S2.1</os>
        <first_found_date>2020-08-18T07:08:12Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
      <host>
        <id>1295155</id>
        <asset_id>5856524</asset_id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <netbios>COM-XP-64-32-93</netbios>
        <first_found_date>2020-08-18T07:08:14Z</first_found_date>
        <last_compliance_scan_datetime>2020-08-
18T07:04:32Z</last_compliance_scan_datetime>
      </host>
....
      <host>
        <id>6162135</id>
        <asset_id>47773653</asset_id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:35Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-17T07:15:35Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
17T06:46:48Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-17T06:48:56Z</pc_auth_success_date>
      </host>
      <host>
        <id>6171463</id>
        <asset_id>47817089</asset_id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 8.6</os>
        <first_found_date>2024-09-16T17:55:07Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
```

```
16T17:30:19Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T17:55:08Z</pc_auth_success_date>
      </host>
    </host_list>
    <glossary>
      <user_list>
        <user>
          <user_login>username</user_login>
          <first_name>xxxx</first_name>
          <last_name>yyyy</last_name>
        </user>
      </user_list>
    </glossary>
  </response>
</host_list_output>
```

Sample - List assets based on scan end date, scan processed date

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"<qualys_base_url>/api/6.0/fo/asset/host/?action=list&truncation_limit=10
&details=All
/AGs&vm_scan_date_before=2017-09-
14T06:32:15Z&vm_auth_scan_date_before=2017-09-
14T06:32:15Z&vm_scan_date_after=2016-05-
12T06:32:15Z&vm_auth_scan_date_after=2016-05-
12T06:32:15Z&vm_processed_before=2017-09&scap_scan_since=2018-08-29
-14T06:33:24Z&vm_processed_after=2016-09-12T06:33:24Z"-12T06:33:24Z"
```

Sample - List assets with specific TruRisk score

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/?action=list&ips=10.115.126.190&
show_trurisk=1&trurisk_min=1&trurisk_max=1000&show_trurisk_factors=1'
--header 'X-Requested-With: curl demo2'
--header 'Authorization: Basic <token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-06-21T06:46:04Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1800139</ID>
        <IP>xx.xx.xx.xxx</IP>
        <ASSET_RISK_SCORE>680</ASSET_RISK_SCORE>
        <TRURISK_SCORE>680</TRURISK_SCORE>
        <ASSET_CRITICALITY_SCORE>4</ASSET_CRITICALITY_SCORE>
        <TRURISK_SCORE_FACTORS>
          <TRURISK_SCORE_FORMULA>4 *
{(1.0*95*(14^0.01))+(0.6*74*(31^0.01))+(0.4*47*(73^0.01))+(0.2*33*(66^0.0
1))}</TRURISK_SCORE_FORMULA>
```

```
            <VULN_COUNT qds_severity="1">0</VULN_COUNT>
            <VULN_COUNT qds_severity="2">66</VULN_COUNT>
            <VULN_COUNT qds_severity="3">73</VULN_COUNT>
            <VULN_COUNT qds_severity="4">31</VULN_COUNT>
            <VULN_COUNT qds_severity="5">14</VULN_COUNT>
          </TRURISK_SCORE_FACTORS>
          <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
          <NETWORK_ID>0</NETWORK_ID>
          <DNS><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></DNS>
          <DNS_DATA>
            <HOSTNAME><![CDATA[ca1]]></HOSTNAME>
            <DOMAIN><![CDATA[rdlab.in03.qualys.com.abc123]]></DOMAIN>
            <FQDN><![CDATA[ca1.rdlab.in03.qualys.com.abc123]]></FQDN>
          </DNS_DATA>
          <NETBIOS><![CDATA[SYS_10_115_126_190]]></NETBIOS>
          <OS><![CDATA[CentOS Linux 7.5.1804]]></OS>
          <QG_HOSTID><![CDATA[6fc281d4-40e2-4145-bcaa-
753f3f0d57d7]]></QG_HOSTID>
          <LAST_BOOT>2022-05-27T18:18:43Z</LAST_BOOT>
         <SERIAL_NUMBER><![CDATA[VMware-56 4d 99 7a 19 f5 a6 94-b5 f0 07 68
7c 9a e5 b5]]></SERIAL_NUMBER>
          <HARDWARE_UUID><![CDATA[564D997A-19F5-A694-B5F0-
07687C9AE5B5]]></HARDWARE_UUID>
          <FIRST_FOUND_DATE>2021-07-28T08:37:55Z</FIRST_FOUND_DATE>
          <LAST_ACTIVITY>2023-06-21T06:15:43Z</LAST_ACTIVITY>
          <AGENT_STATUS><![CDATA[Inventory Scan Complete]]></AGENT_STATUS>

<CLOUD_AGENT_RUNNING_ON><![CDATA[QAGENT]]></CLOUD_AGENT_RUNNING_ON>
        </HOST>
        ...
      </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List scanned assets with certain EC2 metadata

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,ac
countId,instanceId"
"<qualys_base_url>/api/6.0/fo/asset/host/"
```

XML output:

```
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/host_list_output.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-15T09:50:46Z</DATETIME>
    <HOST_LIST>
       <HOST>
       <ID>135151</ID>
       <IP>xx.xx.xx.xxx</IP>
       <TRACKING_METHOD>EC2</TRACKING_METHOD>
       <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>
       <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>
```

```
        <OS><![CDATA[Amazon Linux 2016.09]]></OS>
        <METADATA>
          <EC2>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/region]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[us-east-1]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
               identity/document/accountId]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[205767712438]]></VALUE>
              <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
          </EC2>
        </METADATA>
        <LAST_VULN_SCAN_DATETIME>2017-03-
         21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
        <LAST_VM_AUTH_SCANNED_DATE>2017-03-
         21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
        <LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
        <LAST_COMPLIANCE_SCAN_DATETIME>2017-03-
         21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - Record Limit Exceeded Warning

In this case 1,000 host records are included in the XML output and the Warning message (shown below) indicates the URL you need to use to request the next 1,000 host records.

```
<RESPONSE>
    ...
        <WARNING>
            <CODE>1980</CODE>
            <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>
            <URL>

<![CDATA[<qualys_base_url>/api/4.0/fo/asset/host/?action=list&details=Non
e&truncation_limit=100&cloud_agent_activationkey=0&id_min=145359]]>
            </URL>
        </WARNING>
    </RESPONSE>
```

```
...
```

Sample - Display the hosts that have completed the compliance scan before the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:yyyy123#" -d
"action=list&pc_auth_success_date_before=2022-06-06&details=All"
"<qualys_base_url>/api/6.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T10:58:10Z</datetime>
    <host_list>
      <host>
        <id>2584392</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>compaix6lpr01</dns>
        <dns_data>
          <hostname>compaix6lpr01</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>AIX 6.1.0.0</os>
        <qg_hostid>2f06cf12-c127-4cfa-93c1-2fe3b9a1cdec</qg_hostid>
        <last_boot>2022-04-01T18:03:47Z</last_boot>
        <first_found_date>2022-04-27T09:51:52Z</first_found_date>
        <last_activity>2022-05-11T05:36:34Z</last_activity>
        <agent_status>Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
11T06:52:31Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-11T06:39:13Z</pc_auth_success_date>
      </host>
      <host>
        <id>2588281</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>tomcat10.rdlab.in03.qualys.com</dns>
        <dns_data>
          <hostname>tomcat10</hostname>
          <domain>rdlab.in03.qualys.com</domain>
          <fqdn>tomcat10.rdlab.in03.qualys.com</fqdn>
        </dns_data>
        <os>CentOS Linux 7.5.1804 (Core) 7.5.1804</os>
        <qg_hostid>4400c88b-95ba-435d-94f2-8dfc1a1ebe38</qg_hostid>
        <last_boot>2022-01-14T05:41:41Z</last_boot>
        <hardware_uuid>422af3eb-59b3-d7c4-aa71-
dd20780e4c0a</hardware_uuid>
        <first_found_date>2022-04-29T07:16:12Z</first_found_date>
        <last_activity>2022-05-17T09:08:13Z</last_activity>
```

```
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
17T00:12:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-17T00:15:23Z</pc_auth_success_date>
      </host>
      <host>
        <id>2612147</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>comwls14c</dns>
        <dns_data>
          <hostname>comwls14c</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.8.2003 (Core) 7.8.2003</os>
        <qg_hostid>6020ae3c-cefa-4540-8690-aa9c23cdfd2d</qg_hostid>
        <last_boot>2021-06-15T06:52:48Z</last_boot>
        <hardware_uuid>420cf117-1fcb-0325-1d67-
def7b2161823</hardware_uuid>
        <first_found_date>2022-05-05T11:48:45Z</first_found_date>
        <last_activity>2022-05-09T04:49:16Z</last_activity>
        <agent_status>Configuration Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2022-05-
09T00:19:37Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2022-05-09T00:38:21Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

Sample - Display the hosts that have completed the compliance scan after the given date.

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "<username>:<password>" -d
"action=list&pc_auth_success_date_after=2024-08-26&details=All"
"<qualys_base_url>/api/6.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
<host_list_output>
  <response>
    <datetime>2024-09-16T11:07:45Z</datetime>
    <host_list>
      <host>
        <id>5583053</id>
        <IP>xx.xx.xx.xxx</IP> >
        <tracking_method>Cloud Agent</tracking_method>
        <dns>nileshcentous7_9</dns>
        <dns_data>
```

```
          <hostname>nileshcentous7_9</hostname>
          <domain/>
          <fqdn/>
        </dns_data>
        <os>CentOS Linux 7.9.2009</os>
        <qg_hostid>694b795c-39b2-4e15-b5d1-2015888ecd76</qg_hostid>
        <last_boot>2022-12-08T12:20:16Z</last_boot>
       <serial_number>VMware-42 13 0c f3 66 e0 b6 17-18 37 0c 69 bd 6d b5
2d</serial_number>
        <hardware_uuid>f30c1342-e066-17b6-1837-
0c69bd6db52d</hardware_uuid>
        <first_found_date>2024-06-11T04:52:09Z</first_found_date>
        <last_activity>2024-09-16T10:53:53Z</last_activity>
        <agent_status>PC Manifest Downloaded</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
11T07:13:49Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T07:14:45Z</pc_auth_success_date>
      </host>
      <host>
        <id>5953668</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
        <os>Windows Microsoft Windows Server 2022 Datacenter 10.0.20348
Build 20348</os>
        <qg_hostid>660e9f09-03a8-0004-0046-0050568cb2b6</qg_hostid>
        <last_boot>2024-07-11T16:13:07Z</last_boot>
       <serial_number>VMware-42 0c 7e 00 c9 37 08 c4-1f 5c b3 f4 8b 19 02
fe</serial_number>
        <hardware_uuid>007E0C42-37C9-C408-1F5C-
B3F48B1902FE</hardware_uuid>
        <first_found_date>2024-08-05T08:40:14Z</first_found_date>
        <last_activity>2024-09-16T05:51:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
16T08:21:17Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-16T08:24:54Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964522</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <dns>pcw2022.com.local</dns>
        <dns_data>
          <hostname>pcw2022</hostname>
          <domain>com.local</domain>
```

```
          <fqdn>pcw2022.com.local</fqdn>
        </dns_data>
        <netbios>PCW2022</netbios>
       <os>Windows Server 2022 Datacenter 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:34Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:16:35Z</pc_auth_success_date>
      </host>
      <host>
        <id>5964524</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <dns>win-dc01.veda.local</dns>
        <dns_data>
          <hostname>win-dc01</hostname>
          <domain>veda.local</domain>
          <fqdn>win-dc01.veda.local</fqdn>
        </dns_data>
        <netbios>WIN-DC01</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-08-08T12:02:59Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
09T06:31:57Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-09T07:18:01Z</pc_auth_success_date>
      </host>
      <host>
        <id>5985791</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <os>Red Hat Enterprise Linux 9.0</os>
        <qg_hostid>2c4b95d3-51e1-4457-8049-979e80b06527</qg_hostid>
        <first_found_date>2024-08-12T11:17:54Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:42:27Z</pc_auth_success_date>
      </host>
      <host>
        <id>6130324</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <os>Oracle Enterprise Linux 9.0</os>
        <first_found_date>2024-09-06T10:55:16Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:42:36Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:03:22Z</pc_auth_success_date>
      </host>
      <host>
        <id>6143865</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <dns>win-cr35vneg5h9</dns>
        <dns_data>
          <hostname>win-cr35vneg5h9</hostname>
```

```
          <domain/>
          <fqdn/>
        </dns_data>
        <netbios>WIN-CR35VNEG5H9</netbios>
        <os>Windows Server 2022 Standard 64 bit Edition Version 21H2</os>
        <first_found_date>2024-09-10T04:06:38Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
11T09:47:04Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-11T12:04:32Z</pc_auth_success_date>
      </host>
      <host>
        <id>6144034</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>orac23cvm.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>orac23cvm</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>orac23cvm.comp.rdlab.qualys.com</fqdn>
        </dns_data>
        <os>Oracle Enterprise Linux 9.0</os>
        <qg_hostid>a2126498-3b97-4d0c-883c-28615acbf0fb</qg_hostid>
        <last_boot>2024-09-13T08:46:06Z</last_boot>
       <serial_number>VMware-42 2e ce a2 1e 23 43 8b-9c d5 82 50 b6 f3 48
9d</serial_number>
        <hardware_uuid>a2ce2e42-231e-8b43-9cd5-
8250b6f3489d</hardware_uuid>
        <first_found_date>2024-09-10T05:31:09Z</first_found_date>
        <last_activity>2024-09-16T10:46:06Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T15:07:12Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T15:12:17Z</pc_auth_success_date>
      </host>
      <host>
        <id>6149368</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>IP</tracking_method>
        <os>Alibaba Cloud Linux 3</os>
        <first_found_date>2024-09-10T21:53:40Z</first_found_date>
        <last_compliance_scan_datetime>2024-09-
12T06:41:52Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-12T07:02:33Z</pc_auth_success_date>
      </host>
      <host>
        <id>6162135</id>
        <IP>xx.xx.xx.xxx</IP>
        <tracking_method>Cloud Agent</tracking_method>
        <dns>singlestore_test.comp.rdlab.qualys.com</dns>
        <dns_data>
          <hostname>singlestore_test</hostname>
          <domain>comp.rdlab.qualys.com</domain>
          <fqdn>singlestore_test.comp.rdlab.qualys.com</fqdn>
```

```
        </dns_data>
        <os>Oracle Enterprise Linux 8.6</os>
        <qg_hostid>24a561a4-5746-4bcb-8229-009a3d4034f2</qg_hostid>
        <last_boot>2024-09-16T09:16:42Z</last_boot>
       <serial_number>VMware-42 2e 4c 03 e3 e6 ba c1-53 66 da 59 f9 60 c4
0a</serial_number>
        <hardware_uuid>034c2e42-e6e3-c1ba-5366-
da59f960c40a</hardware_uuid>
        <first_found_date>2024-09-13T09:37:09Z</first_found_date>
        <last_activity>2024-09-16T10:47:42Z</last_activity>
        <agent_status>Inventory Scan Complete</agent_status>
        <cloud_agent_running_on>QAGENT</cloud_agent_running_on>
        <last_compliance_scan_datetime>2024-09-
13T14:16:06Z</last_compliance_scan_datetime>
        <pc_auth_success_date>2024-09-13T14:18:16Z</pc_auth_success_date>
      </host>
    </host_list>
  </response>
</host_list_output>
```

Sample - Display the Activation Key and Activation Title associated with the agent assets

API Request:

```
curl
"<qualys_base_url>/api/6.0/fo/asset/host/?ips=11.111.11.111,11.111.11.111
&action=list&details=All&cloud_agent_activationkey=1" -X POST -b
"QualysSession=ae630e1f345b6503324a93d52b3a69de" -H "Content-Type:
application/x-www-form-urlencoded" -H "X-Requested-With: curl demo2" -H
"Accept: /" -H "Content-Length: 0" --compressed -v
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-12-20T07:41:21Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>5962587</ID>
                    <IP>xx.xx.xx.xxx</IP>
                    <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[centos7-dns-11-111.rdlab.com]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[centos7-hostname-11-111]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[rdlab.com]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
```

```
                    </FQDN>
                </DNS_DATA>
                <OS>
                    <![CDATA[CentOS Linux 7.9.2009]]>
                </OS>
                <QG_HOSTID>
                    <![CDATA[b4192ceb-de61-4884-b392-55135e14ce25]]>
                </QG_HOSTID>
                <LAST_BOOT>2024-06-07T04:33:55Z</LAST_BOOT>
                <SERIAL_NUMBER>
                    <![CDATA[VMware-42 2a 6c b2 02 2c 46 38-fb 92 8d
5f 02 44 b4 ac]]>
                </SERIAL_NUMBER>
                <HARDWARE_UUID>
                    <![CDATA[b26c2a42-2c02-3846-fb92-8d5f0244b4ac]]>
                </HARDWARE_UUID>
                <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                <LAST_ACTIVITY>2024-08-12T10:20:55Z</LAST_ACTIVITY>
                <AGENT_STATUS>
                    <![CDATA[Inventory Scan Complete]]>
                </AGENT_STATUS>
                <CLOUD_AGENT_RUNNING_ON>
                    <![CDATA[QAGENT]]>
                </CLOUD_AGENT_RUNNING_ON>
                <AGENT_ACTIVATION_TITLE>
                    <![CDATA[title_Activation_key]]>
                </AGENT_ACTIVATION_TITLE>
                <AGENT_ACTIVATION_KEY>
                    <![CDATA[e5decf50-c20a-4782-8e9e-b6a712261a4d]]>
                </AGENT_ACTIVATION_KEY>
                <LAST_VULN_SCAN_DATETIME>2024-08-
13T03:41:08Z</LAST_VULN_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_AUTH_SCANNED_DATE>2024-08-
13T03:41:08Z</LAST_VM_AUTH_SCANNED_DATE>
                <LAST_COMPLIANCE_SCAN_DATETIME>2024-08-
12T18:33:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
            </HOST>
            <HOST>
                <ID>5962589</ID>
                <IP>xx.xx.xx.xxx</IP>
                <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[centos7-dns-11-111.rdlab.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[centos7-hostname-11-111]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[rdlab.com]]>
```

```
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[centos7-fqdn-11-111.rdlab.com]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[CentOS Linux 7.9.2009]]>
                    </OS>
                    <QG_HOSTID>
                        <![CDATA[0714edfe-8a72-44d9-98eb-95401672b235]]>
                    </QG_HOSTID>
                    <LAST_BOOT>2024-06-07T04:45:05Z</LAST_BOOT>
                    <SERIAL_NUMBER>
                        <![CDATA[VMware-42 2a 60 7f 5c 9d 67 71-4b 17 71
35 9b 73 28 d4]]>
                    </SERIAL_NUMBER>
                    <HARDWARE_UUID>
                        <![CDATA[7f602a42-9d5c-7167-4b17-71359b7328d4]]>
                    </HARDWARE_UUID>
                    <FIRST_FOUND_DATE>2024-08-
07T07:32:25Z</FIRST_FOUND_DATE>
                    <LAST_ACTIVITY>2024-09-19T12:05:05Z</LAST_ACTIVITY>
                    <AGENT_STATUS>
                        <![CDATA[Inventory Scan Complete]]>
                    </AGENT_STATUS>
                    <CLOUD_AGENT_RUNNING_ON>
                        <![CDATA[QAGENT]]>
                    </CLOUD_AGENT_RUNNING_ON>
                    <AGENT_ACTIVATION_KEY>
                        <![CDATA[fcce41e6-446e-4818-bf3e-4b3e3860574b]]>
                    </AGENT_ACTIVATION_KEY>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
19T09:54:48Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_SCANNED_DATE>
                    <LAST_VM_AUTH_SCANNED_DATE>2024-09-
19T09:54:48Z</LAST_VM_AUTH_SCANNED_DATE>
                    <LAST_COMPLIANCE_SCAN_DATETIME>2024-09-
19T04:25:11Z</LAST_COMPLIANCE_SCAN_DATETIME>
                </HOST>
                <HOST>
                    <ID>6060439</ID>
                    <IP>xx.xx.xx.xxx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:32Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:32Z</LAST_VM_SCANNED_DATE>
```

```
<LAST_VM_SCANNED_DURATION>519</LAST_VM_SCANNED_DURATION>
                </HOST>
                <HOST>
                    <ID>6060639</ID>
                    <IP>xx.xx.xx.xxx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>6008</NETWORK_ID>
                    <OS>
                       <![CDATA[EulerOS / SuSE Linux / Scientific Linux]]>
                    </OS>
                    <FIRST_FOUND_DATE>2024-08-
22T18:10:07Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2024-09-
01T18:03:58Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-09-
01T18:03:58Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>544</LAST_VM_SCANNED_DURATION>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_OUTPUT>
```

Sample - Display the VM authentication insufficient privilege status

API Request:

```
curl --location 'https://
<qualys_base_url>/api/6.0/fo/asset/host/?action=list&details=All&truncati
on_limit=0&ids=5811143' \
--header 'X-Requested-With: curl demo 2' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2025-04-21T11:58:09Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>5811143</ID>
                    <IP>xx.xx.xx.xxx</IP>
                    <TRACKING_METHOD>DNS</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[w2k3r2-2.vuln.qa.qualys.com]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[w2k3r2-2]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[vuln.qa.qualys.com]]>
```

```
                            </DOMAIN>
                            <FQDN>
                                <![CDATA[w2k3r2-2.vuln.qa.qualys.com]]>
                            </FQDN>
                        </DNS_DATA>
                        <OS>
                            <![CDATA[Red Hat Linux 7.3]]>
                        </OS>
                        <FIRST_FOUND_DATE>2024-07-
02T09:52:57Z</FIRST_FOUND_DATE>
                        <LAST_VULN_SCAN_DATETIME>2025-04-
09T05:33:21Z</LAST_VULN_SCAN_DATETIME>
                        <LAST_VM_SCANNED_DATE>2025-04-
09T05:33:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>59</LAST_VM_SCANNED_DURATION>
                        <LAST_VM_AUTH_SCANNED_DATE>2025-04-
09T05:33:21Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>59</LAST_VM_AUTH_SCANNED_DURATION>

<VM_AUTH_INSUFFICIENT_PRIVILEGE>Yes</VM_AUTH_INSUFFICIENT_PRIVILEGE>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_OUTPUT>


Sample - Display the list of all the hosts for OCI tracked assets
API Request:
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/?action=list&host_metadata=oci&d
etails=All' \
--header 'X-Requested-With: curl' \
--header 'Authorization: <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "
<qualys_base_url>/api/6.0/fo/asset/host/dtd/list/output.dtd">
    <HOST_LIST_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-07-31T12:38:15Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>17663907</ID>
                    <IP>xx.xxx.xx.xxx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <DNS>
                        <![CDATA[10-115-67-236.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
```

```
                        <HOSTNAME>
                            <![CDATA[10-115-67-236]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[10-115-67-236.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <OS>
                        <![CDATA[Red Hat Linux Advanced Server 2.1AS]]>
                    </OS>
                    <FIRST_FOUND_DATE>2026-01-
07T12:29:09Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2026-01-
08T10:14:13Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-01-
08T10:14:13Z</LAST_VM_SCANNED_DATE>
                   <LAST_VM_SCANNED_DURATION>19</LAST_VM_SCANNED_DURATION>
                    <LAST_VM_AUTH_SCANNED_DATE>2026-01-
08T10:14:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>19</LAST_VM_AUTH_SCANNED_DURATION>
                </HOST>
                <HOST>
                    <ID>17664739</ID>
                    <IP>xx.xx.xx.xx</IP>
                    <TRACKING_METHOD>Azure VM</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CLOUD_PROVIDER>
                        <![CDATA[Azure]]>
                    </CLOUD_PROVIDER>
                    <CLOUD_SERVICE>
                        <![CDATA[VM]]>
                    </CLOUD_SERVICE>
                    <CLOUD_RESOURCE_ID>
                        <![CDATA[8cc39bd5-42ef-4cfc-a671-446228bdcd56]]>
                    </CLOUD_RESOURCE_ID>
                   <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                    <EC2_INSTANCE_ID>
                        <![CDATA[8cc39bd5-42ef-4cfc-a671-446228bdcd56]]>
                    </EC2_INSTANCE_ID>
                    <FIRST_FOUND_DATE>2026-01-
07T18:10:02Z</FIRST_FOUND_DATE>
                </HOST>
                <HOST>
                    <ID>19524551</ID>
                    <IP>xx.xxx.xx.xx</IP>
                    <TRACKING_METHOD>EC2</TRACKING_METHOD>
                    <NETWORK_ID>6703806</NETWORK_ID>
                    <DNS>
                        <![CDATA[ip-172-16-2-88.eu-west-
```

```
1.compute.internal]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[ip-172-16-2-88]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[eu-west-1.compute.internal]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[ip-172-16-2-88.eu-west-
1.compute.internal]]>
                        </FQDN>
                    </DNS_DATA>
                    <CLOUD_PROVIDER>
                        <![CDATA[AWS]]>
                    </CLOUD_PROVIDER>
                    <CLOUD_SERVICE>
                        <![CDATA[EC2]]>
                    </CLOUD_SERVICE>
                    <CLOUD_RESOURCE_ID>
                        <![CDATA[i-0cd4ef5a6b7890123]]>
                    </CLOUD_RESOURCE_ID>
                   <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                    <EC2_INSTANCE_ID>
                        <![CDATA[i-0cd4ef5a6b7890123]]>
                    </EC2_INSTANCE_ID>
                    <QG_HOSTID>
                        <![CDATA[d4e5f6a7-b8c9-4d0e-af12-345678901bcd]]>
                    </QG_HOSTID>
                    <FIRST_FOUND_DATE>2026-05-
18T05:42:19Z</FIRST_FOUND_DATE>
                    <METADATA>
                        <EC2>
                            <ATTRIBUTE>
                                <NAME>
                                  <![CDATA[latest/meta-data/instance-id]]>
                                </NAME>
                                <LAST_STATUS>Success</LAST_STATUS>
                                <VALUE>
                                    <![CDATA[i-0cd4ef5a6b7890123]]>
                                </VALUE>
                                <LAST_SUCCESS_DATE></LAST_SUCCESS_DATE>
                                <LAST_ERROR_DATE></LAST_ERROR_DATE>
                                <LAST_ERROR>
                                    <![CDATA[]]>
                                </LAST_ERROR>
                            </ATTRIBUTE>
                            <ATTRIBUTE>
                                <NAME>
                                    <![CDATA[latest/dynamic/instance-
identity/document/instanceId]]>
                                </NAME>
```

```
                                <LAST_STATUS>Success</LAST_STATUS>
                                <VALUE>
                                    <![CDATA[i-0cd4ef5a6b7890123]]>
                                </VALUE>
                                <LAST_SUCCESS_DATE></LAST_SUCCESS_DATE>
                                <LAST_ERROR_DATE></LAST_ERROR_DATE>
                                <LAST_ERROR>
                                    <![CDATA[]]>
                                </LAST_ERROR>
                            </ATTRIBUTE>
                        </EC2>
                    </METADATA>
                </HOST>
                <HOST>
                    <ID>19942296</ID>
                    <IP>xxx.xxx.xx.xxx</IP>
                   <TRACKING_METHOD>OCI Compute Instance</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CLOUD_PROVIDER>
                        <![CDATA[OCI]]>
                    </CLOUD_PROVIDER>
                    <CLOUD_SERVICE>
                        <![CDATA[Compute Instance]]>
                    </CLOUD_SERVICE>
                    <CLOUD_RESOURCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-singapore-
1.anzwsljrchxdvzyczua6ezrzmejjopkd5zur7ssodz6mw3xc6eiv56lafyla]]>
                    </CLOUD_RESOURCE_ID>
                   <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                    <EC2_INSTANCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-singapore-
1.anzwsljrchxdvzyczua6ezrzmejjopkd5zur7ssodz6mw3xc6eiv56lafyla]]>
                    </EC2_INSTANCE_ID>
                    <FIRST_FOUND_DATE>2026-06-
23T06:15:28Z</FIRST_FOUND_DATE>
                    <LAST_VULN_SCAN_DATETIME>2026-07-
29T08:12:24Z</LAST_VULN_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-07-
29T08:12:24Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>1456</LAST_VM_SCANNED_DURATION>
                </HOST>
                <HOST>
                    <ID>19951433</ID>
                    <IP>10.0.0.130</IP>
                   <TRACKING_METHOD>OCI Compute Instance</TRACKING_METHOD>
                    <NETWORK_ID>6804810</NETWORK_ID>
                    <CLOUD_PROVIDER>
                        <![CDATA[OCI]]>
                    </CLOUD_PROVIDER>
                    <CLOUD_SERVICE>
                        <![CDATA[Compute Instance]]>
                    </CLOUD_SERVICE>
```

```
                    <CLOUD_RESOURCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-osaka-
1.anvwsljrchxdvzycgden4wbitnq6dtk6bzn7exkoyfd3kxouuajdjckil7ua]]>
                    </CLOUD_RESOURCE_ID>
                   <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                    <EC2_INSTANCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-osaka-
1.anvwsljrchxdvzycgden4wbitnq6dtk6bzn7exkoyfd3kxouuajdjckil7ua]]>
                    </EC2_INSTANCE_ID>
                    <FIRST_FOUND_DATE>2026-06-
23T11:47:18Z</FIRST_FOUND_DATE>
                </HOST>
.......
                <HOST>
                    <ID>19951434</ID>
                    <IP>xx.x.x.xxx</IP>
                   <TRACKING_METHOD>OCI Compute Instance</TRACKING_METHOD>
                    <NETWORK_ID>6804810</NETWORK_ID>
                    <CLOUD_PROVIDER>
                        <![CDATA[OCI]]>
                    </CLOUD_PROVIDER>
                    <CLOUD_SERVICE>
                        <![CDATA[Compute Instance]]>
                    </CLOUD_SERVICE>
                    <CLOUD_RESOURCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-osaka-
1.anvwsljrchxdvzychw56fjwbrrbgzgwrh7yqf4kh3xhz2dnwy6zfvrz66r3q]]>
                    </CLOUD_RESOURCE_ID>
                   <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                    <EC2_INSTANCE_ID>
                        <![CDATA[ocid1.instance.oc1.ap-osaka-
1.anvwsljrchxdvzychw56fjwbrrbgzgwrh7yqf4kh3xhz2dnwy6zfvrz66r3q]]>
                    </EC2_INSTANCE_ID>
                    <FIRST_FOUND_DATE>2026-06-
23T11:47:18Z</FIRST_FOUND_DATE>
                </HOST>
                <!-- keep-alive for HOST_LIST_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_OUTPUT  -->
            </HOST_LIST>
            <WARNING>
                <CODE>1980</CODE>
              <TEXT>1000 record limit exceeded. Use URL to get next batch
of results.</TEXT>
                <URL>

<![CDATA[https://qualysapi.p04.eng.sjc01.qualys.com/api/6.0/fo/asset/host
/?action=list&host_metadata=oci&details=All&id_min=19951633]]>
                </URL>
            </WARNING>
```

```
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

DTD

<platform API server>/api/6.0/fo/asset/host/dtd/list/output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/6.0/fo/asset/host/?action=list	Active	Active
/api/5.0/fo/asset/host/?action=list	February 2027	August 2027
/api/4.0/fo/asset/host/?action=list	December 2025	December 2026
/api/3.0/fo/asset/host/?action=list	December 2025	December 2026
/api/2.0/fo/asset/host/?action=list	December 2025	December 2026

Host Update

/api/2.0/fo/asset/host/?action=update

[POST]

Here you can filter host assets based on input parameters and then you can update host attributes using new update parameters (new_tracking_method, new_owner, new_ud1, new_ud2, new_ud3, and new_comment).

Good to Know

- With host update API, you can update host attributes like tracking method (IP, DNS, NETBIOS), owner, user defined fields (ud1, ud2, ud3), and comments.

- You cannot update an IP to use tracking method EC2 or AGENT. Also, if an IP is already tracked by EC2 or AGENT, you cannot change the tracking method to something else. We will skip the tracking method update in these cases.

Identify the hosts you want to update

As part of the update request you'll need to tell us which hosts you want to update. You can do this in a number of ways. You can simply specify the host IDs, or you can specify IP addresses, asset group IDs or asset group titles. When specifying IP addresses or asset groups, there are additional optional input parameters available.

Specify hosts using one of these combinations of input parameters:

- ids (required) only

- ips (required) with any of these optional parameters: host_dns, host_netbios, network_id, network_name, tracking_method

- ag_ids (required) with or without tracking_method

- ag_titles (required) with or without tracking_method

These input parameters are described in more detail below.

Identify the changes you want to make

Use new input parameters to tell us the host attributes you want to change. New input parameters include new_tracking_method, new_owner, new_ud1, new_ud2, new_ud3, and new_comment. The new values you specify will overwrite the existing values, and your changes will apply to all hosts included in the API request.

Input Parameters

Use these input parameters when updating hosts:

Parameter	Description
General	
action=update	(Required)
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.

Host Filters	
ids={value}	Show only certain host IDs. One or more host IDs may be specified. Multiple entries are comma separated. Valid host IDs are required. **Note**: The 'ids' input parameter does not accept host ranges. You can enter either a single host ID or a comma-separated list of host IDs for the parameter.
ips={value} -or- {POSTed CSV raw data}	The hosts within the subscription you want to update. IPs must be specified by using the "ips" parameter (using the POST method) or by uploading CSV raw data (using the POST method). To upload CSV raw data, specify --data-binary <data>. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.30.1-10.10.30.50). CIDR notation is supported.
network_id={value}	(Valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network by specifying the network ID. When unspecified, we default to "0" for Global Default Network.
network_name={value}	(Valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network by specifying the network name.
tracking_method={value}	Show only IP addresses/ranges which have a certain tracking method.
host_dns={value}	The DNS hostname for the IP you want to update. A single IP must be specified in the same request and the IP will only be updated if it matches the hostname specified.
host_netbios={value}	The NetBIOS hostname for the IP you want to update. A single IP must be specified in the same request and the IP will only be updated if it matches the hostname specified.
Host Changes	
new_tracking_method={value}	(Optional) Change the tracking method. Specify IP for IP address, DNS or NETBIOS. Note - You cannot change the tracking method to EC2 or AGENT. If an IP is already tracked by EC2 or AGENT, you cannot change the tracking method to something else.
new_owner={value}	(Optional) Change the owner of the host asset(s). The owner must be a Manager. Another user (Unit Manager, Scanner, Reader) can be the owner if the IP address is in the user's account.
new_ud1={value} new_ud2={value} new_ud3={value}	(Optional) Change values for user-defined fields 1, 2 and 3. You can specify a maximum of 128 characters (ascii) for each field value.
new_comment={value}	(Optional) Change the user-defined comments. Specify new comments for the host asset(s).

Sample - Update Host Attributes with Host IDs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2"
"POST" -d
"action=update&ids=2332017&new_tracking_method=DNS&new_ud1=Loc&new
_ud2=Fun&new_ud3=AT&new_comment=API_Comment&new_owner=akreb_nb"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/update/out
put.dtd">
<HOST_UPDATE_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-03-09T10:38:17Z</DATETIME>
    <TEXT>Assets successfully updated</TEXT>
  </RESPONSE>
</HOST_UPDATE_OUTPUT>
```

Sample - Update Host Attributes with IPs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2"
"POST" -d
"action=update&ips=10.10.32.31&new_tracking_method=DNS&new_ud1=Loc
&new_ud2=Fun&new_ud3=AT&new_comment=API_Comment&new_owner=akreb_nb
" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/update/out
put.dtd">
<HOST_UPDATE_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-03-09T06:03:42Z</DATETIME>
    <TEXT>Assets successfully updated</TEXT>
  </RESPONSE>
</HOST_UPDATE_OUTPUT>
```

Sample - Update Host Attributes with Asset Group IDs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2"
"POST" -d
"action=update&ag_ids=4580719&new_tracking_method=IP&new_ud1=Loc&n
ew_ud2=Fun&new_ud3=AT&new_comment=API_Comment&new_owner=akreb_nb"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/update/out
put.dtd">
<HOST_UPDATE_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-03-09T10:39:11Z</DATETIME>
    <TEXT>Assets successfully updated</TEXT>
  </RESPONSE>
</HOST_UPDATE_OUTPUT>
```

Sample - Update Host Attributes with Asset Group Titles

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl demo2"
"POST" -d
"action=update&ag_titles=AG_Update&new_tracking_method=IP&new_ud1=
Loc&new_ud2=Fun&new_ud3=AT&new_comment=API_Comment&new_owner=akreb
_nb" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/update/out
put.dtd">
<HOST_UPDATE_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-03-09T10:39:43Z</DATETIME>
    <TEXT>Assets successfully updated</TEXT>
  </RESPONSE>
</HOST_UPDATE_OUTPUT>
```

DTD for Host Update

<platform API server>/api/2.0/fo/asset/host/dtd/update/output.dtd

Host List Detection

For API version information, refer to API Version History section.

V2.0|V3.0|V4.0| V5.0 | V6.0

V2.0

/api/2.0/fo/asset/host/vm/detection/?action=list

[GET] [POST]

Download a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. This data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information.

The Host List VM Detection API also shows the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score, EPSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Permissions - Managers view all VM scanned hosts in subscription. Auditors have no permission to view VM scanned hosts. Unit Managers view VM scanned hosts in the user's assigned business unit. Scanners and Readers view VM scanned hosts in the user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

Note:

- To grant access to sub-users to Cloud Agent hosts, the hosts should be added as IP-tracked assets to the users' subscriptions. The corresponding IP addresses should then be included in an Asset Group, and access to that Asset Group should be provided to the concerned sub-users. For more information, refer to Hosts with Cloud Agent in the VMDR Online Help.

- If you experience delays or increased API response time when making requests to the VM Detection endpoint, you can provide the request without the id parameter, or use the id_min and id_max parameters in the request.

- When you generate or automate queries that require unique values across QIDs and assets, you may observe that the same Unique Vulnerability ID appears across multiple QIDs and assets. This is expected behavior by design. A Vulnerability has its own Unique Vulnerability ID, and an Information Gathering (IG) finding has its own Unique ID. In some cases, both may share the same ID. To ensure accurate identification and avoid duplicates, use a combination of Unique Vulnerability ID and QID.

Express Lite - This API is available to Express Lite users.

Input Parameters

The input parameter **`action=list`** is required. All other input parameters are optional. Several filtering parameters are provided for filtering hosts and QIDs. When multiple filter parameters are specified, the service combines the effects of all the parameters in a way that corresponds to a logical "AND". So if two filter parameters are specified in the request, the service returns hosts that match both filters.

Quick Links: Detection Filters | Host Filters | QID Filters | Asset tags | Qualys Detection Score (QDS) | EC2/Azure/GCP metadata

API Request

Parameter	Description
action=list	(Required)
os_hostname={0|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List Detection API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={0|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.

Parameter	Description
include_vuln_type={confirmed|potential}	(Optional)Use to download vulnerability information based on their type, confirmed or potential. Specify: `include_vuln_type=confirmed` to download only confirmed vulnerabilities. `include_vuln_type=potential` to download only potential vulnerabilities. Exceptional Scenarios • After passing the parameter value include_vuln_type=confirmed, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase. • After passing the parameter value include_vuln_type=potential, some confirmed vulnerabilities show up in the API response. • This happens with the vulnerabilities assigned with a half red/half yellow severity level. • After passing the parameter value include_vuln_type=confirmed, some confirmed vulnerabilities may not be shown in API response. This will happen when vulnerabilities are assigned with a half red/half yellow severity level. • This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.
show_host_services={0|1}	(Optional) When specified, the service tag of the scanned hosts is displayed in the output. The default value of this parameter is set to 0. When set to 1, the service tag of the scanned hosts is displayed in the output.

Detection Filters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the output. When unspecified, parameters are not included in the output. Specify 1 to view parameters in the output.
show_results={0|**1**}	(Optional) When not specified, results are included in the output. Specify show_results=0 to exclude the results. If you exclude the results, CSV will have an empty Results column, and XML will not contain the Results tag.
show_reopened_info={**0**|1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify show_reopened_info=1 to include reopened info i.e. first/last reopened date, times reopened.
arf_kernel_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running Linux kernels. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Info Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for each detection. When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for each detection. When set to 4, only include kernel related vulnerabilities. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 or 1 for each detection.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
arf_service_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running ports/services. When unspecified, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> does not appear in the output. When set to 0, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities. When set to 1, exclude service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities that have a value of 1. When set to 2, only include service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 for each detection. When set to 3, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 1 for each detection. When set to 4, only include service related vulnerabilities. <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 or 1 for each detection.
arf_config_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration. When unspecified, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> does not appear in the output. When set to 0, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related vulnerabilities. When set to 1, exclude vulnerabilities that are exploitable due to host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related detections that have a value of 1. When set to 2, only include config related vulnerabilities that are exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 for each detection. When set to 3, only include config related vulnerabilities that are not exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 1 for each detection. When set to 4, only include config related vulnerabilities. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 or 1 for each detection.

Parameter	Description
active_kernels_only={0|1|2|3}	Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag <AFFECT_RUNNING_KERNEL>. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Information Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities. When set to 3, only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
output_format={**XML**|CSV|CSV_NO_METADATA|CSV_NO_METADATA_MS_EXCEL|CSV_MS_EXCEL}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. Valid values are: XML, CSV or CSV_NO_METADATA, CSV_NO_METADATA_MS_EXCEL or CSV_MS_EXCEL XML (default) - Specifies XML format for the output. CSV - Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA - Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. CSV_NO_METADATA_MS_EXCEL - When specified we will use CSV format for the output with no metadata with MS Excel restrictions on the maximum length allowed for a string value in the output. CSV_MS_EXCEL - When specified we will use CSV format for the output with MS Excel restriction on the maximum length allowed for a string value in the output. A value in the output will be truncated if the length of the value exceeds the maximum length supported in MS Excel.
suppress_duplicated_data_from_csv={**0**|1}	(Optional) By default or when set to 0, host details will be repeated in each line of detection information in the CSV output. When set to 1, host details will not be repeated (suppressed) in each detection line. This parameter must be specified with: output_format=CSV or output_format=CSV_NO_METADATA. **Note**: When set to 1, EC2 details are displayed in the Cloud Resource metadata column and the EC2 column is set bank in CSV output, if you have Azure/GCP enabled.

Parameter	Description
truncation_limit={value}	(Optional) Specifies the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). Specify 0 for no truncation limit. If the requested list identifies more host records than the truncation limit and output_format=XML, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. If the requested list identifies more host records than the truncation limit and output_format=CSV, then the CSV output includes "Truncated" in the FOOTER_CSV section and the URL for making another request for the next batch of host records. Check API samples (2, 4, 16) Qualys API - Host List Detection API samples (GitHub) **Note:** When you launch the API with the truncation limit set to 0 or not specified, it is recommended to use a specific and limited range of IPs or IDs to avoid performance issues. Launching the API without specifying IPs or IDs may result in performance lag.
max_days_since_detection_updated={value}	(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_updated_since={value}	(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like "2017-02-15" or "2017-02-15T23:15:00Z". Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated

Parameter	Description
detection_updated_before={value}	(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_processed_before={date}	(Optional) Show detections with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_processed_after={date}	(Optional) Show detections with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_last_tested_since={date}	(Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYYMM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range. This parameter cannot be specified in the same request as detection_last_tested_since_days.
detection_last_tested_since_days={value}	(Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.

Parameter	Description
	This parameter cannot be specified in the same request as detection_last_tested_since.
detection_last_tested_before={date}	(Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYYMM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before_days.
detection_last_tested_before_days={value}	(Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before.
include_ignored={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were ignored during detection. Specify include_ignored=1 to include results in the output.
include_disabled={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were disabled during detection. Specify include_disabled=1 to include results in the output.

Host Filters

Parameter	Description
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example: 190-400).Valid host IDs are required. **Note:** Use short ID ranges instead of broad ones. Broad ranges can include hosts that are not part of your subscription. Use asset groups. Asset groups provide greater reliability and allow more precise control. If your subscription is on the Private Cloud Provider (PCP), you can continue using ID ranges, as all hosts within that range are automatically included in your subscription.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value (for example: If id_min=44286508, then hosts with Ids 44286508 & higher value are displayed).
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required for example: If id_max=44286508, then hosts with Ids 44286508 & lower value are displayed).
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example: 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example: 386941-386945). Valid asset group IDs are required.
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.

Parameter	Description
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
network_name={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account.) Displays the name of the network corresponding to the network ID. The name will be displayed only if you subscribe to it and the tweak is enabled at the backend.
vm_scan_since={date}	(Optional) Show hosts scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
no_vm_scan_since={date}	(Optional) Show hosts not scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
max_days_since_last_vm_scan={value}	
	(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.
	This parameter cannot be specified with any of these parameters in the same request: vm_scan_since and no_vm_scan_since.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_before=date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".

Parameter	Description
vm_auth_scan_date_before ={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_after= {date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
status={value}	(Optional) Show only hosts with one or more of these status values: New, Active, Re-Opened, Fixed. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with New, Active or Re-Opened <STATUS> only. To get hosts with Fixed status, check this API sample Qualys API - Host List Detection API samples (GitHub, sample 11)
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list compliance hosts in the user’s account that have been scanned and processed. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use “%5E%24” to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Note: If either the Information Gathered (IG) processed date or the vulnerability processed date is missing or null for a host, the host will still be included in the results when using the parameters vm_processed_before and show_igs=1 in the Host List Detection (HLD) API.

However, if show_igs=0 or is not specified along with vm_processed_before, the API will behave as before, excluding hosts where either IG processed date or the vulnerability processed date value is null.

QID Filters

Parameter	Description
qids={value}	(Optional) Show only detection records with certain QIDs. One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma separated. Valid QIDs are required.
severities={value}	(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example: 1-3). Multiple entries are comma separated.
filter_superseded_qids={0|1}	(Optional) When unspecified or set to 0, the XML output includes all QIDs even if they've been superseded. Specify 1 to filter out QIDs that have been superseded by another QID in the results.
show_igs={0|1}	(Optional except as noted) Specify 1 to show detection records with information gathered along with confirmed vulnerabilities and potential vulnerabilities. Specify 0 (default) to hide information gathered.
	The show_igs parameter is required in one use case. The parameter show_igs=1 must be specified if both these conditions are met: 1) search lists are included using the parameter include_search_list_titles or include_search_list_ids, and 2) if the included search lists contain only information gathered.
include_search_list_titles={value}	(Optional) Show detection records only when a record's QID is INCLUDED IN in one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_ids.
exclude_search_list_titles={value}	(Optional) Show detection records only when a record's QID is IS EXCLUDED from one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_ids.
include_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS INCLUDED in one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 10-15). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_titles.

Parameter	Description
exclude_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS EXCLUDED from one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 40-42). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_titles.

Asset tags

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. **Note:** You must select an include tag before selecting an exclude tag.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

Qualys Detection Score (QDS)

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

EC2/Azure/GCP metadata

Note: Ensure to enable the EC2 scanning and ensure this setting remains active. To enable this, reach out to your Technical Account Manager or Qualys Support.

Parameter	Description
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes. To retrieve information about the host instance type, use the metadata field, "instance-type".
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.

Parameter	Description
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Keep Alive Mechanism

The service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the host detection list API request. To keep the connection alive, the service sends some "dummy" data back to the client every 30 to 40 seconds if no "real" data has been sent already by the API during that time.

In XML output, this "dummy" data appears as a "<!-- keep-alive -->" line (since comments should be safely ignored by downstream XML parsers).

In CSV and CSV_NO_METADATA output, this "dummy" data appears as a <CR><LF> (carriage return, linefeed) pair (since empty lines clearly do not contain any CSV data).

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \--header 'X-Requested-With:
curl'--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
```

```
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
```

```
                <ID>524323</ID>
                <IP>11.110.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
```

```
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List VM scanned hosts

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://
<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.10.40.10&truncation_limit=4">
  <HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
      <DATETIME>2024-03-28T09:03:45Z</DATETIME>
```

```
      <HOST_LIST>
        <HOST>
          <ID>4203254</ID>
          <IP>11.11.11.11</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <ASSET_GROUP_LIST />
          <NETWORK_ID>2458227</NETWORK_ID>
          <NETWORK_NAME>network1</NETWORK_NAME>
          <OS>
            <![CDATA[Windows XP]]>
          </OS>
          <DNS>
            <![CDATA[w2kserver-tmp3.vuln.example.com]]>
          </DNS>
          <DNS_DATA>
            <HOSTNAME>
              <![CDATA[w2kserver-tmp3]]>
            </HOSTNAME>
            <DOMAIN>
              <![CDATA[vuln.example.com]]>
            </DOMAIN>
            <FQDN>
              <![CDATA[w2kserver-tmp3.vuln.example.com]]>
            </FQDN>
          </DNS_DATA>
          <LAST_SCAN_DATETIME>2023-10-11T07:18:36Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>149</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>149</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>61198372</UNIQUE_VULN_ID>
              <QID>11</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>2</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[NameProgramVersionProtocolPort
portmap/rpcbind1000002-4tcp111
portmap/rpcbind1000002-4udp895
portmap/rpcbind1000002-4udp111]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
```

```
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>61198518</UNIQUE_VULN_ID>
              <QID>13361</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <PORT>22</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[User Nameroot
Authentication Schemepassword
ProtocolSSH Version 2
Discovery MethodLogin credentials provided by user
Using sudoNo
Key exchange algorithmdiffie-hellman-group-exchange-sha256
Host key algorithmssh-rsa
Compression algorithmzlib@openssh.com
Encryption algorithmaes128-ctr
MAC algorithmhmac-sha2-256
Authentication Record10.113.197.133]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
  </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host Detection XML Output, with truncation

A truncated response is returned when the API request returns more host records than the truncation limit. In this sample, the truncation limit is set to 100 host records.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&truncation_limit=100"
```

The Warning message in the XML output (shown below) indicates the URL you need to use to request the next 100 host records.

XML output:

```
...
          </DETECTION>
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
    <WARNING>
      <CODE>1980</CODE>
      <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>

<URL><![CDATA[<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?actio
n=list&truncation_limit=100&id_min=5641289]]></URL>
    </WARNING>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Filter superseded QIDs (filter_superseded_qids=1)

In this example any QID superseded by another QID has been filtered out of the results. The XML output includes QID 370584 and QID 370613. QID 370610 was filtered out because it was superseded by QID 370613.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&filter_superseded_qids=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/dtd/outpu
t.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-03T10:22:34Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1145</ID>
        <IP>10.10.10.9</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[win2003.sample.qualys.com]]></DNS>
        <DNS_DATA>
            <HOSTNAME>
                <![CDATA[win2003]]>
            </HOSTNAME>
```

```
            <DOMAIN>
                <![CDATA[sample.qualys.com]]>
            </DOMAIN>
            <FQDN>
                <![CDATA[win2003.sample.qualys.com]]>
            </FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[LWIN2003HP1]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-01-08T19:50:18Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-01-08T19:36:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>619</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2017-11-15T16:58:16Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
<DETECTION>
            <QID>370584</QID>
            <UNIQUE_VULN_ID>45654</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
          <RESULTS><![CDATA[C:\Program Files\Mozilla Firefox\firefox.exe
Version is  42.0.0.0]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-10-
10T10:30:48Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>183</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-08-
27T22:48:04Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
<DETECTION>
            <QID>370613</QID>
            <UNIQUE_VULN_ID>43664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[C:\Program
Files\Google\Chrome\Application\33.0.1750.149\chrome.dll file version is
33.0.1750.149
%ProgramFiles%\Google\Chrome\Application\33.0.1750.149\chrome.dll file
version is 33.0.1750.149]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-11-
12T20:11:32Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>162</TIMES_FOUND>
```

```
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-10-
30T22:28:59Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
</DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List assets with Qualys Detection Score (QDS)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/dtd/outp
ut.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
               <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
```

```
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS">
                     <![CDATA[9.3]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_version">
                      <![CDATA[v2]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="epss">
                       <![CDATA[0.24142]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_vector">
                       <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                 </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>          </DETECTION>
...
```

```
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List Assets with Tag Details in the Response

API request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list
&ips=xx.xxx.xxx.xxx&show_tags=1' \--header 'X-Requested-With: curl'--
header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-03-17T09:40:25Z</DATETIME>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST_LIST>
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <HOST>
                    <ID>14125607</ID>
                    <IP>10.113.197.133</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Linux 2.6]]>
                    </OS>
                    <DNS>
                        <![CDATA[10-101-87-231.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[10-101-87-231]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[10-101-87-231.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <LAST_SCAN_DATETIME>2026-02-
26T08:23:48Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-02-
26T08:23:21Z</LAST_VM_SCANNED_DATE>
```

```
<LAST_VM_SCANNED_DURATION>386</LAST_VM_SCANNED_DURATION>
                    <TAGS>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143644527]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_Demo]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143710805]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[BU2]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143651023]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[demo_BU]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143668042]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_AG]]>
                            </NAME>
                        </TAG>
                    </TAGS>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467336</UNIQUE_VULN_ID>
                            <QID>38611</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>22</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
```

```
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467334</UNIQUE_VULN_ID>
                            <QID>38623</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                    ...
                    ...
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_VM_DETECTION_OUTPUT>
```

More Samples

Qualys API - Host List Detection API samples (GitHub)

DTD

<platform API server>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd

V3.0

/api/3.0/fo/asset/host/vm/detection/

[GET] [POST]

Download a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. This data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information.

The Host List VM Detection API also shows the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score, EPSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Permissions - Managers view all VM scanned hosts in subscription. Auditors have no permission to view VM scanned hosts. Unit Managers view VM scanned hosts in the user's assigned business unit. Scanners and Readers view VM scanned hosts in the user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

Note:

- If you experience delays or increased API response time when making requests to the VM Detection endpoint, you can provide the request without the id parameter, or use the id_min and id_max parameters in the request.

- When you generate or automate queries that require unique values across QIDs and assets, you may observe that the same Unique Vulnerability ID appears across multiple QIDs and assets. This is expected behavior by design. A Vulnerability has its own Unique Vulnerability ID, and an Information Gathering (IG) finding has its own Unique ID. In some cases, both may share the same ID. To ensure accurate identification and avoid duplicates, use a combination of Unique Vulnerability ID and QID.

Express Lite - This API is available to Express Lite users.

Input Parameters

The input parameter **`action=list`** is required. All other input parameters are optional. Several filtering parameters are provided for filtering hosts and QIDs. When multiple filter parameters are specified, the service combines the effects of all the parameters in a way that corresponds to a logical "AND". So if two filter parameters are specified in the request, the service returns hosts that match both filters.

Quick Links: Detection Filters | Host Filters | QID Filters | Asset tags | Qualys Detection Score (QDS)| EC2/Azure/GCP metadata

API Request

Parameter	Description
action=list	(Required)
os_hostname={0|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List Detection API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={0|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
show_host_service={0|1}	(Optional) When specified, the service tag of the scanned hosts is displayed in the output. The default value of this parameter is set to 0. When set to 1, the service tag of the scanned hosts is displayed in the output.
arf_filter_keys={value}	(Optional) Accepts one of these values: non-running-kernel, non-running-service, and config-not-exploitable. You can apply these values independently or in any combination to refine their filter criteria. For instance, you can use non-running-kernel and non-running-service values together. **Note:** You can use either this input parameter or arf_kernel_filter input parameter.

Parameter	Description
show_arf_data={0|1}	(Optional) Displays the ARF-affected QIDs, with the value as (1/0). If user passes value as 0, it does not show the ARF filter output data in the output, and if the user passes value as 1, it shows the ARF filter output data in the output.
include_vuln_type={confirmed|potential}	(Optional)Use to download vulnerability information based on their type, confirmed or potential. Specify: `include_vuln_type=confirmed` to download only confirmed vulnerabilities. `include_vuln_type=potential` to download only potential vulnerabilities. Exceptional Scenarios • After passing the parameter value include_vuln_type=confirmed, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase. • After passing the parameter value include_vuln_type=potential, some confirmed vulnerabilities show up in the API response. • This happens with the vulnerabilities assigned with a half red/half yellow severity level. • After passing the parameter value include_vuln_type=confirmed, some confirmed vulnerabilities may not be shown in API response. This will happen when vulnerabilities are assigned with a half red/half yellow severity level. • This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.

Detection Filters

Parameter	Description
show_results={0|**1**}	(Optional) When not specified, results are included in the output. Specify show_results=0 to exclude the results. If you exclude the results, CSV will have an empty Results column, and XML will not contain the Results tag.
show_reopened_info={**0**|1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify show_reopened_info=1 to include reopened info i.e. first/last reopened date, times reopened.
arf_kernel_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running Linux kernels. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Info Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for each detection. When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for each detection. When set to 4, only include kernel related vulnerabilities. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
arf_service_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running ports/services. When unspecified, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> does not appear in the output. When set to 0, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities. When set to 1, exclude service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities that have a value of 1. When set to 2, only include service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 for each detection. When set to 3, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 1 for each detection. When set to 4, only include service related vulnerabilities. <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.

Parameter	Description
arf_config_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration. When unspecified, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> does not appear in the output. When set to 0, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related vulnerabilities. When set to 1, exclude vulnerabilities that are exploitable due to host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related detections that have a value of 1. When set to 2, only include config related vulnerabilities that are exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 for each detection. When set to 3, only include config related vulnerabilities that are not exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 1 for each detection. When set to 4, only include config related vulnerabilities. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities that may or may not be exploitable due to the current host configuration.

Parameter	Description
active_kernels_only={0|1|2|3}	Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag <AFFECT_RUNNING_KERNEL>. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Information Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities. When set to 3, only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
output_format={**XML**|CSV|CSV_NO_METADATA|CSV_NO_METADATA_MS_EXCEL|CSV_MS_EXCEL}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. Valid values are: XML, CSV or CSV_NO_METADATA, CSV_NO_METADATA_MS_EXCEL and CSV_MS_EXCEL XML (default) - Specifies XML format for the output. CSV - Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA - Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. CSV_NO_METADATA_MS_EXCEL - When specified we will use CSV format for the output with no metadata with MS Excel restrictions on the maximum length allowed for a string value in the output. CSV_MS_EXCEL - When specified we will use CSV format for the output with MS Excel restriction on the maximum length allowed for a string value in the output. A value in the output will be truncated if the length of the value exceeds the maximum length supported in MS Excel.
suppress_duplicated_data_from_csv={**0**|1}	(Optional) By default or when set to 0, host details will be repeated in each line of detection information in the CSV output. When set to 1, host details will not be repeated (suppressed) in each detection line. This parameter must be specified with: output_format=CSV or output_format=CSV_NO_METADATA. **Note**: When set to 1, EC2 details are displayed in the Cloud Resource metadata column and the EC2 column is set bank in CSV output, if you have Azure/GCP enabled.

Parameter	Description
truncation_limit={value}	(Optional) Specifies the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). Specify 0 for no truncation limit. If the requested list identifies more host records than the truncation limit and output_format=XML, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. If the requested list identifies more host records than the truncation limit and output_format=CSV, then the CSV output includes "Truncated" in the FOOTER_CSV section and the URL for making another request for the next batch of host records. Check API samples (2, 4, 16) Qualys API - Host List Detection API samples (GitHub) **Note:** When you launch the API with the truncation limit set to 0 or not specified, it is recommended to use a specific and limited range of IPs or IDs to avoid performance issues. Launching the API without specifying IPs or IDs may result in performance lag.
max_days_since_detection_updated={value}	(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_updated_since={value}	(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2017-02-15" or "2017-02-15T23:15:00Z". Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated

Parameter	Description
detection_updated_before={value}	
	(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_processed_before={date}	
	(Optional) Show detections with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_processed_after={date}	
	(Optional) Show detections with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_last_tested_since={date}	
	(Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range. This parameter cannot be specified in the same request as detection_last_tested_since_days.
detection_last_tested_since_days={value}	
	(Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.

Parameter	Description
	This parameter cannot be specified in the same request as detection_last_tested_since.
detection_last_tested_before={date}	(Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before_days.
detection_last_tested_before_days={value}	(Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before.
include_ignored={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were ignored during detection. Specify include_ignored=1 to include results in the output.
include_disabled={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were disabled during detection. Specify include_disabled=1 to include results in the output.

Host Filters

Parameter	Description
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example: 190-400).Valid host IDs are required. **Note:** Use short ID ranges instead of broad ones. Broad ranges can include hosts that are not part of your subscription. Use asset groups. Asset groups provide greater reliability and allow more precise control. If your subscription is on the Private Cloud Provider (PCP), you can continue using ID ranges, as all hosts within that range are automatically included in your subscription.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value (for example: If id_min=44286508, then hosts with Ids 44286508 & higher value are displayed).
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required for example: If id_max=44286508, then hosts with Ids 44286508 & lower value are displayed).
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example: 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example: 386941-386945). Valid asset group IDs are required.
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.

Parameter	Description
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
network_name={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account.) Displays the name of the network corresponding to the network ID. The name will be displayed only if you subscribe to it and the tweak is enabled at the backend.
vm_scan_since={date}	(Optional) Show hosts scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
no_vm_scan_since={date}	(Optional) Show hosts not scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
max_days_since_last_vm_scan={value}	
	(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.
	This parameter cannot be specified with any of these parameters in the same request: vm_scan_since and no_vm_scan_since.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_before=date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".

Parameter	Description
vm_auth_scan_date_before ={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_after= {date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
status={value}	(Optional) Show only hosts with one or more of these status values: New, Active, Re-Opened, Fixed. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with New, Active or Re-Opened <STATUS> only. To get hosts with Fixed status, check this API sample Qualys API - Host List Detection API samples (GitHub, sample 11)
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list compliance hosts in the user’s account that have been scanned and processed. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use “%5E%24” to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Note: If either the Information Gathered (IG) processed date or the vulnerability processed date is missing or null for a host, the host will still be included in the results when using the parameters vm_processed_before and show_igs=1 in the Host List Detection (HLD) API.

However, if show_igs=0 or is not specified along with vm_processed_before, the API will behave as before, excluding hosts where either IG processed date or the vulnerability processed date value is null.

QID Filters

Parameter	Description
qids={value}	(Optional) Show only detection records with certain QIDs. One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma separated. Valid QIDs are required.
severities={value}	(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example: 1-3). Multiple entries are comma separated.
filter_superseded_qids={0|1}	(Optional) When unspecified or set to 0, the XML output includes all QIDs even if they've been superseded. Specify 1 to filter out QIDs that have been superseded by another QID in the results.
show_igs={0|1}	(Optional except as noted) Specify 1 to show detection records with information gathered along with confirmed vulnerabilities and potential vulnerabilities. Specify 0 (default) to hide information gathered.
	The show_igs parameter is required in one use case. The parameter show_igs=1 must be specified if both these conditions are met: 1) search lists are included using the parameter include_search_list_titles or include_search_list_ids, and 2) if the included search lists contain only information gathered.
include_search_list_titles={value}	(Optional) Show detection records only when a record's QID is INCLUDED IN in one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_ids.
exclude_search_list_titles={value}	(Optional) Show detection records only when a record's QID is IS EXCLUDED from one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_ids.
include_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS INCLUDED in one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 10-15). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_titles.

Parameter	Description
exclude_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS EXCLUDED from one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 40-42). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_titles.

Asset tags

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. **Note:** You must select an include tag before selecting an exclude tag.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

Qualys Detection Score (QDS)

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

EC2/Azure/GCP metadata

Note: Ensure to enable the EC2 scanning and ensure this setting remains active. To enable this, reach out to your Technical Account Manager or Qualys Support.

Parameter	Description
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes. To retrieve information about the host instance type, use the metadata field, "instance-type".
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.

Parameter	Description
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Keep Alive Mechanism

The service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the host detection list API request. To keep the connection alive, the service sends some "dummy" data back to the client every 30 to 40 seconds if no "real" data has been sent already by the API during that time.

In XML output, this "dummy" data appears as a "<!-- keep-alive -->" line (since comments should be safely ignored by downstream XML parsers).

In CSV and CSV_NO_METADATA output, this "dummy" data appears as a <CR><LF> (carriage return, linefeed) pair (since empty lines clearly do not contain any CSV data).

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \--header 'X-Requested-With:
curl'--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
```

```
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
```

```
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List VM scanned hosts

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://
<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.10.40.10&truncation_limit=4">
  <HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
      <DATETIME>2024-03-28T09:03:45Z</DATETIME>
      <HOST_LIST>
        <HOST>
          <ID>4203254</ID>
          <IP>11.11.11.11</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <ASSET_GROUP_LIST />
          <NETWORK_ID>2458227</NETWORK_ID>
          <NETWORK_NAME>network1</NETWORK_NAME>
          <OS>
            <![CDATA[Windows XP]]>
          </OS>
          <DNS>
            <![CDATA[w2kserver-tmp3.vuln.example.com]]>
          </DNS>
          <DNS_DATA>
            <HOSTNAME>
              <![CDATA[w2kserver-tmp3]]>
            </HOSTNAME>
            <DOMAIN>
              <![CDATA[vuln.example.com]]>
            </DOMAIN>
            <FQDN>
              <![CDATA[w2kserver-tmp3.vuln.example.com]]>
            </FQDN>
          </DNS_DATA>
          <LAST_SCAN_DATETIME>2023-10-11T07:18:36Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>149</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>149</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>61198372</UNIQUE_VULN_ID>
              <QID>11</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>2</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[NameProgramVersionProtocolPort
portmap/rpcbind1000002-4tcp111
portmap/rpcbind1000002-4udp895
portmap/rpcbind1000002-4udp111]]>
              </RESULTS>
              <STATUS>New</STATUS>
```

```
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>61198518</UNIQUE_VULN_ID>
              <QID>13361</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <PORT>22</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[User Nameroot
Authentication Schemepassword
ProtocolSSH Version 2
Discovery MethodLogin credentials provided by user
Using sudoNo
Key exchange algorithmdiffie-hellman-group-exchange-sha256
Host key algorithmssh-rsa
Compression algorithmzlib@openssh.com
Encryption algorithmaes128-ctr
MAC algorithmhmac-sha2-256
Authentication Record10.113.197.133]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
```

```
  </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host Detection XML Output, with truncation

A truncated response is returned when the API request returns more host records than the truncation limit. In this sample, the truncation limit is set to 100 host records.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100"
```

The Warning message in the XML output (shown below) indicates the URL you need to use to request the next 100 host records.

XML output:

```
...
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
      <WARNING>
        <CODE>1980</CODE>
        <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>

<URL><![CDATA[<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100&id_min=5641289]]></URL>
      </WARNING>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Filter superseded QIDs (filter_superseded_qids=1)

In this example any QID superseded by another QID has been filtered out of the results. The XML output includes QID 370584 and QID 370613. QID 370610 was filtered out because it was superseded by QID 370613.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/3.0/fo/asset/host/vm/detection/?action=list&filter_superseded_qids=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-03T10:22:34Z</DATETIME>
    <HOST_LIST>
```

```
      <HOST>
        <ID>1145</ID>
        <IP>10.10.10.9</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[win2003.sample.qualys.com]]></DNS>
        <DNS_DATA>
            <HOSTNAME>
                <![CDATA[win2003]]>
            </HOSTNAME>
            <DOMAIN>
                <![CDATA[sample.qualys.com]]>
            </DOMAIN>
            <FQDN>
                <![CDATA[win2003.sample.qualys.com]]>
            </FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[LWIN2003HP1]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-01-08T19:50:18Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-01-08T19:36:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>619</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2017-11-15T16:58:16Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
<DETECTION>
            <QID>370584</QID>
            <UNIQUE_VULN_ID>45654</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
          <RESULTS><![CDATA[C:\Program Files\Mozilla Firefox\firefox.exe
Version is  42.0.0.0]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-10-
10T10:30:48Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>183</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-08-
27T22:48:04Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
<DETECTION>
            <QID>370613</QID>
            <UNIQUE_VULN_ID>43664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[C:\Program
```

```
Files\Google\Chrome\Application\33.0.1750.149\chrome.dll file version is
33.0.1750.149
%ProgramFiles%\Google\Chrome\Application\33.0.1750.149\chrome.dll file
version is 33.0.1750.149]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-11-
12T20:11:32Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>162</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-10-
30T22:28:59Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
</DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List assets with Qualys Detection Score (QDS)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
```

```
              <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS">
                     <![CDATA[9.3]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_version">
                      <![CDATA[v2]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="epss">
                       <![CDATA[0.24142]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_vector">
                       <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
```

```
                </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>          </DETECTION>
...
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - VM Detection API

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&show_a
rf_data=1&arf_filter_keys=config-not- exploitable&truncation_limit=10' \
--header 'X-Requested-With: POSTMAN' \
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd>"
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-08-26T11:52:53Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>2454304</ID>
                    <IP>11.111.22.44</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>952199</NETWORK_ID>
                    <LAST_SCAN_DATETIME>2022-08-14T18:56:13Z
                    </LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2022-08-14T18:40:15Z
                    </LAST_VM_SCANNED_DATE>
                    <LAST_VM_SCANNED_DURATION>447</LAST_VM_
                    SCANNED_DURATION>
                    <DETECTION_LIST>
                          <DETECTION>
                             <UNIQUE_VULN_ID>35787259</UNIQUE_VULN_ID>
                             <QID>316406</QID>
                             <TYPE>Potential</TYPE>
                             <SEVERITY>3</SEVERITY>
                             <SSL>0</SSL>
                             <RESULTS>
```

```
                                <![CDATA[Package Installed Version
                                Required Version
                               firefox 31.3.0-3.el6.centos.x86_64 38.0-4.el6.
                                centos]]>
                                </RESULTS>
                                <STATUS>New</STATUS>
                                <FIRST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </FIRST_FOUND_DATETIME>
                                <LAST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </LAST_FOUND_DATETIME>
                                <TIMES_FOUND>1</TIMES_FOUND>
                                <LAST_TEST_DATETIME>2022-03-22T06:54:47Z
                                </LAST_TEST_DATETIME>
                                <LAST_UPDATE_DATETIME>2022-03-22T07:14:30Z
                                </LAST_UPDATE_DATETIME>
                                <IS_IGNORED>0</IS_IGNORED>
                                <IS_DISABLED>0</IS_DISABLED>
                                <AFFECT_EXPLOITABLE_CONFIG>0
                                </AFFECT_EXPLOITABLE_CONFIG>
                                <LAST_PROCESSED_DATETIME>2022-
                                0322T07:14:30Z</LAST_PROCESSED_DATETIME>
                            </DETECTION>
                        </DETECTION_LIST>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List Assets with Tag Details in the Response

API request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list
&ips=xx.xxx.xxx.xxx&show_tags=1' \--header 'X-Requested-With: curl'--
header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-03-17T09:40:25Z</DATETIME>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST_LIST>
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <HOST>
                    <ID>14125607</ID>
                    <IP>10.113.197.133</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
```

```
                    <OS>
                        <![CDATA[Linux 2.6]]>
                    </OS>
                    <DNS>
                        <![CDATA[10-101-87-231.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[10-101-87-231]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[10-101-87-231.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <LAST_SCAN_DATETIME>2026-02-
26T08:23:48Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-02-
26T08:23:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>386</LAST_VM_SCANNED_DURATION>
                    <TAGS>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143644527]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_Demo]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143710805]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[BU2]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143651023]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[demo_BU]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143668042]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_AG]]>
```

```
                            </NAME>
                        </TAG>
                    </TAGS>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467336</UNIQUE_VULN_ID>
                            <QID>38611</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>22</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467334</UNIQUE_VULN_ID>
                            <QID>38623</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
```

```
                              <IS_DISABLED>0</IS_DISABLED>
                              <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                           </DETECTION>
                        ...
                        ...
                        </DETECTION_LIST>
                     </HOST>
                  </HOST_LIST>
               </RESPONSE>
            </HOST_LIST_VM_DETECTION_OUTPUT>
```

More Samples

Qualys API - Host List Detection API samples (GitHub)

DTD

<platform API server>/api/3.0/fo/asset/host/vm/detection/dtd/output.dtd

V4.0

/api/4.0/fo/asset/host/vm/detection/

[GET] [POST]

Download a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. This data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information.

The Host List VM Detection API also shows the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score, EPSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Permissions - Managers view all VM scanned hosts in subscription. Auditors have no permission to view VM scanned hosts. Unit Managers view VM scanned hosts in the user's assigned business unit. Scanners and Readers view VM scanned hosts in the user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

Note:

- If you experience delays or increased API response time when making requests to the VM Detection endpoint, you can provide the request without the id parameter, or use the id_min and id_max parameters in the request.

- When you generate or automate queries that require unique values across QIDs and assets, you may observe that the same Unique Vulnerability ID appears across multiple QIDs and assets. This is expected behavior by design. A Vulnerability has its own Unique Vulnerability ID, and an Information Gathering (IG) finding has its own Unique ID. In some cases, both may share the same ID. To ensure accurate identification and avoid duplicates, use a combination of Unique Vulnerability ID and QID.

Express Lite - This API is available to Express Lite users.

Input Parameters

The input parameter **`action=list`** is required. All other input parameters are optional. Several filtering parameters are provided for filtering hosts and QIDs. When multiple filter parameters are specified, the service combines the effects of all the parameters in a way that corresponds to a logical “AND”. So if two filter parameters are specified in the request, the service returns hosts that match both filters.

Quick Links: Detection Filters | Host Filters | QID Filters | Asset tags | Qualys Detection Score (QDS) | EC2/Azure/GCP metadata

API Request

Parameter	Description
action=list	(Required)
os_hostname={0|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List Detection API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={0|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
show_host_service={0|1}	(Optional) When specified, the service tag of the scanned hosts is displayed in the output. The default value of this parameter is set to 0. When set to 1, the service tag of the scanned hosts is displayed in the output.
arf_filter_keys={value}	(Optional) Accepts one of these values: non-running-kernel, non-running-service, and config-not-exploitable. You can apply these values independently or in any combination to refine their filter criteria. For instance, you can use non-running-kernel and non-running-service values together. **Note:** You can use either this input parameter or arf_kernel_filter input parameter.

Parameter	Description
show_arf_data={0|1}	(Optional) Displays the ARF-affected QIDs, with the value as (1/0). If user passes value as 0, it does not show the ARF filter output data in the output, and if the user passes value as 1, it shows the ARF filter output data in the output.
include_vuln_type={confirmed|potential}	(Optional)Use to download vulnerability information based on their type, confirmed or potential. Specify: `include_vuln_type=confirmed` to download only confirmed vulnerabilities. `include_vuln_type=potential` to download only potential vulnerabilities. Exceptional Scenarios • After passing the parameter value include_vuln_type=confirmed, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase. • After passing the parameter value include_vuln_type=potential, some confirmed vulnerabilities show up in the API response. • This happens with the vulnerabilities assigned with a half red/half yellow severity level. • After passing the parameter value include_vuln_type=confirmed, some confirmed vulnerabilities may not be shown in API response. This will happen when vulnerabilities are assigned with a half red/half yellow severity level. • This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.

Detection Filters

Parameter	Description
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0.
show_results={0|**1**}	(Optional) When not specified, results are included in the output. Specify show_results=0 to exclude the results. If you exclude the results, CSV will have an empty Results column, and XML will not contain the Results tag.
show_reopened_info={**0**|1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify show_reopened_info=1 to include reopened info i.e. first/last reopened date, times reopened.

Parameter	Description
arf_kernel_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running Linux kernels. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Info Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for each detection. When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for each detection. When set to 4, only include kernel related vulnerabilities. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
arf_service_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running ports/services. When unspecified, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> does not appear in the output. When set to 0, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities. When set to 1, exclude service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities that have a value of 1. When set to 2, only include service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 for each detection. When set to 3, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 1 for each detection. When set to 4, only include service related vulnerabilities. <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.

Parameter	Description
arf_config_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration. When unspecified, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> does not appear in the output. When set to 0, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related vulnerabilities. When set to 1, exclude vulnerabilities that are exploitable due to host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related detections that have a value of 1. When set to 2, only include config related vulnerabilities that are exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 for each detection. When set to 3, only include config related vulnerabilities that are not exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 1 for each detection. When set to 4, only include config related vulnerabilities. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities that may or may not be exploitable due to the current host configuration.

Parameter	Description
active_kernels_only={0|1|2|3}	Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag <AFFECT_RUNNING_KERNEL>. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Information Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities. When set to 3, only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
output_format={**XML**|CSV|CSV_NO_METADATA|CSV_NO_METADATA_MS_EXCEL|CSV_MS_EXCEL}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. Valid values are: XML, CSV or CSV_NO_METADATA, CSV_NO_METADATA_MS_EXCEL and CSV_MS_EXCEL XML (default) - Specifies XML format for the output. CSV - Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA - Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. CSV_NO_METADATA_MS_EXCEL - When specified we will use CSV format for the output with no metadata with MS Excel restrictions on the maximum length allowed for a string value in the output. CSV_MS_EXCEL - When specified we will use CSV format for the output with MS Excel restriction on the maximum length allowed for a string value in the output. A value in the output will be truncated if the length of the value exceeds the maximum length supported in MS Excel.
suppress_duplicated_data_from_csv={**0**|1}	(Optional) By default or when set to 0, host details will be repeated in each line of detection information in the CSV output. When set to 1, host details will not be repeated (suppressed) in each detection line. This parameter must be specified with: output_format=CSV or output_format=CSV_NO_METADATA. **Note**: When set to 1, EC2 details are displayed in the Cloud Resource metadata column and the EC2 column is set bank in CSV output, if you have Azure/GCP enabled.

Parameter	Description
truncation_limit={value}	(Optional) Specifies the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). Specify 0 for no truncation limit. If the requested list identifies more host records than the truncation limit and output_format=XML, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. If the requested list identifies more host records than the truncation limit and output_format=CSV, then the CSV output includes "Truncated" in the FOOTER_CSV section and the URL for making another request for the next batch of host records. Check API samples (2, 4, 16) Qualys API - Host List Detection API samples (GitHub) **Note:** When you launch the API with the truncation limit set to 0 or not specified, it is recommended to use a specific and limited range of IPs or IDs to avoid performance issues. Launching the API without specifying IPs or IDs may result in performance lag.
max_days_since_detection_updated={value}	(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_updated_since={value}	(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2017-02-15" or "2017-02-15T23:15:00Z". Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated

Parameter	Description
detection_updated_before={value}	(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_processed_before={date}	(Optional) Show detections with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_processed_after={date}	(Optional) Show detections with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_last_tested_since={date}	(Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range. This parameter cannot be specified in the same request as detection_last_tested_since_days.
detection_last_tested_since_days={value}	(Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.

Parameter	Description
	This parameter cannot be specified in the same request as detection_last_tested_since.
detection_last_tested_before={date}	(Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before_days.
detection_last_tested_before_days={value}	(Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before.
include_ignored={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were ignored during detection. Specify include_ignored=1 to include results in the output.
include_disabled={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were disabled during detection. Specify include_disabled=1 to include results in the output.

Host Filters

Parameter	Description
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example: 190-400).Valid host IDs are required. **Note:** Use short ID ranges instead of broad ones. Broad ranges can include hosts that are not part of your subscription. Use asset groups. Asset groups provide greater reliability and allow more precise control. If your subscription is on the Private Cloud Provider (PCP), you can continue using ID ranges, as all hosts within that range are automatically included in your subscription.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value (for example: If id_min=44286508, then hosts with Ids 44286508 & higher value are displayed).
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required for example: If id_max=44286508, then hosts with Ids 44286508 & lower value are displayed).
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example: 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example: 386941-386945). Valid asset group IDs are required.
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.

Parameter	Description
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
network_name={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account.) Displays the name of the network corresponding to the network ID. The name will be displayed only if you subscribe to it and the tweak is enabled at the backend.
vm_scan_since={date}	(Optional) Show hosts scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
no_vm_scan_since={date}	(Optional) Show hosts not scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
max_days_since_last_vm_scan={value}	
	(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.
	This parameter cannot be specified with any of these parameters in the same request: vm_scan_since and no_vm_scan_since.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_before=date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2016-09-12" or "2016-09-12T23:15:00Z".

Parameter	Description
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
status={value}	(Optional) Show only hosts with one or more of these status values: New, Active, Re-Opened, Fixed. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with New, Active or Re-Opened <STATUS> only. To get hosts with Fixed status, check this API sample Qualys API - Host List Detection API samples (GitHub, sample 11)
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list compliance hosts in the user’s account that have been scanned and processed. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use “%5E%24” to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Note: If either the Information Gathered (IG) processed date or the vulnerability processed date is missing or null for a host, the host will still be included in the results when using the parameters vm_processed_before and show_igs=1 in the Host List Detection (HLD) API.

However, if show_igs=0 or is not specified along with vm_processed_before, the API will behave as before, excluding hosts where either IG processed date or the vulnerability processed date value is null.

QID Filters

Parameter	Description
qids={value}	(Optional) Show only detection records with certain QIDs. One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma separated. Valid QIDs are required.
severities={value}	(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example: 1-3). Multiple entries are comma separated.
filter_superseded_qids={0|1}	(Optional) When unspecified or set to 0, the XML output includes all QIDs even if they've been superseded. Specify 1 to filter out QIDs that have been superseded by another QID in the results.
show_igs={0|1}	(Optional except as noted) Specify 1 to show detection records with information gathered along with confirmed vulnerabilities and potential vulnerabilities. Specify 0 (default) to hide information gathered.
	The show_igs parameter is required in one use case. The parameter show_igs=1 must be specified if both these conditions are met: 1) search lists are included using the parameter include_search_list_titles or include_search_list_ids, and 2) if the included search lists contain only information gathered.
include_search_list_titles={value}	(Optional) Show detection records only when a record's QID is INCLUDED IN in one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_ids.
exclude_search_list_titles={value}	(Optional) Show detection records only when a record's QID is IS EXCLUDED from one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_ids.
include_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS INCLUDED in one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 10-15). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_titles.

Parameter	Description
exclude_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS EXCLUDED from one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 40-42). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_titles.

Asset tags

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. **Note:** You must select an include tag before selecting an exclude tag.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

Qualys Detection Score (QDS)

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

EC2/Azure/GCP metadata

Note: Ensure to enable the EC2 scanning and ensure this setting remains active. To enable this, reach out to your Technical Account Manager or Qualys Support.

Parameter	Description
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes. To retrieve information about the host instance type, use the metadata field, "instance-type".
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.

Parameter	Description
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Keep Alive Mechanism

The service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the host detection list API request. To keep the connection alive, the service sends some "dummy" data back to the client every 30 to 40 seconds if no "real" data has been sent already by the API during that time.

In XML output, this "dummy" data appears as a "<!-- keep-alive -->" line (since comments should be safely ignored by downstream XML parsers).

In CSV and CSV_NO_METADATA output, this "dummy" data appears as a <CR><LF> (carriage return, linefeed) pair (since empty lines clearly do not contain any CSV data).

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \--header 'X-Requested-With:
curl'--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
```

```
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
```

```
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List VM scanned hosts

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://
<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=lis
```

```
t&ips=10.10.40.10&truncation_limit=4">
  <HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
      <DATETIME>2024-03-28T09:03:45Z</DATETIME>
      <HOST_LIST>
        <HOST>
          <ID>4203254</ID>
          <IP>11.11.11.11</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <ASSET_GROUP_LIST />
          <NETWORK_ID>2458227</NETWORK_ID>
          <NETWORK_NAME>network1</NETWORK_NAME>
          <OS>
            <![CDATA[Windows XP]]>
          </OS>
          <DNS>
            <![CDATA[w2kserver-tmp3.vuln.example.com]]>
          </DNS>
          <DNS_DATA>
            <HOSTNAME>
              <![CDATA[w2kserver-tmp3]]>
            </HOSTNAME>
            <DOMAIN>
              <![CDATA[vuln.example.com]]>
            </DOMAIN>
            <FQDN>
              <![CDATA[w2kserver-tmp3.vuln.example.com]]>
            </FQDN>
          </DNS_DATA>
          <LAST_SCAN_DATETIME>2023-10-11T07:18:36Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>149</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>149</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>61198372</UNIQUE_VULN_ID>
              <QID>11</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>2</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[NameProgramVersionProtocolPort
portmap/rpcbind1000002-4tcp111
portmap/rpcbind1000002-4udp895
portmap/rpcbind1000002-4udp111]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
```

```
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>61198518</UNIQUE_VULN_ID>
              <QID>13361</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <PORT>22</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[User Nameroot
Authentication Schemepassword
ProtocolSSH Version 2
Discovery MethodLogin credentials provided by user
Using sudoNo
Key exchange algorithmdiffie-hellman-group-exchange-sha256
Host key algorithmssh-rsa
Compression algorithmzlib@openssh.com
Encryption algorithmaes128-ctr
MAC algorithmhmac-sha2-256
Authentication Record10.113.197.133]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
  </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host Detection XML Output, with truncation

A truncated response is returned when the API request returns more host records than the truncation limit. In this sample, the truncation limit is set to 100 host records.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100"
```

The Warning message in the XML output (shown below) indicates the URL you need to use to request the next 100 host records.

XML output:

```
...
          </DETECTION>
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
    <WARNING>
      <CODE>1980</CODE>
      <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>

<URL><![CDATA[<qualys_base_url>/api/3.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100&id_min=5641289]]></URL>
    </WARNING>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Filter superseded QIDs (filter_superseded_qids=1)

In this example any QID superseded by another QID has been filtered out of the results. The XML output includes QID 370584 and QID 370613. QID 370610 was filtered out because it was superseded by QID 370613.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/4.0/fo/asset/host/vm/detection/?action=list&filter_superseded_qids=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-03T10:22:34Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1145</ID>
        <IP>10.10.10.9</IP>
```

```
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[win2003.sample.qualys.com]]></DNS>
        <DNS_DATA>
            <HOSTNAME>
                <![CDATA[win2003]]>
            </HOSTNAME>
            <DOMAIN>
                <![CDATA[sample.qualys.com]]>
            </DOMAIN>
            <FQDN>
                <![CDATA[win2003.sample.qualys.com]]>
            </FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[LWIN2003HP1]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-01-08T19:50:18Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-01-08T19:36:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>619</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2017-11-15T16:58:16Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
<DETECTION>
            <QID>370584</QID>
            <UNIQUE_VULN_ID>45654</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
          <RESULTS><![CDATA[C:\Program Files\Mozilla Firefox\firefox.exe
Version is  42.0.0.0]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-10-
10T10:30:48Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>183</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-08-
27T22:48:04Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
<DETECTION>
            <QID>370613</QID>
            <UNIQUE_VULN_ID>43664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[C:\Program
Files\Google\Chrome\Application\33.0.1750.149\chrome.dll file version is
33.0.1750.149
%ProgramFiles%\Google\Chrome\Application\33.0.1750.149\chrome.dll file
```

```
version is 33.0.1750.149]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-11-
12T20:11:32Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>162</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-10-
30T22:28:59Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
</DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List assets with Qualys Detection Score (QDS)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
               <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
```

```
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS">
                     <![CDATA[9.3]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_version">
                      <![CDATA[v2]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="epss">
                       <![CDATA[0.24142]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_vector">
                       <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                 </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
```

```
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>          </DETECTION>
...
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - VM Detection API

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list&show_a
rf_data=1&arf_filter_keys=config-not- exploitable&truncation_limit=10' \
--header 'X-Requested-With: POSTMAN' \
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd>"
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-08-26T11:52:53Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>2454304</ID>
                    <IP>11.111.22.44</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>952199</NETWORK_ID>
                    <LAST_SCAN_DATETIME>2022-08-14T18:56:13Z
                    </LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2022-08-14T18:40:15Z
                    </LAST_VM_SCANNED_DATE>
                    <LAST_VM_SCANNED_DURATION>447</LAST_VM_
                    SCANNED_DURATION>
                    <DETECTION_LIST>
                          <DETECTION>
                             <UNIQUE_VULN_ID>35787259</UNIQUE_VULN_ID>
                             <QID>316406</QID>
                             <TYPE>Potential</TYPE>
                             <SEVERITY>3</SEVERITY>
                             <SSL>0</SSL>
                             <RESULTS>
                             <![CDATA[Package Installed Version
                             Required Version
                           firefox 31.3.0-3.el6.centos.x86_64 38.0-4.el6.
```

```
                                centos]]>
                                </RESULTS>
                                <STATUS>New</STATUS>
                                <FIRST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </FIRST_FOUND_DATETIME>
                                <LAST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </LAST_FOUND_DATETIME>
                                <TIMES_FOUND>1</TIMES_FOUND>
                                <LAST_TEST_DATETIME>2022-03-22T06:54:47Z
                                </LAST_TEST_DATETIME>
                                <LAST_UPDATE_DATETIME>2022-03-22T07:14:30Z
                                </LAST_UPDATE_DATETIME>
                                <IS_IGNORED>0</IS_IGNORED>
                                <IS_DISABLED>0</IS_DISABLED>
                                <AFFECT_EXPLOITABLE_CONFIG>0
                                </AFFECT_EXPLOITABLE_CONFIG>
                                <LAST_PROCESSED_DATETIME>2022-
                                0322T07:14:30Z</LAST_PROCESSED_DATETIME>
                            </DETECTION>
                        </DETECTION_LIST>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List Assets with Tag Details in the Response

API request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list
&ips=xx.xxx.xxx.xxx&show_tags=1' \--header 'X-Requested-With: curl'--
header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-03-17T09:40:25Z</DATETIME>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST_LIST>
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <HOST>
                    <ID>14125607</ID>
                    <IP>10.113.197.133</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Linux 2.6]]>
                    </OS>
```

```
                    <DNS>
                        <![CDATA[10-101-87-231.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[10-101-87-231]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[10-101-87-231.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <LAST_SCAN_DATETIME>2026-02-
26T08:23:48Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-02-
26T08:23:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>386</LAST_VM_SCANNED_DURATION>
                    <TAGS>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143644527]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_Demo]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143710805]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[BU2]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143651023]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[demo_BU]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143668042]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_AG]]>
                            </NAME>
                        </TAG>
                    </TAGS>
```

```
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467336</UNIQUE_VULN_ID>
                            <QID>38611</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>22</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467334</UNIQUE_VULN_ID>
                            <QID>38623</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
```

```
                        </DETECTION>
                    ...
                    ...
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - list MITRE ATT&CK Details

API Request

```
curl --location
'<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/?action=list
&show_arf_data=1&arf_filter_keys=config-not-
exploitable&truncation_limit=10' \ --header 'X-Requested-With:
POSTMAN' \
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-03-04T07:30:28Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST>
                <ID>6553022</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>AGENT</TRACKING_METHOD>
                <OS>
                    <![CDATA[Windows 10 Pro N 64 bit Edition Version
22H2]]>
                </OS>
                <DNS>
                    <![CDATA[solution2]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[solution2]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[SOLUTION2]]>
                </NETBIOS>
                <QG_HOSTID>
                    <![CDATA[311ee428-62a0-4604-b9f9-d874c1efbd88]]>
```

```
                </QG_HOSTID>
                <LAST_SCAN_DATETIME>2025-03-
04T04:08:01Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>238</LAST_VM_SCANNED_DURATION>
                <LAST_VM_AUTH_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_AUTH_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66009800</UNIQUE_VULN_ID>
                        <QID>378827</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files\VMware\VMware
Tools\vmtoolsd.exe  Version is  12.2.6.44976]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>credential-
access</MITRE_TACTIC_NAME>
                       <MITRE_TECHNIQUE_NAME>Exploitation for Credential
Access</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0006</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1212</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66010782</UNIQUE_VULN_ID>
                        <QID>380293</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
```

```
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement, execution,
privilege-escalation</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution, Exploitation for Privilege
Escalation</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002,
TA0004</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210, T1203,
T1068</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307447</UNIQUE_VULN_ID>
                        <QID>380734</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement,
execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210,
T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
```

```
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307454</UNIQUE_VULN_ID>
                        <QID>382524</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307462</UNIQUE_VULN_ID>
                        <QID>382691</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
```

```
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

More Samples

Qualys API - Host List Detection API samples (GitHub)

DTD

<platform API server>/api/4.0/fo/asset/host/vm/detection/dtd/output.dtd

V5.0

/api/5.0/fo/asset/host/vm/detection/

[GET] [POST]

Download a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. This data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information.

The Host List VM Detection API also shows the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score, EPSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Permissions - Managers view all VM scanned hosts in subscription. Auditors have no permission to view VM scanned hosts. Unit Managers view VM scanned hosts in the user's assigned business unit. Scanners and Readers view VM scanned hosts in the user's

account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

Note:

- If you experience delays or increased API response time when making requests to the VM Detection endpoint, you can provide the request without the id parameter, or use the id_min and id_max parameters in the request.

- When you generate or automate queries that require unique values across QIDs and assets, you may observe that the same Unique Vulnerability ID appears across multiple QIDs and assets. This is expected behavior by design. A Vulnerability has its own Unique Vulnerability ID, and an Information Gathering (IG) finding has its own Unique ID. In some cases, both may share the same ID. To ensure accurate identification and avoid duplicates, use a combination of Unique Vulnerability ID and QID.

Express Lite - This API is available to Express Lite users.

Input Parameters

The input parameter **`action=list`** is required. All other input parameters are optional. Several filtering parameters are provided for filtering hosts and QIDs. When multiple filter parameters are specified, the service combines the effects of all the parameters in a way that corresponds to a logical “AND”. So if two filter parameters are specified in the request, the service returns hosts that match both filters.

Quick Links: Detection Filters | Host Filters | QID Filters | Asset tags | Qualys Detection Score (QDS) | EC2/Azure/GCP metadata

API Request

Parameter	Description
action=list	(Required)
os_hostname={0|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List Detection API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={0|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
show_host_service={0|1}	(Optional) When specified, the service tag of the scanned hosts is displayed in the output. The default value of this parameter is set to 0. When set to 1, the service tag of the scanned hosts is displayed in the output.
arf_filter_keys={value}	(Optional) Accepts one of these values: non-running-kernel, non-running-service, and config-not-exploitable. You can apply these values independently or in any combination to refine their filter criteria. For instance, you can use non-running-kernel and non-running-service values together. **Note:** You can use either this input parameter or arf_kernel_filter input parameter.

Parameter	Description
show_arf_data={0|1}	(Optional) Displays the ARF-affected QIDs, with the value as (1/0). If user passes value as 0, it does not show the ARF filter output data in the output, and if the user passes value as 1, it shows the ARF filter output data in the output.
include_vuln_type={confirmed|potential}	(Optional)Use to download vulnerability information based on their type, confirmed or potential. Specify: `include_vuln_type=confirmed` to download only confirmed vulnerabilities. `include_vuln_type=potential` to download only potential vulnerabilities. Exceptional Scenarios • After passing the parameter value include_vuln_type=confirmed, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase. • After passing the parameter value include_vuln_type=potential, some confirmed vulnerabilities show up in the API response. • This happens with the vulnerabilities assigned with a half red/half yellow severity level. • After passing the parameter value include_vuln_type=confirmed, some confirmed vulnerabilities may not be shown in API response. This will happen when vulnerabilities are assigned with a half red/half yellow severity level. • This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.

Detection Filters

Parameter	Description
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0.
show_results={0|**1**}	(Optional) When not specified, results are included in the output. Specify show_results=0 to exclude the results. If you exclude the results, CSV will have an empty Results column, and XML will not contain the Results tag.
show_reopened_info={**0**|1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify show_reopened_info=1 to include reopened info i.e. first/last reopened date, times reopened.

Parameter	Description
arf_kernel_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running Linux kernels. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Info Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for each detection. When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for each detection. When set to 4, only include kernel related vulnerabilities. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
arf_service_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running ports/services. When unspecified, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> does not appear in the output. When set to 0, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities. When set to 1, exclude service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities that have a value of 1. When set to 2, only include service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 for each detection. When set to 3, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 1 for each detection. When set to 4, only include service related vulnerabilities. <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.

Parameter	Description
arf_config_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration. When unspecified, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> does not appear in the output. When set to 0, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related vulnerabilities. When set to 1, exclude vulnerabilities that are exploitable due to host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related detections that have a value of 1. When set to 2, only include config related vulnerabilities that are exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 for each detection. When set to 3, only include config related vulnerabilities that are not exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 1 for each detection. When set to 4, only include config related vulnerabilities. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities that may or may not be exploitable due to the current host configuration.

Parameter	Description
active_kernels_only={0|1|2|3}	Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag <AFFECT_RUNNING_KERNEL>. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Information Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities. When set to 3, only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
output_format={**XML**|CSV|CSV_NO_METADATA|CSV_NO_METADATA_MS_EXCEL|CSV_MS_EXCEL}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. Valid values are: XML, CSV or CSV_NO_METADATA, CSV_NO_METADATA_MS_EXCEL and CSV_MS_EXCEL XML (default) - Specifies XML format for the output. CSV - Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA - Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. CSV_NO_METADATA_MS_EXCEL - When specified we will use CSV format for the output with no metadata with MS Excel restrictions on the maximum length allowed for a string value in the output. CSV_MS_EXCEL - When specified we will use CSV format for the output with MS Excel restriction on the maximum length allowed for a string value in the output. A value in the output will be truncated if the length of the value exceeds the maximum length supported in MS Excel.
suppress_duplicated_data_from_csv={**0**|1}	(Optional) By default or when set to 0, host details will be repeated in each line of detection information in the CSV output. When set to 1, host details will not be repeated (suppressed) in each detection line. This parameter must be specified with: output_format=CSV or output_format=CSV_NO_METADATA. **Note**: When set to 1, EC2 details are displayed in the Cloud Resource metadata column and the EC2 column is set bank in CSV output, if you have Azure/GCP enabled.

Parameter	Description
truncation_limit={value}	(Optional) Specifies the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). Specify 0 for no truncation limit. If the requested list identifies more host records than the truncation limit and output_format=XML, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. If the requested list identifies more host records than the truncation limit and output_format=CSV, then the CSV output includes "Truncated" in the FOOTER_CSV section and the URL for making another request for the next batch of host records. Check API samples (2, 4, 16) Qualys API - Host List Detection API samples (GitHub) **Note:** When you launch the API with the truncation limit set to 0 or not specified, it is recommended to use a specific and limited range of IPs or IDs to avoid performance issues. Launching the API without specifying IPs or IDs may result in performance lag.
max_days_since_detection_updated={value}	(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_updated_since={value}	(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2017-02-15" or "2017-02-15T23:15:00Z". Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated

Parameter	Description
detection_updated_before={value}	
	(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_processed_before={date}	
	(Optional) Show detections with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_processed_after={date}	
	(Optional) Show detections with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_last_tested_since={date}	
	(Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range. This parameter cannot be specified in the same request as detection_last_tested_since_days.
detection_last_tested_since_days={value}	
	(Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.

Parameter	Description
	This parameter cannot be specified in the same request as detection_last_tested_since.
detection_last_tested_before={date}	(Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before_days.
detection_last_tested_before_days={value}	(Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before.
include_ignored={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were ignored during detection. Specify include_ignored=1 to include results in the output.
include_disabled={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were disabled during detection. Specify include_disabled=1 to include results in the output.

Host Filters

Parameter	Description
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example: 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value (for example: If id_min=44286508, then hosts with Ids 44286508 & higher value are displayed).

Parameter	Description
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required for example: If id_max=44286508, then hosts with Ids 44286508 & lower value are displayed).
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example: 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example: 386941-386945). Valid asset group IDs are required.
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
network_name={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account.) Displays the name of the network corresponding to the network ID. The name will be displayed only if you subscribe to it and the tweak is enabled at the backend.
vm_scan_since={date}	(Optional) Show hosts scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.

Parameter	Description
no_vm_scan_since={date}	(Optional) Show hosts not scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”.
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
max_days_since_last_vm_scan={value}	
	(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.
	This parameter cannot be specified with any of these parameters in the same request: vm_scan_since and no_vm_scan_since.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_scan_date_before=date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.

Parameter	Description
status={value}	(Optional) Show only hosts with one or more of these status values: New, Active, Re-Opened, Fixed. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with New, Active or Re-Opened <STATUS> only. To get hosts with Fixed status, check this API sample Qualys API - Host List Detection API samples (GitHub, sample 11)
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list compliance hosts in the user's account that have been scanned and processed. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Note: If either the Information Gathered (IG) processed date or the vulnerability processed date is missing or null for a host, the host will still be included in the results when using the parameters vm_processed_before and show_igs=1 in the Host List Detection (HLD) API.

However, if show_igs=0 or is not specified along with vm_processed_before, the API will behave as before, excluding hosts where either IG processed date or the vulnerability processed date value is null.

QID Filters

Parameter	Description
qids={value}	(Optional) Show only detection records with certain QIDs. One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma separated. Valid QIDs are required.
severities={value}	(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example: 1-3). Multiple entries are comma separated.
filter_superseded_qids={0|1}	(Optional) When unspecified or set to 0, the XML output includes all QIDs even if they've been superseded. Specify 1 to filter out QIDs that have been superseded by another QID in the results.
show_igs={0|1}	(Optional except as noted) Specify 1 to show detection records with information gathered along with confirmed vulnerabilities and potential vulnerabilities. Specify 0 (default) to hide information gathered.
	The show_igs parameter is required in one use case. The parameter show_igs=1 must be specified if both these conditions are met: 1) search lists are included using the parameter include_search_list_titles or include_search_list_ids, and 2) if the included search lists contain only information gathered.
include_search_list_titles={value}	(Optional) Show detection records only when a record's QID is INCLUDED IN in one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_ids.
exclude_search_list_titles={value}	(Optional) Show detection records only when a record's QID is IS EXCLUDED from one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_ids.
include_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS INCLUDED in one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 10-15). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_titles.

Parameter	Description
exclude_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS EXCLUDED from one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 40-42). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_titles.

Asset tags

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. **Note:** You must select an include tag before selecting an exclude tag.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

Qualys Detection Score (QDS)

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

EC2/Azure/GCP metadata

Note: Ensure to enable the EC2 scanning and ensure this setting remains active. To enable this, reach out to your Technical Account Manager or Qualys Support.

Parameter	Description
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes. To retrieve information about the host instance type, use the metadata field, "instance-type".
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.

Parameter	Description
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Keep Alive Mechanism

The service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the host detection list API request. To keep the connection alive, the service sends some "dummy" data back to the client every 30 to 40 seconds if no "real" data has been sent already by the API during that time.

In XML output, this "dummy" data appears as a "<!-- keep-alive -->" line (since comments should be safely ignored by downstream XML parsers).

In CSV and CSV_NO_METADATA output, this "dummy" data appears as a <CR><LF> (carriage return, linefeed) pair (since empty lines clearly do not contain any CSV data).

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \--header 'X-Requested-With:
curl'--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
```

```
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
```

```
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List VM scanned hosts

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://
<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=lis
```

```
t&ips=10.10.40.10&truncation_limit=4">
  <HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
      <DATETIME>2024-03-28T09:03:45Z</DATETIME>
      <HOST_LIST>
        <HOST>
          <ID>4203254</ID>
          <IP>11.11.11.11</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <ASSET_GROUP_LIST />
          <NETWORK_ID>2458227</NETWORK_ID>
          <NETWORK_NAME>network1</NETWORK_NAME>
          <OS>
            <![CDATA[Windows XP]]>
          </OS>
          <DNS>
            <![CDATA[w2kserver-tmp3.vuln.example.com]]>
          </DNS>
          <DNS_DATA>
            <HOSTNAME>
              <![CDATA[w2kserver-tmp3]]>
            </HOSTNAME>
            <DOMAIN>
              <![CDATA[vuln.example.com]]>
            </DOMAIN>
            <FQDN>
              <![CDATA[w2kserver-tmp3.vuln.example.com]]>
            </FQDN>
          </DNS_DATA>
          <LAST_SCAN_DATETIME>2023-10-11T07:18:36Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>149</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>149</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>61198372</UNIQUE_VULN_ID>
              <QID>11</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>2</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[NameProgramVersionProtocolPort
portmap/rpcbind1000002-4tcp111
portmap/rpcbind1000002-4udp895
portmap/rpcbind1000002-4udp111]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
```

```
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>61198518</UNIQUE_VULN_ID>
              <QID>13361</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <PORT>22</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[User Nameroot
Authentication Schemepassword
ProtocolSSH Version 2
Discovery MethodLogin credentials provided by user
Using sudoNo
Key exchange algorithmdiffie-hellman-group-exchange-sha256
Host key algorithmssh-rsa
Compression algorithmzlib@openssh.com
Encryption algorithmaes128-ctr
MAC algorithmhmac-sha2-256
Authentication Record10.113.197.133]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
  </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host Detection XML Output, with truncation

A truncated response is returned when the API request returns more host records than the truncation limit. In this sample, the truncation limit is set to 100 host records.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100"
```

The Warning message in the XML output (shown below) indicates the URL you need to use to request the next 100 host records.

XML output:

```
...
          </DETECTION>
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
    <WARNING>
      <CODE>1980</CODE>
      <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>

<URL><![CDATA[<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100&id_min=5641289]]></URL>
    </WARNING>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Filter superseded QIDs (filter_superseded_qids=1)

In this example any QID superseded by another QID has been filtered out of the results. The XML output includes QID 370584 and QID 370613. QID 370610 was filtered out because it was superseded by QID 370613.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/5.0/fo/asset/host/vm/detection/?action=list&filter_superseded_qids=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-03T10:22:34Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1145</ID>
        <IP>10.10.10.9</IP>
```

```
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[win2003.sample.qualys.com]]></DNS>
        <DNS_DATA>
            <HOSTNAME>
                <![CDATA[win2003]]>
            </HOSTNAME>
            <DOMAIN>
                <![CDATA[sample.qualys.com]]>
            </DOMAIN>
            <FQDN>
                <![CDATA[win2003.sample.qualys.com]]>
            </FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[LWIN2003HP1]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-01-08T19:50:18Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-01-08T19:36:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>619</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2017-11-15T16:58:16Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
<DETECTION>
            <QID>370584</QID>
            <UNIQUE_VULN_ID>45654</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
          <RESULTS><![CDATA[C:\Program Files\Mozilla Firefox\firefox.exe
Version is  42.0.0.0]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-10-
10T10:30:48Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>183</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-08-
27T22:48:04Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
<DETECTION>
            <QID>370613</QID>
            <UNIQUE_VULN_ID>43664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[C:\Program
Files\Google\Chrome\Application\33.0.1750.149\chrome.dll file version is
33.0.1750.149
%ProgramFiles%\Google\Chrome\Application\33.0.1750.149\chrome.dll file
```

```
version is 33.0.1750.149]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-11-
12T20:11:32Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>162</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-10-
30T22:28:59Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
</DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List assets with Qualys Detection Score (QDS)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
               <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
```

```
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS">
                     <![CDATA[9.3]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_version">
                      <![CDATA[v2]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="epss">
                       <![CDATA[0.24142]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_vector">
                       <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                 </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
```

```
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>          </DETECTION>
...
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - VM Detection API

API request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&show_a
rf_data=1&arf_filter_keys=config-not- exploitable&truncation_limit=10' \
--header 'X-Requested-With: POSTMAN' \
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd>"
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-08-26T11:52:53Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>2454304</ID>
                    <IP>11.xxx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>952199</NETWORK_ID>
                    <LAST_SCAN_DATETIME>2022-08-14T18:56:13Z
                    </LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2022-08-14T18:40:15Z
                    </LAST_VM_SCANNED_DATE>
                    <LAST_VM_SCANNED_DURATION>447</LAST_VM_
                    SCANNED_DURATION>
                    <DETECTION_LIST>
                          <DETECTION>
                             <UNIQUE_VULN_ID>35787259</UNIQUE_VULN_ID>
                             <QID>316406</QID>
                             <TYPE>Potential</TYPE>
                             <SEVERITY>3</SEVERITY>
                             <SSL>0</SSL>
                             <RESULTS>
                             <![CDATA[Package Installed Version
                             Required Version
                           firefox 31.3.0-3.el6.centos.x86_64 38.0-4.el6.
```

```
                                centos]]>
                                </RESULTS>
                                <STATUS>New</STATUS>
                                <FIRST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </FIRST_FOUND_DATETIME>
                                <LAST_FOUND_DATETIME>2022-03-22T06:54:47Z
                                </LAST_FOUND_DATETIME>
                                <TIMES_FOUND>1</TIMES_FOUND>
                                <LAST_TEST_DATETIME>2022-03-22T06:54:47Z
                                </LAST_TEST_DATETIME>
                                <LAST_UPDATE_DATETIME>2022-03-22T07:14:30Z
                                </LAST_UPDATE_DATETIME>
                                <IS_IGNORED>0</IS_IGNORED>
                                <IS_DISABLED>0</IS_DISABLED>
                                <AFFECT_EXPLOITABLE_CONFIG>0
                                </AFFECT_EXPLOITABLE_CONFIG>
                                <LAST_PROCESSED_DATETIME>2022-
                                0322T07:14:30Z</LAST_PROCESSED_DATETIME>
                            </DETECTION>
                        </DETECTION_LIST>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List Assets with Tag Details in the Response

API request:

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list
&ips=xx.xxx.xxx.xxx&show_tags=1' \--header 'X-Requested-With: curl'--
header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-03-17T09:40:25Z</DATETIME>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST_LIST>
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <HOST>
                    <ID>14125607</ID>
                    <IP>10.113.197.133</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Linux 2.6]]>
                    </OS>
```

```
                    <DNS>
                        <![CDATA[10-101-87-231.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[10-101-87-231]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
                            <![CDATA[10-101-87-231.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <LAST_SCAN_DATETIME>2026-02-
26T08:23:48Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-02-
26T08:23:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>386</LAST_VM_SCANNED_DURATION>
                    <TAGS>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143644527]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_Demo]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143710805]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[BU2]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143651023]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[demo_BU]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143668042]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_AG]]>
                            </NAME>
                        </TAG>
                    </TAGS>
```

```
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467336</UNIQUE_VULN_ID>
                            <QID>38611</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>22</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467334</UNIQUE_VULN_ID>
                            <QID>38623</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
```

```
                        </DETECTION>
                    ...
                    ...
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - list MITRE ATT&CK Details

API Request

```
curl --location
'<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list
&show_arf_data=1&arf_filter_keys=config-not-
exploitable&truncation_limit=10' \ --header 'X-Requested-With:
POSTMAN' \
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-03-04T07:30:28Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST>
                <ID>6553022</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>AGENT</TRACKING_METHOD>
                <OS>
                    <![CDATA[Windows 10 Pro N 64 bit Edition Version
22H2]]>
                </OS>
                <DNS>
                    <![CDATA[solution2]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[solution2]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[SOLUTION2]]>
                </NETBIOS>
                <QG_HOSTID>
                    <![CDATA[311ee428-62a0-4604-b9f9-d874c1efbd88]]>
```

```
                </QG_HOSTID>
                <LAST_SCAN_DATETIME>2025-03-
04T04:08:01Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>238</LAST_VM_SCANNED_DURATION>
                <LAST_VM_AUTH_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_AUTH_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66009800</UNIQUE_VULN_ID>
                        <QID>378827</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files\VMware\VMware
Tools\vmtoolsd.exe  Version is  12.2.6.44976]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>credential-
access</MITRE_TACTIC_NAME>
                       <MITRE_TECHNIQUE_NAME>Exploitation for Credential
Access</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0006</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1212</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66010782</UNIQUE_VULN_ID>
                        <QID>380293</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
```

```
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement, execution,
privilege-escalation</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution, Exploitation for Privilege
Escalation</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002,
TA0004</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210, T1203,
T1068</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307447</UNIQUE_VULN_ID>
                        <QID>380734</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement,
execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210,
T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
```

```
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307454</UNIQUE_VULN_ID>
                        <QID>382524</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307462</UNIQUE_VULN_ID>
                        <QID>382691</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
```

```
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Display the highest contributing CVEs and associated risk factor

API Request

```
curl --location --request POST '
<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/?action=list&
show_qds_factors=1&show_qds=1
--header 'X-Requested-With: xxx' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2025-10-23T05:42:36Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>6885606</ID>
                    <IP>10.xx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Windows 2012 R2 Standard]]>
                    </OS>
                    <DNS>
                        <![CDATA[wdw2012r2ntlm]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[wdw2012r2ntlm]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
```

```
                        <![CDATA[WDW2012R2NTLM]]>
                    </NETBIOS>
                    <LAST_SCAN_DATETIME>2024-06-
02T05:14:11Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-06-
02T05:14:03Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>570</LAST_VM_SCANNED_DURATION>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>89625105</UNIQUE_VULN_ID>
                            <QID>90882</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>3389</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                              <![CDATA[RDP Supported Encryption methods:
RC4(40 bit),RC4(56 bit)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-04-
19T10:14:24Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2024-06-
02T05:14:03Z</LAST_FOUND_DATETIME>
                            <QDS severity="LOW">30</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[No_Patch,High_Data_Loss]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[4.7]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="QID_severity">
                                    <![CDATA[3.0]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[90882]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>2</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2024-06-
02T05:14:03Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2024-06-
02T05:14:11Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2024-06-
02T05:14:11Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
```

```
                    </DETECTION_LIST>
                </HOST>
                <HOST>
                    <ID>6885818</ID>
                    <IP>10.xx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Windows 7 Ultimate]]>
                    </OS>
                    <DNS>
                        <![CDATA[pat-65-37]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[pat-65-37]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[PAT-65-37]]>
                    </NETBIOS>
                    <LAST_SCAN_DATETIME>2025-10-
22T14:06:29Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2025-10-
22T14:06:22Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>863</LAST_VM_SCANNED_DURATION>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073263</UNIQUE_VULN_ID>
                            <QID>90783</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>5</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[QID: 90783 detected on port 3389
over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="CRITICAL">95</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[dos]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="exploit_maturity">
                                    <![CDATA[poc,weaponized]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_name">
```

```
<![CDATA[SlowLoris,Generic,Heuristic,FlyStudio]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[9.3]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="epss">
                                    <![CDATA[0.8547]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_vector">
                                   <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[9bd81d4142a4cd962727332e09982d4df588e777321b442c174c69114becbcbf
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[226f7341be64b865955bbe2d339ad28c49bbec08bb9e4086f3c98e03e5409b4c
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[83d9e97bc58123ae1842fa3e9f8d19ee685170a94588ff4df81cadaedaf27c87
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[a58bcf58422572184759fe64c1746b1cd7a8af5cb8826b76dfeefe6dc7cd6f04
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[1038f183ff1d11066c427923756705c5959d3665fd2726d842ad55ee3c133c30
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[181b169328a15072938c5759392a4d288caea1382460cda636b37a6aadce0d4c
]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[CVE-2012-0002]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>557</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
```

```
                            <LAST_FIXED_DATETIME>2025-09-
27T14:09:05Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073265</UNIQUE_VULN_ID>
                            <QID>90882</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>3389</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                              <![CDATA[RDP Supported Encryption methods:
RC4(40 bit),RC4(56 bit)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="LOW">30</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[No_Patch,High_Data_Loss]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[4.7]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="QID_severity">
                                    <![CDATA[3.0]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[90882]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>558</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
                            <LAST_FIXED_DATETIME>2023-08-
29T13:30:08Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
```

```
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073262</UNIQUE_VULN_ID>
                            <QID>91541</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>5</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                               <![CDATA[Microsoft Windows Remote Desktop
Services Remote Code Execution Vulnerability Detected (BlueKeep)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="CRITICAL">100</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[remote,dos]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="exploit_maturity">
                                    <![CDATA[weaponized,poc]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_name">

<![CDATA[Lockbit,Redkeeper,Unattributed,Doppelpaymer,Netwalker,Mailto]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="threat_actors">
                                    <![CDATA[Velvet Chollima,Silent
Chollima,Wizard Spider,Unattributed,Invisimole,Vicious
Panda,Microcin,Larva-24005,Emennet Pasargad,China Attribution]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_vuln">
                                    <![CDATA[YES]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[10.0]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="epss">
                                    <![CDATA[0.94445]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="trending">

<![CDATA[10102025,10052025,10072025,10122025,10032025,10042025,09252025,1
0082025,10062025,09242025,09282025,10132025,10142025,09272025,10012025,09
292025,10152025]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_vector">
                                   <![CDATA[AV:N/AC:L/Au:N/C:C/I:C/A:C]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">
```

```
<![CDATA[9966826ada8b1f366a9e7b9b1e7c430a2a49dda60eb7025c7481295e3ab7f9e4
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[8b561784fb52edcdd86adf387c9e2cb152aec027c14cafbee60957b50af7d550
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[28fb99f0193d20d3fff6c40b9b85c0c4b5073166ca50ec83e85c276f4fab8647
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[8402e053d5ad4e21c2c96a04e117d113f7bbdb295e2c55dcf8b94054d83fc1af
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[d4e2240c194c291d9c98454dca2c040902146def53bdee9900f1b9724d418268
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[76991e2f91e7ac9066c94489fdd332ea8e15995a15eabc29647920366e5591b5
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_DUE_DATE">
                                    <![CDATA[1651536000000]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_ADDED_DATE">
                                    <![CDATA[1635897600000]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[CVE-2019-0708]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>543</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
                            <LAST_FIXED_DATETIME>2025-09-
27T14:09:05Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
```

```
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

More Samples

Qualys API - Host List Detection API samples (GitHub)

DTD

<platform API server>/api/5.0/fo/asset/host/vm/detection/dtd/output.dtd

V6.0

/api/6.0/fo/asset/host/vm/detection/

[GET] [POST]

Download a list of hosts with the hosts latest vulnerability data, based on the host based scan data available in the user's account. This data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information.

The Host List VM Detection API also shows the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score, EPSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Permissions - Managers view all VM scanned hosts in subscription. Auditors have no permission to view VM scanned hosts. Unit Managers view VM scanned hosts in the user's assigned business unit. Scanners and Readers view VM scanned hosts in the user's account. Please note that this API only returns information for hosts that are assigned to each user through asset groups in VM/VMDR. When Tag-based user scoping (TBUS) is enabled, hosts that are in scope can be retrieved using asset tag-related parameters through TBUS.

Note:

- If you experience delays or increased API response time when making requests to the VM Detection endpoint, you can provide the request without the id parameter, or use the id_min and id_max parameters in the request.

- When you generate or automate queries that require unique values across QIDs and assets, you may observe that the same Unique Vulnerability ID appears across multiple QIDs and assets. This is expected behavior by design. A Vulnerability has its own Unique Vulnerability ID, and an Information Gathering (IG) finding has its own Unique ID. In some cases, both may share the same ID. To ensure accurate identification and avoid duplicates, use a combination of Unique Vulnerability ID and QID.

Express Lite - This API is available to Express Lite users.

Input Parameters

The input parameter **`action=list`** is required. All other input parameters are optional. Several filtering parameters are provided for filtering hosts and QIDs. When multiple filter parameters are specified, the service combines the effects of all the parameters in a way that corresponds to a logical "AND". So if two filter parameters are specified in the request, the service returns hosts that match both filters.

Quick Links: Detection Filters | Host Filters | QID Filters | Asset tags | Qualys Detection Score (QDS) | EC2/Azure/GCP metadata

API Request

Parameter	Description
action=list	(Required)
os_hostname={0|1}	(Optional) Specify 1 to view the OS hostname in the XML output of Host List Detection API request. Else, OS hostname is not displayed in the XML output. By default this parameter is set to 0.
echo_request={0|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
show_asset_id={**0**|1}	(Optional) When specified, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
show_host_service={0|1}	(Optional) When specified, the service tag of the scanned hosts is displayed in the output. The default value of this parameter is set to 0. When set to 1, the service tag of the scanned hosts is displayed in the output.
arf_filter_keys={value}	(Optional) Accepts one of these values: non-running-kernel, non-running-service, and config-not-exploitable. You can apply these values independently or in any combination to refine their filter criteria. For instance, you can use non-running-kernel and non-running-service values together. **Note:** You can use either this input parameter or arf_kernel_filter input parameter.

Parameter	Description
show_arf_data={0|1}	(Optional) Displays the ARF-affected QIDs, with the value as (1/0). If user passes value as 0, it does not show the ARF filter output data in the output, and if the user passes value as 1, it shows the ARF filter output data in the output.
include_vuln_type={confirmed|potential}	(Optional)Use to download vulnerability information based on their type, confirmed or potential. Specify: `include_vuln_type=confirmed` to download only confirmed vulnerabilities. `include_vuln_type=potential` to download only potential vulnerabilities. Exceptional Scenarios • After passing the parameter value include_vuln_type=confirmed, some potential vulnerabilities may show up in the API response. This happens when the vulnerability type for the QID is modified in the Qualys KnowledgeBase. • After passing the parameter value include_vuln_type=potential, some confirmed vulnerabilities show up in the API response. • This happens with the vulnerabilities assigned with a half red/half yellow severity level. • After passing the parameter value include_vuln_type=confirmed, some confirmed vulnerabilities may not be shown in API response. This will happen when vulnerabilities are assigned with a half red/half yellow severity level. • This happens when the vulnerability type for the QID is changed while running the authenticated scan. It is because of various factors affecting scan results.

Detection Filters

Parameter	Description
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0.
show_results={0|**1**}	(Optional) When not specified, results are included in the output. Specify show_results=0 to exclude the results. If you exclude the results, CSV will have an empty Results column, and XML will not contain the Results tag.
show_reopened_info={**0**|1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify show_reopened_info=1 to include reopened info i.e. first/last reopened date, times reopened.

Parameter	Description
arf_kernel_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running Linux kernels. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Info Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for each detection. When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for each detection. When set to 4, only include kernel related vulnerabilities. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
arf_service_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities found on running or non-running ports/services. When unspecified, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> does not appear in the output. When set to 0, vulnerabilities are not filtered based on running ports/services. <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities. When set to 1, exclude service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output for service related vulnerabilities that have a value of 1. When set to 2, only include service related vulnerabilities that are exploitable (found on running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 for each detection. When set to 3, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). <AFFECT_RUNNING_SERVICE> appears in the output with a value of 1 for each detection. When set to 4, only include service related vulnerabilities. <AFFECT_RUNNING_SERVICE> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities found on running or non-running Linux kernels.

Parameter	Description
arf_config_filter={0|1|2|3|4}	(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration. When unspecified, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> does not appear in the output. When set to 0, vulnerabilities are not filtered based on host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related vulnerabilities. When set to 1, exclude vulnerabilities that are exploitable due to host configuration. <AFFECT_EXPLOITABLE_CONFIG> appears in the output for config related detections that have a value of 1. When set to 2, only include config related vulnerabilities that are exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 for each detection. When set to 3, only include config related vulnerabilities that are not exploitable. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 1 for each detection. When set to 4, only include config related vulnerabilities. <AFFECT_EXPLOITABLE_CONFIG> appears in the output with a value of 0 or 1 for each detection. **Note:** You can use this parameter or arf_filter_keys to Identify vulnerabilities that may or may not be exploitable due to the current host configuration.

Parameter	Description
active_kernels_only={0|1|2|3}	Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag <AFFECT_RUNNING_KERNEL>. Good to Know - It's possible that multiple kernels are detected on a single Linux host. You'll notice the scan results report the running kernel on each Linux host in Information Gathered QID 45097. When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities. When set to 0, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 1, exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities. When set to 2, only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities. When set to 3, only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.
	Note that active_kernels_only is deprecated and will be removed in a future release. Please use arf_kernel_filter instead.

Parameter	Description
output_format={**XML**|CSV|CSV_NO_METADATA|CSV_NO_METADATA_MS_EXCEL|CSV_MS_EXCEL}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. Valid values are: XML, CSV or CSV_NO_METADATA, CSV_NO_METADATA_MS_EXCEL and CSV_MS_EXCEL XML (default) - Specifies XML format for the output. CSV - Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA - Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. CSV_NO_METADATA_MS_EXCEL - When specified we will use CSV format for the output with no metadata with MS Excel restrictions on the maximum length allowed for a string value in the output. CSV_MS_EXCEL - When specified we will use CSV format for the output with MS Excel restriction on the maximum length allowed for a string value in the output. A value in the output will be truncated if the length of the value exceeds the maximum length supported in MS Excel.
suppress_duplicated_data_from_csv={**0**|1}	(Optional) By default or when set to 0, host details will be repeated in each line of detection information in the CSV output. When set to 1, host details will not be repeated (suppressed) in each detection line. This parameter must be specified with: output_format=CSV or output_format=CSV_NO_METADATA. **Note**: When set to 1, EC2 details are displayed in the Cloud Resource metadata column and the EC2 column is set bank in CSV output, if you have Azure/GCP enabled.

Parameter	Description
truncation_limit={value}	(Optional) Specifies the maximum number of host records processed per request. When not specified, the truncation limit is set to 1000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). Specify 0 for no truncation limit. If the requested list identifies more host records than the truncation limit and output_format=XML, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of host records. If the requested list identifies more host records than the truncation limit and output_format=CSV, then the CSV output includes "Truncated" in the FOOTER_CSV section and the URL for making another request for the next batch of host records. Check API samples (2, 4, 16) Qualys API - Host List Detection API samples (GitHub) **Note:** When you launch the API with the truncation limit set to 0 or not specified, it is recommended to use a specific and limited range of IPs or IDs to avoid performance issues. Launching the API without specifying IPs or IDs may result in performance lag.
max_days_since_detection_updated={value}	(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_updated_since={value}	(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2017-02-15" or "2017-02-15T23:15:00Z". Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated

Parameter	Description
detection_updated_before={value}	
	(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated
detection_processed_before={date}	
	(Optional) Show detections with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_processed_after={date}	
	(Optional) Show detections with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
detection_last_tested_since={date}	
	(Optional) Show only detections that were last tested on or after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a date range. This parameter cannot be specified in the same request as detection_last_tested_since_days.
detection_last_tested_since_days={value}	
	(Optional) Show only detections that were last tested within the number of days you specify. For example, show detections last tested in the past 10 days. You can use this parameter in conjunction with detection_last_tested_before or detection_last_tested_before_days to limit the detections shown to a specific date range.

Parameter	Description
	This parameter cannot be specified in the same request as detection_last_tested_since.
detection_last_tested_before={date}	(Optional) Show only detections that were last tested before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2018-07-01” or “2018-01-25T23:12:00Z”. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before_days.
detection_last_tested_before_days={value}	(Optional) Show only detections that were last tested before the number of days you specify. For example, show detections last tested more than 30 days ago. You can use this parameter in conjunction with detection_last_tested_since or detection_last_tested_since_days to limit the detections shown to a specific date range.
	This parameter cannot be specified in the same request as detection_last_tested_before.
include_ignored={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were ignored during detection. Specify include_ignored=1 to include results in the output.
include_disabled={0|1}	(Optional) Use this parameter to include or exclude the QIDs that were disabled during detection. Specify include_disabled=1 to include results in the output.

Host Filters

Parameter	Description
ids={value}	(Optional) Show only certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example: 190-400).Valid host IDs are required.
id_min={value}	(Optional) Show only hosts which have a minimum host ID value (for example: If id_min=44286508, then hosts with Ids 44286508 & higher value are displayed).

Parameter	Description
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required for example: If id_max=44286508, then hosts with Ids 44286508 & lower value are displayed).
ips={value}	(Optional) Show only certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example: 10.10.10.1-10.10.10.100).
ipv6={value}	(Optional) A valid IPv6 address. Multiple entries are comma separated. If ipv6 is used as filter parameter then other target input filter parameters are not accepted.
ag_ids={value}	(Optional) Show only hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example: 386941-386945). Valid asset group IDs are required.
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
ag_titles={value}	(Optional) Show only hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group).
	The ag_ids and ag_titles parameters are mutually exclusive and cannot be specified together in the same request.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
network_name={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account.) Displays the name of the network corresponding to the network ID. The name will be displayed only if you subscribe to it and the tweak is enabled at the backend.
vm_scan_since={date}	(Optional) Show hosts scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
	This parameter cannot be specified with max_days_since_vm_scan in the same request.

Parameter	Description
no_vm_scan_since={date}	(Optional) Show hosts not scanned and processed since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”.
	This parameter cannot be specified with max_days_since_vm_scan in the same request.
max_days_since_last_vm_scan={value}	
	(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.
	This parameter cannot be specified with any of these parameters in the same request: vm_scan_since and no_vm_scan_since.
vm_processed_before={date}	(Optional) Show hosts with vulnerability scan results processed before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_processed_after={date}	(Optional) Show hosts with vulnerability scan results processed after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_scan_date_before=date}	(Optional) Show hosts with a vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_scan_date_after={date}	(Optional) Show hosts with a vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_before={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date before a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.
vm_auth_scan_date_after={date}	(Optional) Show hosts with a successful authenticated vulnerability scan end date after a certain date and time. Specify the date in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2016-09-12” or “2016-09-12T23:15:00Z”.

Parameter	Description
status={value}	(Optional) Show only hosts with one or more of these status values: New, Active, Re-Opened, Fixed. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with New, Active or Re-Opened <STATUS> only. To get hosts with Fixed status, check this API sample Qualys API - Host List Detection API samples (GitHub, sample 11)
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. This parameter is invalid for an Express Lite user. Specify 1 to list compliance hosts in the user's account that have been scanned and processed. These hosts are assigned to the policy compliance module. Specify 0 to list scanned hosts which are not assigned to the policy compliance module.
os_pattern={expression}	(Optional) Show only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Note: If either the Information Gathered (IG) processed date or the vulnerability processed date is missing or null for a host, the host will still be included in the results when using the parameters vm_processed_before and show_igs=1 in the Host List Detection (HLD) API.

However, if show_igs=0 or is not specified along with vm_processed_before, the API will behave as before, excluding hosts where either IG processed date or the vulnerability processed date value is null.

QID Filters

Parameter	Description
qids={value}	(Optional) Show only detection records with certain QIDs. One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma separated. Valid QIDs are required.
severities={value}	(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example: 1-3). Multiple entries are comma separated.
filter_superseded_qids={0|1}	(Optional) When unspecified or set to 0, the XML output includes all QIDs even if they've been superseded. Specify 1 to filter out QIDs that have been superseded by another QID in the results.
show_igs={0|1}	(Optional except as noted) Specify 1 to show detection records with information gathered along with confirmed vulnerabilities and potential vulnerabilities. Specify 0 (default) to hide information gathered.
	The show_igs parameter is required in one use case. The parameter show_igs=1 must be specified if both these conditions are met: 1) search lists are included using the parameter include_search_list_titles or include_search_list_ids, and 2) if the included search lists contain only information gathered.
include_search_list_titles={value}	(Optional) Show detection records only when a record's QID is INCLUDED IN in one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_ids.
exclude_search_list_titles={value}	(Optional) Show detection records only when a record's QID is IS EXCLUDED from one or more of the specified search list titles. One or more titles may be specified. Multiple titles are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_ids.
include_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS INCLUDED in one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 10-15). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or include_search_list_titles.

Parameter	Description
exclude_search_list_ids={value,value...}	(Optional) Show detection records only when a record's QID IS EXCLUDED from one or more of the specified search list titles. One or more IDs may be specified. A range is specified with a dash (for example: 40-42). Multiple entries are comma separated.
	This parameter cannot be specified with any of these parameters in the same request: qids, severities or exclude_search_list_titles.

Asset tags

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
tag_set_by={**id**|name}	(Optional when use_tags=1) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={**any**|all}	(Optional when use_tags=1) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated. **Note:** You must select an include tag before selecting an exclude tag.
show_tags={**0**|1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

Qualys Detection Score (QDS)

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

EC2/Azure/GCP metadata

Note: Ensure to enable the EC2 scanning and ensure this setting remains active. To enable this, reach out to your Technical Account Manager or Qualys Support.

Parameter	Description
host_metadata={value}	(Optional) Specify "all" to list all assets (cloud and non-cloud assets) and the metadata output applicable for cloud assets. For example, if the value is set to ec2, the output lists all assets (cloud and non cloud assets), and the metadata applicable only for ec2 assets. Valid values: all, ec2, google, azure
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes. To retrieve information about the host instance type, use the metadata field, "instance-type".
show_cloud_tags={**0**|1}	(Optional) Specify 1 to display cloud provider tags for each scanned host asset in the output. The default value of the parameter is set to 0. When set to 0, we will not show the cloud provider tags for the scanned assets.

Parameter	Description
cloud_tag_fields={value1, value2}	(Optional when show_cloud_tags is specified) Specify cloud tags or cloud tag and name combinations to only return information for specified cloud tags. A cloud tag name and value combination is specified with a colon (for example:SomeTag6:AY_ec2). For each cloud tag, we show the cloud tag's name, its value, and last success date (the tag last success date/time, fetched from instance).
	If this parameter is not specified and "show_cloud_tags" is set to 1, we will show all the cloud provider tags for the assets.

Keep Alive Mechanism

The service uses a "keep alive" mechanism to maintain an open connection to the Qualys server for the duration of the host detection list API request. To keep the connection alive, the service sends some "dummy" data back to the client every 30 to 40 seconds if no "real" data has been sent already by the API during that time.

In XML output, this "dummy" data appears as a "<!-- keep-alive -->" line (since comments should be safely ignored by downstream XML parsers).

In CSV and CSV_NO_METADATA output, this "dummy" data appears as a <CR><LF> (carriage return, linefeed) pair (since empty lines clearly do not contain any CSV data).

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, confirmed

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&ips=11
.111.11.111&include_vuln_type=confirmed' \--header 'X-Requested-With:
curl'--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T13:34:18Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
```

```
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978355</UNIQUE_VULN_ID>
                        <QID>82054</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Download a list of hosts with the latest vulnerability data, based on vulnerability type, potential

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&ips=11
.110.11.111&include_vuln_type=potential' \
--header 'X-Requested-With: curl'
--header 'Authorization: Basic <encoded username:password string>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2023-08-16T11:51:13Z</DATETIME>
        <HOST_LIST>
            <HOST>
```

```
                <ID>524323</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <OS>
                   <![CDATA[Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP]]>
                </OS>
                <LAST_SCAN_DATETIME>2019-11-
08T09:15:14Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2019-11-
08T06:37:29Z</LAST_VM_SCANNED_DATE>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978356</UNIQUE_VULN_ID>
                        <QID>38469</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978354</UNIQUE_VULN_ID>
                        <QID>38560</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
```

```
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>3978353</UNIQUE_VULN_ID>
                        <QID>115317</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[SSH-2.0-OpenSSH_3.9p1-AuthSelect-
SecurID-log]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2019-11-
08T06:37:29Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2019-11-
08T06:37:29Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2019-11-
08T06:37:29Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2019-11-
08T09:15:14Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2019-11-
08T09:15:14Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List VM scanned hosts

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://
<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.10.40.10&truncation_limit=4">
  <HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
      <DATETIME>2024-03-28T09:03:45Z</DATETIME>
```

```
      <HOST_LIST>
        <HOST>
          <ID>4203254</ID>
          <IP>xx.xx.xx.xx</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <ASSET_GROUP_LIST />
          <NETWORK_ID>2458227</NETWORK_ID>
          <NETWORK_NAME>network1</NETWORK_NAME>
          <OS>
            <![CDATA[Windows XP]]>
          </OS>
          <DNS>
            <![CDATA[w2kserver-tmp3.vuln.example.com]]>
          </DNS>
          <DNS_DATA>
            <HOSTNAME>
              <![CDATA[w2kserver-tmp3]]>
            </HOSTNAME>
            <DOMAIN>
              <![CDATA[vuln.example.com]]>
            </DOMAIN>
            <FQDN>
              <![CDATA[w2kserver-tmp3.vuln.example.com]]>
            </FQDN>
          </DNS_DATA>
          <LAST_SCAN_DATETIME>2023-10-11T07:18:36Z</LAST_SCAN_DATETIME>
          <LAST_VM_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_SCANNED_DATE>
          <LAST_VM_SCANNED_DURATION>149</LAST_VM_SCANNED_DURATION>
          <LAST_VM_AUTH_SCANNED_DATE>2023-10-
11T07:11:13Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>149</LAST_VM_AUTH_SCANNED_DURATION>
          <DETECTION_LIST>
            <DETECTION>
              <UNIQUE_VULN_ID>61198372</UNIQUE_VULN_ID>
              <QID>11</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>2</SEVERITY>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[NameProgramVersionProtocolPort
portmap/rpcbind1000002-4tcp111
portmap/rpcbind1000002-4udp895
portmap/rpcbind1000002-4udp111]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
```

```
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
            <DETECTION>
              <UNIQUE_VULN_ID>61198518</UNIQUE_VULN_ID>
              <QID>13361</QID>
              <TYPE>Confirmed</TYPE>
              <SEVERITY>4</SEVERITY>
              <PORT>22</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS>
                <![CDATA[User Nameroot
Authentication Schemepassword
ProtocolSSH Version 2
Discovery MethodLogin credentials provided by user
Using sudoNo
Key exchange algorithmdiffie-hellman-group-exchange-sha256
Host key algorithmssh-rsa
Compression algorithmzlib@openssh.com
Encryption algorithmaes128-ctr
MAC algorithmhmac-sha2-256
Authentication Record10.113.197.133]]>
              </RESULTS>
              <STATUS>New</STATUS>
              <FIRST_FOUND_DATETIME>2023-10-
11T07:11:13Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2023-10-
11T07:11:13Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>1</TIMES_FOUND>
              <LAST_TEST_DATETIME>2023-10-
11T07:11:13Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2023-10-
11T07:18:36Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2023-10-
11T07:18:36Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
          </DETECTION_LIST>
        </HOST>
      </HOST_LIST>
    </RESPONSE>
  </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host Detection XML Output, with truncation

A truncated response is returned when the API request returns more host records than the truncation limit. In this sample, the truncation limit is set to 100 host records.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl"
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100"
```

The Warning message in the XML output (shown below) indicates the URL you need to use to request the next 100 host records.

XML output:

```
...
          </DETECTION>
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
    <WARNING>
      <CODE>1980</CODE>
      <TEXT>100 record limit exceeded. Use URL to get next batch of
results.</TEXT>

<URL><![CDATA[<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&truncation_limit=100&id_min=5641289]]></URL>
    </WARNING>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Filter superseded QIDs (filter_superseded_qids=1)

In this example any QID superseded by another QID has been filtered out of the results. The XML output includes QID 370584 and QID 370613. QID 370610 was filtered out because it was superseded by QID 370613.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/6.0/fo/asset/host/vm/detection/?action=list&filter_superseded_qids=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-03T10:22:34Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1145</ID>
        <IP>xx.xx.xx.xx</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[win2003.sample.qualys.com]]></DNS>
        <DNS_DATA>
            <HOSTNAME>
                <![CDATA[win2003]]>
            </HOSTNAME>
```

```
            <DOMAIN>
                <![CDATA[sample.qualys.com]]>
            </DOMAIN>
            <FQDN>
                <![CDATA[win2003.sample.qualys.com]]>
            </FQDN>
        </DNS_DATA>
        <NETBIOS><![CDATA[LWIN2003HP1]]></NETBIOS>
        <LAST_SCAN_DATETIME>2018-01-08T19:50:18Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2018-01-08T19:36:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>619</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2017-11-15T16:58:16Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
<DETECTION>
            <QID>370584</QID>
            <UNIQUE_VULN_ID>45654</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
          <RESULTS><![CDATA[C:\Program Files\Mozilla Firefox\firefox.exe
Version is  42.0.0.0]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-10-
10T10:30:48Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>183</TIMES_FOUND>
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-08-
27T22:48:04Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
<DETECTION>
            <QID>370613</QID>
            <UNIQUE_VULN_ID>43664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>5</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[C:\Program
Files\Google\Chrome\Application\33.0.1750.149\chrome.dll file version is
33.0.1750.149
%ProgramFiles%\Google\Chrome\Application\33.0.1750.149\chrome.dll file
version is 33.0.1750.149]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2017-11-
12T20:11:32Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2020-04-
27T23:04:10Z</LAST_FOUND_DATETIME>
            <TIMES_FOUND>162</TIMES_FOUND>
```

```
            <LAST_TEST_DATETIME>2020-04-27T23:04:10Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2020-04-
27T23:05:41Z</LAST_UPDATE_DATETIME>
            <LAST_FIXED_DATETIME>2019-10-
30T22:28:59Z</LAST_FIXED_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2020-04-
27T23:05:41Z</LAST_PROCESSED_DATETIME>
          </DETECTION>
</DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List assets with Qualys Detection Score (QDS)

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=lis
t&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <UNIQUE_VULN_ID>52664</UNIQUE_VULN_ID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
               <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
```

```
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS">
                     <![CDATA[9.3]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_version">
                      <![CDATA[v2]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="epss">
                       <![CDATA[0.24142]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="CVSS_vector">
                       <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                 </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>           </DETECTION>
...
```

```
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - VM Detection API

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&show_a
rf_data=1&arf_filter_keys=config-not- exploitable&truncation_limit=10' \
--header 'X-Requested-With: POSTMAN' \
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd>"
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2024-08-26T11:52:53Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>2454304</ID>
                    <IP>11.xxx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>952199</NETWORK_ID>
                    <LAST_SCAN_DATETIME>2022-08-14T18:56:13Z
                    </LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2022-08-14T18:40:15Z
                    </LAST_VM_SCANNED_DATE>
                    <LAST_VM_SCANNED_DURATION>447</LAST_VM_
                    SCANNED_DURATION>
                    <DETECTION_LIST>
                          <DETECTION>
                             <UNIQUE_VULN_ID>35787259</UNIQUE_VULN_ID>
                             <QID>316406</QID>
                             <TYPE>Potential</TYPE>
                             <SEVERITY>3</SEVERITY>
                             <SSL>0</SSL>
                             <RESULTS>
                             <![CDATA[Package Installed Version
                             Required Version
                           firefox 31.3.0-3.el6.centos.x86_64 38.0-4.el6.
                             centos]]>
                             </RESULTS>
                             <STATUS>New</STATUS>
                             <FIRST_FOUND_DATETIME>2022-03-22T06:54:47Z
                             </FIRST_FOUND_DATETIME>
                             <LAST_FOUND_DATETIME>2022-03-22T06:54:47Z
                             </LAST_FOUND_DATETIME>
                             <TIMES_FOUND>1</TIMES_FOUND>
                             <LAST_TEST_DATETIME>2022-03-22T06:54:47Z
                             </LAST_TEST_DATETIME>
```

```
                                <LAST_UPDATE_DATETIME>2022-03-22T07:14:30Z
                                </LAST_UPDATE_DATETIME>
                                <IS_IGNORED>0</IS_IGNORED>
                                <IS_DISABLED>0</IS_DISABLED>
                                <AFFECT_EXPLOITABLE_CONFIG>0
                                </AFFECT_EXPLOITABLE_CONFIG>
                                <LAST_PROCESSED_DATETIME>2022-
                                0322T07:14:30Z</LAST_PROCESSED_DATETIME>
                            </DETECTION>
                        </DETECTION_LIST>
                    </HOST>
                </HOST_LIST>
            </RESPONSE>
        </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - List Assets with Tag Details in the Response

API request:

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list
&ips=xx.xxx.xxx.xxx&show_tags=1' \--header 'X-Requested-With: curl'--
header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2026-03-17T09:40:25Z</DATETIME>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST_LIST>
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
                <HOST>
                    <ID>14125607</ID>
                    <IP>10.113.197.133</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Linux 2.6]]>
                    </OS>
                    <DNS>
                        <![CDATA[10-101-87-231.bogus.tld]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[10-101-87-231]]>
                        </HOSTNAME>
                        <DOMAIN>
                            <![CDATA[bogus.tld]]>
                        </DOMAIN>
                        <FQDN>
```

```
                            <![CDATA[10-101-87-231.bogus.tld]]>
                        </FQDN>
                    </DNS_DATA>
                    <LAST_SCAN_DATETIME>2026-02-
26T08:23:48Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2026-02-
26T08:23:21Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>386</LAST_VM_SCANNED_DURATION>
                    <TAGS>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143644527]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_Demo]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143710805]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[BU2]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143651023]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[demo_BU]]>
                            </NAME>
                        </TAG>
                        <TAG>
                            <TAG_ID>
                                <![CDATA[143668042]]>
                            </TAG_ID>
                            <NAME>
                                <![CDATA[VM_AG]]>
                            </NAME>
                        </TAG>
                    </TAGS>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467336</UNIQUE_VULN_ID>
                            <QID>38611</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>22</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
```

```
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>106467334</UNIQUE_VULN_ID>
                            <QID>38623</QID>
                            <TYPE>Potential</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[SSH-2.0-OpenSSH_5.3 detected on
port 22 over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2024-11-
08T13:24:50Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2026-02-
26T08:23:21Z</LAST_FOUND_DATETIME>
                            <SOURCE>QUALYS</SOURCE>
                            <TIMES_FOUND>4</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2026-02-
26T08:23:21Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2026-02-
26T08:23:48Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2026-02-
26T08:23:48Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                    ...
                    ...
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - list MITRE ATT&CK Details

API Request

```
curl --location
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list
&show_arf_data=1&arf_filter_keys=config-not-
exploitable&truncation_limit=10' \ --header 'X-Requested-With:
POSTMAN' \
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.
dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-03-04T07:30:28Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
            <HOST>
                <ID>6553022</ID>
                <IP>11.111.11.111</IP>
                <TRACKING_METHOD>AGENT</TRACKING_METHOD>
                <OS>
                    <![CDATA[Windows 10 Pro N 64 bit Edition Version
22H2]]>
                </OS>
                <DNS>
                    <![CDATA[solution2]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[solution2]]>
                    </HOSTNAME>
                    <DOMAIN />
                    <FQDN />
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[SOLUTION2]]>
                </NETBIOS>
                <QG_HOSTID>
                    <![CDATA[311ee428-62a0-4604-b9f9-d874c1efbd88]]>
                </QG_HOSTID>
                <LAST_SCAN_DATETIME>2025-03-
04T04:08:01Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>238</LAST_VM_SCANNED_DURATION>
                <LAST_VM_AUTH_SCANNED_DATE>2025-03-
04T04:07:51Z</LAST_VM_AUTH_SCANNED_DATE>
                <DETECTION_LIST>
```

```
                    <DETECTION>
                        <UNIQUE_VULN_ID>66009800</UNIQUE_VULN_ID>
                        <QID>378827</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files\VMware\VMware
Tools\vmtoolsd.exe  Version is  12.2.6.44976]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>credential-
access</MITRE_TACTIC_NAME>
                       <MITRE_TECHNIQUE_NAME>Exploitation for Credential
Access</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0006</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1212</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66010782</UNIQUE_VULN_ID>
                        <QID>380293</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2024-12-
18T09:59:37Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement, execution,
privilege-escalation</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution, Exploitation for Privilege
Escalation</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002,
```

```
TA0004</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210, T1203,
T1068</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>305</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307447</UNIQUE_VULN_ID>
                        <QID>380734</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>lateral-movement,
execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation of Remote
Services, Exploitation for Client Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0008, TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1210,
T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307454</UNIQUE_VULN_ID>
                        <QID>382524</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
```

```
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                    <DETECTION>
                        <UNIQUE_VULN_ID>66307462</UNIQUE_VULN_ID>
                        <QID>382691</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[C:\Program Files
(x86)\Microsoft\Edge\Application\msedge.exe  Version is  92.0.902.67]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2025-02-
03T12:29:55Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2025-03-
04T04:07:51Z</LAST_FOUND_DATETIME>
                        <SOURCE>QUALYS</SOURCE>
                        <MITRE_TACTIC_NAME>execution</MITRE_TACTIC_NAME>
                        <MITRE_TECHNIQUE_NAME>Exploitation for Client
Execution</MITRE_TECHNIQUE_NAME>
                        <MITRE_TACTIC_ID>TA0002</MITRE_TACTIC_ID>
                        <MITRE_TECHNIQUE_ID>T1203</MITRE_TECHNIQUE_ID>
                        <TIMES_FOUND>104</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2025-03-
04T04:07:51Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2025-03-
04T04:08:01Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2025-03-
04T04:08:01Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
```

```
                </DETECTION_LIST>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Display the highest contributing CVEs and associated risk factor

API Request

```
curl --location --request POST '
<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&show_qd
s_factors=1&show_qds=1
--header 'X-Requested-With: xxx' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM "
<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
    <HOST_LIST_VM_DETECTION_OUTPUT>
        <RESPONSE>
            <DATETIME>2025-10-23T05:42:36Z</DATETIME>
            <HOST_LIST>
                <HOST>
                    <ID>6885606</ID>
                    <IP>10.xx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Windows 2012 R2 Standard]]>
                    </OS>
                    <DNS>
                        <![CDATA[wdw2012r2ntlm]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[wdw2012r2ntlm]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[WDW2012R2NTLM]]>
                    </NETBIOS>
                    <LAST_SCAN_DATETIME>2024-06-
02T05:14:11Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2024-06-
02T05:14:03Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>570</LAST_VM_SCANNED_DURATION>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>89625105</UNIQUE_VULN_ID>
```

```
                            <QID>90882</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>3</SEVERITY>
                            <PORT>3389</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                              <![CDATA[RDP Supported Encryption methods:
RC4(40 bit),RC4(56 bit)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-04-
19T10:14:24Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2024-06-
02T05:14:03Z</LAST_FOUND_DATETIME>
                            <QDS severity="LOW">30</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[No_Patch,High_Data_Loss]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[4.7]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="QID_severity">
                                    <![CDATA[3.0]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[90882]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>2</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2024-06-
02T05:14:03Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2024-06-
02T05:14:11Z</LAST_UPDATE_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2024-06-
02T05:14:11Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                    </DETECTION_LIST>
                </HOST>
                <HOST>
                    <ID>6885818</ID>
                    <IP>10.xx.xx.xx</IP>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK_ID>0</NETWORK_ID>
                    <OS>
                        <![CDATA[Windows 7 Ultimate]]>
                    </OS>
                    <DNS>
```

```
                        <![CDATA[pat-65-37]]>
                    </DNS>
                    <DNS_DATA>
                        <HOSTNAME>
                            <![CDATA[pat-65-37]]>
                        </HOSTNAME>
                        <DOMAIN />
                        <FQDN />
                    </DNS_DATA>
                    <NETBIOS>
                        <![CDATA[PAT-65-37]]>
                    </NETBIOS>
                    <LAST_SCAN_DATETIME>2025-10-
22T14:06:29Z</LAST_SCAN_DATETIME>
                    <LAST_VM_SCANNED_DATE>2025-10-
22T14:06:22Z</LAST_VM_SCANNED_DATE>

<LAST_VM_SCANNED_DURATION>863</LAST_VM_SCANNED_DURATION>
                    <DETECTION_LIST>
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073263</UNIQUE_VULN_ID>
                            <QID>90783</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>5</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                                <![CDATA[QID: 90783 detected on port 3389
over TCP.]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="CRITICAL">95</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[dos]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="exploit_maturity">
                                    <![CDATA[poc,weaponized]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_name">

<![CDATA[SlowLoris,Generic,Heuristic,FlyStudio]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[9.3]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="epss">
                                    <![CDATA[0.8547]]>
```

```
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_vector">
                                    <![CDATA[AV:N/AC:M/Au:N/C:C/I:C/A:C]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[9bd81d4142a4cd962727332e09982d4df588e777321b442c174c69114becbcbf
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[226f7341be64b865955bbe2d339ad28c49bbec08bb9e4086f3c98e03e5409b4c
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[83d9e97bc58123ae1842fa3e9f8d19ee685170a94588ff4df81cadaedaf27c87
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[a58bcf58422572184759fe64c1746b1cd7a8af5cb8826b76dfeefe6dc7cd6f04
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[1038f183ff1d11066c427923756705c5959d3665fd2726d842ad55ee3c133c30
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[181b169328a15072938c5759392a4d288caea1382460cda636b37a6aadce0d4c
]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[CVE-2012-0002]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>557</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
                            <LAST_FIXED_DATETIME>2025-09-
27T14:09:05Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073265</UNIQUE_VULN_ID>
                            <QID>90882</QID>
                            <TYPE>Confirmed</TYPE>
```

```
                            <SEVERITY>3</SEVERITY>
                            <PORT>3389</PORT>
                            <PROTOCOL>tcp</PROTOCOL>
                            <SSL>0</SSL>
                            <RESULTS>
                              <![CDATA[RDP Supported Encryption methods:
RC4(40 bit),RC4(56 bit)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="LOW">30</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[No_Patch,High_Data_Loss]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[4.7]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="QID_severity">
                                    <![CDATA[3.0]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[90882]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>558</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
                            <LAST_FIXED_DATETIME>2023-08-
29T13:30:08Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                        <DETECTION>
                            <UNIQUE_VULN_ID>90073262</UNIQUE_VULN_ID>
                            <QID>91541</QID>
                            <TYPE>Confirmed</TYPE>
                            <SEVERITY>5</SEVERITY>
                            <SSL>0</SSL>
                            <RESULTS>
                               <![CDATA[Microsoft Windows Remote Desktop
Services Remote Code Execution Vulnerability Detected (BlueKeep)]]>
                            </RESULTS>
                            <STATUS>Active</STATUS>
```

```
                            <FIRST_FOUND_DATETIME>2021-05-
23T11:28:17Z</FIRST_FOUND_DATETIME>
                            <LAST_FOUND_DATETIME>2025-10-
22T14:06:22Z</LAST_FOUND_DATETIME>
                            <QDS severity="CRITICAL">100</QDS>
                            <QDS_FACTORS>
                                <QDS_FACTOR name="RTI">
                                    <![CDATA[remote,dos]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="exploit_maturity">
                                    <![CDATA[weaponized,poc]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_name">

<![CDATA[Lockbit,Redkeeper,Unattributed,Doppelpaymer,Netwalker,Mailto]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="threat_actors">
                                    <![CDATA[Velvet Chollima,Silent
Chollima,Wizard Spider,Unattributed,Invisimole,Vicious
Panda,Microcin,Larva-24005,Emennet Pasargad,China Attribution]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_vuln">
                                    <![CDATA[YES]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS">
                                    <![CDATA[10.0]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_version">
                                    <![CDATA[v2]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="epss">
                                    <![CDATA[0.94445]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="trending">

<![CDATA[10102025,10052025,10072025,10122025,10032025,10042025,09252025,1
0082025,10062025,09242025,09282025,10132025,10142025,09272025,10012025,09
292025,10152025]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CVSS_vector">
                                    <![CDATA[AV:N/AC:L/Au:N/C:C/I:C/A:C]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[9966826ada8b1f366a9e7b9b1e7c430a2a49dda60eb7025c7481295e3ab7f9e4
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[8b561784fb52edcdd86adf387c9e2cb152aec027c14cafbee60957b50af7d550
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">
```

```
<![CDATA[28fb99f0193d20d3fff6c40b9b85c0c4b5073166ca50ec83e85c276f4fab8647
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[8402e053d5ad4e21c2c96a04e117d113f7bbdb295e2c55dcf8b94054d83fc1af
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[d4e2240c194c291d9c98454dca2c040902146def53bdee9900f1b9724d418268
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="malware_hash">

<![CDATA[76991e2f91e7ac9066c94489fdd332ea8e15995a15eabc29647920366e5591b5
]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_DUE_DATE">
                                    <![CDATA[1651536000000]]>
                                </QDS_FACTOR>
                                <QDS_FACTOR name="CISA_ADDED_DATE">
                                    <![CDATA[1635897600000]]>
                                </QDS_FACTOR>
                              <QDS_FACTOR name="HIGHEST_CONTRIBUTING_CVE">
                                    <![CDATA[CVE-2019-0708]]>
                                </QDS_FACTOR>
                            </QDS_FACTORS>
                            <TIMES_FOUND>543</TIMES_FOUND>
                            <LAST_TEST_DATETIME>2025-10-
22T14:06:22Z</LAST_TEST_DATETIME>
                            <LAST_UPDATE_DATETIME>2025-10-
22T14:06:29Z</LAST_UPDATE_DATETIME>
                            <LAST_FIXED_DATETIME>2025-09-
27T14:09:05Z</LAST_FIXED_DATETIME>
                            <IS_IGNORED>0</IS_IGNORED>
                            <IS_DISABLED>0</IS_DISABLED>
                            <LAST_PROCESSED_DATETIME>2025-10-
22T14:06:29Z</LAST_PROCESSED_DATETIME>
                        </DETECTION>
                    </DETECTION_LIST>
                </HOST>
            </HOST_LIST>
        </RESPONSE>
    </HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Display the list of all the hosts for OCI tracked assets

API Request

```
curl --location --request POST
'<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/?action=list&host_m
etadata=oci' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"<qualys_base_url>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2026-07-30T11:49:07Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>19942296</ID>
                <IP>xxx.xxx.xx.xxx</IP>
                <TRACKING_METHOD>OCI Compute Instance</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <LAST_SCAN_DATETIME>2026-07-
29T08:12:24Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2026-07-
29T08:12:24Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>1456</LAST_VM_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <UNIQUE_VULN_ID>213184238</UNIQUE_VULN_ID>
                        <QID>38229</QID>
                        <TYPE>Potential</TYPE>
                        <SEVERITY>3</SEVERITY>
                        <PORT>22</PORT>
                        <PROTOCOL>tcp</PROTOCOL>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[
3 consecutive connection attempts failed after a total number of 83
successful connections.
                            ]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2026-07-
29T08:12:24Z</FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2026-07-
29T08:12:24Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2026-07-
29T08:12:24Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2026-07-
29T08:12:24Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2026-07-
29T08:12:24Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
                </DETECTION_LIST>
            </HOST>

        </HOST_LIST>
```

```
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

More Samples

Qualys API - Host List Detection API samples (GitHub)

DTD

<platform API server>/api/6.0/fo/asset/host/vm/detection/dtd/output.dtd

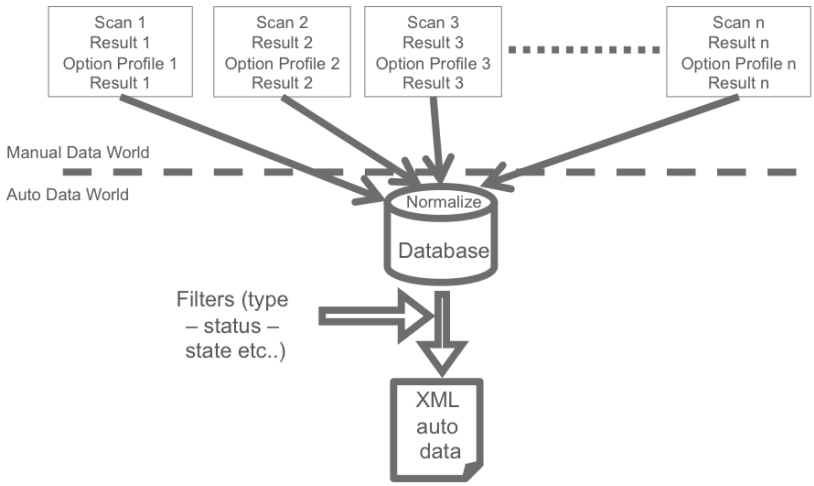
API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/6.0/fo/asset/host/vm/detection/?action=list	Active	Active
/api/5.0/fo/asset/host/vm/detection/?action=list	February 2027	August 2027
/api/4.0/fo/asset/host/vm/detection/?action=list	December 2025	June 2027
/api/3.0/fo/asset/host/vm/detection/?action=list	December 2025	June 2027
/api/2.0/fo/asset/host/vm/detection/?action=list	December 2025	June 2027

Host List Detection - Normalized Data

Qualys normalizes the vulnerability scan results into the database using a complex and sophisticated process. This mechanism generates what is called the vulnerability “host based”scan results. Normalized data brings a lot of value to customers because they provide the latest complete vulnerability status for the hosts (NEW, ACTIVE, FIXED, REOPENED) and history information. Normalized data is completely independent of scan results and option profiles, as shown in the diagram below.



The Qualys database stores automatic data for VM scanned hosts. For each of these hosts there can be multiple detection records.

What is a VM Scanned Host? A VM scanned host is a host that has been successfully scanned by the Qualys VM service for vulnerabilities. Note that a host is considered successfully scanned when it was included as a scan target, the scan was launched and it completed successfully.

What is a Detection Record? A detection record is a unique instance of a discovered vulnerability for a given host. It identifies the host IP address, QID, port, service, FQDN and SSL flag (whether the vulnerability was detected over SSL).

Host List Detection - Use Cases

The host detection API is often used in conjunction with other information that can be downloaded using other Qualys APIs.

Create Custom Technical Reports with vulnerability details

Technical reports need additional information for each vulnerability such as the description, solution, threat or impact. The detection API provides the QID for each vulnerability found for an asset. The QID is a unique ID that references a vulnerability within the Qualys KnowledgeBase.

Use the following workflow to create custom technical reports:

Step 1 - Use the host list detection API to return “host based” vulnerability data for hosts in your account.

Step 2 - Use the KnowlegeBase API (/api/2.0/fo/knowledge_base/vuln/?action=list) to obtain vulnerability data, such as the vulnerability description, threat and impact. It’s possible to make a request for all vulnerabilities (QIDs) in the KnowledgeBase or just a specific vulnerability.

For example, to make a request for QID 90082 use the following URL:

```
<qualys_base_url>/api/2.0/fo/knowledge_base/vuln/?action=list&ids=
90082
```

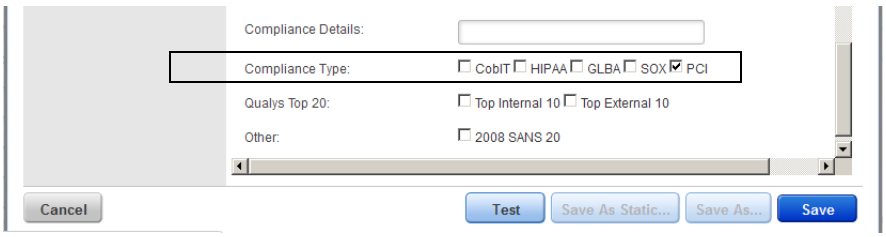
where “qualysapi.qualys.com” is the name of the API server where your account is located (in this case US Platform 1).

Step 3 - Correlate the vulnerability information in the third party application using the QID number provided in the <QID> XML output which is returned by the host detection API (Step 1) and the KnowledgeBase API (Step 2).

A typical integration would be to create tables in a database for the XML output from both Qualys API functions and use QID as a key for a join. This way it would be possible to create queries that will provide all the vulnerabilities for a given set of hosts (according to custom search criteria) and their descriptions.

Get All PCI Vulnerabilities

Step 1 - First you need to create a dynamic search list titled “PCI Vulns” using the Qualys user interface. When creating the dynamic search list, select the PCI option next to Compliance Type as shown below.



Step 2 - Create an asset group titled “PCI Hosts” containing the hosts which are in scope for PCI compliance.

Step 3 - Make the following host list detection API request using the asset group title “PCI Hosts” and the search list title “PCI Vulns”:

```
<qualys_base_url>/api/2.0/fo/asset/host/vm/detection/?action=list&
ag_titles=PCI+Hosts&include_search_list_titles=PCI+Vulns'
```

where “qualysapi.qualys.com” is the name of the API server where your account is located (in this case US Platform 1).

Host List Detection - Best Practices

Some background

When API calls are done to pull large sets of data, the backend will process data by streaming that information in batches to ensure data integrity and preventing overloading the backend services. That means that there will be brief periods of speeds declining while the next batch is being retrieved and processed to stream back to the client. However, the overall speed averages itself out in the long run.

You also need to keep in mind the contributing factors that could impact performance on a shared resource. Such as performing data pulls during peak usage, which will hit congestion and speeds will not be as fast as those conducted during off peak hours. There are also additional factors from the use of optional parameters used in API calls that do extra processing before streaming the data, active_kernels_only being an example.

To ensure accurate results, use short ID ranges rather than broad ones. Broad ranges can include hosts that are not part of your subscription. Use asset groups. Asset groups provide greater reliability and allow more precise control.

If your subscription is on the Private Cloud Provider (PCP), you can continue using ID ranges, as all hosts within that range are automatically included in your subscription.

Notes:

- It is recommended to avoid simultaneous execution of the same API with identical parameters by multiple users. If both API calls are necessary, then schedule the call at different time. For example, user1 at 01:00 AM GMT and user2 at 04:00 PM GMT.

- If your account has fewer hosts, we recommend to avoid the use of very large ID ranges in this API. Instead, use All asset groups along with other necessary filters for better results.

Multi-Threading

We have been, and will continue to innovate and re-architect the capabilities of processing large amount of encrypted data for streaming through API to scale to our customers needs. While being able to provide customers with all of their Vulnerability information as quickly as possible is a primary focal point, it should be innovated in such a way that keeps data integrity in the forefront of every release. To do this, it takes time, effort, and dedicated resources to ensure full testing is done to account for all aspects. With that in mind, the use of automation, threading, and parallelism are techniques to that can assist with increasing performance with data pulls.

While fetching host information in an automated fashion, you can make use of multi-threading to collect data in batch sizes for optimum performance.

Maximum benefit has seen when the batch size is set evenly throughout the number of parallel threads used. For example, a host detection call resulting in a return of 100k assets, and using 10 threads in parallel, would benefit the most by using a batch size of (100,000 / 10) = 10,000. To reduce having one thread slow down the entire process by hitting a congested server, you can break this out further into batches of 5,000 hosts, resulting in 20 output files.

Looking for help? Check our examples here

Qualys API - Host List Detection API samples - Multithreading (GitHub)

Excluded Host List

/api/2.0/fo/asset/excluded_ip/?action=list

[GET} [POST]

Show the excluded host list for the user's account. Hosts in your excluded host list will not be scanned.

Permissions - Managers, Auditors view all excluded hosts in subscription. Unit Managers view excluded hosts in their own business unit. Scanners, Readers view excluded hosts in their account.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ips={value}	(Optional) Show only certain excluded IP addresses/ranges. When unspecified, all excluded IPs/ranges in your account will be listed. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20).
network_id={value}	(Optional and valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network ID. You might need to use this parameter to get the excluded host list you're interested in. See User Scenarios to know more about the behavior of this parameter.
Asset Groups	
ag_ids={value}	(Optional and valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network ID. You might need to use this parameter to get the excluded host list you're interested in.
ag_titles={value}	(Optional) Show excluded hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group). These parameters are mutually exclusive and cannot be specified together: ag_ids and ag_titles.
Asset Tags	
use_tags={0|1}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.

Parameter	Description
tag_include_selector={any|all}	(Optional when use_tags=1) Specify "any" (the default) to include excluded hosts that match at least one of the selected tags. Specify "all" to include excluded hosts that match all of the selected tags.
tag_exclude_selector={any|all}	(Optional when use_tags=1) Specify "any" (the default) to ignore excluded hosts that match at least one of the selected tags. Specify "all" to ignore excluded hosts that match all of the selected tags.
tag_set_by = {id|name}	(Optional when use_tags=1) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names.
tag_set_include={value}	(Optional when use_tags=1) Specify a tag set to include. Excluded hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Excluded hosts that match these tags will be ignored. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

User Scenarios

Let us consider different user scenarios to know more about the behavior of network_id parameter:

User	Networks with access	network_id mandatory?	What does output include?
User 1	Global Default Network, Network 1, Network 2	No	Excluded host list from all the networks the user has access to.
User 2	Global Default Network	No	Excluded host list for global default network.
User 3	Network 1	Yes	Excluded host list for Network 1.
User 4	Network 1, Network 2, Network 3	Yes	Excluded host list for network that is listed in the request. Multiple entries are comma separated (for example, Network+1,Network+2,Network+3).

Sample - List all excluded hosts

API request:

```
curl -u user:password -H "X-Requested-With: curl demo 2" -D
headers.15
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/?action
```

```
=list"
```

XML output

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/ip_list
_output.dtd">
<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-01-23T00:33:24Z</DATETIME>
    <IP_SET>
      <IP_RANGE network_id="0" expiration_date="2015-04-
28T00:00:00Z">10.100.100.101-10.100.100.255</IP_RANGE>
      <IP network_id="14665885">10.10.10.1</IP>
      <IP network_id="0">10.100.100.100</IP>
    </IP_SET>
  </RESPONSE>
</IP_LIST_OUTPUT>
```

Sample - List all excluded hosts in IP range

API request:

```
curl -u user:password -H "X-Requested-With: curl demo 2" -D
headers.16
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/
?action=list&ips=10.10.24.1-10.10.24.255"
```

DTD

<platform API server>/api/2.0/fo/asset/excluded_ip/ip_list_output.dtd

Excluded Hosts Change History

/api/2.0/fo/asset/excluded_ip/history/?action=list

[GET] {POST}

View change history for excluded hosts in the user's subscription. History record IDs in the XML output are listed in decreasing order.

Permissions - Users with these roles have permission to view all excluded hosts in the subscription: Manager, Auditor, Unit Manager, Scanner and Reader.

Unlike other APIs, an excluded hosts change history request returns change history records for all relevant IP addresses in the subscription, regardless of whether the user has access to these IP addresses in their account.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ips={value}	(Optional) Show only certain excluded IP addresses/ranges. When unspecified, all excluded IPs/ranges in your subscription will be listed. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.24.1-10.10.24.20).
network_id={value}	(Optional and valid only when the Network Support feature is enabled for the user's account) Specify a network ID to restrict the request to a certain custom network.
id_min={value}	(Optional) Show only those history records in your subscription that have an ID number greater than or equal to an ID number you specify.
id_max={value}	(Optional) Show only those history records in your subscription that have an ID number less than or equal to an ID number you specify.
ids={value}	(Optional) Show only those history records in your subscription that have ID numbers matching the ID numbers you specify.

Sample - Change list for all excluded IPs

API request:

```
curl -u user:password -H "X-Requested-With: curl demo 2" -D
headers.15
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/history
/?action=list"
```

XML output:

```
<!DOCTYPE HISTORY_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/history
/history_list_output.dtd">

<HISTORY_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-01-18T01:48:42Z</DATETIME>
    <HISTORY_LIST>
      <HISTORY>
        <ID>1923</ID>
        <IP_SET>
          <IP_RANGE>10.10.10.2-10.10.10.11</IP_RANGE>
```

```
          <IP_RANGE>10.10.10.32-10.10.10.34</IP_RANGE>
          <IP>10.10.30.70</IP>
        </IP_SET>
        <ACTION>Added</ACTION>
        <DATETIME>2017-12-02T05:19:06Z</DATETIME>
        <USER_LOGIN>quays_ab</USER_LOGIN>
        <COMMENTS><![CDATA[DD]]></COMMENTS>
      </HISTORY>
      <HISTORY>
        <ID>1863</ID>
        <IP_SET>
          <IP_RANGE>10.10.10.102-10.10.10.120</IP_RANGE>
        </IP_SET>
        <ACTION>Removed</ACTION>
        <DATETIME>2017-06-01T23:51:26Z</DATETIME>
        <USER_LOGIN>quays_ab</USER_LOGIN>
        <COMMENTS><![CDATA[Removing 10.10.10.102-
10.10.10.120]]></COMMENTS>
      </HISTORY>
      <HISTORY>
        <ID>1663</ID>
        <IP_SET>
          <IP_RANGE>10.10.10.100-10.10.10.120</IP_RANGE>
        </IP_SET>
        <ACTION>Added</ACTION>
        <DATETIME>2016-04-29T06:56:13Z</DATETIME>
        <USER_LOGIN>quays_ss</USER_LOGIN>
        <COMMENTS><![CDATA[Scanner shouldn't add Exclude
hosts]]></COMMENTS>
      </HISTORY>

    ...

    </HISTORY_LIST>
    <WARNING>
      <CODE>1980</CODE>
      <TEXT>1,000 record limit exceeded. Use URL to get next batch
of results.</TEXT>
<URL><![CDATA[<qualys_base_url>/api/2.0/fo/asset/excluded_ip/histo
ry/?action=list&id_max=1660]]></URL>
    </WARNING>
    <GLOSSARY>
      <USER_LIST>
        <USER>
          <USER_LOGIN>quays_ss</USER_LOGIN>
          <FIRST_NAME>Sally Unassigned</FIRST_NAME>
```

```
            <LAST_NAME>Storm</LAST_NAME>
            <ROLE>Scanner</ROLE>
          </USER>
          <USER>
            <USER_LOGIN>quays_ab</USER_LOGIN>
            <FIRST_NAME>Al</FIRST_NAME>
            <LAST_NAME>Berger</LAST_NAME>
            <ROLE>Manager</ROLE>
          </USER>
        </USER_LIST>
      </GLOSSARY>
    </RESPONSE>
</HISTORY_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/asset/excluded_ip/history/history_list_output.dtd

Manage Excluded Hosts

The excluded hosts endpoint (**/api/2.0/fo/asset/excluded_ip**) allows you to add and remove excluded hosts from your account.

Add excluded hosts

/api/2.0/fo/asset/excluded_ip/?action=add

[POST]

Add hosts (IPs) to your excluded host list. Hosts in your excluded host list will not be scanned.

Permissions - Managers and Unit Managers have permission to add IPs to the excluded host list.

Input Parameters

Parameter	Description
action=add	(Required)
ips={value}	(Required) The IP addresses to be added to the excluded IPs list. Enter a comma separated list of IPv4 singletons or ranges. For example: 10.10.10.13,10.10.10.25-10.10.10.29

Parameter	Description
expiry_days={value}	(Optional) The number of days the IPs being added to the excluded IPs list will be considered valid for exclusion. When the expiration is reached, the IPs are removed from the list and made available again for scanning. When unspecified, the IPs being added have no expiration and will remain on the list until removed by a user.
dg_names={value}	(Optional) Specify users who will be notified 7 days before hosts are removed from the excluded hosts list (i.e. supply distribution group names as defined in the Qualys UI). Multiple distribution groups are comma separated. A maximum of 15 distribution groups may be entered.
comment={value}	(Required) User-defined notes (up to 1024 characters).
network_id={value}	(Optional and valid only when the user making the request has access to more than one network) Assign a network ID to the IPs being added to the excluded IPs list. By default, the user's default network ID is assigned.

Sample - Add excluded hosts

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -d
"action=add&ips=10.100.100.101-10.100.100.255&comment=adding
ips&expiry_days=5"
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-23T00:33:21Z</DATETIME>
    <TEXT>Adding IPs to Excluded IPs list.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>Added IPs</KEY>
        <VALUE>10.100.100.101-10.100.100.255</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Add IPs already in excluded hosts list

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -d
"action=add&ips=10.10.34.210-10.10.34.212&comment=adding, added
IPs " "https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-05-14T13:09:03Z</DATETIME>
    <TEXT>Not Adding any IPs to Excluded IPs list.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>IPs already in Excluded IPs list.</KEY>
        <VALUE>10.10.34.210-10.10.34.212</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Remove excluded hosts

/api/2.0/fo/asset/excluded_ip/?action=remove

[POST]

Remove certain hosts from your excluded hosts list. You can choose to remove certain hosts (IPs) or all hosts from your excluded hosts list.

Permissions - Managers and Unit Managers have permission to remove IPs from the excluded host list.

Input Parameters

Parameter	Description
action=remove	(Required)
ips={value}	(Required) The IP addresses to be removed from the excluded IPs list. Enter a comma separated list of IPv4 singletons or ranges. For example: 10.10.10.13,10.10.10.25-10.10.10.29
comment={value}	(Required) User-defined notes (up to 1024 characters).
network_id={value}	(Optional and valid only when the user making the request has access to more than one network) Identify a network ID that is assigned to the IPs being removed from the excluded IPs list. By default, the user's default network ID is assigned.

Sample - Remove certain excluded hosts

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -d
"action=remove&ips=10.10.34.250-10.10.34.254&comment=remove IPS"
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-15T04:05:04Z</DATETIME>
    <TEXT>Removed IPs from Excluded IPs list.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>Removed IPs</KEY>
        <VALUE>10.10.34.250-10.10.34.254</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Remove all excluded hosts

/api/2.0/fo/asset/excluded_ip/?action=remove_all

[POST]

Remove all hosts from your excluded hosts list.

Permissions - Managers and Unit Managers have permission to remove IPs from the excluded host list.

Input Parameters

Parameter	Description
action=remove_all	(Required)
comment={value}	(Required) User-defined notes (up to 1024 characters).
network_id={value}	(Optional and valid only when the user making the request has access to more than one network) Identify a network ID that is assigned to the IPs being removed from the excluded IPs list. By default, the user's default network ID is assigned.

Sample - Remove all excluded hosts

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -d
"action=remove_all&comment=remove all ips"
"<qualys_base_url>/api/2.0/fo/asset/excluded_ip/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-24T00:08:19Z</DATETIME>
    <TEXT>Removed IPs from Excluded IPs list.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>Removed IPs</KEY>
        <VALUE>10.100.100.101-10.100.100.255,100.100.100.101-
100.100.100.255</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

DTD returned by requests to add and remove excluded hosts

<platform API server>/api/2.0/simple_return.dtd

Virtual Host List

/api/2.0/fo/asset/vhost/?action=list)

[GET] [POST]

List virtual hosts in the user's account. By default, all virtual hosts in the user's account are included.

Permissions - Managers view virtual hosts in the subscription. Unit Managers view virtual hosts in their own business unit. Scanners and Readers view virtual hosts in their own account.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ip={value}	(Optional) Show only virtual hosts that have a certain IP address.
port={value}	(Optional) Show only virtual hosts that have a certain port.

Sample - List virtual hosts in account

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/?action=list"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VIRTUAL_HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/vhost_list_ou
tput.dtd">
<VIRTUAL_HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-04-26T11:20:42Z</DATETIME>
    <VIRTUAL_HOST_LIST>
      <VIRTUAL_HOST>
        <IP>10.11.65.3</IP>
        <PORT>255</PORT>
        <FQDN>asadfsadf-123.com</FQDN>
      </VIRTUAL_HOST>
      <VIRTUAL_HOST>
        <IP>10.11.65.5</IP>
        <PORT>246</PORT>
        <FQDN>asdfsahydk.com</FQDN>
      </VIRTUAL_HOST>
    </VIRTUAL_HOST_LIST>
```

```
  </RESPONSE>
</VIRTUAL_HOST_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/asset/vhost/vhost_list_output.dtd

Manage Virtual Hosts

/api/2.0/fo/asset/vhost/?action={value}

[POST]

Create, edit and delete virtual hosts in the user account. One subscription can have a maximum of 5000 virtual hosts. The POST access method may be used to make an API request.

Note: The total limit of all the FQDNs, including commas, must be less than 4000 bytes per virtual host.

Permissions - Managers manage virtual hosts in the subscription. Unit Managers manage virtual hosts in their own business unit when granted this permission. Scanners have permission to manage virtual hosts in their account when granted this permission. Readers, Auditors do not have permission to manage virtual hosts.

Input Parameters

Parameter	Description
action={action}	(Required) A flag used to make a virtual host request: create (create a virtual host) update (update/edit a virtual host) delete (delete a virtual host) add_fqdn (add one or more FQDNs to a virtual host) delete_fqdn (remove one or more FQDNs from a virtual host)
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ip={value}	(Required) An IP address for the virtual host configuration.
network_id={value}	(Optional) Network support must be enabled to specify the network_id. If network support is enabled and you do not provide a network_id, then the Default Global Network is considered. You can specify only one network_id.

Parameter	Description
port={value}	(Required) A port number for the virtual host configuration.
fqdn={value}	(Required for all actions except "delete". Invalid for "delete".) One or more fully-qualified domain names (FQDNs) for the virtual host configuration. Multiple entries are comma separated.*

Sample - Create virtual host

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&ip=10.10.25.212&port=80&fqdn=www.abc123abc.com"
"<qualys_base_url>/api/2.0/fo/asset/vhost/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
 <RESPONSE>
   <DATETIME>2018-04-27T08:45:22Z</DATETIME>
   <TEXT>Virtual host successfully created.</TEXT>
 </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create virtual host in a network

Specify network_id to create a virtual host in the specified network.

API request:

```
curl -u "username:password" -H "X-Requested-With: curl" -H
"Content-type: text/xml" -X POST
-d "action=create&network_id=5004&ip=10.10.10.20
&port=8080&fqdn=example1.fqdn.com,example2.fqdn.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:27:52Z</DATETIME>
        <TEXT>Virtual host successfully created.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Add FQDNs to a virtual host

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -H "X-
Requested-With:curl" -X POST
"action=add_fqdn&ip=10.10.25.212&port=80&fqdn=www.abc123abc.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
 <RESPONSE>
   <DATETIME>2018-04-27T08:45:48Z</DATETIME>
   <TEXT>Virtual host FQDN(s) successfully added.</TEXT>
 </RESPONSE>
</SIMPLE_RETURN>
```

More Samples

Qualys API - Virtual Host samples - Manage Virtual Hosts (GitHub)

DTD

<platform API server>/api/2.0/simple_return.dtd

Restricted IPs List

/api/2.0/fo/setup/restricted_ips/?action=list

[GET] [POST]

List restricted IPs within the user's subscription. Managers only have permission to perform these actions using this API.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Set to 1 if you want to include the input parameters in the XML output.
output_format={CSV|**XML**}	(Optional) The list output will be in XML format by default. For CSV format, set output_format=CSV.

Sample - Download restricted IPs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/" >
output.txt
```

XML output:

The DTD for the restricted IPs list XML is provided in Appendix B - Ports used for scanning.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE RESTRICTED_IPS_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/setup/restricted_ips/restricted_ips_
output.dtd">
<RESTRICTED_IPS_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-03-22T11:12:56Z</DATETIME>
    <IP_SET>
      <IP_RANGE>10.10.10.1-10.10.10.255</IP_RANGE>
    </IP_SET>
    <STATUS>disabled</STATUS>
  </RESPONSE>
</RESTRICTED_IPS_OUTPUT>
```

DTD for restricted IPs list

<platform API server>/api/2.0/fo/setup/restricted_ips/restricted_ips_output.dtd

Sample - Download Restricted IPs List in CSV format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&output_format=csv"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
10.0.0.0
10.0.0.101-10.255.255.255
----END_RESPONSE_BODY_CSV
----BEGIN_RESPONSE_FOOTER_CSV
STATUS
enabled
----END_RESPONSE_FOOTER_CSV
```

Manage Restricted IPs

/api/2.0/fo/setup/restricted_ips/

[GET] [POST]

Manage and update the list of restricted IPs within the user's subscription. Managers only have permission to perform these actions using this API.

Input Parameters

Parameter	Description
action={value}	(Required) The action for the request, one of: activate - enable or disable the restricted IPs feature clear - clear all restricted IPs and de-active this feature add - add restricted IPs delete - delete restricted IPs replace - replace restricted IPs
echo_request={**0**|1}	(Optional) Set to 1 if you want to include the input parameters in the XML output.
enable={**0**|1}	(Optional and valid when action is activate) Enable or disable the restricted IPs list. Set enable=1 to enable the list; set enable=0 to clear any IPs in the list and disable the feature.
ips={value} -or- {CSV raw data upload}	(Optional and valid when action is add, replace or delete) The hosts you want to add to, remove from or replace in the restricted IPs list. IPs must be specified by using the “ips” parameter (using the POST method) or by uploading CSV raw data (using the GET or POST method). To upload CSV raw data using POST, specify --data-binary <data>. How to specify IP addresses. One or more IPs/ranges may be specified. Multiple IPs/ranges are comma separated. An IP range is specified with a hyphen (for example, 10.10.30.1-10.10.30.50). CIDR notation is supported.

Sample - Replace restricted IPs

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=replace&ips=10.0.0.0/8"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/" >
output.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-22T11:45:00Z</DATETIME>
    <TEXT>Successfully replaced restricted ips</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
        <VALUE>disabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete restricted IPs, upload CSV raw data

CSV raw data:

```
$ cat file1.csv
10.0.0.1
10.0.0.2-10.0.0.100
```

API request:

```
curl -H "X-Requested-with:curl" -H "Content-type:text/csv" -u
"USERNAME:PASSWORD" --data-binary "@file1.csv"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/?act
ion=delete"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-22T11:45:34Z</DATETIME>
    <TEXT>Successfully deleted restricted ips</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
        <VALUE>disabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Activate Restricted IPs feature and enable list

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=activate&enable=1"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/" >
output.txt
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-22T11:46:45Z</DATETIME>
    <TEXT>Restricted IPs feature has been enabled
successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
        <VALUE>enabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Clear All Restricted IPs and Disable the feature

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=clear"
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-22T12:04:34Z</DATETIME>
    <TEXT>Successfully cleared restricted ips</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
```

```
        <VALUE>disabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Asset Group List

/api/2.0/fo/asset/group/?action=list

[GET] [POST]

List asset groups in the user's account.

Permissions - Managers can view asset groups in the subscription. Unit Managers can view all asset groups in the user's business unit (those assigned to the business unit, and those owned by all users in the business unit). Scanners and Readers can view asset groups in the user's account (those assigned to the user, and those owned by the user).

Input Parameters

Parameter	Description
action=list	(Required)
output_format={csv|**xml**}	(Optional) The requested output format: CSV or XML (the default).
echo_request={**0**|1}	(Optional) Specify 1 to show (echo) the request's input parameters (names, values) in the XML output. When unspecified, parameters are not included in the XML output.
ids={value}	(Optional) Show only asset groups with certain IDs. Multiple IDs are comma separated.
id_min={value}	(Optional) Show only asset groups that have an ID greater than or equal to the specified ID.
id_max={value}	(Optional) Show only asset groups that have an ID less than or equal to the specified ID.
truncation_limit={value}	(Optional) Specify the maximum number of asset group records to output. By default this is set to 1000 records. If you specify truncation_limit=0, the output is not paginated and all records are returned in a single output. WARNING This can generate very large output and processing large XML files can consume a lot of resources on the client side. It is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is being downloaded.

Parameter	Description
network_ids={value}	(Optional and valid only when the Networks feature is enabled in your account) Restrict the request to certain network IDs. Multiple IDs are comma separated.
unit_id={value}	(Optional) Show only asset groups that have a business unit ID equal to the specified ID. **Note**: When the API is executed by manager user with this parameter, it only returns in the response the asset groups created within business unit and not assigned asset groups.
user_id={value}	(Optional) Show only asset groups that have a user ID equal to the specified ID.
title={value}	(Optional) Show only the asset group that has a title equal to the specified string - this must be an exact match.
show_attributes={value}	(Optional) Show attributes for each asset group along with the ID. Specify ALL or a comm-separated list of attribute names. Attribute names: ID, TITLE, OWNER_USER_NAME, OWNER_USER_ID, OWNER_UNIT_ID, NETWORK_IDS, LAST_UPDATE, IP_SET, APPLIANCE_LIST, DOMAIN_LIST, DNS_LIST, NETBIOS_LIST, EC2_ID_LIST, HOST_IDS, ASSIGNED_USER_IDS, ASSIGNED_UNIT_IDS, BUSINESS_IMPACT, CVSS, COMMENTS.

Sample - List asset groups, show default attributes

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=442838"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_GROUP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/asset_group_l
ist_output.dtd">
<ASSET_GROUP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-05-17T08:48:41Z</DATETIME>
    <ASSET_GROUP_LIST>
      <ASSET_GROUP>
        <ID>442838</ID>
        <TITLE><![CDATA[All]]></TITLE>
        <OWNER_ID>103448</OWNER_ID>
        <UNIT_ID>0</UNIT_ID>
        <NETWORK_ID>0</NETWORK_ID>
        <IP_SET>
```

```
            <IP_RANGE>10.10.10.0-10.10.10.1</IP_RANGE>
            <IP_RANGE>10.10.10.3-10.10.10.6</IP_RANGE>
            <IP>10.10.10.14</IP>
            <IP_RANGE>10.10.10.16-10.10.10.20</IP_RANGE>
            <IP_RANGE>10.10.10.22-10.10.10.255</IP_RANGE>
            <IP>10.10.31.26</IP>
          </IP_SET>
        </ASSET_GROUP>
      </ASSET_GROUP_LIST>
    </RESPONSE>
</ASSET_GROUP_LIST_OUTPUT>
```

Sample - List asset groups, show all attributes

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=246385&show_attributes=ALL"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_GROUP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/asset_group_l
ist_output.dtd">
<ASSET_GROUP_LIST_OUTPUT>
   <RESPONSE>
      <DATETIME>2018-03-17T09:52:59Z</DATETIME>
      <ASSET_GROUP_LIST>
         <ASSET_GROUP>
            <ID>246385</ID>
            <TITLE>user_john</TITLE>
            <OWNER_USER_ID>180603</OWNER_USER_ID>
            <LAST_UPDATE>2018-03-07T11:37:57Z</LAST_UPDATE>
            <BUSINESS_IMPACT>High</BUSINESS_IMPACT>
            <DEFAULT_APPLIANCE_ID>199673</DEFAULT_APPLIANCE_ID>
            <APPLIANCE_IDS>199673, 199674</APPLIANCE_IDS>
            <IP_SET>
               <IP_RANGE>10.10.10.10-10.10.10.11</IP_RANGE>
               <IP_RANGE>10.113.197.131-10.113.197.132</IP_RANGE>
            </IP_SET>
            <DNS_LIST>
               <DNS>qualsss1.com</DNS>
            </DNS_LIST>
            <NETBIOS_LIST>
               <NETBIOS>WIN2003-SRV-O</NETBIOS>
            </NETBIOS_LIST>
```

```
            <HOST_IDS>634744, 653133</HOST_IDS>
            <ASSIGNED_USER_IDS>198400, 198401</ASSIGNED_USER_IDS>
            <ASSIGNED_UNIT_IDS>202741</ASSIGNED_UNIT_IDS>
            <OWNER_USER_NAME>John Doe</OWNER_USER_NAME>
          </ASSET_GROUP>
        </ASSET_GROUP_LIST>
      </RESPONSE>
    </ASSET_GROUP_LIST_OUTPUT>
```

DTD for asset group list

<platform API server>/api/2.0/fo/asset/group/asset_group_list_output.dtd

Manage Asset Groups

Create, edit and delete asset groups in the user's account.

Permissions - Managers can manage (create, edit, delete) all asset groups in the subscription. Unit Managers can manage asset groups owned by any user in the user's same business unit. Scanners and Readers can manage asset groups owned by the user.

Add new asset group

/api/2.0/fo/asset/group/?action=add

[POST]

Add a new asset group in the user's account.

Input Parameters

Parameter	Description
action=add	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show (echo) the request's input parameters (names, values) in the XML output. When unspecified, parameters are not included in the XML output.
title={value}	(Required) An asset group title. This name must be unique and can't be "All".
network_id={value}	(Optional) The network ID of the network you want to assign the asset group to.
{parameters}	See "Asset Group Parameters"

Sample - Add asset group

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST"
```

```
-d "title=MY DEMO AG&network_id=1220&comments=This is
comment&division=this is divison&location=this is
location&business_impact=high&cvss_enviro_cdp=low&cvss_enviro_td=l
ow&cvss_enviro_cr=medium&cvss_enviro_ir=high&cvss_enviro_ar=medium
&ips=10.1.1.1/31"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/?action=add"
```

XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-28T22:57:50Z</DATETIME>
    <TEXT>Asset Group successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>395752377</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Edit asset group

/api/2.0/fo/asset/group/?action=edit

[POST]

Edit an existing asset group in the user's account.

Input Parameters

Parameter	Description
action=edit	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to show (echo) the request's input parameters (names, values) in the XML output. When unspecified, parameters are not included in the XML output.
id={value}	(Required) The ID of the asset group you want to edit.
{parameters}	See "Asset Group Parameters"

Sample - Edit asset group

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "id=395752377&set_title=MY ASSET GROUP"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/?action=edit"
```

XML output:

The XML output uses the simple return (/api/2.0/simple_return.dtd).

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-05-29T15:29:00Z</DATETIME>
    <TEXT>Asset Group Updated Successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>395752377</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Delete asset group

/api/2.0/fo/asset/group/?action=delete

[POST]

Delete an asset group present in the user's account. By deleting an asset group any scheduled scans using the asset group will be deactivated.

Input Parameters

Parameter	Description
action=delete	(Required)
echo_request={**0**|1}	Optional) Specify 1 to show (echo) the request's input parameters (names, values) in the XML output. When unspecified, parameters are not included in the XML output.
id={value}	(Required) The ID of the asset group you want to delete.

Sample - Delete asset group

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "id=395752377"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/?action=delet
e"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-29T15:49:35Z</DATETIME>
    <TEXT>Asset Group Deleted Successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>395752377</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Asset Group Parameters

Theses parameters are used for adding and editing an asset group.

The "set" (overwrite) and "remove" operations can cause the asset group to have no IPs, domains, etc depending on the parameter.

Parameter	Parameter Name action=add	Parameter Name action=edit
Comments	comments (255 characters maximum)	set_comments
Division	division (64 characters maximum)	set_division
Function	function (64 characters maximum)	set_function
Location	location (64 characters maximum)	set_location
Business Impact	business_impact (One of: critical, high, medium, low, none)	set_business_impact
IP addresses/ranges	ips	add_ips remove_ips set_ips
Scanner Appliances	appliance_ids Looking for appliance IDs? Use the Appliance API (/api/2.0/fo/appliance/). See KnowledgeBase	add_appliance_ids remove_appliance_ids set_appliance_ids
Default Scanner Appliance	default_appliance_id	set_default_appliance_id
Domains	domains	add_domains remove_domains set_domains
DNS Names	dns_names	add_dns_names remove_dns_names set_dns_names
NetBIOS Names	netbios_names	add_netbios_names remove_netbios_names set_netbios_names
Title	title (255 characters maximum)	set_title
CVSS Environmental Metric: Collateral Damage Potential	cvss_enviro_cdp (One of: high, medium-high, low-medium, low, none)	set_cvss_enviro_cdp

Parameter	Parameter Name action=add	Parameter Name action=edit
CVSS Environmental Metric: Target Distribution	cvss_enviro_td (One of: high, medium, low, none)	set_cvss_enviro_td
CVSS Environmental Metric: Confidentiality Requirement	cvss_enviro_cr (One of: high, medium, low)	set_cvss_enviro_cr
CVSS Environmental Metric: Integrity Requirement	cvss_enviro_ir (One of: high, medium, low)	set_cvss_enviro_ir
CVSS Environmental Metric: Availability Requirement	cvss_enviro_ar (One of: high, medium, low)	set_cvss_enviro_ar

Purge Hosts

/api/2.0/fo/asset/host/?action=purge

[POST]

Purge hosts in your account to remove the assessment data associated with them.

Purging hosts will remove host based data in the user's account (scan results will not be removed). Purged host information will not appear in new reports generated by users. One or both types of host data is removed, based on the user's API request: vulnerability data and compliance data.

Permissions

Managers can purge assessment data for all hosts in the subscription, including vulnerability data and/or compliance data.

Auditors can purge compliance data only for all compliance hosts in the subscription (vulnerability data will not be removed).

Unit Managers, Scanners, and Readers can purge vulnerability data and/or compliance data in their user account if granted the permission "Purge host information/history". The permission "Manage compliance" is required to purge compliance data.

Express Lite - This API is available to Express Lite users.

How to choose data scope for asset purge

The input parameter “data_scope” allows you to specify the type of data to purge from a host. Specify “vm” to purge vulnerability data, “pc” to purge compliance data, or “vm,pc” (irrespective of order) to purge both types of data.

You can also use the input parameter “compliance_enabled” to purge compliance data along with vulnerability data or vulnerability data only. This option does not allow you to purge compliance data only.

You can combine compliance_enabled and data_scope in the same request. Note, however, that anytime compliance_enabled=1 is specified, then both vulnerability and compliance data is purged regardless of the data_scope value. See the table below to understand the different combinations and the type of data purged.

compliance_enabled value	data_scope value	type of data purged
1	unspecified	vulnerability + compliance data
0	unspecified	vulnerability data only
unspecified or 0	vm	vulnerability data only
unspecified or 0	pc	compliance data only
unspecified or 0	vm,pc	vulnerability + compliance data
1	vm	vulnerability + compliance data
1	pc	vulnerability + compliance data
1	vm,pc	vulnerability + compliance data

Input Parameters

Parameter	Description
action=purge	(Required)
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When unspecified, parameters are not included in the XML output.
ids={value}	(Optional) Purge host information for certain host IDs/ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range is specified with a hyphen (for example, 190-400).Valid host IDs are required. One of these host selection parameters must be specified in an API request: ids, ips, ag_ids or ag_titles. Multiple host selection parameters may be specified together in the same request.
ips={value}	(Optional) Purge host information certain IP addresses/ranges. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).

Parameter	Description
ag_ids={value}	(Optional) Purge hosts belonging to asset groups with certain IDs. One or more asset group IDs and/or ranges may be specified. Multiple entries are comma separated. A range is specified with a dash (for example, 386941-386945). Valid asset group IDs are required. One of these host selection parameters must be specified in an API request: ids, ips, ag_ids or ag_titles. Multiple host selection parameters may be specified together in the same request.
ag_titles={value}	(Optional) Purge hosts belonging to asset groups with certain strings in the asset group title. One or more asset group titles may be specified. Multiple entries are comma separated (for example, My+First+Asset+Group,Another+Asset+Group). One of these parameters must be specified in an API request: ids, ips, ag_ids or ag_titles. Multiple host selection parameters may be specified together in the same request. These parameters are mutually exclusive and cannot be specified together: ag_ids and ag_titles.
network_ids={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.
no_vm_scan_since={date}	(Optional) Purge hosts not scanned since a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". User Permissions: An Auditor cannot be specify this parameter.
no_compliance_scan_since ={date}	(Optional) Purge compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z". User Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user account is granted certain permissions to purge compliance information. See "Input Parameters".

Parameter	Description
data_scope={value}	(Optional) The type of data to purge. Specify "vm" to purge vulnerability data, specify "pc" to purge compliance data, or specify both as a comma separated list to purge both types of data. If compliance_enabled=1 is specified in the same request, then vulnerability and compliance data will both be purged regardless of the data_scope value.
compliance_enabled={**0**|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. Specify 1 to purge compliance hosts in the user's account. These hosts are assigned to the PC module. When selected, the service will remove vulnerability data and compliance data associated with the selected hosts. Specify 0 to purge hosts which are not assigned to the PC module. When specified (without data_scope), the service will remove only vulnerability information associated with the selected hosts. Note: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user account is granted permissions to purge compliance information. An Auditor does not have permission to set compliance_enabled=0.
os_pattern={expression}	(Optional) Purge only hosts which have an operating system matching a certain regular expression. An empty value cannot be specified. Use "%5E%24" to match empty string. Important: The regular expression string you enter must follow the PCRE standard and it must be URL encoded. Sample regular expression strings for matching OS names: Qualys API - Host List Detection API samples (GitHub, see sample 17) For information about the Perl Compatible Regular Expressions (PCRE) standard visit: http://php.net/manual/en/book.pcre.php For the PCRE syntax, see: http://php.net/manual/en/reference.pcre.pattern.syntax.php http://www.php.net/manual/en/reference.pcre.pattern.posix.php

Sample 1 - Purge only compliance data

In this example, data_scope=pc so only compliance data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=pc"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:51:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (compliance data) for Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 2 - Purge only vulnerability data

In this example, data_scope=vm so only vulnerability data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:51:45Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability data) for Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 3 - Purge vulnerability and compliance data

In this example, data_scope=pc,vm so both vulnerability and compliance data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=pc,vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:52:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability + compliance data) for
Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 4 - Purge vulnerability and compliance data (using compliance_enabled)

In this example, compliance_enabled=1 and data_scope=pc. Both vulnerability and compliance data will be purged for the host since compliance_enabled=1 takes precedence.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.154&compliance_enabled=1&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T11:25:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability + compliance data) for
Purging</TEXT>
```

```
        <ID_SET>
          <ID>3971340</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 5 - Purge only vulnerability data (using compliance_enabled)

In this example, compliance_enabled=0 and data_scope=vm so only vulnerability data will be purged.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.154&compliance_enabled=0&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T11:25:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability data) for Purging</TEXT>
        <ID_SET>
          <ID>3971340</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD

<platform API server>/api/2.0/fo/asset/host/dtd/purge/output.dtd

Patch List

/api/2.0/fo/asset/patch/index.php

[GET]

The Patch API lets you view the list of all superseding patches for detection on specific host. For the host, the Patch Info List provides information such as detection QID, patch QID, patch severity, patch title, patch vendor ID, patch release date, and patch links.

User permissions - Managers and Unit Managers can fetch the patch list on assets in their own business unit. Scanners and Readers fetch the patch list on assets in their own account.

Input Parameters

Parameter	Description
host_id={value}	(Required) The output lists all the superseding patches that will fix the detections on a single host instance. Specify the ID for the host to include in the report. A valid host ID must be entered.
output_format={xml}	(Optional) Specifies the format of the host detection list output. When not specified, the output format is xml. A valid value is xml.

Sample 1: Patch List

API request:

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "X-Requested-With: curl"
-H "Content-Type: text/xml"
"host_id=136801&output_format=xml"
"https://qualysapi.qualys.com/api/2.0/fo/asset/patch/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PATCH_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/patch/host_patches.
dtd">
<PATCH_LIST_OUTPUT>
  <RESPONSE>
    <SUBSCRIPTION_ID>3058</SUBSCRIPTION_ID>
    <HOST_ID>136801</HOST_ID>
    <IP>10.10.25.249</IP>
    <DNS><![CDATA[ora11107-25-249]]></DNS>
    <NETBIOS><![CDATA[ORA11107-25-249]]></NETBIOS>
    <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
    <OS_CPE><![CDATA[]]></OS_CPE>
```

```
    <NETWORK><![CDATA[Star Trek]]></NETWORK>
    <PATCH_INFO_LIST>
      <PATCH_INFO>
        <DETECTION_QIDS>
          <QID cve_ids=""><![CDATA[19883]]></QID>
        </DETECTION_QIDS>
        <PATCH_QID cve_ids=""><![CDATA[19883]]></PATCH_QID>
        <PATCH_SEVERITY>4</PATCH_SEVERITY>
       <PATCH_TITLE><![CDATA[Oracle 11.1.0.7 on Microsoft Windows
- General Update Multiple Issues (Patch #54)]]></PATCH_TITLE>
        <PATCH_VENDOR_ID><![CDATA[11.1.0.7 Patch 54 -
32bit,11.1.0.7 Patch 54 - 64bit]]></PATCH_VENDOR_ID>
        <PATCH_RELEASE_DATE>2013-10-15
00:00:00</PATCH_RELEASE_DATE>
        <PATCH_LINKS>
          <LINK
os_sw="Windows"><![CDATA[https://support.oracle.com/epmos/faces/ui
/patch/PatchDetail.jspx?patchId=17363759]]></LINK>
          <LINK
os_sw="Windows"><![CDATA[https://support.oracle.com/epmos/faces/ui
/patch/PatchDetail.jspx?patchId=17363760]]></LINK>
        </PATCH_LINKS>
      </PATCH_INFO>
    </PATCH_INFO_LIST>
  </RESPONSE>
</PATCH_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/asset/patch/host_patches.dtd

IPv6 Assets

The IPv6 Assets API allows Manager users to manage IPv6 assets so they can be scanned using Qualys. The IPv6 API can be used when the IPv6 Support feature is enabled in the user's subscription. Please contact Support if you would like this feature enabled for your account.

API Support for IPv6 Asset Management and Scanning

IPv6 Mapping Record List

Add IPv6 Mapping Records

API Support for IPv6 Asset Management and Scanning

IPv6 Support is a subscription-level option that must be enabled for your subscription by Qualys Support in order to start managing and scanning IPv6 hosts. Follow the steps below to get started with managing and scanning IPv6 hosts using the API.

Step 1: Add Special IPv4 Addresses to your subscription

Using the Asset API add to your subscription the special, mapping IPv4 addresses. These IPv4 addresses are used for mapping IPv4 addresses to your IPv6 hosts. The IPv4 addresses for mapping are in the special 0.0.0.0/8 network, in this range:

```
0.0.0.1-0.254.255.255
```

A sample request for adding the special IPv4 addresses is shown below (where qualysapi.qualys.com is the server URL where your Qualys account is located):

```
https://qualysapi.qualys.com/msp/asset_ip.php?action=add&
host_ips=0.0.0.1-0.0.0.255
```

Step 2: Add IPv6 Mapping Records

Manager users can add IPv6 mapping records for the subscription by submitting the records in CSV or XML format. Each mapping record associates one IPv6 address in your network to one IPv4 address in the special mapping range 0.0.0.1-0.254.255.255. A maximum of 10,000 records can be added or removed per API request.

How to Add IPv6 Records in CSV

Review the steps below to learn how to add IPv6 mapping records by submitting the records in CSV format. A curl client is used to illustrate this process.

1) View Mapping Records in CSV

API request:

```
$ curl -u username:password -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/?action=li
st&output_format=csv"
```

XML output:

Note: The service automatically returns an ID value in the ID column for each IPv6 mapping record. This ID is assigned by the service when the record is created.

```
----BEGIN_RESPONSE_BODY_CSV
ID,IPv4,IPv6
"46947","0.0.0.7","2001:db8:85a3::8a2e:370:84"
"47036","0.0.0.1","2001:db8:85a3::8a2e:370:77"
----END_RESPONSE_BODY_CSV
----BEGIN_RESPONSE_FOOTER_CSV
"Status Message"
"Finished"
----END_RESPONSE_FOOTER_CSV
```

2) Prepare file1.csv with records to be added

The CSV file contents identify one or more IPv6 mapping records to be added. The columns in the CSV upload file are described below.

Column	Description
IPv4	(Required) An IPv4 address. The IPv4 address can be defined in only one IPv6 mapping record within your subscription.
IPv6	(Required) An IPv6 address. The IPv6 address can be defined in only one IPv6 mapping record within your subscription.
ID	(Optional) A user-defined, custom ID may be included. Important: Custom ID values will not be saved with record data within your subscription.

The CSV file must include the input parameters action=add and csv_data=. The parameter all_or_nothing is optional. When set to 1 or unspecified, the service cancels the request and does not add any new records if it finds the upload data has one record with an IP conflict. When set to 0 the service does not cancel the request if an IP conflict is found.

Sample file1.csv used to add IPv6 mapping records:

```
$ cat file1.csv
action=add&all_or_nothing=1&csv_data=
"0.0.0.2","2001:470:8418:a18::a0a:1805"%0A
"0.0.0.3","2001:470:8418:a18::a0a:ab7"%0A
"0.0.0.4","2001:470:8418:a18::a0a:1849"%0A
"0.0.0.5","2001:470:8418:a18::a0a:189c"%0A
"0.0.0.6","2001:470:8418:a18::a0a:189d"%0A
"0.0.0.8","2001:470:8418:a18::a0a:189e"%0A
```

```
"0.0.0.9","2001:470:8418:a18::a0a:18d0"%0A
"0.0.0.10","2001:470:8418:a18::a0a:18d1"%0A
"0.0.0.11","2001:470:8418:a18::a0a:18d2"%0A
"0.0.0.12","2001:470:8418:a18::a0a:18d6"%0A
"0.0.0.13","2001:470:8418:a18::a0a:18d7"%0A
"0.0.0.14","2001:470:8418:a18::a0a:18da"%0A
"0.0.0.15","2001:470:8418:a18::a0a:18db"%0A
"0.0.0.16","ff00:abcd::1234"%0A
```

3) POST data from file1.csv (Success)

Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
-d @file1.csv
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2011-11-03T19:31:27Z</DATETIME>
    <TEXT>Successfully imported 14 records
</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

How to Add IPv6 Records in XML

Review the steps below to learn how to add IPv6 mapping records by submitting the records in XML format. A curl client is used to illustrate this process.

1) View mapping records in XML

API request:

```
$ curl -u username:password -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/?action=li
st&output_format=xml"
```

Output:

Note: The service automatically returns an ID value in the <ID> element for each IPv6 mapping record. This ID is assigned by the service when the record is created.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_MAP_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/ip_map_lis
t_output.dtd">
<IP_MAP_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2011-11-28T19:42:10Z</DATETIME>
   <IP_MAP_LIST>
     <IP_MAP>
       <ID>46947</ID>
       <V4>0.0.0.7</V4>
       <V6>2001:db8:85a3::8a2e:370:84</V6>
     </IP_MAP>
     <IP_MAP>
       <ID>47036</ID>
       <V4>0.0.0.1</V4>
       <V6>2001:db8:85a3::8a2e:370:77</V6>
     </IP_MAP>
   </IP_MAP_LIST>
 </RESPONSE>
</IP_MAP_LIST_OUTPUT>
```

2) Prepare file2.xml with records to be added

The XML file contents identify one or more IPv6 mapping records to be added. The element in the XML upload file are described below.

Column	Description
<V4>	(Required) An IPv4 address. The IPv4 address can be defined in only one IPv6 mapping record within your subscription.
<V6>	(Required) An IPv6 address. The IPv6 address can be defined in only one IPv6 mapping record within your subscription.
<ID>	(Optional) A user-defined, custom ID may be included. Important: Custom ID values will not be saved with record data within your subscription.

The XML file must include the input parameters action=add and xml_data=. The parameter all_or_nothing is optional. When set to 1 or unspecified, the service cancels the request and does not add any new records if it finds the upload data has one record with an IP conflict. When set to 0 the service does not cancel the request if an IP conflict is found.

Sample file2.xml used to add IPv6 mapping records:

```
$ cat file2.xml
action=add&xml_data=
<IP_MAP_LIST>
```

```
  <IP_MAP>
    <V4>0.0.0.2</V4>
    <V6>2001:470:8418:a18::a0a:1805</V6>
  </IP_MAP>
  <IP_MAP>
    <V4>0.0.0.3</V4>
    <V6>2001:470:8418:a18::a0a:ab7</V6>
  </IP_MAP>
</IP_MAP_LIST>
```

3) POST data from file2.xml (Success)

API request:

```
$ curl -u username:password -H "X-Requested-With: curl"
-d @file2.xml
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2011-11-03T20:59:07Z</DATETIME>
    <TEXT>Successfully imported 2 records</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Step 3: Enable IPv6 for Scanner Appliance(s)

IPv6 scanning is supported using a scanner appliance enabled with IPv6. You can enable this by editing the appliance within the Qualys user interface. Once IPv6 is enabled, the appliance uses stateless address autoconfiguration to obtain an IPv6 address from the router (note that stateful configuration through DHCPv6 or Static IPv6 is not supported).

Step 4: Launch Scan

Using the Qualys API you can launch scans on the IPv4 addresses which are mapped to IPv6 addresses.

Step 5: View IPv6 Addresses using Host List Detection API

The scan results XML output will include IPv4 addresses only. Also, scan reports downloaded from the user interface will include IPv4 addresses only.

The host list detection output returned from a host list detection API request (api/2.0/fo/asset/host/vm/detection/?action=list) gives you the IPv6 address, if available, along with the “automatic” vulnerability detection data.

To request a list of VM scanned hosts which have IPv4 addresses that are mapped to IPv6 addresses in your account, you enter the IPv4 addresses for the ips parameter.

For example, if the special IPv4 address 0.0.0.199 is mapped to an IPv6 address in your account and this IP address has been scanned, you can make this API request:

```
curl -H "X-Requested-With: Curl Sample" -u "username:password"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?
action=list&ips=0.0.0.100"
```

XML output returned will show the IPv4 address and the IPv6 address for the host, as shown below (XML fragment):

```
...
<HOST>
        <ID>276010</ID>
        <IP>0.0.0.100</IP>
        <IPV6>2001:470:8418:a18::a0a:18c7</IPV6>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows 2003 Service Pack 2]]></OS>
        <DNS><![CDATA[mssql2k8-24-199.patch.qualys.com]]></DNS>
        <LAST_SCAN_DATETIME>2018-06-
17T19:06:31Z</LAST_SCAN_DATETIME>
        <DETECTION_LIST>
        ...
```

IPv6 Mapping Record List

/api/2.0/fo/asset/ip/v4_v6

[GET] [POST]

View a list of IPv6 mapping records in the subscription. Each mapping record associates one IPv6 address in your network with one IPv4 address in the special mapping range 0.0.0.1-0.254.255.255.

A maximum of 5,000 IPv6 mapping records will be processed per request, unless the truncation_limit input parameter is specified. If the requested list identifies more than 5,000 records or the number of records specified using truncation_limit, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of records.

Permissions - Managers can view all IPv6 mapping records when the IPv6 Support feature is enabled for the user's subscription. Other users do not have permission to view IPv6 mapping records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id_min={value}	(Optional) Show only mapping records which have a minimum record ID. A valid mapping record ID is required. When unspecified, records are not filtered by record ID.
id_max={value}	(Optional) Show only mapping records which have a maximum record ID. A valid mapping record ID is required.
ipv4_filter={value}	(Optional) Show only mapping records with certain IPv4 addresses. When unspecified, records are not filtered by IPv4 addresses.
ipv6_network={value}	(Optional) Show only mapping records with certain IPv6 network addresses. When unspecified, records are not filtered by IPv6 network addresses.
output_format={**CSV**|XML}	(Optional) The requested output format: CSV or XML. When unspecified, the output format will be CSV. Note: When the service outputs CSV, each line ends with a carriage-return and linefeed pair (ASCII/CRLF=0x0D 0x0A).
truncation_limit={value}	(Optional) The maximum number of mapping records to be returned by the API request. A valid value is an integer between 1 and 1,000,000. When unspecified, 5,000 records will be returned.

DTD

<platform API server>/api/2.0/fo/asset/ip/v4_v6/asset/ip/v4_v6/ip_map_list_output.dtd

Sample IPv6 Mapping Records List Output

How to Add IPv6 Records in CSV

How to Add IPv6 Records in XML

Add IPv6 Mapping Records

/api/2.0/fo/asset/ip/v4_v6

[POST]

Add IPv6 mapping records to the subscription. Each mapping record associates one IPv6 address in your network with one IPv4 address in the special mapping range 0.0.0.1-0.254.255.255. A maximum of 10,000 mapping records can be added per API request.

Permissions - Managers can add IPv6 mapping records, when the IPv6 Support feature is enabled for the user's subscription. Other user roles do not have these permissions.

Input Parameters

Parameter	Description
action=add	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
csv_data={value}	The CSV data file containing the IPv6 mapping records that you want to add. This parameter or xml_data must be specified. See How to Add IPv6 Records in CSV
	The parameters csv_data and xml_data cannot be specified in the same request.
xml_data={value}	The CSV data file containing the IPv6 mapping records that you want to add. This parameter or csv_data must be specified. See How to Add IPv6 Records in XML
	The parameters csv_data and xml_data cannot be specified in the same request.
all_or_nothing={0|**1**}	(Optional) This parameter controls how the service processes the IPv6 mapping records in the upload data. When unspecified or set to 1, the service cancels the request and does not add any new records once it finds the upload data has one record with an IP conflict. When set to 0 the service does not cancel the request if an IP conflict is found.

DTD

<platform API server>/api/2.0/simple_return.dtd

Sample XML Output

How to Add IPv6 Records in CSV

How to Add IPv6 Records in XML

Networks

The Network API is used to manage networks when the Network Support feature is enabled in the user's subscription.

Network List

Create Network

Update Network

Assign Scanner Appliance to Network

Network List

/api/2.0/fo/network/?action=list

[GET] [POST]

List custom networks in your account.

Permissions - A Manager will view all custom networks in the subscription, a Unit Manager will view custom networks in their business unit's assigned asset groups, and a Scanner/Reader will view custom networks in their account's assigned asset groups.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
ids={value1,value2}	(Optional) Filter the list to view specific networks.

Sample - List custom networks

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/network/?action=list&ids=
7343,7345,7350"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NETWORK_LIST SYSTEM
"https://qualysapi.qualys.com/network_list_output.dtd">
<RESPONSE>
```

```
  <DATETIME>2018-05-28T01:06:45Z</DATETIME>
  <NETWORK_LIST>
    <NETWORK>
      <ID>7343</ID>
      <NAME><![CDATA[My New Network]]></TITLE>
      <SCANNER_APPLIANCE_LIST>
        <SCANNER_APPLIANCE>
          <ID>1234</ID>
          <FRIENDLY_NAME><![[CDATA[abc123]]></FRIENDLY_NAME>
        </SCANNER_APPLIANCE>
      </SCANNER_APPLIANCE_LIST>
    </NETWORK>
    ...
  </NETWORK_LIST>
</RESPONSE>
```

DTD

<platform API server>/api/2.0/fo/network/network_list_output.dtd

Create Network

/api/2.0/fo/network/?action=create

[POST]

Create a new custom network.

Permissions - This API is available to Managers only.

Know more - Before you're ready to start scanning, you'll need to 1) assign scanner appliance(s) to your network, and 2) add host assets to your network (assign asset groups to it).

Input Parameters

Parameter	Description
action=create	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
name={value}	(Required) A user-defined friendly name for your network. A successful request will return a unique network ID and this is used to manage your network using the API.

Sample - Create custom network

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&name=My+Network"
"https://qualysapi.qualys.com/api/2.0/fo/network/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-14T04:37:24Z</DATETIME>
    <TEXT>Network created with ID</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>id</KEY>
        <VALUE>1103</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Update Network

/api/2.0/fo/network/?action=update

[POST]

Create a new custom network.

Permissions - This API is available to Managers only.

Input Parameters

Parameter	Description
action=update	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
name={value}	(Required) Specify a new network name. (The network ID is assigned by our service and it can't be changed.)

Sample - Update network

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"id=1130&action=update&name=Network+123"
"https://qualysapi.qualys.com/api/2.0/fo/network/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-05-20T06:17:06Z</DATETIME>
    <TEXT>Network updated</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>id</KEY>
        <VALUE>1103</VALUE>
      </ITEM>
      <ITEM>
        <KEY>name</KEY>
        <VALUE>Network 123</VALUE>
      </ITEM>
    </ITEM_LIST>
```

```
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Assign Scanner Appliance to Network

/api/2.0/fo/appliance/?action=assign_network_id

[POST]

Assign a scanner appliance to a network. When the network support feature is enabled for your subscription, scanner appliances are assigned to networks. Each appliance can be assigned to 1 network only.

Permissions - This API is available to Managers only.

Input Parameters

Parameter	Description
action=assign_network_id	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
appliance_id={value}	(Required) ID of the scanner appliance you want to assign to a network.
network_id={value}	(Required) ID of the network you want to assign the scanner appliance to.

Sample - Assign scanner appliance to network

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: test" -d
action=assign_network_id&appliance_id=506&network_id=1002"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2018-03-16T22:50:49Z</DATETIME>
    <TEXT>Success: Network ID=[1103] assigned to Appliance with
ID=[506]</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Or, if unsuccessful, the response might look like this:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-03-16T22:53:41Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT>parameter network_id has invalid value: 1103 (No such
network ID)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Reports

Launch and manage reports in your account. Report Share must be enabled for your account.

Report List

Launch Report

Launching Reports Using Asset Tags

Launching and Fetching Compliance Reports in CSV Format

Launching and Fetching Compliance Reports in XML Format

Report Template List

Launch Scorecard

Cancel Running Report

Download Saved Report

Delete Saved Report

Scheduled Reports List

Launch Scheduled Report

Asset Search Report

Report List

For API version information, refer to the API History Version section.

V2.0 | V3.0

V2.0

/api/2.0/fo/report/?action=list

[GET] [POST]

View a list of reports in the user's account when Report Share feature is enabled. The report list output includes all report types, including scorecard reports.

Note: You can generate a scan based report for a paused scan. The scan report still reflects all data processed prior to the pause.

User permissions - Managers and Auditors view all assets in the subscription, Unit Managers view assets in their own business unit, Scanners and Readers view assets in their own account.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id={value}	(Optional) Specifies a report ID of a report that is saved in the Report Share storage space. When specified, information on the selected report will be included in the XML output.
state={value}	(Optional) Specifies that reports with a certain state will be included in the XML output. By default, all states are included. A valid value is: Running (reports are in progress), Finished, Submitted, Canceled, or Errors.
user_login={value}	(Optional) Specifies a user login ID. This parameter is used to restrict the XML output to reports launched by the specified user login ID.
expires_before_datetime={date}	(Optional) Specifies the date and time (optional) when reports will expire in the future. Only reports that expire before this date/time will be included in the XML output. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.

Sample - List reports

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "<qualys_base_url>/api/2.0/fo/report/
?action=list"

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/report/report_list_output.dtd">

<REPORT_LIST_OUTPUT>
  <RESPONSE>
```

```
    <DATETIME>2017-10-30T22:32:15Z</DATETIME>
    <REPORT_LIST>
      <REPORT>
        <ID>42703</ID>
        <TITLE><![CDATA[Test now]]></TITLE>
        <TYPE>Scan</TYPE>
        <USER_LOGIN>acme_aa</USER_LOGIN>
        <LAUNCH_DATETIME>2017-10-30T17:59:22Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
        <SIZE>129.1 MB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2017-11-
06T17:59:24Z</EXPIRATION_DATETIME>
      </REPORT>
      <REPORT>
        <ID>42700</ID>
        <TYPE>Scorecard</TYPE>
        <USER_LOGIN>acme_ts2</USER_LOGIN>
        <LAUNCH_DATETIME>2017-10-29T22:12:42Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>SECURE_PDF</OUTPUT_FORMAT>
        <SIZE>18.1 KB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2017-11-
05T22:12:44Z</EXPIRATION_DATETIME>
      </REPORT>
      <REPORT>
        <ID>42699</ID>
        <TYPE>Scorecard</TYPE>
        <USER_LOGIN>quays_ts2</USER_LOGIN>
        <LAUNCH_DATETIME>2017-10-29T21:52:19Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
        <SIZE>19.87 KB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2017-11-
05T21:52:21Z</EXPIRATION_DATETIME>
      </REPORT>
    </REPORT_LIST>
  </RESPONSE>
</REPORT_LIST_OUTPUT>
```

DTD

<platform API server>/api/2.0/fo/report/report_list_output.dtd

V3.0

/api/3.0/fo/report/?action=list

[GET] [POST]

View a list of reports in the user's account when Report Share feature is enabled. The report list output includes all report types, including scorecard reports.

Note: You can generate a scan based report for a paused scan. The scan report still reflects all data processed prior to the pause.

User permissions - Managers and Auditors view all assets in the subscription, Unit Managers view assets in their own business unit, Scanners and Readers view assets in their own account.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id={value}	(Optional) Specifies a report ID of a report that is saved in the Report Share storage space. When specified, information on the selected report will be included in the XML output.
state={value}	(Optional) Specifies that reports with a certain state will be included in the XML output. By default, all states are included. A valid value is: Running (reports are in progress), Finished, Submitted, Canceled, or Errors.
user_login={value}	(Optional) Specifies a user login ID. This parameter is used to restrict the XML output to reports launched by the specified user login ID.
expires_before_datetime={date}	(Optional) Specifies the date and time (optional) when reports will expire in the future. Only reports that expire before this date/time will be included in the XML output. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like "2007-07-01" or "2007-01-25T23:12:00Z".
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.

Sample - List reports

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/report/?echo_request=1&action=list&i
d=6626811' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML Respnse:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/report/report_list_output.dtd">
```

```
<REPORT_LIST_OUTPUT>
    <REQUEST>
        <DATETIME>2025-06-17T12:25:55Z</DATETIME>
        <USER_LOGIN>John_doe</USER_LOGIN>
        <RESOURCE><qualys_base_url>/api/3.0/fo/report/</RESOURCE>
        <PARAM_LIST>
            <PARAM>
                <KEY>echo_request</KEY>
                <VALUE>1</VALUE>
            </PARAM>
            <PARAM>
                <KEY>action</KEY>
                <VALUE>list</VALUE>
            </PARAM>
            <PARAM>
                <KEY>id</KEY>
                <VALUE>6626811</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2025-06-17T12:25:56Z</DATETIME>
        <REPORT_LIST>
            <REPORT>
                <ID>6626811</ID>
                <TITLE>
                    <![CDATA[FQDN_template_Multiple]]>
                </TITLE>
                <TYPE>Scan</TYPE>
                <USER_LOGIN>John_doe</USER_LOGIN>
                <LAUNCH_DATETIME>2025-06-16T08:57:52Z</LAUNCH_DATETIME>
                <OUTPUT_FORMAT>CSV</OUTPUT_FORMAT>
                <SIZE>1.15 MB</SIZE>
                <STATUS>
                    <STATE>Finished</STATE>
                </STATUS>
                <EXPIRATION_DATETIME>2025-06-
23T08:57:55Z</EXPIRATION_DATETIME>
            </REPORT>
        </REPORT_LIST>
    </RESPONSE>
</REPORT_LIST_OUTPUT>
```

DTD

<platform API server>/api/3.0/fo/report/report_list_output.dtd

API History Version

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/report/?action=list	Active	Active
/api/2.0/fo/report/?action=list	December 2025	December 2026

Launch Report

For API version information, refer to the API History Version section.

V2.0 | V3.0

V2.0

/api/2.0/fo/report

[POST]

Launch a report in the user's account. The Report Share feature must be enabled in the user's subscription. When a report is launched with Report Share, the report is run in the background, and the report generation processing does not timeout until the report has completed.

User permissions - Managers and Auditors can launch scorecard reports on all assets in the subscription, Unit Managers can launch scorecard reports on assets in their own business unit, Scanners and Readers can launch scorecard reports on assets in their own account.

Note: The Launch Report API for Compliance Policy Reports is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Input Parameters

Parameter	Description
action=launch	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Parameter	Description
template_id={value}	(Required) The template ID of the report you want to launch. Use the /msp/report_template_list.php API to find the template ID you're interested in. See Report Template List.
report_title=[value}	(Optional) A user-defined report title. The title may have a maximum of 128 characters. For a PCI compliance report, the report title is provided by Qualys and cannot be changed.
output_format={value}	(Required) One output format may be specified. Supported formats for various reports are below. - map report: pdf, html (a zip file), xml, or csv - scan report: pdf, html (a zip file), xml, csv, or docx - remediation report: pdf, html (a zip file), or csv - compliance report (not PCI): pdf, html (a zip file) - PCI compliance report: pdf or html (a zip file) - patch report: pdf, online, xml or csv - compliance policy report: pdf, html (a zip file), xml, or csv (see Launching and Fetching Compliance Reports in CSV Format)
hide_header={**0**|1}	(Valid for CSV format report only). Specify hide_header=1 to omit the header information from the report. By default this information is included.
pdf_password={value}	(Required for secure PDF distribution, Manager or Unit Manager only) The password to be used for encryption. Requirements: - the password must have a minimum of 8 characters (ascii), and a maximum of 32 characters - the password must contain alpha and numeric characters - the password cannot match the password for the user's Qualys account. - the password must follow the password security guidelines defined for your subscription (log into your account and go to Users > Setup > Security)
recipient_group={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group names, as defined using the Qualys UI. Multiple distribution groups are comma separated. A maximum of 50 distribution groups may be entered.
	The recipient_group parameter can only be specified when the pdf_password parameter is also specified.
	The recipient_group parameter cannot be specified in the same request as recipient_group_id

Parameter	Description
recipient_group_id={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group IDs. Multiple distribution group IDs are comma separated. Where do I find this ID? Log in to your Qualys account, go to Users > Distribution Groups and select Info for a group in the list.
	The recipient_group_id parameter can only be specified when the pdf_password parameter is also specified.
	The recipient_group_id parameter cannot be specified in the same request as recipient_group
MAP REPORT	
report_type=Map	(Optional)
domain={value}	(Required for map report) Specifies the target domain for the map report. Include the domain name only; do not enter "www." at the start of the domain name. When the special "none" domain is specified as a parameter value, the ip_restriction parameter is required.
ip_restriction={value}	(Optional for map report) For a map report, specifies certain IPs/ranges to include in the report. This parameter is required when the domain parameter is specified with the value "none" (for the special "none" domain). Multiple IPs and/or ranges are comma separated.
report_refs={value}	(Required for map report) For a map report, specifies the map references (1 or 2) to include. A map reference starts with the string "map/" followed by a reference ID number. When two map references are given, the report compares map results. Two map references are comma separated.
SCAN REPORT - SCAN BASED FINDINGS	
report_type=Scan	(Optional)
report_refs={value}	(Required for Manual scan report) For a Manual scan report, this parameter specifies the scan references to include. A scan reference starts with the string "scan/" followed by a reference ID number. Multiple scan references are comma separated.
ip_restriction={value}	(Optional for Manual scan report) For a scan report, the report content will be restricted to the specified IPs/ranges. Multiple IPs and/or ranges are comma separated.

Parameter	Description
SCAN REPORT - HOST BASED FINDINGS	
report_type=Scan	(Optional)
ips={value}	(Optional) Specify IPs/ranges to change (overwrite) the report target, as defined in the report template. Multiple IPs/ranges are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional) Specify asset group IDs to change (overwrite) the report target, as defined in the report template. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
ips_network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) The ID of a network that is used to restrict the report's target to the IPs/ranges specified in the "ips" parameter. Set to a custom network ID (note this does not filter IPs/ranges specified in "asset_group_ids"). Or set to "0" (the default) for the Global Default Network - this is used to report on hosts outside of your custom networks.
PATCH REPORT	
ips={value}	(Optional for patch report) Specify IPs/ranges to change (override) the report target, as defined in the patch report template. Multiple IPs/ranges are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional for patch report) Specify IPs/ranges to change (override) the report target, as defined in the patch report template. Multiple asset group IDs are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
REMEDIATION REPORT	
report_type=Remediation	(Optional)

Parameter	Description
ips={value}	(Optional for remediation report) Specify IPs/ranges you want to include in the report. Multiple IPs and/or ranges are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional for remediation report) Specify asset group IDs that identify hosts you want to include in the report. Multiple asset group IDs are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
assignee_type={**User**|All}	(Optional for remediation report) Specifies whether the report will include tickets assigned to the current user (User is set by default), or all tickets in the user account. By default tickets assigned to the current user are included.
COMPLIANCE REPORT	
report_type=Compliance	(Optional) For compliance type report. Compliance type reports are Qualys Top 20 Report, SANS Top 20 Report, Qualys PCI Executive Report, and Qualys PCI Technical Report.
ips={value}	(Optional for compliance report) For a compliance report (except a PCI report), specify the IPs/ranges you want to include in the report. Multiple IPs and/or ranges are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
	Optional: Qualys Top 20 Report, SANS Top 20 Report
	Invalid: PCI Executive Report, PCI Technical Report
asset_group_ids={value}	(Optional for compliance report) For a compliance report (except a PCI report), specify asset groups IDs which identify hosts to include in the report. Multiple asset group IDs are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
	Optional: Qualys Top 20 Report, SANS Top 20 Report
	Invalid: PCI Executive Report, PCI Technical Report

Parameter	Description
report_refs={value}	(Required for PCI compliance report) For a PCI compliance report, either the technical or executive report, this parameter specifies the scan reference to include. A scan reference starts with the string "scan/" followed by a reference ID number. The scan reference must be for a scan that was run using the PCI Options profile. Only one scan reference may be specified.
	Required: PCI Executive Report, PCI Technical Report
	Invalid: Qualys Top 20 Report, SANS Top 20 Report
COMPLIANCE POLICY REPORT	
report_type=Policy	(Optional)
policy_id={value}	(Required) Specifies the policy to run the report on. A valid policy ID must be entered.
asset_group_ids={value}	(Optional) Specify asset group IDS if you want to include only certain asset groups in your report. These asset groups must be assigned to the policy you are reporting on. Multiple asset group IDs are comma separated.
	You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
ips={value}	(Optional) Specify IPs/ranges if you want to include only certain IP addresses in your report. These IPs must be assigned to the policy you're reporting on. Multiple entries are comma separated.
	You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
host_id={value}	(Optional) In the policy report output, show only results for a single host instance. Specify the ID for the host to include in the report. A valid host ID must be entered. This parameter must be specified with instance_string.
instance_string={value}	(Optional) Specifies a single instance on the selected host. The instance string may be "os" or a string like "oracle10:1:1521:ora10204u". Use the Compliance Posture Information API (with the endpoint/api/2.0/fo/compliance/posture/info) to find the appropriate instance string. This parameter must be specified with host_id.

DTD

<platform API server>/api/2.0/simple_return.dtd

Sample - Launch Report

```
curl -H "X-Requested-With: Curl Sample"
-d "action=launch&template_id=55469&output_format=pdf"
```

```
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/report/"

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-06-20T21:45:23Z</DATETIME>
    <TEXT>New report launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1665</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/report

[POST]

Launch a report in the user's account. The Report Share feature must be enabled in the user's subscription. When a report is launched with Report Share, the report is run in the background, and the report generation processing does not timeout until the report has completed.

User permissions - Managers and Auditors can launch scorecard reports on all assets in the subscription, Unit Managers can launch scorecard reports on assets in their own business unit, Scanners and Readers can launch scorecard reports on assets in their own account.

Note: The Launch Report API for Compliance Policy Reports is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Input Parameters

Parameter	Description
action=launch	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Parameter	Description
template_id={value}	(Required) The template ID of the report you want to launch. Use the /msp/report_template_list.php API to find the template ID you're interested in. See Report Template List.
report_title=[value}	(Optional) A user-defined report title. The title may have a maximum of 128 characters. For a PCI compliance report, the report title is provided by Qualys and cannot be changed.
output_format={value}	(Required) One output format may be specified. Supported formats for various reports are below. - map report: pdf, html (a zip file), xml, or csv - scan report: pdf, html (a zip file), xml, csv, or docx - remediation report: pdf, html (a zip file), or csv - compliance report (not PCI): pdf, html (a zip file) - PCI compliance report: pdf or html (a zip file) - patch report: pdf, online, xml or csv - compliance policy report: pdf, html (a zip file), xml, or csv (see Launching and Fetching Compliance Reports in CSV Format)
hide_header={**0**|1}	(Valid for CSV format report only). Specify hide_header=1 to omit the header information from the report. By default this information is included.
pdf_password={value}	(Required for secure PDF distribution, Manager or Unit Manager only) The password to be used for encryption. Requirements: - the password must have a minimum of 8 characters (ascii), and a maximum of 32 characters - the password must contain alpha and numeric characters - the password cannot match the password for the user's Qualys account. - the password must follow the password security guidelines defined for your subscription (log into your account and go to Users > Setup > Security)
recipient_group={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group names, as defined using the Qualys UI. Multiple distribution groups are comma separated. A maximum of 50 distribution groups may be entered.
	The recipient_group parameter can only be specified when the pdf_password parameter is also specified.
	The recipient_group parameter cannot be specified in the same request as recipient_group_id

Parameter	Description
recipient_group_id={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group IDs. Multiple distribution group IDs are comma separated. Where do I find this ID? Log in to your Qualys account, go to Users > Distribution Groups and select Info for a group in the list.
	The recipient_group_id parameter can only be specified when the pdf_password parameter is also specified.
	The recipient_group_id parameter cannot be specified in the same request as recipient_group
MAP REPORT	
report_type=Map	(Optional)
domain={value}	(Required for map report) Specifies the target domain for the map report. Include the domain name only; do not enter "www." at the start of the domain name. When the special "none" domain is specified as a parameter value, the ip_restriction parameter is required.
ip_restriction={value}	(Optional for map report) For a map report, specifies certain IPs/ranges to include in the report. This parameter is required when the domain parameter is specified with the value "none" (for the special "none" domain). Multiple IPs and/or ranges are comma separated.
report_refs={value}	(Required for map report) For a map report, specifies the map references (1 or 2) to include. A map reference starts with the string "map/" followed by a reference ID number. When two map references are given, the report compares map results. Two map references are comma separated.
SCAN REPORT - SCAN BASED FINDINGS	
report_type=Scan	(Optional)
report_refs={value}	(Required for Manual scan report) For a Manual scan report, this parameter specifies the scan references to include. A scan reference starts with the string "scan/" followed by a reference ID number. Multiple scan references are comma separated.
ip_restriction={value}	(Optional for Manual scan report) For a scan report, the report content will be restricted to the specified IPs/ranges. Multiple IPs and/or ranges are comma separated.

Parameter	Description
SCAN REPORT - HOST BASED FINDINGS	
fqdns={value}	(Optional) The target FQDN for a vulnerability scan. You must specify at least one target such as Ips, asset groups, or FQDNs. Multiple values are comma-separated.
report_type=Scan	(Optional) specify the report type as scan
ips={value}	(Optional) Specify IPs/ranges to change (overwrite) the report target, as defined in the report template. Multiple IPs/ranges are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional) Specify asset group IDs to change (overwrite) the report target, as defined in the report template. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
ips_network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) The ID of a network that is used to restrict the report's target to the IPs/ranges specified in the "ips" parameter. Set to a custom network ID (note this does not filter IPs/ranges specified in "asset_group_ids"). Or set to "0" (the default) for the Global Default Network - this is used to report on hosts outside of your custom networks.
PATCH REPORT	
ips={value}	(Optional for patch report) Specify IPs/ranges to change (override) the report target, as defined in the patch report template. Multiple IPs/ranges are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional for patch report) Specify IPs/ranges to change (override) the report target, as defined in the patch report template. Multiple asset group IDs are comma separated. When specified, hosts defined in the report template are not included in the report. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
REMEDIATION REPORT	
report_type=Remediation	(Optional)

Parameter	Description
ips={value}	(Optional for remediation report) Specify IPs/ranges you want to include in the report. Multiple IPs and/or ranges are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
asset_group_ids={value}	(Optional for remediation report) Specify asset group IDs that identify hosts you want to include in the report. Multiple asset group IDs are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
assignee_type={**User**|All}	(Optional for remediation report) Specifies whether the report will include tickets assigned to the current user (User is set by default), or all tickets in the user account. By default tickets assigned to the current user are included.
COMPLIANCE REPORT	
report_type=Compliance	(Optional) For compliance type report. Compliance type reports are Qualys Top 20 Report, SANS Top 20 Report, Qualys PCI Executive Report, and Qualys PCI Technical Report.
ips={value}	(Optional for compliance report) For a compliance report (except a PCI report), specify the IPs/ranges you want to include in the report. Multiple IPs and/or ranges are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
	Optional: Qualys Top 20 Report, SANS Top 20 Report
	Invalid: PCI Executive Report, PCI Technical Report
asset_group_ids={value}	(Optional for compliance report) For a compliance report (except a PCI report), specify asset groups IDs which identify hosts to include in the report. Multiple asset group IDs are comma separated. You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
	Optional: Qualys Top 20 Report, SANS Top 20 Report
	Invalid: PCI Executive Report, PCI Technical Report

Parameter	Description
report_refs={value}	(Required for PCI compliance report) For a PCI compliance report, either the technical or executive report, this parameter specifies the scan reference to include. A scan reference starts with the string "scan/" followed by a reference ID number. The scan reference must be for a scan that was run using the PCI Options profile. Only one scan reference may be specified.
	Required: PCI Executive Report, PCI Technical Report
	Invalid: Qualys Top 20 Report, SANS Top 20 Report
COMPLIANCE POLICY REPORT	
report_type=Policy	(Optional)
policy_id={value}	(Required) Specifies the policy to run the report on. A valid policy ID must be entered.
asset_group_ids={value}	(Optional) Specify asset group IDS if you want to include only certain asset groups in your report. These asset groups must be assigned to the policy you are reporting on. Multiple asset group IDs are comma separated.
	You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
ips={value}	(Optional) Specify IPs/ranges if you want to include only certain IP addresses in your report. These IPs must be assigned to the policy you're reporting on. Multiple entries are comma separated.
	You can specify ips and/or asset_group_ids, or asset tags (see Launching Reports Using Asset Tags).
host_id={value}	(Optional) In the policy report output, show only results for a single host instance. Specify the ID for the host to include in the report. A valid host ID must be entered. This parameter must be specified with instance_string.
instance_string={value}	(Optional) Specifies a single instance on the selected host. The instance string may be "os" or a string like "oracle10:1:1521:ora10204u". Use the Compliance Posture Information API (with the endpoint/api/2.0/fo/compliance/posture/info) to find the appropriate instance string. This parameter must be specified with host_id.

DTD

<platform API server>/api/3.0/simple_return.dtd

Sample - Launch Report

API Request:

```
curl --location
'<qualys_base_url>/api/3.0/fo/report/?action=launch&output_format=csv&tem
plate_id=8737800' \
--header 'X-Requested-With: Curl Sample' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Encoded username:passwordstring' \
--data-urlencode 'action=launch' \
--data-urlencode 'report_title=FQDN_API_CSV_Launch' \
--data-urlencode 'fqdns=ctomcatw2012.cis2016.comp.rdlab.qualys.com'
```

XML Response:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T05:45:04Z</DATETIME>
        <TEXT>New report launched</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>6627423</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

API History Version

he following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
api/3.0/fo/report/	Active	Active
api/2.0/fo/report/	December 2025	June 2026

Launching Reports Using Asset Tags

It's possible to select asset tags for both vulnerability and compliance reports. Use the following tag parameters to launch your report using asset tags.

Parameter	Description
use_tags={**0**|1}	(Optional) Specify 1 when your report target will include asset tags. Specify 0 (the default) when your report target will include IP addresses/ranges and/or asset groups. When not specified, use_tags=0 is used.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
	tag_include_selector is valid only when use_tags=1 is specified.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
	tag_exclude_selector is valid only when use_tags=1 is specified.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
	tag_set_by is valid only when use_tags=1 is specified.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	tag_set_include is valid only when use_tags=1 is specified.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	tag_set_exclude is valid only when use_tags=1 is specified.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=launch&template_id=55469&report_title=My+Windows+Report&ou
tput_format=pdf&use_tags=1&tag_set_by=name&tag_set_include=Windows
" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2014-02-20T21:45:23Z</DATETIME>
        <TEXT>New report launched</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1665</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Launching and Fetching Compliance Reports in CSV Format

Policy Compliance Reporting Service (PCRS) is a new reporting service to improve performance in Policy Compliance report generation. With PCRS, we've enhanced policy reports in CSV format by automatically compressing large size reports. When you run a policy report in CSV format, the report will be in ZIP format if the report size is between 1 GB and 5 GB; while reports less than 1 GB will be in CSV format. Similar improvements to other report formats will be added soon. You can download reports from the user interface or fetch reports by using APIs.

Note: This feature will be automatically enabled for customers with the release of Qualys Policy Compliance Reporting Service 1.0.0. Contact Qualys Support if you do not want this feature to be enabled for your subscription.

Important: If you are currently using the Report API to launch and fetch compliance policy reports in CSV format, then it's important to note that once PCRS is enabled for your subscription, any CSV compliance policy report that is over 1GB in size will be compressed automatically and you will get a ZIP file instead of a CSV file. You'll need to update your code or work with your 3rd party vendor to monitor the response header and if the report is compressed, add a step to uncompress the ZIP file before parsing the data.

When fetching a report using the API, the response header will indicate if the report is compressed or not. See the API samples that follow.

- In case of compressed reports, header content-type is - application/zip

- In case of uncompressed reports, header content-type is - text/csv

Sample: Report size more than 1 GB

In this sample, the report being downloaded is more than 1GB in size.

API Request

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=fetch&id=<REPORT ID>" "<qualys_base_url>/api/2.0/fo/report/"
```

Response Header

You'll notice that the header Content-Type is "application/zip"

```
* About to connect() to qualysapi.xxx.qualys.com port <PORT NUMBER> (#0)
*   Trying xx.xx.x.xxx ...
* Connected to qualysapi.xxx.qualys.com (xx.xx.x.xxx) port <PORT NUMBER>
(#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: CN=*.xxx.qualys.com,OU=Engineering,O="Qualys,
Inc.",L=Foster City,ST=California,C=US
*       start date: Sep 16 09:45:00 2020 GMT
*       expire date: Sep 16 09:45:00 2022 GMT
*       common name: *.xxx.qualys.com
*       issuer: E=xx@qualys.com,CN=Qualys Ops
T2v1,OU=Operations,O="Qualys, Inc.",L=Redwood City,ST=California,C=US
* Server auth using Basic with user '<USER NAME>'
> POST /api/2.0/fo/report/ HTTP/1.1
> Authorization: <AUTHORIZATION TOKEN>
> User-Agent: curl/7.29.0
> Host: qualysapi.xxx.qualys.com
> Accept: */*
> X-Requested-With:curl demo2
> Content-Length: 22
> Content-Type: application/x-www-form-urlencoded
>
} [data not shown]
* upload completely sent off: 22 out of 22 bytes
< HTTP/1.1 200 OK
< Date: Thu, 07 Oct 2021 11:15:03 GMT
< Server: Qualys
< Strict-Transport-Security: max-age=63072000;
< X-XSS-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< X-RateLimit-Limit: 300
< X-RateLimit-Window-Sec: 3600
< X-Concurrency-Limit-Limit: 2
< X-Concurrency-Limit-Running: 0
< X-RateLimit-ToWait-Sec: 0
< X-RateLimit-Remaining: 297
< Content-Length: 221540169
< Connection: keep-alive
< Content-Disposition: attachment; filename=<FILENAME>.zip
< Content-Type: application/zip
```

Sample: Report size less than 1 GB

In this sample, the report being downloaded is less than 1GB in size.

API Request

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=fetch&id=<REPORT ID>" "<qualys_base_url>/api/2.0/fo/report/"
```

Response Header

You'll notice that the header Content-Type is "text/csv;charset=UTF-8"

```
* About to connect() to qualysapi.xxx.qualys.com port <PORT NUMBER> (#0)
*   Trying xx.xx.x.xxx...
* Connected to qualysapi.xxx.qualys.com (xx.xx.x.xxx) port <PORT NUMBER>
(#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: CN=*.xxx.qualys.com,OU=Engineering,O="Qualys,
Inc.",L=Foster City,ST=California,C=US
*       start date: Sep 16 09:45:00 2020 GMT
*       expire date: Sep 16 09:45:00 2022 GMT
*       common name: *.xxx.qualys.com
*       issuer: E=xx@qualys.com,CN=Qualys Ops
T2v1,OU=Operations,O="Qualys, Inc.",L=Redwood City,ST=California,C=US
* Server auth using Basic with user '<user name>'
> POST /api/2.0/fo/report/ HTTP/1.1
> Authorization: <AUTHORIZATION TOKEN>
> User-Agent: curl/7.29.0
> Host: qualysapi.xxx.qualys.com
> Accept: */*
> X-Requested-With:curl demo2
> Content-Length: 22
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 22 out of 22 bytes
< HTTP/1.1 200 OK
< Date: Thu, 07 Oct 2021 11:16:21 GMT
< Server: Qualys
< Strict-Transport-Security: max-age=63072000;
< X-XSS-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< X-RateLimit-Limit: 300
< X-RateLimit-Window-Sec: 3600
< X-Concurrency-Limit-Limit: 2
< X-Concurrency-Limit-Running: 0
< X-RateLimit-ToWait-Sec: 0
< X-RateLimit-Remaining: 296
< Content-Length: 294850
< Connection: keep-alive
```

```
< Content-Disposition: attachment;
filename=Compliance_Report_PCRA_326___xxx.csv
< Content-Type: text/csv;charset=UTF-8
```

Launching and Fetching Compliance Reports in XML Format

You can now retrieve the posture modification date in the Compliance policy report when each control posture status changes from Pass to Fail. Retrieving the posture modification date in the compliance policy report helps you monitor the 90-day SLA to remediate failed controls.

To display the posture modification date in the report, you must select the Posture Modified Date checkbox in the report template (Reports > Templates > Policy Template > Layout > Posture Modified Date) in the user interface or fetch reports by using API for XML.

When you run the policy report in XML, a new DTD tag Posture_Modified_Date is added to the XML structure of the report downloaded in XML format. This tag displays the control posture modification date when the Posture Modified Date checkbox is selected in the report template.

Note: There are no changes to the input parameters or API response when launching the report.

Sample - Download Compliance Policy Report in XML Format

API Request

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "xx_xx:Xxxx123#" -d
"action=fetch&id=2346276"
"https://<qualys_base_url>/api/2.0/fo/report/
```

API Response

```
[root@panzer Xxxxx]# curl -k -s -S -H 'X-Requested-With:curl
demo2' -u "xxx_xx:Xxxxx123#" -d "action=fetch&id=2349933"
"https://<qualys_base_url>/api/2.0/fo/report/"
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM
"https://<qualys_base_url>/compliance_policy_report.dtd">
<COMPLIANCE_POLICY_REPORT>
  <HEADER>
    <NAME><![CDATA[DEF]]></NAME>
    <GENERATION_DATETIME>2024-12-
16T05:40:36Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[vish]]></NAME>
      <ADDRESS><![CDATA[457,890]]></ADDRESS>
      <CITY><![CDATA[Pune]]></CITY>
      <STATE><![CDATA[None]]></STATE>
      <COUNTRY><![CDATA[Iceland]]></COUNTRY>
```

```
      <ZIP_CODE><![CDATA[87]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[username]]></NAME>
      <USERNAME>user_name</USERNAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
    <FILTERS>
      <POLICY_ID><![CDATA[892678]]></POLICY_ID>
      <POLICY><![CDATA[Postgre_SQL_policy]]></POLICY>
      <POLICY_LOCKING><![CDATA[Unlocked]]></POLICY_LOCKING>
      <ASSET_GROUPS>
        <ASSET_GROUP>
          <ID><![CDATA[786415]]></ID>
          <NAME><![CDATA[10.10.
32.227 HA]]></NAME>
        </ASSET_GROUP>
      </ASSET_GROUPS>
      <PC_AGENT_IPS><![CDATA[No]]></PC_AGENT_IPS>
      <POLICY_LAST_EVALUATED><![CDATA[04/18/2023 at 21:10:46
(GMT+0530)]]></POLICY_LAST_EVALUATED>
    </FILTERS>
  </HEADER>
  <SUMMARY>
    <TOTAL_ASSETS>1</TOTAL_ASSETS>
    <TOTAL_CONTROLS>82</TOTAL_CONTROLS>
    <CONTROL_INSTANCES>
      <TOTAL>75</TOTAL>
      <TOTAL_PASSED>69</TOTAL_PASSED>
      <TOTAL_FAILED>0</TOTAL_FAILED>
      <TOTAL_ERROR>6</TOTAL_ERROR>
      <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
    </CONTROL_INSTANCES>
    <HOST_STATISTICS>
      <HOST_INFO>
        <IP><![CDATA[10.
11.70.116]]></IP>
        <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
        <DNS><![CDATA[-]]></DNS>
        <NETBIOS><![CDATA[-]]></NETBIOS>
        <OPERATING_SYSTEM><![CDATA[CentOS
6.9]]></OPERATING_SYSTEM>
        <LAST_SCAN_DATE><![CDATA[2023-04-
18T15:33:51Z]]></LAST_SCAN_DATE>
        <PERCENTAGE>92% (69 of 75)</PERCENTAGE>
        <HOST_ID><![CDATA[16
```

```
80546]]></HOST_ID>
      </HOST_INFO>
    </HOST_STATISTICS>
  </SUMMARY>
  <RESULTS>
    <HOST_LIST>
      <HOST>
        <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
        <QG_HOSTID><![CDATA[]]></QG_HOSTID>
        <IP><![CDATA[10.
11.70.116]]></IP>
        <OPERATING_SYSTEM><![CDATA[CentOS
6.9]]></OPERATING_SYSTEM>
        <LAST_SCAN_DATE>2023-04-18T15:33:51Z</LAST_SCAN_DATE>
        <TOTAL_PASSED>69</TOTAL_PASSED>
        <TOTAL_FAILED>0</TOTAL_FAILED>
        <TOTAL_ERROR>6</TOTAL_ERROR>
        <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
        <ASSET_TAGS>
          <ASSET_TAG><![CDATA[WIn 2008]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[Mongo DB 3.x]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[Dee_BU]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[Postgre SQL AG]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[Postgre SQL]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[
Amol Business Unit]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[10.
10.32.227 HA]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[10.
11.70.116 HA]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[centos 6]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[BU with Specific AG]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[BU1]]></ASSET_TAG>
          <ASSET_TAG><![CDATA[Nov6 Beta]]></ASSET_TAG>
        </ASSET_TAGS>
        <CONTROL_LIST>
          <CONTROL>
            <CID>15835</CID>
            <STATEMENT><![CDATA[Status of parameter
'log_rotation_age' in postgresql.conf]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[MINIMAL1]]></LABEL>
              <VALUE>1</VALUE>
            </CRITICALITY>
            <RATIONALE><![CDATA[The 'log_rotation_age'  this
parameter determines the maximum lifetime of an individual log
```

```
file.</RATIONALE>
            <INSTANCE><![CDATA[PostgreSQL 10.x (Port: 5
432, Database: postgres)]]></INSTANCE>
            <STATUS><![CDATA[Passed]]></STATUS>
            <TECHNOLOGY>
              <ID><![CDATA[143]]></ID>
              <NAME>PostgreSQL 10.x</NAME>
            </TECHNOLOGY>
           <EVALUATION_DATE>2023-04-18T15:40:46Z</EVALUATION_DATE>
            <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
            <POSTURE_MODIFIED_DATE>2021-12-
06T11:29:13Z</POSTURE_MODIFIED_DATE>
            <EVIDENCE><![CDATA[CHECK1]]></EVIDENCE>
            </CONTROL>
            <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,log_min_messages,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK3</NAME>
        <DP_NAME>pgsql.secman.hba_rule.unix_socket_trust</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z" />
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK4</NAME>

<DP_NAME>pgsql.secman.hba_rule.tcpip_socket_trust</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
```

```
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z" />
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK5</NAME>
        <DP_NAME>pgsql.secman.conf_file.log_connections</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK13</NAME>
        <DP_NAME>pgsql.secman.perms_bin_files</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/clusterdb]]></V>
```

```
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/createdb]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/createuser]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/dropdb]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/dropuser]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/ecpg]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/initdb]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/oid2name]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pgbench]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_archivecleanup]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_basebackup]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_config]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_controldata]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_ctl]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_dump]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_dumpall]]></V>
          <V><![CDATA[
root:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_isready]]></V>
          <V><![CDATA[root
:root:rwxr-xr-x:/usr/pgsql-10/bin/pg_receivewal]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_recvlogical]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_resetwal]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_restore]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_rewind]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_standby]]></V>
          <V><![CDATA[root:
```

```
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_test_fsync]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_test_timing]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_upgrade]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/pg_waldump]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/postgres]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/postmaster]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/psql]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/reindexdb]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/vacuumdb]]></V>
          <V><![CDATA[root:
root:rwxr-xr-x:/usr/pgsql-10/bin/vacuumlo]]></V>
        </ACTUAL>
         Row 2:
/var/lib/pgsql/10/data/postgresql.conf,log_rotation_size,
            Row 2:
/var/lib/pgsql/10/data/postgresql.conf,tcp_keepalives_idle,
            Row 2:
/var/lib/pgsql/10/data/postgresql.conf,password_encryption,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK52</NAME>

<DP_NAME>pgsql.secman.conf_file.log_error_verbosity</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
```

```
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,log_error_verbosity,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK53</NAME>
        <DP_NAME>pgsql.secman.perms_external_pid_file</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-
x][.+]*:.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,data_directory,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK54</NAME>
        <DP_NAME>pgsql.secman.ls_pkg_pgsql</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Package Not Found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[postgresql10-10.3-1PGDG.rhel6.x86_64]]></V>
```

```
          <V><![CDATA[postgresql10-contrib-10.3-
1PGDG.rhel6.x86_64]]></V>
          <V><![CDATA[postgresql10-devel-10.3-
1PGDG.rhel6.x86_64]]></V>
          <V><![CDATA[postgresql10-libs-10.3-
1PGDG.rhel6.x86_64]]></V>
          <V><![CDATA[postgresql10-server-10.3-
1PGDG.rhel6.x86_64]]></V>
        </ACTUAL>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK55</NAME>
        <DP_NAME>pgsql.secman.openssl_version</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[OpenSSL not installed]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[OpenSSL 1.0.1e-fips 11 Feb 2013]]></V>
        </ACTUAL>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK56</NAME>

<DP_NAME>pgsql.secman.list_files_perms_in_datadir</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Files not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[Files not found]]></V>
```

```
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,data_directory,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK57</NAME>
        <DP_NAME>pgsql.secman.log_directory_mountpoint</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[Mounted point not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[does not contain regular
expression list]]></EVALUATION>
            <V><![CDATA[.*:/$]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[Mounted point not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,log_directory,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK58</NAME>
        <DP_NAME>pgsql.secman.hba_rule.tcpip_socket</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z" />
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
```

```
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK59</NAME>
        <DP_NAME>pgsql.secman.user_acc_umask</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[User account not found]]></V>
          <V><![CDATA[Umask Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[^[0-6][0-6][0-6][0-6]]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[no-data-from-signature]]></V>
        </ACTUAL>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK60</NAME>
        <DP_NAME>pgsql.secman.conf_file.log_hostname</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,log_hostname,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK61</NAME>
```

```
<DP_NAME>pgsql.secman.conf_file.logging_collector</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,logging_collector,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK62</NAME>

<DP_NAME>pgsql.secman.perms_logfile_log_directory</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-
x]:.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,data_directory,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
```

```
      <CHECK>
        <NAME>CHECK63</NAME>
        <DP_NAME>pgsql.secman.conf_file.syslog_ident</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,syslog_ident,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK64</NAME>

<DP_NAME>pgsql.secman.conf_file.pgaudit.log_statement_once</DP_NAM
E>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,pgaudit.log_statement_once,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
```

```
      </CHECK>
      <CHECK>
        <NAME>CHECK65</NAME>

<DP_NAME>pgsql.secman.conf_file.tcp_keepalives_count</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,tcp_keepalives_count,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK66</NAME>
        <DP_NAME>pgsql.secman.perms_pgsql_binaries</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Setting not found]]></V>
          <V><![CDATA[File not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-
x][.+]*:.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[root:root:rwxr-xr-x:/usr/pgsql-10/bin]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row
1:bindir,File/Directory(${bindir})
      Row 2:/usr/pgsql-10/bin,/usr/pgsql-10/bin
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
```

```
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK67</NAME>
        <DP_NAME>pgsql.secman.conf_file.log_duration</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,log_duration,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK68</NAME>

<DP_NAME>pgsql.secman.conf_file.tcp_keepalives_interval</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,tcp_keepalives_interval,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
```

```
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK69</NAME>
        <DP_NAME>pgsql.secman.postgresql_srvc</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[Service not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
         <V><![CDATA[postgresql-10 0:off 1:off 2:on 3:on 4:on 5:on
6:off]]></V>
        </ACTUAL>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK70</NAME>
        <DP_NAME>pgsql.secman.conf_file.ssl_crl_file</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,ssl_crl_file,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK71</NAME>
```

```
<DP_NAME>pgsql.secman.conf_file.pgaudit.log_level</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,pgaudit.log_level,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK72</NAME>

<DP_NAME>pgsql.secman.conf_file.statement_timeout</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,statement_timeout,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
```

```
      <CHECK>
        <NAME>CHECK73</NAME>
        <DP_NAME>pgsql.secman.conf_file.ssl_key_file</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2: /var/lib/pgsql/10/data/postgresql.conf,ssl_key_file,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
        <NAME>CHECK74</NAME>
        <DP_NAME>pgsql.secman.conf_file.log_line_prefix</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,log_line_prefix,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
      <CHECK>
```

```
        <NAME>CHECK75</NAME>
        <DP_NAME>pgsql.xxxx.xxx_file.client_min_messages</DP_NAME>
        <EXPECTED logic="OR">
          <V><![CDATA[File not found]]></V>
          <V><![CDATA[Setting not found]]></V>
          <CRITERIA>
            <EVALUATION><![CDATA[matches regular expression
list]]></EVALUATION>
            <V><![CDATA[.*]]></V>
          </CRITERIA>
        </EXPECTED>
        <ACTUAL lastUpdated="2023-04-18T15:33:51Z">
          <V><![CDATA[File not found]]></V>
        </ACTUAL>
        <EXTENDED_EVIDENCE><![CDATA[Row 1:File,name,setting
      Row 2:
/var/lib/pgsql/10/data/postgresql.conf,client_min_messages,
      ]]></EXTENDED_EVIDENCE>
        <STATISTICS>
          <ERRORS><![CDATA[]]></ERRORS>
        </STATISTICS>
      </CHECK>
    </CHECKS>
    <DP_DESCRIPTIONS>
      <DP>
        <DP_NAME>pgsql.secman.conf_file.log_rotation_age</DP_NAME>
       <DESCRIPTION><![CDATA[The following List String value(s) of
<b>X</b> indicates the status of the <b>log_rotation_age</b>
parameter in <b>postgresql.conf</b> file.]]></DESCRIPTION>
      </DP>
```

Report Template List

/msp/report_template_list.php

[GET] [POST]

List available report templates, including template titles and IDs, in the user account. The report list includes templates for all report types.

DTD

<platform API server>/report_template_list.dtd

Sample - Report template list

API request:

```
curl -u username:password -H "X-Requested-With: curl"
"<qualys_base_url>/msp/report_template_list.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_TEMPLATE_LIST SYSTEM
"<qualys_base_url>/report_template_list.dtd">
<REPORT_TEMPLATE_LIST>
  <REPORT_TEMPLATE>
    <ID>235288</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Windows Authentication QIDs]]></TITLE>
    <USER>
      <LOGIN><![CDATA[acme_jk]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2018-02-12T18:09:10Z</LAST_UPDATE>
    <GLOBAL>0</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>235164</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Policy</TEMPLATE_TYPE>
    <TITLE><![CDATA[My Policy Report Template]]></TITLE>
    <USER>
      <LOGIN><![CDATA[acme_vs]]></LOGIN>
      <FIRSTNAME><![CDATA[Victor]]></FIRSTNAME>
      <LASTNAME><![CDATA[Smith]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2017-12-09T22:47:58Z</LAST_UPDATE>
    <GLOBAL>0</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>232556</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Executive Report]]></TITLE>
    <USER>
      <LOGIN><![CDATA[acme_jk]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2017-11-11T17:11:55Z</LAST_UPDATE>
```

```
    <GLOBAL>1</GLOBAL>
  </REPORT_TEMPLATE>
  <REPORT_TEMPLATE>
    <ID>232557</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Technical Report]]></TITLE>
    <USER>
      <LOGIN><![CDATA[acme_jk]]></LOGIN>
      <FIRSTNAME><![CDATA[Jason]]></FIRSTNAME>
      <LASTNAME><![CDATA[Kim]]></LASTNAME>
 ...
</REPORT_TEMPLATE_LIST>
```

Each <REPORT_TEMPLATE> element identifies template properties, including the report template ID, template type and title, in the sub-elements described below.

Element	Description
<ID>	The template ID number.
<TYPE>	The template type: Auto (for automatic) or Manual.
<TEMPLATE_TYPE>	The report template type: Scan (for a scan report template) Map (for a map report template) Remediation (for a remediation report template) Compliance (for a compliance report template) Policy (for a compliance policy report template) Patch (for a patch report template)
<TITLE>	The template title, as defined in the Qualys user interface.
<USER>	The template owner, identified by login, first name and last name. For a system template, the login “system” is reported.
<LAST_UPDATE>	The most recent date and time when the template was updated.
<GLOBAL>	For a global template, the value 1 appears. For a non global template, the value 0 appears.

Launch Scorecard

/api/2.0/fo/report/scorecard

[POST]

Launch a vulnerability scorecard report in the user’s Report Share. It is not possible to launch any compliance scorecard reports or WAS scorecard reports using this API at this time.

When a scorecard report is launched, the report is run in the background, and the report generation processing does not timeout until the report has completed.

User Permissions - Managers and Auditors can launch scorecard reports on all assets in the subscription, Unit Managers can launch scorecard reports on assets in their own business unit, Scanners and Readers can launch scorecard reports on assets in their own account.

Input Parameters

Parameter	Description
action=launch	(Required)
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
name={value}	(Required) Specifies the scorecard name for the vulnerability scorecard report that you want to launch. This name corresponds to a service-provided scorecard or a user-created scorecard. For a service-provided scorecard, specify one of these names: Asset Group Vulnerability Report Ignored Vulnerabilities Report Most Prevalent Vulnerabilities Report Most Vulnerable Hosts Report Patch Report
report_title=[value}	(Optional) Specifies a user-defined report title. The title may have a maximum of 128 characters. When unspecified, the report title will be the scorecard name.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. A valid value is: pdf, html (a zip file), xml, or csv. When output_format=pdf is specified, the Secure PDF Distribution may be used. See "Sample - Launch Report."
hide_header={**0**|1}	(Valid for CSV format report only). Specify hide_header=1 to omit the header information from the report. By default this information is included.

Parameter	Description
pdf_password={value}	(Required for secure PDF distribution, Manager or Unit Manager only) The password to be used for encryption. The password may have a maximum of 32 characters (ascii). The password cannot match the password for the user's Qualys login account. The password must follow the password security guidelines defined for the user's subscription. Conditions: a) The pdf_password parameter can only be specified by a Manager or Unit Manager. b) The pdf_password parameter can only be specified when Report Share is enabled for your subscription and the option "Enable Secure PDF Distribution" is selected (log into your account and go to Users > Setup > Security).
recipient_group={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group names, as defined in your Qualys account. Each distribution group identifies a list of users who will receive the secure PDF report. Multiple distribution groups are comma separated. A maximum of 50 distribution groups may be entered. Conditions: a) The recipient_group parameter can only be specified when the pdf_password parameter is also specified. b) The recipient_group parameter can only be specified by a Manager or Unit Manager. c) The recipient_group parameter can only be specified when Report Share is enabled for your subscription and the option "Enable Secure PDF Distribution" is selected (Setup—>Report Share). d) The recipient_group parameter cannot be specified in the same request as recipient_group_id

Parameter	Description
recipient_group_id={value}	(Optional for secure PDF distribution, Manager or Unit Manager only) The report recipients in the form of one or more distribution group IDs. Multiple distribution group IDs are comma separated. Where do I find this ID? Log in to your Qualys account, go to Users > Distribution Groups and select Info for a group in the list. Conditions: a) The recipient_group_id parameter can only be specified when the pdf_password parameter is also specified. b) The recipient_group_id parameter can only be specified by a Manager or Unit Manager. c) The recipient_group_id parameter can only be specified when Report Share is enabled for your subscription and the option “Enable Secure PDF Distribution” is selected (Setup—>Report Share). d) The recipient_group_id parameter cannot be specified in the same request as recipient_group
source={value}	(Conditional) The source asset groups for the report. Specify asset_groups to select asset groups. Specify business_unit to select all the asset groups in a business unit. For a user scorecard, this parameter is optional. When unspecified, the source selection set in the scorecard attributes (as defined in your Qualys account) is used. Conditions: a) The source parameter is required for a service-provided scorecard. b) For a user scorecard, the source selection specified in the source parameter replaces an existing source selection set in the scorecard attributes (as defined in your Qualys account). If you set this parameter to asset_groups, you must specify one of these parameters: asset_groups or all_asset_groups. If you set this parameter to business_unit then you must specify one or more of these parameters: business_unit, division, function and/or location.

Parameter	Description
asset_groups={value}	(Conditional) The titles of asset groups to be used as source asset groups for the scorecard report. One or more asset group titles in your account may be specified. Multiple asset group titles are comma separated. Conditions: a) The asset_groups parameter can only be specified when source=asset_groups. b) These parameters cannot be specified for the same API request: asset_groups and all_asset_groups.
all_asset_groups={1}	(Conditional) Set to 1 to select all asset groups available in your account as the source asset groups for the scorecard report. Conditions: a) The asset_groups parameter can only be specified when source=asset_groups. b) These parameters cannot be specified for the same API request: asset_groups and all_asset_groups.
business_unit={value}	(Conditional for a Manager; not valid for other users) The title of a business unit containing the source asset groups for the scorecard report. All asset groups in the business unit will be included in the report source. You may enter the title of a business unit in your account that was created by a Manager user, or you may enter "Unassigned" for the unassigned business unit. For a user scorecard, the business unit replaces an existing business unit set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (business_unit=), the existing business unit in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) When source=business_unit, one or more of these parameters must be specified: business_unit, division, function and/or location. b) The business_unit parameter can only be specified by a Manager.

Parameter	Description
division={value}	(Conditional) A business info tag identifying a division that asset group(s) belong to. The tag must be defined for an asset group in your account. When specified, only asset groups with this tag are included in the scorecard report source. For a user scorecard, the division tag replaces an existing tag set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (division=), the existing division tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) When source=business_unit, one or more of these parameters must be specified: business_unit, division, function and/or location. b) The division parameter can only be specified when source=business_unit.
function={value}	(Conditional) A business info tag identifying a business function for asset group(s). The tag must be defined for an asset group in your account. When specified, only asset groups with this tag are included in the scorecard report source. For a user scorecard, the function tag replaces an existing function tag set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (function=), the existing function tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) When source=business_unit, one or more of these parameters must be specified: business_unit, division, function and/or location. b) The function parameter can only be specified when source=business_unit.

Parameter	Description
location={value}	(Conditional) A business info tag identifying a location where asset group(s) are located. The tag must be defined for an asset group in your account. When specified, only asset groups with this tag are included in the scorecard report source. For a user scorecard, the location tag replaces an existing location tag set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (location=), the existing location tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) When source=business_unit, one or more of these parameters must be specified: business_unit, division, function and/or location. b) The location parameter can only be specified when source=business_unit.
patch_qids={value}	(Conditional for Patch Report scorecard; not valid for other scorecards) Up to 10 QIDs for vulnerabilities or potential vulnerabilities with available patches. Multiple QIDs are comma separated. When the QIDs are detected on a host this means the host does not have the patches installed and it will be reported in the scorecard output. For a user-defined Patch Report, the patch QIDs list replaces the patch QIDs list set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (patch_qids=), the existing patches QIDs list in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) The patch_qids parameter may be specified only for a Patch Report. b) For a Patch Report, patch_qids or missing_qids must be specified. Both parameters may be specified together.

Parameter	Description
missing_qids={value}	(Conditional for Patch Report scorecard; not valid for other scorecards) One or two QIDs for missing software. Two QIDs are comma separated. Typically missing software QIDs are information gathered checks. When the QIDs are not detected on a host this means the host is missing software and it will be reported in the scorecard output. For a user-defined Patch Report, the missing QIDs list replaces the missing QIDs list set in the scorecard attributes (as defined in your Qualys account). If an empty value is set (missing_qids=), the existing missing QIDs list in the scorecard attributes is not included in the scorecard parameters submitted with the API request. Conditions: a) The missing_qids parameter may be specified only for a Patch Report. b) For a Patch Report, patch_qids or missing_qids must be specified. Both parameters may be specified together.

DTD

<platform API server>/api/2.0/simple_return.dtd

Cancel Running Report

For API version information, refer to API History Version section.

V2.0 | V3.0

V2.0

/api/2.0/fo/report

[POST]

Cancel a running report in the user's account. This is an option when Report Share is enabled in the user's subscription.

User permissions - Managers can cancel any running report. Unit Managers can cancel a running report in their own business unit (report launched by user in their own business unit). Scanners and Readers can cancel their own running report.

Input Parameters

Parameter	Description
action=cancel	(Required)
id={value}	(Required) Specifies the report ID of a running report that you want to cancel. The status of the report must be "running".
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Sample - Cancel running report

```
curl -H "X-Requested-With: Curl Sample"
-d "action=cancel&id=1462"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "<qualys_base_url>/api/2.0/fo/scan/"
```

DTD

<platform API server>/api/2.0/simple_return.dtd

V3.0

/api/3.0/fo/report

[POST]

Cancel a running report in the user's account. This is an option when Report Share is enabled in the user's subscription.

User permissions - Managers can cancel any running report. Unit Managers can cancel a running report in their own business unit (report launched by user in their own business unit). Scanners and Readers can cancel their own running report.

Input Parameters

Parameter	Description
action=cancel	(Required)
id={value}	(Required) Specifies the report ID of a running report that you want to cancel. The status of the report must be "running".
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Sample - Cancel running report

API Request:

```
curl --location --request POST
'<qualys_base_url>/api/3.0/fo/report/?echo_request=1&action=cancel&id=661
9731' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <REQUEST>
            <DATETIME>2025-06-17T11:05:51Z</DATETIME>
            <USER_LOGIN>akkqa_tq</USER_LOGIN>
            <RESOURCE>
                <qualys_base_url>/api/3.0/fo/report/
                </RESOURCE>
                <PARAM_LIST>
                    <PARAM>
                        <KEY>echo_request</KEY>
                        <VALUE>1</VALUE>
                    </PARAM>
                    <PARAM>
                        <KEY>action</KEY>
                        <VALUE>cancel</VALUE>
                    </PARAM>
                    <PARAM>
                        <KEY>id</KEY>
                        <VALUE>6627719</VALUE>
                    </PARAM>
                </PARAM_LIST>
            </REQUEST>
```

```
        <RESPONSE>
            <DATETIME>2025-06-17T11:05:51Z</DATETIME>
            <TEXT>Report canceled</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>6627719</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

DTD

<platform API server>/api/3.0/simple_return.dtd

API History Version

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/report/action=cancel	Active	Active
/api/2.0/fo/report/action=cancel	December 2025	June 2026

Download Saved Report

For API version information, refer to API History Version section.

V2.0 | V3.0

V2.0

/api/2.0/fo/report/

[GET] [POST]

Download a saved report in the user's account. You can download all report types (map, scan, patch, authentication, scorecard, remediation, compliance). This option is available when the Report Share feature is enabled in the user's subscription.

You can also view risk scores to Host Based Scan Reports, including TruRisk score, Asset Criticality Score (ACS) and Qualys Detection Score (QDS). These values appear in all report formats, including XML and CSV. You can download reports from the UI or fetch reports using the API.

Downloading a Policy Report in CSV format? When PCRS is enabled for your subscription, we'll automatically compress large CSV policy reports and you'll get a Zip file instead of CSV when the report is greater than 1GB in size. See Launching and Fetching Compliance Reports in CSV Format for important details.

User permissions - Managers can download any saved report. Unit Managers can download a saved report in their own business unit (reports launched by users in their own business unit). Scanners and Readers can download their own saved report.

Input Parameters

Parameter	Description
action=fetch	(Required)
id={value}	(Required) Specifies the report ID of a saved report that you want to download. The status of the report must be "finished".
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When not specified, parameters are not included in the XML output.

Where do I get the report ID?

Run the report list API

API request:

```
curl -X POST -H "X-Requested-With:POSTMAN" -H "Authorization:Basic
<TOKEN>" -F "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/report_list_output
.dtd">
<REPORT_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-07-02T15:29:52Z</DATETIME>
    <REPORT_LIST>
      <REPORT>
        <ID>7592049</ID>
        <TITLE><![CDATA[FIXED Vuln Report]]></TITLE>
        <TYPE>Scan</TYPE>
        <USER_LOGIN>acme_ur15</USER_LOGIN>
        <LAUNCH_DATETIME>2018-07-02T14:52:45Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>HTML</OUTPUT_FORMAT>
        <SIZE>-</SIZE>
```

```
        <STATUS>
          <STATE>Running</STATE>
          <MESSAGE><![CDATA[Rendering...]]></MESSAGE>
          <PERCENT>80</PERCENT>
        </STATUS>
<EXPIRATION_DATETIME>2018-07-30T14:52:48Z</EXPIRATION_DATETIME>
      </REPORT>
...
      <REPORT>
        <ID>7589800</ID>
        <TITLE><![CDATA[My Authentication Report]]></TITLE>
        <TYPE>Authentication</TYPE>
        <USER_LOGIN>acme_ee17</USER_LOGIN>
        <LAUNCH_DATETIME>2018-07-02T07:00:21Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
        <SIZE>15 KB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2018-07-
30T07:00:24Z</EXPIRATION_DATETIME>
      </REPORT>
    </REPORT_LIST>
  </RESPONSE>
</REPORT_LIST_OUTPUT>
```

Another option - go to the user interface

Within the user interface find the report you want to download (go to Reports > Reports) then choose View Report. In the Report Information window, at the top you'll see the ID in the window URL after id= like this:

```
https://qualysguard.qualys.qualys.com/fo/report/view_report.php?id
=2281953
```

Sample - Download report

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/report/
?action=fetch&id=1462"
```

Sample - Download Host Based Scan Report in CSV Format

In this sample, we're downloading a Host Based Scan Report in CSV format. You'll see the new column headers "QDS", "ARS" and "ACS".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=123457"
```

CSV output:

```
"Sample Report","05/24/2022 at 18:17:24 (GMT-0800)"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Joe User","joe_user","Manager"

...

"IP","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq
ID","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","OS
CPE","Category","Associated Ags","Cloud Provider","Cloud Provider
Service","Cloud Service","Cloud Resource ID","Cloud Resource Type","Cloud
Account","Cloud Image ID","Cloud Resource Metadata","EC2 Instance
ID","Public Hostname","Image ID","VPC ID","Instance State","Private
Hostname","Instance Type","Account ID","Region Code","Subnet ID","Host
ID","Asset ID","QDS","ARS","TRURISK SCORE","ACS"
"10.20.30.40","10-20-30-40.bogus.tld",,,,"DNS",,"host scanned, found
vuln","100021","Microsoft Internet Explorer TABLE Status Bar URI
Obfuscation Weakness","New","Vuln","2",,,,,"05/24/2022
10:07:23","05/24/2022 10:07:23","1",,,,,"CVE-2005-
4679",,"11561","Microsoft Internet Explorer is reported prone to a URI
obfuscation weakness. The issue presents itself when a HREF tag contains
an additional HREF tag contained within a TABLE tag. It is reported that
hovering over the link of the second HREF tag will display the hostname
address of the first HREF tag in the status bar of Internet Explorer.

This weakness is reported to affect Internet Explorer 6, but other
versions may also be affected. Windows XP Service Pack 2 is not reported
to be vulnerable.","This issue may be leveraged by an attacker to display
false information in the status bar of an unsuspecting user, allowing an
attacker to present Web pages to users that seem to originate from a
trusted location. This may facilitate phishing style attacks. Other
attacks may also be possible.","This vulnerability is not exploitable with
Windows XP Service Pack 2. There are no solutions available at this time
for Windows 2000 or Windows XP Service Pack 1.",,,,"yes",,,,"Internet
Explorer",,,,,,,,,"[]",,,,,,,,,,,"2685870","14617851","28","104","4"

...
```

Sample - Download Host Based Scan Report in XML Format

In this sample, we're downloading a Host Based Scan Report in XML format. You'll see <ARS> and <ACS> as part of Host details, and you'll see <QDS> as part of Vuln Info.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=123456"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_DATA_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_data_report.dtd">
<ASSET_DATA_REPORT>
  <HEADER>
    <COMPANY>
      <![CDATA[ Qualys ]]>
    </COMPANY>
    <USERNAME>joe_user</USERNAME>
    <GENERATION_DATETIME>2022-05-24T15:30:56Z</GENERATION_DATETIME>
    <TEMPLATE>
      <![CDATA[ ARS_Report ]]>
    </TEMPLATE>
    <TARGET>
      <USER_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
        </RANGE>
      </USER_IP_LIST>
      <COMBINED_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
        </RANGE>
      </COMBINED_IP_LIST>
    </TARGET>
    <RISK_SCORE_SUMMARY>
      <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
      <AVG_SECURITY_RISK>2.2</AVG_SECURITY_RISK>
      <BUSINESS_RISK>10/100</BUSINESS_RISK>
    </RISK_SCORE_SUMMARY>
  </HEADER>
  <RISK_SCORE_PER_HOST>
    <HOSTS>
      <IP_ADDRESS>10.20.30.40</IP_ADDRESS>
      <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
      <SECURITY_RISK>2.2</SECURITY_RISK>
    </HOSTS>
  </RISK_SCORE_PER_HOST>
  <HOST_LIST>
    <HOST>
      <IP>10.20.30.40</IP>
      <TRACKING_METHOD>DNS</TRACKING_METHOD>
      <HOST_ID>2685870</HOST_ID>
      <ASSET_ID>14617851</ASSET_ID>
      <DNS>
```

```
          <![CDATA[ 10-20-30-40.bogus.tld ]]>
        </DNS>
        <ARS>104</ARS>
        <TRURISK_SCORE>104</TRURISK_SCORE>
        <ACS>4</ACS>
        <VULN_INFO_LIST>
          <VULN_INFO>
            <QID id="qid_100027">100027</QID>
            <TYPE>Practice</TYPE>
            <SSL>false</SSL>
            <FIRST_FOUND>2022-05-24T04:37:23Z</FIRST_FOUND>
            <LAST_FOUND>2022-05-24T04:37:23Z</LAST_FOUND>
            <TIMES_FOUND>1</TIMES_FOUND>
            <VULN_STATUS>New</VULN_STATUS>
            <QDS>
              <![CDATA[ 32 ]]>
            </QDS>
          </VULN_INFO>
...
```

DTD

<platform API server>/asset_data_report.dtd

V3.0

/api/3.0/fo/report/

[GET] [POST]

Download a saved report in the user's account. You can download all report types (map, scan, patch, authentication, scorecard, remediation, compliance). This option is available when the Report Share feature is enabled in the user's subscription.

You can also view risk scores to Host Based Scan Reports, including TruRisk score, Asset Criticality Score (ACS) and Qualys Detection Score (QDS). These values appear in all report formats, including XML and CSV. You can download reports from the UI or fetch reports using the API.

Downloading a Policy Report in CSV format? When PCRS is enabled for your subscription, we'll automatically compress large CSV policy reports and you'll get a Zip file instead of CSV when the report is greater than 1GB in size. See Launching and Fetching Compliance Reports in CSV Format for important details.

User permissions - Managers can download any saved report. Unit Managers can download a saved report in their own business unit (reports launched by users in their own business unit). Scanners and Readers can download their own saved report.

Input Parameters

Parameter	Description
action=fetch	(Required)
id={value}	(Required) Specifies the report ID of a saved report that you want to download. The status of the report must be "finished".
echo_request={**0**|1}	(Optional) Specify 1 to view input parameters in the XML output. When not specified, parameters are not included in the XML output.

Where do I get the report ID?

Run the report list API

API request:

```
curl -X POST -H "X-Requested-With:POSTMAN" -H "Authorization:Basic
<TOKEN>" -F "action=list"
"https://qualysapi.qualys.com/api/3.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/3.0/fo/report/report_list_output
.dtd">
<REPORT_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-07-02T15:29:52Z</DATETIME>
    <REPORT_LIST>
      <REPORT>
        <ID>7592049</ID>
        <TITLE><![CDATA[FIXED Vuln Report]]></TITLE>
        <TYPE>Scan</TYPE>
        <USER_LOGIN>acme_ur15</USER_LOGIN>
        <LAUNCH_DATETIME>2018-07-02T14:52:45Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>HTML</OUTPUT_FORMAT>
        <SIZE>-</SIZE>
        <STATUS>
          <STATE>Running</STATE>
          <MESSAGE><![CDATA[Rendering...]]></MESSAGE>
          <PERCENT>80</PERCENT>
        </STATUS>
<EXPIRATION_DATETIME>2018-07-30T14:52:48Z</EXPIRATION_DATETIME>
      </REPORT>
...
      <REPORT>
```

```
        <ID>7589800</ID>
        <TITLE><![CDATA[My Authentication Report]]></TITLE>
        <TYPE>Authentication</TYPE>
        <USER_LOGIN>acme_ee17</USER_LOGIN>
        <LAUNCH_DATETIME>2018-07-02T07:00:21Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
        <SIZE>15 KB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2018-07-
30T07:00:24Z</EXPIRATION_DATETIME>
      </REPORT>
    </REPORT_LIST>
  </RESPONSE>
</REPORT_LIST_OUTPUT>
```

Another option - go to the user interface

Within the user interface find the report you want to download (go to Reports > Reports) then choose View Report. In the Report Information window, at the top you'll see the ID in the window URL after id= like this:

```
https://qualysguard.qualys.qualys.com/fo/report/view_report.php?id
=2281953
```

Sample - Download report

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/3.0/fo/report/
?action=fetch&id=1462"
```

Sample - Download Host Based Scan Report in CSV Format

In this sample, we're downloading a Host Based Scan Report in CSV format. You'll see the new column headers "QDS", "ARS" and "ACS".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/3.0/fo/report/?action=fetch&id=123457"
```

CSV output:

```
"Sample Report","05/24/2022 at 18:17:24 (GMT-0800)"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Joe User","joe_user","Manager"
```

```
...

"IP","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq
ID","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","OS
CPE","Category","Associated Ags","Cloud Provider","Cloud Provider
Service","Cloud Service","Cloud Resource ID","Cloud Resource Type","Cloud
Account","Cloud Image ID","Cloud Resource Metadata","EC2 Instance
ID","Public Hostname","Image ID","VPC ID","Instance State","Private
Hostname","Instance Type","Account ID","Region Code","Subnet ID","Host
ID","Asset ID","QDS","ARS","TRURISK SCORE","ACS"
"10.20.30.40","10-20-30-40.bogus.tld",,,,"DNS",,"host scanned, found
vuln","100021","Microsoft Internet Explorer TABLE Status Bar URI
Obfuscation Weakness","New","Vuln","2",,,,,"05/24/2022
10:07:23","05/24/2022 10:07:23","1",,,,,"CVE-2005-
4679",,"11561","Microsoft Internet Explorer is reported prone to a URI
obfuscation weakness. The issue presents itself when a HREF tag contains
an additional HREF tag contained within a TABLE tag. It is reported that
hovering over the link of the second HREF tag will display the hostname
address of the first HREF tag in the status bar of Internet Explorer.

This weakness is reported to affect Internet Explorer 6, but other
versions may also be affected. Windows XP Service Pack 2 is not reported
to be vulnerable.","This issue may be leveraged by an attacker to display
false information in the status bar of an unsuspecting user, allowing an
attacker to present Web pages to users that seem to originate from a
trusted location. This may facilitate phishing style attacks. Other
attacks may also be possible.","This vulnerability is not exploitable with
Windows XP Service Pack 2. There are no solutions available at this time
for Windows 2000 or Windows XP Service Pack 1.",,,,"yes",,,,"Internet
Explorer",,,,,,,,,"[]",,,,,,,,,,,"2685870","14617851","28","104","4"

...
```

Sample - Download Host Based Scan Report in XML Format

In this sample, we're downloading a Host Based Scan Report in XML format. You'll see <ARS> and <ACS> as part of Host details, and you'll see <QDS> as part of Vuln Info.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/3.0/fo/report/?action=fetch&id=123456"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_DATA_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_data_report.dtd">
```

```
<ASSET_DATA_REPORT>
  <HEADER>
    <COMPANY>
      <![CDATA[ Qualys ]]>
    </COMPANY>
    <USERNAME>joe_user</USERNAME>
    <GENERATION_DATETIME>2022-05-24T15:30:56Z</GENERATION_DATETIME>
    <TEMPLATE>
      <![CDATA[ ARS_Report ]]>
    </TEMPLATE>
    <TARGET>
      <USER_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
        </RANGE>
      </USER_IP_LIST>
      <COMBINED_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
        </RANGE>
      </COMBINED_IP_LIST>
    </TARGET>
    <RISK_SCORE_SUMMARY>
      <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
      <AVG_SECURITY_RISK>2.2</AVG_SECURITY_RISK>
      <BUSINESS_RISK>10/100</BUSINESS_RISK>
    </RISK_SCORE_SUMMARY>
  </HEADER>
  <RISK_SCORE_PER_HOST>
    <HOSTS>
      <IP_ADDRESS>10.20.30.40</IP_ADDRESS>
      <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
      <SECURITY_RISK>2.2</SECURITY_RISK>
    </HOSTS>
  </RISK_SCORE_PER_HOST>
  <HOST_LIST>
    <HOST>
      <IP>10.20.30.40</IP>
      <TRACKING_METHOD>DNS</TRACKING_METHOD>
      <HOST_ID>2685870</HOST_ID>
      <ASSET_ID>14617851</ASSET_ID>
      <DNS>
        <![CDATA[ 10-20-30-40.bogus.tld ]]>
      </DNS>
      <ARS>104</ARS>
      <TRURISK_SCORE>104</TRURISK_SCORE>
      <ACS>4</ACS>
      <VULN_INFO_LIST>
        <VULN_INFO>
          <QID id="qid_100027">100027</QID>
          <TYPE>Practice</TYPE>
          <SSL>false</SSL>
```

```
            <FIRST_FOUND>2022-05-24T04:37:23Z</FIRST_FOUND>
            <LAST_FOUND>2022-05-24T04:37:23Z</LAST_FOUND>
            <TIMES_FOUND>1</TIMES_FOUND>
            <VULN_STATUS>New</VULN_STATUS>
            <QDS>
              <![CDATA[ 32 ]]>
            </QDS>
          </VULN_INFO>
...
```

Sample: Fetch the report

API Request:

```
curl --location
'https://qualysapi.qualys.com/api/3.0/fo/report/?echo_request=1&action=fe
tch&id=6626811' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML Response:

```
"FQDN_template_Multiple","06/16/2025 at 14:30:35 (GMT+0530)"
"QA testing Team","pune","pune","pune","Georgia","United States of
America","111"
"Testing QA Manager","john_doe","Manager"

"Asset Groups","IPs","Active Hosts","Hosts Matching Filters","Trend
Analysis","Date Range","Network","Asset Tags"
"NONE","NONE","5","5","Past 2 detections","N/A","Global Default
Network","NONE"

"Total Vulnerabilities","Avg Security Risk","Business Risk"
"500","3.4","0"

"IP","Network","Total Vulnerabilities","Security Risk"
"10.xx.xx.94","ACustom_Net1","104","3.1"
"10.xx.xx.94","Global Default Network","139","3.5"
"10.xx.xx.71","Global Default Network","60","3.9"
"10.xx.xx.86","Global Default Network","63","3.2"
"10.xx.xx.1","Global Default Network","134","3.2"


"IP","Network","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq ID","CVSS","CVSS Base","CVSS Temporal","CVSS
Environment","CVSS3.1","CVSS3.1 Base","CVSS3.1
Temporal","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket
State","Instance","Category","Associated AGs","Non-running Kernel","Cloud
Provider","Cloud Provider Service","Cloud Service","Cloud Resource
```

ID","Cloud Resource Type","Cloud Account","Cloud Image ID","Cloud Resource Metadata","EC2 Instance ID","Public Hostname","Image ID","VPC ID","Instance State","Private Hostname","Instance Type","Account ID","Region Code","Subnet ID","Host ID","Asset ID","QDS","ARS","ACS","TruRisk Score","MITRE ATT&CK Tactic Name","MITRE ATT&CK Technique Name","MITRE ATT&CK Tactic ID","MITRE ATT&CK Technique ID"
"10.44.201.71","Global Default Network","qwiki.intranet.qualys.com",,,,"DNS",,"host scanned, found vuln","732544","Atlassian Confluence Server and Data Center Xstream Dependency Vulnerability (CONFSERVER-99568)","New","Vuln","4","443","tcp",,,"06/02/2025 13:56:58","06/02/2025 13:56:58","1",,,,,"CVE-2024-47072","CONFSERVER-99568",,"4","5.4 (AV:A/AC:M/Au:M/C:N/I:C/A:P)","4.0 (E:U/RL:OF/RC:C)","Asset Group: -, Collateral Damage Potential: -, Target Distribution: -, Confidentiality Requirement: -, Integrity Requirement: -, Availability Requirement: -","6.5","7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)","6.5 (E:U/RL:O/RC:C)","Confluence is team collaboration software written in Java. Affected version: PLEASE FILL THE AFFECTED VERSIONS MANUALLY QID Detection Logic:(Unauthenticated) It checks for vulnerable version of Atlassian Confluence Server. QID Detection Logic(Authenticated): Operating System: (Windows) The QID checks for vulnerable versions of Confluence Server with registry path QID Detection Logic(Authenticated): Operating System: (Unix) The QID checks for vulnerable versions of Confluence Server advised by the vendor using install location","Successful exploitation of this vulnerability could lead to a security breach or affect confidentiality, integrity, and availability.","Customers are advised to refer to CONFSERVER-99568 (https://jira.atlassian.com/browse/CONFSERVER-99568) for updates pertaining to this vulnerability.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
CONFSERVER-99568 (https://jira.atlassian.com/browse/CONFSERVER-99568)",,,"Vulnerable Atlassian Confluence detected on port: 443 Printed by Atlassian Confluence 8.9.1
#","no","Open",,"CGI",,"No",,,,,,,,"[]",,,,,,,,,,"15840097","69114947","35","333","2","333",,,,
"10.xx.xx.71","Global Default Network","qwiki.intranet.qualys.com",,,,"DNS",,"host scanned, found vuln","732543","Atlassian Confluence Server and Data Center Third-Party Dependency Vulnerability (CONFSERVER-99686)","New","Vuln","4","443","tcp",,,"06/02/2025 13:56:58","06/02/2025 13:56:58","1",,,,,"CVE-2025-31650","CONFSERVER-99686",,"4.2","5.4 (AV:A/AC:M/Au:M/C:N/I:C/A:P)","4.3 (E:POC/RL:OF/RC:C)","Asset Group: -, Collateral Damage Potential: -, Target Distribution: -, Confidentiality Requirement: -, Integrity Requirement: -, Availability Requirement: -","6.7","7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)","6.7 (E:P/RL:O/RC:C)","Confluence is team collaboration software written in Java. Affected version: PLEASE FILL THE AFFECTED VERSIONS MANUALLY QID Detection Logic:(Unauthenticated) It checks for vulnerable version of Atlassian Confluence Server. QID Detection Logic(Authenticated): Operating System: (Windows) The QID checks for vulnerable versions of Confluence Server with registry path QID Detection Logic(Authenticated): Operating System: (Unix) The QID checks for vulnerable versions of

Confluence Server advised by the vendor using install
location","Successful exploitation of this vulnerability could lead to a
security breach or affect confidentiality, integrity, and
availability.","Customers are advised to refer to CONFSERVER-99686
(https://jira.atlassian.com/browse/CONFSERVER-99686) for updates
pertaining to this vulnerability.
 Patch:
Following are links for downloading patches to fix the vulnerabilities:
  CONFSERVER-99686 (https://jira.atlassian.com/browse/CONFSERVER-
99686)","Source: github-exploits
Reference:CVE-2025-31650
Description:sattarbug/Analysis-of-TomcatKiller---CVE-2025-31650-Exploit-
Tool exploit repository
Link:https://github.com/sattarbug/Analysis-of-TomcatKiller---CVE-2025-
31650-Exploit-Tool
Reference:CVE-2025-31650
Description:assad12341/Dos-exploit- exploit repository
Link:https://github.com/assad12341/Dos-exploit-
Reference:CVE-2025-31650
Description:tunahantekeoglu/CVE-2025-31650 exploit repository
Link:https://github.com/tunahantekeoglu/CVE-2025-31650
Reference:CVE-2025-31650
Description:absholi7ly/TomcatKiller-CVE-2025-31650 exploit repository
Link:https://github.com/absholi7ly/TomcatKiller-CVE-2025-31650

Source: exploitdb
Reference:CVE-2025-31650
Description:Apache Tomcat 10.1.39 - Denial of Service (DoS)
Link:https://www.exploit-db.com/exploits/52318

Source: blogs
Reference:CVE-2025-31650
Description:Apache Tomcat 10.1.39 - Denial of Service (DOS)
Link:https://www.exploit-db.com/raw/52318",,"Vulnerable Atlassian
Confluence detected on port: 443
Printed by Atlassian Confluence 8.9.1
#","no","Open",,"CGI",,"No",,,,,,,,"[]",,,,,,,,,,"15840097","69114947","
42","333","2","333",,,,
"10.44.201.71","Global Default
Network","qwiki.intranet.qualys.com",,,,"DNS",,"host scanned, found
vuln","732438","Atlassian Confluence Server and Data Center Denial of
Service (DoS) Vulnerability (CONFSERVER-
99540)","New","Vuln","4","443","tcp",,,"06/02/2025 13:56:58","06/02/2025
13:56:58","1",,,,,"CVE-2025-24970","CONFSERVER-99540",,"4","5.4
(AV:A/AC:M/Au:M/C:N/I:C/A:P)","4.0 (E:U/RL:OF/RC:C)","Asset Group: -,
Collateral Damage Potential: -, Target Distribution: -, Confidentiality
Requirement: -, Integrity Requirement: -, Availability Requirement: -
","6.5","7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)","6.5
(E:U/RL:O/RC:C)","Confluence is team collaboration software written in
Java.

Affected version:
All versions of Confluence Data Center and Server from 7.19 to 7.19.30
All versions of Confluence Data Center and Server from 7.20 to 7.20.3

```
All versions of Confluence Data Center and Server from 8.0 to 8.5.19
All versions of Confluence Data Center and Server from 8.6.0 to 8.6.2
All versions of Confluence Data Center and Server from 8.7.0 to 8.7.2
All versions of Confluence Data Center and Server from 8.8.0 to 8.8.1
All versions of Confluence Data Center and Server from 8.9.0 to 8.9.8
All versions of Confluence Data Center and Server from 9.0.0 to 9.0.3
All versions of Confluence Data Center and Server from 9.1.0 to 9.1.1
All versions of Confluence Data Center and Server from 9.2.0 to 9.2.1
All versions of Confluence Data Center and Server from 9.3.0 to 9.3.1

QID Detection Logic:(Unauthenticated)
It checks for vulnerable version of Atlassian Confluence Server by hitting
the GET request on ""login.action"" endpoint.

QID Detection Logic(Authenticated): Operating System: (Windows)
The QID checks for vulnerable versions of Confluence Server with registry
path

QID Detection Logic(Authenticated): Operating System: (Unix)
The QID checks for vulnerable versions of Confluence Server advised by the
vendor using install location","Successful exploitation of this
vulnerability could lead to a security breach or affect confidentiality,
integrity, and availability.","Customers are advised to refer to
CONFSERVER-99540 (https://jira.atlassian.com/browse/CONFSERVER-99540) for
updates pertaining to this vulnerability.
```

DTD

<platform API server>/asset_data_report.dtd

API History Version

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/report/action=fetch	Active	Active
/api/2.0/fo/report/action=fetch	December 2025	June 2026

Delete Saved Report

/api/2.0/fo/report

[POST]

Delete a saved report in the user's account. This option is available when the Report Share feature is enabled in the user's subscription.

User permissions - Managers can delete any saved report. Unit Managers can delete a saved report in their own business unit (report launched by users in their own business unit). Scanners and Readers can delete their own saved report.

Input Parameters

Parameter	Description
action=delete	(Required)
id={value}	(Required) Specifies the report ID of a saved report in Report Share that you want to delete. The status of the report must be "finished".
echo_request={**0**|1}	(Optional) Specifies whether to echo the request's input parameters in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Sample - Delete saved report

```
curl -H "X-Requested-With: Curl Sample"
-d "action=delete&id=1234"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Scheduled Reports List

/api/2.0/fo/schedule/report/ with action=list

[GET] [POST]

List scheduled reports in your account.

Input parameters

Parameter	Description
action=list	(Required)
id={value}	(Optional) Show only 1 scheduled report that has the report ID you specify.
is_active={0|1}	(Optional) Active and inactive scheduled reports are listed by default. Specify 1 to list active scheduled reports only, or specify 0 to list inactive scheduled reports only.

Sample - List all scheduled reports in account

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/report/?action=l
ist"
```

DTD

<platform API server>/api/2.0/fo/schedule/report/schedule_report_list_output.dtd

Launch Scheduled Report

/api/2.0/fo/schedule/report/ with action=launch_now

[POST]

Launch a scheduled report now.

Input parameters

Parameter	Description
action=launch_now	(Required)
id={value}	(Required) A valid scheduled report ID.

Sample - Launch scheduled report

```
curl -H "X-Requested-With: Curl" -u USERNAME:PASSWORD -X "POST" -d
"action=launch_now&id=12345"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/report/"
```

DTD

<platform API server>/api/2.0/simple_return.dtd

Asset Search Report

/api/2.0/fo/report/asset/?action=search

[GET] [POST]

Download report on assets you're interested in.

Input parameters

Parameter	Description
action=search	(Required)
output_format={csv|xml}	(Required) The output format of the asset search report. One output format may be specified: csv or xml.
tracking_method={value}	(Optional) Show only IP addresses/ranges which have a certain tracking method. Valid values: IP, DNS, NETBIOS, AZURE VM,EC2, GCP Compute Engine, AGENT

Parameter	Description
ips={value}	(Optional) Use this parameter if you want to include only certain IP addresses in the report. One or more IPs/ranges may be specified. Multiple entries are comma separated. An IP range is specified with a hyphen (for example, 10.10.10.1-10.10.10.100).
	One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.
ips_network_id={value}	(Optional) The network ID applied on IPs. The default value is ALL.
asset_group_ids={value}	(Optional) The IDs of asset groups containing the hosts to be included in the asset search report. Multiple IDs are comma separated.
	One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.
asset_groups={value}	(Optional) The titles of asset groups containing the hosts to be included in the asset search report. Multiple titles are comma separated.
	One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.
assets_in_my_network_only={**0**|1}	(Optional) Specify 1 to include the specified asset groups and/or IP ranges. Valid for 'All' Asset Group and/or specified IP ranges.
ec2_instance_status={value}	(Optional) Specify the EC2 instance status to be searched. Possible values: RUNNING,TERMINATED, PENDING, STOPPING, SHUTTING_DOWN, STOPPED. Values are case-sensitive. ec2_instance_status is valid only when tracking_method=EC2 or tracking_method=AGENT is specified. See EC2 search samples
ec2_instance_id={value}	(Optional) Specify the EC2 instance ID to be searched. See EC2 search samples
	ec2_instance_id is valid only when ec2_instance_id_modifier is specified
ec2_instance_id_modifier={value}	(Optional) Show only hosts with ec2_instance_id that is either: beginning with, containing, matching, ending with, not empty. See EC2 search samples
	ec2_instance_id_modifier is valid only when ec2_instance_id is specified

Parameter	Description
azure_vm_state={value}	(Optional) Specify the Azure virtual machine state to be searched. Possible values are: STARTING, RUNNING, STOPPING, STOPPED, DEALLOCATING, DEALLOCATED, UNKNOWN. Values are case-sensitive. azure_vm_state is valid only when tracking_method=AZURE VM or tracking_method=AGENT is specified.
azure_vm_id={value}	(Optional) Specify the Azure virtual machine ID to be searched.
	azure_vm_id is valid only when azure_vm_id_modifier is specified.
azure_vm_id_modifier={value}	(Optional) Show only assets with azure_vm_id that is either: beginning with, containing, matching, ending with, not empty.
	azure_vm_id_modifier is valid only when azure_vm_id is specified.
gcp_vm_instance_state={value}	(Optional) Specify the GCP virtual machine state to be searched. Possible values are: PROVISIONING, STAGING,RUNNING, STOPPING, STOPPED, REPAIRING, TERMINATED, SUSPENDING, SUSPENDED. Values are case-sensitive. gcp_vm_instance_state is valid only when tracking_method=GCP or tracking_method=AGENT is specified.
gcp_vm_instance_id={value}	(Optional) Specify the GCP virtual machine ID to be searched. gcp_vm_instance_id is valid only when gcp_vm_instance_id_modifier is specified.
gcp_vm_instance_id_modifier	(Optional) Show only assets with gcp_vm_id that is either: beginning with, containing, matching, ending with, not empty gcp_vm_instance_id_modifier is valid only when gcp_vm_instance_id is specified.
display_ag_titles={**0**|1}	(Optional) Specify 1 to display AssetGroup Titles for each Host in the output. Otherwise the AssetGroup Titles are not displayed in the output.
ports={value}	(Optional) Shows the hosts that has the specified open ports. One or more ports may be specified. Multiple ports are comma separated. You can specify upto 10 values.

Parameter	Description
services={value}	(Optional) Shows the hosts that has the specified services running on it. One or more services may be specified. Multiple services are comma separated.You can specify upto 10 values.
qids={value}	(Optional) Shows vulnerabilities (QIDs) in the KnowledgeBase applicable to the host. Allows up to 20 values.
qid_with_text={value}	(Optional) Shows vulnerabilities (QIDs) with the specified text in the KnowledgeBase applicable to the host.
	qid_with_text is valid only when qids parameter is specified.
qid_with_modifier={value}	(Optional) Show only hosts with QID that is either: beginning with, containing, matching, ending with.
	qid_with_modifier is valid only when qid_with_text is specified.
use_tags={**0**|1}}	(Optional) Specify 0 (the default) if you want to select hosts based on IP addresses/ranges and/or asset groups. Specify 1 if you want to select hosts based on asset tags.
	One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.
tag_set_by={id|name}	(Optional when use_tags=1) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names.
tag_include_selector={any|all}	(Optional when use_tags=1) Select “any” (the default) to include hosts that match at least one of the selected tags. Select “all” to include hosts that match all of the selected tags.
tag_exclude_selector={any|all}	(Optional when use_tags=1) Select “any” (the default) to exclude hosts that match at least one of the selected tags. Select “all” to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Required when use_tags=1) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional when use_tags=1) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

Parameter	Description
first_found_days={value}	(Optional) Specify a number of days along with the first_found_modifier so that the range includes the first found date to be searched for
	first_found_days is valid only when first_found_modifier is specified.
first_found_modifier={within|not within}	(Optional) Show only hosts whose first found date is within or not within the specified days.
	first_found_modifier is valid only when first_found_days is specified.
last_vm_scan_days={value}	(Optional) Specify a number of days so that it includes the last vm scan date to be searched for.
	last_vm_scan_days is valid only when last_vm_scan_modifier is specified.
last_vm_scan_modifier={within|not within}	(Optional) Show only hosts whose last_vm_scan_date is within or not within the specified days.
	last_vm_scan_modifier is valid only when last_vm_scan_days is specified.
last_pc_scan_days={value}	(Optional) Specify a number of days so that the specified value along with the modifier forms the date range that includes the last scan date to be searched for.
	This parameter is valid only when the policy compliance module is enabled for the user account.
last_pc_scan_modifier={within|not within}	(Optional) Show only hosts whose last_pc_scan_date is within or not within the specified days.
	This parameter is valid only when the policy compliance module is enabled for the user account.
last_scap_scan_days={value}	(Optional) Specify a number of days so that the specified value along with the modifier forms the date range that includes the last SCAP scan date to be searched for.
	This parameter is valid only when the policy compliance module is enabled for the user account.
last_scap_scan_modifier={within|not within}	(Optional) Show only hosts whose last_scap_scan_date is within or not within the specified days.
	This parameter is valid only when the policy compliance module is enabled for the user account.
dns_name={value}	(Optional) Specify the DNS name of the host that needs to be searched.
	dns_name is valid only when dns_modifier is specified.

Parameter	Description
dns_modifier={value}	(Optional) Show only hosts with dns_name that is either: beginning with, containing, matching, ending with, not empty.
	dns_modifier is valid only when dns_name is specified.
netbios_name={value}	(Optional) Specify the NETBIOS name of the host to be searched.
	netbios_name is valid only when netbios_modifier is specified.
netbios_modifier={value}	(Optional) Show only hosts with netbios_name that is either: beginning with, containing, matching, ending with, not empty.
	netbios_modifier is valid only when netbios_name is specified.
os_cpe_name={value}	(Optional) Specify the OS CPE name of the host to searched.
	os_cpe_name is valid only when os_cpe_name is specified.
os_cpe_modifier={value}	(Optional)) Show only hosts with os cpe_name that is either: beginning with, containing, matching, ending with, not empty.
	os_cpe_modifier is valid only when os_cpe_name is specified.
os_name={value}	(Optional) Specify the operating system name of the host to be searched.
	os_name is valid only when os_modifier is specified.
os_modifier={value}	(Optional) Show only hosts with os_name that is either: beginning with, containing, matching, ending with.
	os_modifier is valid only when os_name is specified.

Sample - Request Asset Search report

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/?action=sear
ch&output_format=xml&echo_request=1&ips=10.10.10.10-10.10.10.20"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">

<ASSET_SEARCH_REPORT>
<HEADER>
```

```
  <REQUEST>
    <DATETIME>2018-06-03T20:21:13Z</DATETIME>
    <USER_LOGIN>john_sm</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/report/asset/
     </RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>search</VALUE>
      </PARAM>
      <PARAM>
        <KEY>output_format</KEY>
        <VALUE>xml</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ips</KEY>
        <VALUE>10.10.10.10-10.10.10.15</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <COMPANY>Corsa</COMPANY>
  <USERNAME>John Smith</USERNAME>
  <GENERATION_DATETIME>2018-06-03T20:21:13Z</GENERATION_DATETIME>
  <TOTAL>2</TOTAL>
  <FILTERS>
    <IP_LIST>
      <RANGE>
        <START>10.10.10.10</START>
        <END>10.10.10.15</END>
      </RANGE>
    </IP_LIST>
  </FILTERS>
</HEADER>

<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.10.10.10]]></IP>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
   <OPERATING_SYSTEM><![CDATA[Linux 2.4-2.6 / Embedded Device / F5
Networks Big-IP]]></OPERATING_SYSTEM>
    <LAST_SCAN_DATE>2018-06-03T09:11:21Z</LAST_SCAN_DATE>
```

```
    <FIRST_FOUND_DATE>2018-06-03T07:11:46Z</FIRST_FOUND_DATE>
  </HOST>

  <HOST>
    <IP><![CDATA[10.10.10.11]]></IP>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
    <DNS><![CDATA[10-10-10-11.bogus.tld]]></DNS>
    <NETBIOS><![CDATA[SYS_10_10_10_11]]></NETBIOS>
    <OPERATING_SYSTEM><![CDATA[Windows 2000 Server Service Pack
4]]></OPERATING_SYSTEM>
    <LAST_SCAN_DATE>2018-06-03T07:12:47Z</LAST_SCAN_DATE>
    <LAST_COMPLIANCE_SCAN_DATE>2018-05-
13T21:15:01Z</LAST_COMPLIANCE_SCAN_DATE>
    <FIRST_FOUND_DATE>2018-05-12T15:16:54Z</FIRST_FOUND_DATE>
  </HOST>

</HOST_LIST>
</ASSET_SEARCH_REPORT>
```

DTD:

<platform API server>/asset_search_report_v2.dtd

Sample - Asset Search report CSV

CSV output:

```
----BEGIN_RESPONSE_HEADER_CSV
"Launch Datetime","User Login","Resource","Parameter
Name","Parameter Value"
"2018-06-
07T22:51:23Z","john_sm","https://qualysapi.qualys.com/api/2.0/fo/r
eport/asset/",,
,,,"action","search"
,,,"output_format","csv"
,,,"echo_request","1"
,,,"ips","10.10.10.10-10.10.10.20"
----END_RESPONSE_HEADER_CSV
"Company","UserName","ReportDate","AssetGroups","IPAddresses","DNS
Hostname","NetBIOSHostname","TargetTrackingMethod","TargetOperatin
gSystem","TargetService","TargetPort","TargetQID","QIDTitle","Targ
etLastScanDate","TargetFirstFoundDate","OSCPE","Tags","TargetCompl
ianceLastScanDate","Total"
"Corsa","John Smith","2018-06-07T22:51:23Z",,"10.10.10.10-
10.10.10.20",,,,,,,,,,,,,"2"
"IP","DNSHostname","NetBIOSHostname","OperatingSystem","OSCPE","Po
rt/Service/Default
Service","TrackingMethod","LastScanDate","LastComplianceScanDate",
"First Found","Tags"
```

```
"10.10.10.10",,,"Linux 2.4-2.6 / Embedded Device / F5 Networks
Big-IP",,,"IP address","2018-06-03T09:11:21Z",,"2018-06-
03T07:11:46Z",
"10.10.10.11",,"SYS_10_10_10_11",,,,"IP address","2018-06-
03T07:12:47Z","2018-05-13T21:15:01Z","2018-05-12T15:16:54Z",
```

Sample - Asset Search Report in XML output for Azure VM instances

This sample will return the asset search report in XML format. In XML output, you'll see these Azure VM instance specific tags: FILTER_AZURE_VM_ID, FILTER_AZURE_VM_STATE with Azure filter values.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/?action=search&asse
t_groups=All&azure_vm_id=399af5dc-c32a-4c40-95a5-
c6ed0e786430&azure_vm_id_modifier=beginning+with&tracking_method=AZURE+VM
&azure_vm_state=RUNNING&output_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">

<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[Qualys]]></COMPANY>
  <USERNAME>Patrick Slimmer</USERNAME>
  <GENERATION_DATETIME>2020-06-22T23:24:25Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_GROUPS>
      <ASSET_GROUP_TITLE><![CDATA[All]]></ASSET_GROUP_TITLE>
    </ASSET_GROUPS>
    <FILTER_AZURE_VM_ID><![CDATA[Beginning With 399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></FILTER_AZURE_VM_ID>
    <TRACKING_METHOD><![CDATA[Azure VM]]></TRACKING_METHOD>
    <FILTER_AZURE_VM_STATE><![CDATA[RUNNING]]></FILTER_AZURE_VM_STATE>
  </FILTERS>
</HEADER>
<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.4.8.4]]></IP>
    <TRACKING_METHOD>Azure VM</TRACKING_METHOD>
    <CLOUD_PROVIDER>Azure</CLOUD_PROVIDER>
    <CLOUD_SERVICE>VM</CLOUD_SERVICE>
    <CLOUD_RESOURCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></CLOUD_RESOURCE_ID>
    <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
```

```
    <EC2_INSTANCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></EC2_INSTANCE_ID>
...
```

Sample - Search EC2 asset with certain EC2 instance ID

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=search&output_format=xml&tracking_method=EC2&use_tags=1&ta
g_set_by=name&tag_set_include=useasttag&ec2_instance_id=i-
0fb7086f985856fa4&ec2_instance_id_modifier=containing"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">
<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[qualys-test]]></COMPANY>
  <USERNAME>qualys_ps</USERNAME>
  <GENERATION_DATETIME>2018-04-11T10:17:32Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_TAGS>
      <INCLUDED_TAGS scope="any">
        <ASSET_TAG><![CDATA[useasttag]]></ASSET_TAG>
      </INCLUDED_TAGS>
    </ASSET_TAGS>
    <TRACKING_METHOD><![CDATA[EC2]]></TRACKING_METHOD>
  </FILTERS>
</HEADER>
<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.73.188.6]]></IP>
    <HOST_TAGS><![CDATA[EC2, Virginia, agec2, sada-0117-targets,
sada-new-0308, useasttag;
]]></HOST_TAGS>
    <TRACKING_METHOD>EC2</TRACKING_METHOD>
    <DNS><![CDATA[ip-10-73-188-6.ec2.internal]]></DNS>
    <EC2_INSTANCE_ID><![CDATA[i-
0fb7086f985856fa4]]></EC2_INSTANCE_ID>
    <LAST_SCAN_DATE />
    <FIRST_FOUND_DATE />
  </HOST>
</HOST_LIST>
```

Sample - Search EC2 assets with certain status

Search all EC2 assets which are currently in TERMINATED state and having instance ID i-0b121b9211d7e25cb.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=search&output_format=xml&tracking_method=EC2&use_tags=1&ta
g_set_by=name&tag_set_include=useasttag&ec2_instance_status=TERMIN
ATED&ec2_instance_id=i-
0b121b9211d7e25cb&ec2_instance_id_modifier=containing"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">
<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[qualys-test]]></COMPANY>
  <USERNAME>sada-customer customer</USERNAME>
  <GENERATION_DATETIME>2018-04-11T10:49:05Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_TAGS>
      <INCLUDED_TAGS scope="any">
        <ASSET_TAG><![CDATA[useasttag]]></ASSET_TAG>
      </INCLUDED_TAGS>
    </ASSET_TAGS>
    <TRACKING_METHOD><![CDATA[EC2]]></TRACKING_METHOD>
  </FILTERS>
</HEADER>
<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.90.2.175]]></IP>
    <HOST_TAGS><![CDATA[EC2, Vriginia, por-6586, sada-0117-
targets, sada-new-0308, useasttag;
]]></HOST_TAGS>
    <TRACKING_METHOD>EC2</TRACKING_METHOD>
    <DNS><![CDATA[i-0b121b9211d7e25cb]]></DNS>
    <EC2_INSTANCE_ID><![CDATA[i-
0b121b9211d7e25cb]]></EC2_INSTANCE_ID>
    <LAST_SCAN_DATE />
    <FIRST_FOUND_DATE />
  </HOST>
</HOST_LIST>
```

Sample - Search assets with SCAP scan performed

API request:

```
curl -u "username:password" -H "X-Requested-With:"
"action=search&output_format=xml&asset_groups=Winodws+7+Scap&last_
scap_scan_days=300&last_scap_scan_modifier=within"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">
<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[qualys]]></COMPANY>
  <USERNAME>POC Manager</USERNAME>
  <GENERATION_DATETIME>2018-11-06T00:42:13Z</GENERATION_DATETIME>
  <TOTAL>26</TOTAL>
  <FILTERS>
    <ASSET_GROUPS>
      <ASSET_GROUP_TITLE><![CDATA[Winodws 7
Scap]]></ASSET_GROUP_TITLE>
    </ASSET_GROUPS>
    <FILTER_LAST_SCAP_SCAN_DATE><![CDATA[Within
300]]></FILTER_LAST_SCAP_SCAN_DATE>
  </FILTERS>
</HEADER>

<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.10.10.10]]></IP>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
    <DNS><![CDATA[bridge.qualys.com]]></DNS>
    <NETBIOS><![CDATA[WIN7-10-10]]></NETBIOS>
    <OPERATING_SYSTEM><![CDATA[Windows 7 Ultimate 64 bit Edition
Service Pack 1]]></OPERATING_SYSTEM>
    <OS_CPE><![CDATA[cpe:/o:microsoft:windows_7::sp1:x64-
ultimate:]]></OS_CPE>
    <LAST_SCAN_DATE>2018-10-18T20:55:10Z</LAST_SCAN_DATE>
    <LAST_COMPLIANCE_SCAN_DATE>2018-09-
14T21:57:53Z</LAST_COMPLIANCE_SCAN_DATE>
    <LAST_SCAP_SCAN_DATE>2018-08-
28T10:57:06Z</LAST_SCAP_SCAN_DATE>
    <FIRST_FOUND_DATE>2018-04-03T23:18:26Z</FIRST_FOUND_DATE>
  </HOST>
```

VM Report Templates

The Report Template API is used to manage report templates and their settings in the user's subscription.

API Support for Report Templates

Scan Template

PCI Scan Template

Patch Template

Map Template

API Support for Report Templates

You can now use APIs to create custom reports with views on your scan results and the current vulnerabilities on your hosts. Use various report templates provided by Qualys as a starting point.

APIs are now available to perform various actions on templates for the following report types: Scan Template, PCI Scan Template, Patch Template, Map Template

The Report Template API allows users to perform the following actions.

Action	Supported Access Method	Description
Create	POST	Create a report template. A unique template ID is generated for the new template.
Update	PUT	Update an existing report template.
Delete	POST	Delete an existing report template.
Export	GET	Export a specific report template based on the template ID, or all templates for the report type.

Once you have your template the way you want you can run reports using the templates using the Report API /api/2.0/fo/report.

Scan Template

For API version information, refer to API Version History section.

V2.0|V3.0 | V4.0 | V7.0

Note: Scan report templates now support enhanced capabilities across versions:

- Kernel Live Patch (v5): Provides the ability to exclude Linux kernel CVEs that are already fixed by live patches, reducing false positives and improving visibility into truly actionable vulnerabilities.

- Deep Scan (v6): Discovers vulnerable software and binaries in non-standard locations that traditional scans may miss. This API allows Deep Scan findings to be included in scan report templates.

- CVSS v4.0 Support (v7): Uses enhanced vulnerability scoring for greater precision and context?aware reporting in API?driven workflows.

To enable features from earlier versions (v5 and v6) and the current version (v7), if CVSS v4 is not visible in your environment, contact your Technical Account Manager (TAM) or Qualys Support.

V2.0

/api/2.0/fo/report/template/scan/

Perform actions such as create, update, delete and export on the Scan Template.

Scan Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Scan Template	<base_url>/api/2.0/fo/report/template/scan/ Required parameters: action=create report_format=xml	POST
Update Scan Template	<base_url>/api/2.0/fo/report/template/scan/ Required parameters: template_id={value} action=update report_format=xml	PUT

Action	API Endpoint /required parameters	Method
Delete Scan Template	<base_url>/api/2.0/fo/report/template/scan/ Required parameters: template_id={value} action=delete	POST
Export Scan Template	<base_url>/api/2.0/fo/report/template/scan/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Scan Template settings

These parameters (all are optional) are used for a create or update request to define scan template settings. When creating a new template the default value is shown in bold where applicable.

Parameter	Description
Title	The template title and owner.
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .
Target	What target assets to include in the report.
scan_selection={**HostBased**|ScanBased|}	Specify HostBased for Host Based Findings (default for new template) or ScanBased for Scan Based Findings. Choosing Host Based Findings allows you to report on the latest vulnerability data from all of your scans. Choosing Scan Based Findings allows you to run a report based on saved scan results.
include_trending={**0**|1}	Specify 1 to include trending. Choose a timeframe (daily, weekly or monthly) to analyze the vulnerability status for the timeframe selected. This parameter is required only if scan_selection=HostBased.
limit_timeframe={**0**|1}	Specify 1 to only include scan results from the specified time frame. This ensures that only vulnerability information gathered in the timeframe that you've specified is included in the report. If unspecified, vulnerability information for hosts that were last scanned prior to the report timeframe may be included. This parameter is required only if scan_selection=HostBased.

Parameter	Description
selection_type={day|month|weeks|date|none|scans}	Specify whether to include trending information for number of weeks, days or months or a specific date. Specifying none will create a report without any trending information included. Specifying scans will include trending information for the last two detections. This parameter is required only if scan_selection=HostBased.
selection_range={value}	Specify the range for the selection type. Specify a number of units (1|3|5|7|15|30|60|90) for days, weeks or months. Date must be in the format yyyy-mm-dd (2017-04-05), and must be less than or equal to today's date. Trending information since the last number of units or the specified date will be included. This parameter is required only if scan_selection=HostBased.
asset_groups={value}	Specify the name of the asset group(s) to report on. Multiple asset groups are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
asset_group_ids={value}	Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
network={value}	(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.
ips={value}	Specify the IPs or IP ranges to report on. Multiple IPs or IP ranges are comma separated. This parameter is required only if scan_selection=HostBased.
tag_set_by={name|id}	Specify the name of the tags or the ID of the tags for the hosts you want to report on. Multiple tag names or tag IDs are comma separated.
tag_include_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.

Parameter	Description
tag_set_include={value}	Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
tag_exclude_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_exclude={value}	Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
host_with_cloud_agents={all|scan|agent}	What host findings to include in the report when CA module is enabled. Your options are: all - All data scan - Scan data, i.e. include findings from scans that didn't use Agentless Tracking agent - Agent data, i.e. include findings from the agent when merging is enabled (i.e. Show unified view hosts option in UI under Users > Setup > Cloud Agent Setup)
display_text_summary={**0**|1}	Specify 1 to include the following summary info for the entire report: total vulnerabilities detected, overall security risk, business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.
graph_business_risk={**0**|1}	Specify 1 to include the business risk information. Note that some graphs are only available when trend information is included. Keep in mind that your filter settings will affect the data reflected in your graphs.
graph_vuln_over_time={**0**|1}	Specify 1 to include the vulnerabilities by severity over time.
graph_status={**0**|1}	Specify 1 to include the vulnerabilities by status.
graph_potential_status={**0**|1}	Specify 1 to include the potential vulnerabilities by status.
graph_severity={**0**|1}	Specify 1 to include the vulnerabilities by severity.
Display	Display options such as graphs amount of detail.
graph_potential_severity={**0**|1}	Specify 1 to include the potential vulnerabilities by severity.

Parameter	Description
graph_ig_severity={**0**|1}	Specify 1 to include the information gathered by severity.
graph_top_categories={**0**|1}	Specify 1 to include the top five vulnerable categories.
graph_top_vulns={**0**|1}	Specify 1 to include the ten most prevalent vulnerabilities.
graph_os={**0**|1}	Specify 1 to include the operating systems detected.
graph_services={**0**|1}	Specify 1 to include the services detected.
graph_top_ports={**0**|1}	Specify 1 to include the ports detected.
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
sort_by={host|vuln|os|group|service|port}	Specify how you want to organize the Detailed Results section of your report - by host, vuln (i.e. vulnerability), group (i.e. asset group), service or port.
cvss={**all**|cvssv2|cvssv3}	Specify the CVSS version score you want to display in reports. all - both CVSS versions cvssv2 - CVSS version 2 cvssv3 - CVSS version 3
host_details={0|**1**}	Specify 1 to include identifying information for each host agent like the asset ID and related IPs (IPv4, IPv6 and MAC addresses). This parameter is required only if scan_selection=HostBased and sort_by=host.
metadata_ec2_instances={0|1}	Specify 1 to display “Legacy EC2/Azure Fields” for each EC2 asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
cloud_provider_metadata={**0**|1}	Specify 1 to display “Cloud Provider Metadata Fields” for each cloud asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
qualys_system_ids={0|1}	Specify 1 to include host ID/asset ID in the host-based scan report.
include_text_summary={**0**|1}	Specify 1 to include the following summary info for each host, vulnerability, asset group, etc (depending on the sorting method you selected): total vulnerabilities detected, the security risk, the business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.

Parameter	Description
include_vuln_details={**0**|1}	Specify 1 to include additional details for each vulnerability in the report.
include_vuln_details_threat ={**0**|1}	Specify 1 to include a description of the threat.
include_vuln_details_impact ={**0**|1}	Specify 1 to include possible consequences that may occur if the vulnerability is exploited.
include_vuln_details_solutio n={**0**|1}	Specify 1 to include a verified solution to remedy the issue, such as a link to the vendor's patch, Web site, or a workaround.
include_vuln_details_vpatch ={**0**|1}	Specify 1 to include virtual patch information correlated with the vulnerability, obtained from Trend Micro real-time feeds.
include_vuln_details_compli ance={**0**|1}	Specify 1 to include compliance information correlated with the vulnerability.
include_vuln_details_exploit ={**0**|1}	Specify 1 to include exploitability information correlated with the vulnerability, includes references to known exploits and related security resources.
include_vuln_details_malwa re={**0**|1}	Specify 1 to include malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.
include_vuln_details_results ={**0**|1}	Specify 1 to include specific scan test results for each host, when available. We'll also show the date the vulnerability was first detected, last detected and the number of times it was detected.
include_vuln_details_reopen ed={0|1}	Specify 1 to include information related to reopened vulnerabilities.
include_vuln_details_appen dix={**0**|1}	Specify 1 to include more information like IPs in your report target that don't have any scan results, and IPs that were scanned but results are not shown (no vulnerabilities were detected or all vulnerabilities were filtered out).
include_trurisk_details={0|1}	Specify 0 to exclude and 1 to include TruRisk details in the report template. By default, the value is set to 1. **Note**: This parameter is applicable only if: - The scan type is host-based scan (scan_selection= HostBased). - The subscription has Asset Risk Scoring (ARS) enabled.
exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.
Filters	Filter options such as vulnerability status, categories, QIDs, OS.

Parameter	Description
selective_vulns={**complete**|custom}	Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value}	Specify search list ID or QID. Multiple search list IDs or QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={**0**|1}	Specify 1 to exclude QIDs from the report.
exclude_search_list_ids={value}	Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
included_os={value}	Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.
status_new={0|**1**}	Specify 1 to include vulnerabilities in your report based on the current vulnerability status - New.
status_active={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Active.
status_reopen={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Re-Opened.
status_fixed={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Fixed.
qds_score_min{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS greater than or equal to a QDS score you specify.
qds_score_max{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS less than or equal to a QDS score you specify.
vuln_active={0|**1**}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Active.
vuln_disabled={**1**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Disabled.
vuln_ignored={**0**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Ignored.
potential_active={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Active.

Parameter	Description
potential_disabled={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Disabled.
potential_ignored={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Ignored.
ig_active={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Active.
ig_disabled={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Disabled.
ig_ignored={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Ignored.
display_non_running_kernels={**0**|1}	Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={**0**|1}	Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={**0**|1}	Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={**0**|1}	Specify 1 to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host.
exclude_superceded_patches={**0**|1}	Specify 1 to exclude every patch QID which is superceded (replaced) by another patch QID recommended for the same Host.
categories_list={value}	Specify the category name to filter hosts in your report based on various categories. For example, if you're only interested in Windows vulnerabilities make sure you provide the category name for Windows. Multiple category names can be provided using values separated by a comma. Specify ALL to include all categories. See Categories.
Services and Ports	Services and ports to include in report.
required_services={value}	Specify the name of a required service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38228 (when a required service is NOT detected). See Identified Services.
unauthorized_services={value}	Specify the name of an unauthorized service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38175 (when an unauthorized service is detected). See Identified Services.
required_ports={value}	Specify required ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82051 (when a required port is NOT detected).

Parameter	Description
unauthorized_ports={value}	Specify unauthorized ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82043 (when an unauthorized port is detected).
User Access	Control user access to template and reports generated from template.
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.
report_access_users={value}	Specify the username to share the report with a user who wouldn't already have access to the report. Multiple usernames can be provided using values separated by a comma. Each user you add will be able to view reports generated from this template even if they don't have access to the IPs in the report.

Cloud Asset Metadata Fields in CSV Format

See the table below to know which cloud asset metadata columns will appear in your CSV reports based on your report template settings. Columns will appear in the order shown.

Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
EC2 Instance ID	Cloud Provider	Cloud Provider
Public Hostname	Cloud Provider Service	Cloud Provider Service
Image ID	Cloud Service	Cloud Service
VPC ID	Cloud Resource ID	Cloud Resource ID
Instance State	Cloud Resource Type	Cloud Resource Type
Private Hostname	Cloud Account	Cloud Account
Instance Type	Cloud Image ID	Cloud Image ID
Account ID	Cloud Resource Metadata	Cloud Resource Metadata
Region Code		EC2 Instance ID
Subnet ID		Public Hostname
		Image ID
		VPC ID
		Instance State
		Private Hostname
		Instance Type
		Account ID
		Region Code
		Subnet ID

Important note about the Legacy EC2/Azure Fields in CSV

These fields were originally introduced for AWS cloud assets and will be populated with metadata for your AWS EC2 assets.

For Azure and GCP assets, all Legacy EC2/Azure columns will appear blank in the CSV report, except for the EC2 Instance ID column. We will continue to populate the EC2 Instance ID column for all cloud assets (AWS, Azure, GCP). The EC2 Instance ID column is replaced by Cloud Resource ID, and will be deprecated in a future release.

Cloud Asset Metadata Fields in XML Format

See the table below to know which cloud asset metadata tags will appear in your XML reports based on your report template settings.

Cloud Provider	Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
AWS	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID EC2_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID EC2_INFO CLOUD_RESOURCE_METADATA
Azure	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID AZURE_VM_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID AZURE_VM_INFO CLOUD_RESOURCE_METADATA
GCP	CLOUD_RESOURCE_ID EC2_INSTANCE_ID	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA

EC2_INFO includes: PUBLIC_DNS_NAME, IMAGE_ID, VPC_ID, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID

AZURE_VM_INFO includes: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTON_ID, LOCATION, RESOURCE_GROUP_NAME

CLOUD_RESOURCE_METADATA for AWS includes: INSTANCE_ID, PUBLIC_DNS_NAME, PUBLIC_IP_ADDRESS, PRIVATE_IP_ADDRESS, IMAGE_ID, SPOT_INSTANCE, AVAILABILITY_ZONE, VPC_ID, GROUP_ID, GROUP_NAME, LOCAL_HOSTNAME, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID, RESERVATION_ID, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for Azure includes: VM_ID, VM_NAME, PLATFORM, PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_PUBLISHER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for GCP includes: INSTANCE_ID, HOST_NAME, MACHINE_TYPE, MACHINE_STATE, PROJECT_ID, PUBLIC_IP_ADDRESS, VPC_NETWORK, ZONE, PRIVATE_IP_ADDRESS, MAC_ADDRESS

DTD

<platform API server>/api/2.0/fo/report/template/scan/scanreporttemplate_info.dtd

Sample - Create scan template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -H
"Content-type: text/xml" --data-binary @scan_export.xml
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?act
ion=create&report_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-06T05:41:32Z</DATETIME>
    <CODE>Scan Report Template(s) Created Successfully
[89876]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Scan template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X PUT -H
"Content-type: text/xml" --data-binary @scan_export.xml
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?act
ion=update&template_id=8209&report_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-04T10:52:34Z</DATETIME>
    <CODE>Scan Report Template Updated Successfully [8209]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete Scan template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=delete&template_id=8209"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-04T10:54:37Z</DATETIME>
    <CODE>Scan Report Template(s) Deleted Successfully
[8209]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Export Scan template

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?act
ion=export&template_id=89470&report_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/scan
reporttemplate_info.dtd">
<REPORTTEMPLATE>
  <SCANTEMPLATE>
    <TITLE>
      <INFO key="title"><![CDATA[Scan-Report-To-Create-Do not
Change]]></INFO>
      <INFO key="owner"><![CDATA[1086]]></INFO>
    </TITLE>
    <TARGET>
```

```
      <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
      <INFO key="include_trending"><![CDATA[1]]></INFO>
      <INFO key="selection_type"><![CDATA[days]]></INFO>
      <INFO key="selection_range"><![CDATA[5]]></INFO>
      <INFO key="limit_timeframe"><![CDATA[1]]></INFO>
      <INFO key="asset_groups"><![CDATA[PBPS-Targets]]></INFO>
      <INFO key="tag_set_by"><![CDATA[id]]></INFO>
      <INFO key="tag_set_include"><![CDATA[8644659]]></INFO>
      <INFO key="tag_set_exclude"><![CDATA[8262228]]></INFO>
      <INFO key="tag_include_selector"><![CDATA[ALL]]></INFO>
      <INFO key="tag_exclude_selector"><![CDATA[ALL]]></INFO>
      <INFO key="network"><![CDATA[-100]]></INFO>
      <INFO key="ips"><![CDATA[10.10.0.1,10.10.0.5]]></INFO>
      <INFO key="host_with_cloud_agents"><![CDATA[all]]></INFO>
    </TARGET>
    <DISPLAY>
      <INFO key="graph_business_risk"><![CDATA[1]]></INFO>
      <INFO key="graph_vuln_over_time"><![CDATA[1]]></INFO>
      <INFO key="display_text_summary"><![CDATA[1]]></INFO>
      <INFO key="graph_status"><![CDATA[1]]></INFO>
      <INFO key="graph_potential_status"><![CDATA[1]]></INFO>
      <INFO key="graph_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_potential_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_ig_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_top_categories"><![CDATA[1]]></INFO>
      <INFO key="graph_top_vulns"><![CDATA[1]]></INFO>
      <INFO key="graph_os"><![CDATA[1]]></INFO>
      <INFO key="graph_services"><![CDATA[1]]></INFO>
      <INFO key="graph_top_ports"><![CDATA[1]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[1]]></INFO>
      <INFO
key="display_custom_footer_text"><![CDATA[Test@123]]></INFO>
      <INFO key="sort_by"><![CDATA[host]]></INFO>
      <INFO key="cvss"><![CDATA[all]]></INFO>
      <INFO key="host_details"><![CDATA[0]]></INFO>
      <INFO key="qualys_system_ids"><![CDATA[1]]></INFO>
      <INFO key="include_text_summary"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details_threat"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details_impact"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_solution"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details_vpatch"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_compliance"><![CDATA[1]]></INFO>
      <INFO
```

```
key="include_vuln_details_exploit"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_malware"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_results"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_appendix"><![CDATA[1]]></INFO>
      <INFO key="exclude_account_id"><![CDATA[1]]></INFO>
      <INFO
key="include_vuln_details_reopened"><![CDATA[1]]></INFO>
      <INFO key="metadata_ec2_instances"><![CDATA[1]]></INFO>
      <INFO key="cloud_provider_metadata"><![CDATA[1]]></INFO>
      <INFO key="metadata_ec2_instances"><![CDATA[0]]></INFO>
    </DISPLAY>
    <FILTER>
      <INFO key="selective_vulns"><![CDATA[complete]]></INFO>
      <INFO key="search_list_ids"><![CDATA[]]></INFO>
      <INFO key="exclude_qid_option"><![CDATA[1]]></INFO>
      <INFO key="exclude_search_list_ids"><![CDATA[]]></INFO>
      <INFO key="included_os"><![CDATA[ALL]]></INFO>
      <INFO key="status_new"><![CDATA[1]]></INFO>
      <INFO key="status_active"><![CDATA[1]]></INFO>
      <INFO key="status_reopen"><![CDATA[1]]></INFO>
      <INFO key="status_fixed"><![CDATA[1]]></INFO>
      <INFO key="vuln_active"><![CDATA[1]]></INFO>
      <INFO key="vuln_disabled"><![CDATA[1]]></INFO>
      <INFO key="vuln_ignored"><![CDATA[1]]></INFO>
      <INFO key="potential_active"><![CDATA[1]]></INFO>
      <INFO key="potential_disabled"><![CDATA[1]]></INFO>
      <INFO key="potential_ignored"><![CDATA[1]]></INFO>
      <INFO key="ig_active"><![CDATA[1]]></INFO>
      <INFO key="ig_disabled"><![CDATA[1]]></INFO>
      <INFO key="ig_ignored"><![CDATA[0]]></INFO>
      <INFO key="display_non_running_kernels"><![CDATA[1]]></INFO>
      <INFO key="exclude_non_running_kernel"><![CDATA[0]]></INFO>
      <INFO
key="exclude_non_running_services"><![CDATA[1]]></INFO>
      <INFO key="exclude_superceded_patches"><![CDATA[1]]></INFO>
      <INFO
key="exclude_qids_not_exploitable_due_to_configuration"><![CDATA[1
]]></INFO>
      <INFO key="categories_list"><![CDATA[ALL]]></INFO>
    </FILTER>
    <SERVICESPORTS>
      <INFO key="required_services"><![CDATA[ActiveSync,akak
trojan,Apple
```

```
        Airport Management,Applix TM1 Server]]></INFO>
       <INFO key="unauthorized_services"><![CDATA[aml,Arkeiad
Network
        Backup,auth]]></INFO>
       <INFO key="services_info"><![CDATA[aml,Arkeiad Network
        Backup,auth]]></INFO>
       <INFO key="required_ports"><![CDATA[12]]></INFO>
       <INFO key="unauthorized_ports"><![CDATA[21]]></INFO>
     </SERVICESPORTS>
     <USERACCESS>
       <INFO

key="report_access_users"><![CDATA[start_rm2,start_su]]></INFO>
       <INFO key="global"><![CDATA[1]]></INFO>
     </USERACCESS>
   </SCANTEMPLATE>
</REPORTTEMPLATE>
```

V3.0

/api/3.0/fo/report/template/scan/

Perform actions such as create, update, delete and export on the Scan Template.

Scan Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Scan Template	<base_url>/api/3.0/fo/report/template/scan/ Required parameters: action=create report_format=xml	POST
Update Scan Template	<base_url>/api/3.0/fo/report/template/scan/ Required parameters: template_id={value} action=update report_format=xml	PUT

Action	API Endpoint /required parameters	Method
Delete Scan Template	<base_url>/api/3.0/fo/report/template/scan/ Required parameters: template_id={value} action=delete	POST
Export Scan Template	<base_url>/api/3.0/fo/report/template/scan/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Scan Template settings

These parameters (all are optional) are used for a create or update request to define scan template settings. When creating a new template the default value is shown in bold where applicable.

Parameter	Description
Title	The template title and owner.
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .
Target	What target assets to include in the report.
scan_selection={**HostBased**|ScanBased|}	Specify HostBased for Host Based Findings (default for new template) or ScanBased for Scan Based Findings. Choosing Host Based Findings allows you to report on the latest vulnerability data from all of your scans. Choosing Scan Based Findings allows you to run a report based on saved scan results.
include_trending={**0**|1}	Specify 1 to include trending. Choose a timeframe (daily, weekly or monthly) to analyze the vulnerability status for the timeframe selected. This parameter is required only if scan_selection=HostBased.
limit_timeframe={**0**|1}	Specify 1 to only include scan results from the specified time frame. This ensures that only vulnerability information gathered in the timeframe that you've specified is included in the report. If unspecified, vulnerability information for hosts that were last scanned prior to the report timeframe may be included. This parameter is required only if scan_selection=HostBased.

Parameter	Description
selection_type={day|month|weeks|date|none|scans}	Specify whether to include trending information for number of weeks, days or months or a specific date. Specifying none will create a report without any trending information included. Specifying scans will include trending information for the last two detections. This parameter is required only if scan_selection=HostBased.
selection_range={value}	Specify the range for the selection type. Specify a number of units (1|3|5|7|15|30|60|90) for days, weeks or months. Date must be in the format yyyy-mm-dd (2017-04-05), and must be less than or equal to today's date. Trending information since the last number of units or the specified date will be included. This parameter is required only if scan_selection=HostBased.
asset_groups={value}	Specify the name of the asset group(s) to report on. Multiple asset groups are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
asset_group_ids={value}	Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
network={value}	(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.
ips={value}	Specify the IPs or IP ranges to report on. Multiple IPs or IP ranges are comma separated. This parameter is required only if scan_selection=HostBased.
tag_set_by={name|id}	Specify the name of the tags or the ID of the tags for the hosts you want to report on. Multiple tag names or tag IDs are comma separated.
tag_include_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.

Parameter	Description
tag_set_include={value}	Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
tag_exclude_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_exclude={value}	Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
host_with_cloud_agents={all|scan|agent}	What host findings to include in the report when CA module is enabled. Your options are: all - All data scan - Scan data, i.e. include findings from scans that didn't use Agentless Tracking agent - Agent data, i.e. include findings from the agent when merging is enabled (i.e. Show unified view hosts option in UI under Users > Setup > Cloud Agent Setup)
display_text_summary={**0**|1}	Specify 1 to include the following summary info for the entire report: total vulnerabilities detected, overall security risk, business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.
graph_business_risk={**0**|1}	Specify 1 to include the business risk information. Note that some graphs are only available when trend information is included. Keep in mind that your filter settings will affect the data reflected in your graphs.
graph_vuln_over_time={**0**|1}	Specify 1 to include the vulnerabilities by severity over time.
graph_status={**0**|1}	Specify 1 to include the vulnerabilities by status.
graph_potential_status={**0**|1}	Specify 1 to include the potential vulnerabilities by status.
graph_severity={**0**|1}	Specify 1 to include the vulnerabilities by severity.
Display	Display options such as graphs amount of detail.
graph_potential_severity={**0**|1}	Specify 1 to include the potential vulnerabilities by severity.

Parameter	Description
graph_ig_severity={**0**|1}	Specify 1 to include the information gathered by severity.
graph_top_categories={**0**|1}	Specify 1 to include the top five vulnerable categories.
graph_top_vulns={**0**|1}	Specify 1 to include the ten most prevalent vulnerabilities.
graph_os={**0**|1}	Specify 1 to include the operating systems detected.
graph_services={**0**|1}	Specify 1 to include the services detected.
graph_top_ports={**0**|1}	Specify 1 to include the ports detected.
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
sort_by={host|vuln|os|group|service|port}	Specify how you want to organize the Detailed Results section of your report - by host, vuln (i.e. vulnerability), group (i.e. asset group), service or port.
cvss={**all**|cvssv2|cvssv3}	Specify the CVSS version score you want to display in reports. all - both CVSS versions cvssv2 - CVSS version 2 cvssv3 - CVSS version 3
host_details={0|**1**}	Specify 1 to include identifying information for each host agent like the asset ID and related IPs (IPv4, IPv6 and MAC addresses). This parameter is required only if scan_selection=HostBased and sort_by=host.
metadata_ec2_instances={0|1}	Specify 1 to display “Legacy EC2/Azure Fields” for each EC2 asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
cloud_provider_metadata={**0**|1}	Specify 1 to display “Cloud Provider Metadata Fields” for each cloud asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
qualys_system_ids={0|1}	Specify 1 to include host ID/asset ID in the host-based scan report.
include_text_summary={**0**|1}	Specify 1 to include the following summary info for each host, vulnerability, asset group, etc (depending on the sorting method you selected): total vulnerabilities detected, the security risk, the business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.

Parameter	Description
include_vuln_details={**0**|1}	Specify 1 to include additional details for each vulnerability in the report.
include_vuln_details_threat ={**0**|1}	Specify 1 to include a description of the threat.
include_vuln_details_impact ={**0**|1}	Specify 1 to include possible consequences that may occur if the vulnerability is exploited.
include_vuln_details_solutio n={**0**|1}	Specify 1 to include a verified solution to remedy the issue, such as a link to the vendor's patch, Web site, or a workaround.
include_vuln_details_vpatch ={**0**|1}	Specify 1 to include virtual patch information correlated with the vulnerability, obtained from Trend Micro real-time feeds.
include_vuln_details_compli ance={**0**|1}	Specify 1 to include compliance information correlated with the vulnerability.
include_vuln_details_exploit ={**0**|1}	Specify 1 to include exploitability information correlated with the vulnerability, includes references to known exploits and related security resources.
include_vuln_details_malwa re={**0**|1}	Specify 1 to include malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.
include_vuln_details_results ={**0**|1}	Specify 1 to include specific scan test results for each host, when available. We'll also show the date the vulnerability was first detected, last detected and the number of times it was detected.
include_vuln_details_reopen ed={0|1}	Specify 1 to include information related to reopened vulnerabilities.
include_vuln_details_appen dix={**0**|1}	Specify 1 to include more information like IPs in your report target that don't have any scan results, and IPs that were scanned but results are not shown (no vulnerabilities were detected or all vulnerabilities were filtered out).
include_trurisk_details={0|1}	Specify 0 to exclude and 1 to include TruRisk details in the report template. By default, the value is set to 1. **Note**: This parameter is applicable only if: - The scan type is host-based scan (scan_selection= HostBased). - The subscription has Asset Risk Scoring (ARS) enabled.
exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.

Parameter	Description
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0.
Filters	Filter options such as vulnerability status, categories, QIDs, OS.
selective_vulns={**complete**|custom}	Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value}	Specify search list ID or QID. Multiple search list IDs or QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={**0**|1}	Specify 1 to exclude QIDs from the report.
exclude_search_list_ids={value}	Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
included_os={value}	Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.
status_new={0|**1**}	Specify 1 to include vulnerabilities in your report based on the current vulnerability status - New.
status_active={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Active.
status_reopen={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Re-Opened.
status_fixed={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Fixed.
qds_score_min{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS greater than or equal to a QDS score you specify.
qds_score_max{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS less than or equal to a QDS score you specify.

Parameter	Description
vuln_active={0|**1**}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Active.
vuln_disabled={**1**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Disabled.
vuln_ignored={**0**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Ignored.
potential_active={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Active.
potential_disabled={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Disabled.
potential_ignored={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Ignored.
ig_active={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Active.
ig_disabled={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Disabled.
ig_ignored={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Ignored.
display_non_running_kernels={**0**|1}	Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={**0**|1}	Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={**0**|1}	Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={**0**|1}	Specify 1 to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host.
exclude_superceded_patches={**0**|1}	Specify 1 to exclude every patch QID which is superceded (replaced) by another patch QID recommended for the same Host.
categories_list={value}	Specify the category name to filter hosts in your report based on various categories. For example, if you're only interested in Windows vulnerabilities make sure you provide the category name for Windows. Multiple category names can be provided using values separated by a comma. Specify ALL to include all categories. See Categories.
Services and Ports	Services and ports to include in report.

Parameter	Description
required_services={value}	Specify the name of a required service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38228 (when a required service is NOT detected). See Identified Services.
unauthorized_services={value}	Specify the name of an unauthorized service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38175 (when an unauthorized service is detected). See Identified Services.
required_ports={value}	Specify required ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82051 (when a required port is NOT detected).
unauthorized_ports={value}	Specify unauthorized ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82043 (when an unauthorized port is detected).
User Access	Control user access to template and reports generated from template.
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.
report_access_users={value}	Specify the username to share the report with a user who wouldn't already have access to the report. Multiple usernames can be provided using values separated by a comma. Each user you add will be able to view reports generated from this template even if they don't have access to the IPs in the report.

Cloud Asset Metadata Fields in CSV Format

See the table below to know which cloud asset metadata columns will appear in your CSV reports based on your report template settings. Columns will appear in the order shown.

Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
EC2 Instance ID	Cloud Provider	Cloud Provider
Public Hostname	Cloud Provider Service	Cloud Provider Service
Image ID	Cloud Service	Cloud Service
VPC ID	Cloud Resource ID	Cloud Resource ID
Instance State	Cloud Resource Type	Cloud Resource Type
Private Hostname	Cloud Account	Cloud Account
Instance Type	Cloud Image ID	Cloud Image ID
Account ID	Cloud Resource Metadata	Cloud Resource Metadata
Region Code		EC2 Instance ID
Subnet ID		Public Hostname
		Image ID
		VPC ID
		Instance State
		Private Hostname
		Instance Type
		Account ID
		Region Code
		Subnet ID

Important note about the Legacy EC2/Azure Fields in CSV

These fields were originally introduced for AWS cloud assets and will be populated with metadata for your AWS EC2 assets.

For Azure and GCP assets, all Legacy EC2/Azure columns will appear blank in the CSV report, except for the EC2 Instance ID column. We will continue to populate the EC2 Instance ID column for all cloud assets (AWS, Azure, GCP). The EC2 Instance ID column is replaced by Cloud Resource ID, and will be deprecated in a future release.

Cloud Asset Metadata Fields in XML Format

See the table below to know which cloud asset metadata tags will appear in your XML reports based on your report template settings.

Cloud Provider	Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
AWS	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID EC2_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID EC2_INFO CLOUD_RESOURCE_METADATA
Azure	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID AZURE_VM_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID AZURE_VM_INFO CLOUD_RESOURCE_METADATA
GCP	CLOUD_RESOURCE_ID EC2_INSTANCE_ID	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA

EC2_INFO includes: PUBLIC_DNS_NAME, IMAGE_ID, VPC_ID, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID

AZURE_VM_INFO includes: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTON_ID, LOCATION, RESOURCE_GROUP_NAME

CLOUD_RESOURCE_METADATA for AWS includes: INSTANCE_ID, PUBLIC_DNS_NAME, PUBLIC_IP_ADDRESS, PRIVATE_IP_ADDRESS, IMAGE_ID, SPOT_INSTANCE, AVAILABILITY_ZONE, VPC_ID, GROUP_ID, GROUP_NAME, LOCAL_HOSTNAME, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID, RESERVATION_ID, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for Azure includes: VM_ID, VM_NAME, PLATFORM, PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_PUBLISHER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for GCP includes: INSTANCE_ID, HOST_NAME, MACHINE_TYPE, MACHINE_STATE, PROJECT_ID, PUBLIC_IP_ADDRESS, VPC_NETWORK, ZONE, PRIVATE_IP_ADDRESS, MAC_ADDRESS

DTD

<platform API server>/api/3.0/fo/report/template/scan/scanreporttemplate_info.dtd

Sample - Create scan template

API request:

```
curl --location 'https://
/api/3.0/fo/report/template/scan/?action=create&report_format=xml' \
--header 'X-Requested-With: curl' \
--header 'Content-Type: text/xml' \
--header 'Authorization: encoded username:passwordstring' \
--data '
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://
https://qualysapi.qualys.com/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-03-04T06:04:28Z</DATETIME>
            <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>3038061</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Update Scan template

API request:

```
curl --location 'https://
/api/3.0/fo/report/template/scan/?action=update&report_format=xml&templat
e_id=3038062' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: encoded username:passwordstring' \
--data '<?xml version="1.0" encoding="UTF-8" ?>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM "https://
https://qualysapi.qualys.com/api/3.0/simple_return.dtd">
    <SIMPLE_RETURN>
        <RESPONSE>
            <DATETIME>2025-03-04T06:10:09Z</DATETIME>
            <TEXT>Scan Report Template Successfully Updated.</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>3038062</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Delete Scan template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
 "action=delete&template_id=8209""https://https://qualysapi.qualys.com/ap
i/3.0/fo/report/template/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://https://qualysapi.qualys.com/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-04T10:54:37Z</DATETIME>
    <CODE>Scan Report Template(s) Deleted Successfully [8209]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Export Scan template

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl --location 'https://
/api/3.0/fo/report/template/scan/?action=export&report_format=xml&templat
e_id=3037411' \
--header 'X-Requested-With: curl' \
--header 'Authorization: encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "https://
https://qualysapi.qualys.com/api/3.0/fo/report/template/scan/scanreportte
mplate_info.dtd">
    <REPORTTEMPLATE>
        <SCANTEMPLATE>
```

```
<TITLE>
    <INFO key="template_id">
        <![CDATA[3037411]]>
    </INFO>
    <INFO key="title">
        <![CDATA[API_vapmpdsomiPT]]>
    </INFO>
    <INFO key="owner">
        <![CDATA[895512]]>
    </INFO>
</TITLE>
<TARGET>
    <INFO key="scan_selection">
        <![CDATA[HostBased]]>
    </INFO>
    <INFO key="include_trending">
        <![CDATA[0]]>
    </INFO>
    <INFO key="asset_groups">
        <![CDATA[All]]>
    </INFO>
    <INFO key="network">
        <![CDATA[]]>
    </INFO>
    <INFO key="ips">
        <![CDATA[]]>
    </INFO>
    <INFO key="host_with_cloud_agents">
        <![CDATA[]]>
    </INFO>
</TARGET>
<DISPLAY>
    <INFO key="graph_business_risk">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_vuln_over_time">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_text_summary">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_ig_severity">
```

```
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_categories">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_vulns">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_os">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_services">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_ports">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
    <![CDATA[]]>
</INFO>
<INFO key="sort_by">
    <![CDATA[host]]>
</INFO>
<INFO key="cvss">
    <![CDATA[all]]>
</INFO>
<INFO key="host_details">
    <![CDATA[0]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[0]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[0]]>
</INFO>
<INFO key="include_text_summary">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_solution">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
```

```
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_compliance">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_exploit">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_malware">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_results">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_appendix">
            <![CDATA[1]]>
        </INFO>
        <INFO key="exclude_account_id">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_reopened">
            <![CDATA[0]]>
        </INFO>
        <INFO key="metadata_ec2_instances">
            <![CDATA[0]]>
        </INFO>
        <INFO key="cloud_provider_metadata">
            <![CDATA[0]]>
        </INFO>
        <INFO key="mitre_attack_details">
            <![CDATA[1]]>
        </INFO>
    </DISPLAY>
    <FILTER>
        <INFO key="selective_vulns">
            <![CDATA[complete]]>
        </INFO>
        <INFO key="search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="exclude_qid_option">
            <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="included_os">
            <![CDATA[ALL]]>
        </INFO>
        <INFO key="status_new">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_active">
            <![CDATA[1]]>
```

```
                </INFO>
                <INFO key="status_reopen">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="status_fixed">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="vuln_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_disabled">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="vuln_ignored">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="potential_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="potential_disabled">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="potential_ignored">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="ig_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_disabled">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="ig_ignored">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="display_non_running_kernels">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_kernel">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                    <![CDATA[0]]>
                </INFO>
                <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                    <![CDATA[ALL]]>
                </INFO>
                <INFO key="vuln_source_qualys">
```

```
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_source_thirdparty">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="qds_score_min">
                    <![CDATA[]]>
                </INFO>
                <INFO key="qds_score_max">
                    <![CDATA[]]>
                </INFO>
            </FILTER>
            <SERVICESPORTS>
                <INFO key="required_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                    <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                    <![CDATA[]]>
                </INFO>
            </SERVICESPORTS>
            <USERACCESS>
                <INFO key="global">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="report_access_users">
                    <![CDATA[]]>
                </INFO>
            </USERACCESS>
        </SCANTEMPLATE>
    </REPORTTEMPLATE>
```

V4.0

api/4.0/fo/report/template/scan/

Perform actions such as create, update, delete and export on the Scan Template.

Scan Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Scan Template	<base_url>/api/4.0/fo/report/template/scan/ Required parameters: action=create report_format=xml	POST
Update Scan Template	<base_url>/api/4.0/fo/report/template/scan/ Required parameters: template_id={value} action=update report_format=xml	PUT
Delete Scan Template	<base_url>/api/4.0/fo/report/template/scan/ Required parameters: template_id={value} action=delete	POST
Export Scan Template	<base_url>/api/4.0/fo/report/template/scan/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Scan Template settings

These parameters (all are optional) are used for a create or update request to define scan template settings. When creating a new template the default value is shown in bold where applicable.

Parameter	Description
Title	The template title and owner.
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .
Target	What target assets to include in the report.
scan_selection={**HostBased**|ScanBased|}	Specify HostBased for Host Based Findings (default for new template) or ScanBased for Scan Based Findings. Choosing Host Based Findings allows you to report on the latest vulnerability data from all of your scans. Choosing Scan Based Findings allows you to run a report based on saved scan results.

Parameter	Description
fqdns={value}	(Optional) The target FQDN for a vulnerability scan. You must specify at least one target such as IPs, assets groups, or FQDNs. Multiple values are comma-separated.
include_trending={**0**|1}	Specify 1 to include trending. Choose a timeframe (daily, weekly or monthly) to analyze the vulnerability status for the timeframe selected. This parameter is required only if scan_selection=HostBased.
limit_timeframe={**0**|1}	Specify 1 to only include scan results from the specified time frame. This ensures that only vulnerability information gathered in the timeframe that you've specified is included in the report. If unspecified, vulnerability information for hosts that were last scanned prior to the report timeframe may be included. This parameter is required only if scan_selection=HostBased.
selection_type={day|month|weeks|date|none|scans}	Specify whether to include trending information for number of weeks, days or months or a specific date. Specifying none will create a report without any trending information included. Specifying scans will include trending information for the last two detections. This parameter is required only if scan_selection=HostBased.
selection_range={value}	Specify the range for the selection type. Specify a number of units (1|3|5|7|15|30|60|90) for days, weeks or months. Date must be in the format yyyy-mm-dd (2017-04-05), and must be less than or equal to today's date. Trending information since the last number of units or the specified date will be included. This parameter is required only if scan_selection=HostBased.
asset_groups={value}	Specify the name of the asset group(s) to report on. Multiple asset groups are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
asset_group_ids={value}	Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
network={value}	(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.

Parameter	Description
ips={value}	Specify the IPs or IP ranges to report on. Multiple IPs or IP ranges are comma separated. This parameter is required only if scan_selection=HostBased.
tag_set_by={name|id}	Specify the name of the tags or the ID of the tags for the hosts you want to report on. Multiple tag names or tag IDs are comma separated.
tag_include_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_include={value}	Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
tag_exclude_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_exclude={value}	Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
host_with_cloud_agents={all|scan|agent}	What host findings to include in the report when CA module is enabled. Your options are: all - All data scan - Scan data, i.e. include findings from scans that didn't use Agentless Tracking agent - Agent data, i.e. include findings from the agent when merging is enabled (i.e. Show unified view hosts option in UI under Users > Setup > Cloud Agent Setup)
display_text_summary={**0**|1}	Specify 1 to include the following summary info for the entire report: total vulnerabilities detected, overall security risk, business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.

Parameter	Description
graph_business_risk={**0**|1}	Specify 1 to include the business risk information. Note that some graphs are only available when trend information is included. Keep in mind that your filter settings will affect the data reflected in your graphs.
graph_vuln_over_time={**0**|1}	Specify 1 to include the vulnerabilities by severity over time.
graph_status={**0**|1}	Specify 1 to include the vulnerabilities by status.
graph_potential_status={**0**|1}	Specify 1 to include the potential vulnerabilities by status.
graph_severity={**0**|1}	Specify 1 to include the vulnerabilities by severity.
Display	Display options such as graphs amount of detail.
graph_potential_severity={**0**|1}	Specify 1 to include the potential vulnerabilities by severity.
graph_ig_severity={**0**|1}	Specify 1 to include the information gathered by severity.
graph_top_categories={**0**|1}	Specify 1 to include the top five vulnerable categories.
graph_top_vulns={**0**|1}	Specify 1 to include the ten most prevalent vulnerabilities.
graph_os={**0**|1}	Specify 1 to include the operating systems detected.
graph_services={**0**|1}	Specify 1 to include the services detected.
graph_top_ports={**0**|1}	Specify 1 to include the ports detected.
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
sort_by={host|vuln|os|group|service|port}	Specify how you want to organize the Detailed Results section of your report - by host, vuln (i.e. vulnerability), group (i.e. asset group), service or port.
cvss={**all**|cvssv2|cvssv3}	Specify the CVSS version score you want to display in reports. all - both CVSS versions cvssv2 - CVSS version 2 cvssv3 - CVSS version 3
host_details={0|**1**}	Specify 1 to include identifying information for each host agent like the asset ID and related IPs (IPv4, IPv6 and MAC addresses). This parameter is required only if scan_selection=HostBased and sort_by=host.
metadata_ec2_instances={0|1}	Specify 1 to display “Legacy EC2/Azure Fields” for each EC2 asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.

Parameter	Description
cloud_provider_metadata={**0**|1}	Specify 1 to display “Cloud Provider Metadata Fields” for each cloud asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
qualys_system_ids={0|1}	Specify 1 to include host ID/asset ID in the host-based scan report.
include_text_summary={**0**|1}	Specify 1 to include the following summary info for each host, vulnerability, asset group, etc (depending on the sorting method you selected): total vulnerabilities detected, the security risk, the business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.
include_vuln_details={**0**|1}	Specify 1 to include additional details for each vulnerability in the report.
include_vuln_details_threat ={**0**|1}	Specify 1 to include a description of the threat.
include_vuln_details_impact ={**0**|1}	Specify 1 to include possible consequences that may occur if the vulnerability is exploited.
include_vuln_details_solutio n={**0**|1}	Specify 1 to include a verified solution to remedy the issue, such as a link to the vendor's patch, Web site, or a workaround.
include_vuln_details_vpatch ={**0**|1}	Specify 1 to include virtual patch information correlated with the vulnerability, obtained from Trend Micro real-time feeds.
include_vuln_details_compli ance={**0**|1}	Specify 1 to include compliance information correlated with the vulnerability.
include_vuln_details_exploit ={**0**|1}	Specify 1 to include exploitability information correlated with the vulnerability, includes references to known exploits and related security resources.
include_vuln_details_malwa re={**0**|1}	Specify 1 to include malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.
include_vuln_details_results ={**0**|1}	Specify 1 to include specific scan test results for each host, when available. We'll also show the date the vulnerability was first detected, last detected and the number of times it was detected.
include_vuln_details_reopen ed={0|1}	Specify 1 to include information related to reopened vulnerabilities.
include_vuln_details_appen dix={**0**|1}	Specify 1 to include more information like IPs in your report target that don't have any scan results, and IPs that were scanned but results are not shown (no vulnerabilities were detected or all vulnerabilities were filtered out).

Parameter	Description
include_trurisk_details={0|1}	Specify 0 to exclude and 1 to include TruRisk details in the report template. By default, the value is set to 1. **Note**: This parameter is applicable only if: - The scan type is host-based scan (scan_selection= HostBased). - The subscription has Asset Risk Scoring (ARS) enabled.
exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0.
Filters	Filter options such as vulnerability status, categories, QIDs, OS.
selective_vulns={**complete**| custom}	Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value}	Specify search list ID or QID. Multiple search list IDs or QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={**0**|1}	Specify 1 to exclude QIDs from the report.
exclude_search_list_ids= {value}	Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
included_os={value}	Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.
status_new={0|**1**}	Specify 1 to include vulnerabilities in your report based on the current vulnerability status - New.
status_active={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Active.
status_reopen={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Re-Opened.

Parameter	Description
status_fixed={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Fixed.
qds_score_min{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS greater than or equal to a QDS score you specify.
qds_score_max{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS less than or equal to a QDS score you specify.
vuln_active={0|**1**}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Active.
vuln_disabled={**1**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Disabled.
vuln_ignored={**0**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Ignored.
potential_active={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Active.
potential_disabled={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Disabled.
potential_ignored={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Ignored.
ig_active={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Active.
ig_disabled={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Disabled.
ig_ignored={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Ignored.
display_non_running_kernels={**0**|1}	Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={**0**|1}	Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={**0**|1}	Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={**0**|1}	Specify 1 to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host.
exclude_superceded_patches={**0**|1}	Specify 1 to exclude every patch QID which is superceded (replaced) by another patch QID recommended for the same Host.

Parameter	Description
categories_list={value}	Specify the category name to filter hosts in your report based on various categories. For example, if you're only interested in Windows vulnerabilities make sure you provide the category name for Windows. Multiple category names can be provided using values separated by a comma. Specify ALL to include all categories. See Categories.
Services and Ports	Services and ports to include in report.
required_services={value}	Specify the name of a required service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38228 (when a required service is NOT detected). See Identified Services.
unauthorized_services={value}	Specify the name of an unauthorized service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38175 (when an unauthorized service is detected). See Identified Services.
required_ports={value}	Specify required ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82051 (when a required port is NOT detected).
unauthorized_ports={value}	Specify unauthorized ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82043 (when an unauthorized port is detected).
User Access	Control user access to template and reports generated from template.
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.
report_access_users={value}	Specify the username to share the report with a user who wouldn't already have access to the report. Multiple usernames can be provided using values separated by a comma. Each user you add will be able to view reports generated from this template even if they don't have access to the IPs in the report.

Cloud Asset Metadata Fields in CSV Format

See the table below to know which cloud asset metadata columns will appear in your CSV reports based on your report template settings. Columns will appear in the order shown.

Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
EC2 Instance ID Public Hostname Image ID VPC ID Instance State Private Hostname Instance Type Account ID Region Code Subnet ID	Cloud Provider Cloud Provider Service Cloud Service Cloud Resource ID Cloud Resource Type Cloud Account Cloud Image ID Cloud Resource Metadata	Cloud Provider Cloud Provider Service Cloud Service Cloud Resource ID Cloud Resource Type Cloud Account Cloud Image ID Cloud Resource Metadata EC2 Instance ID Public Hostname Image ID VPC ID Instance State Private Hostname Instance Type Account ID Region Code Subnet ID

Important note about the Legacy EC2/Azure Fields in CSV

These fields were originally introduced for AWS cloud assets and will be populated with metadata for your AWS EC2 assets.

For Azure and GCP assets, all Legacy EC2/Azure columns will appear blank in the CSV report, except for the EC2 Instance ID column. We will continue to populate the EC2 Instance ID column for all cloud assets (AWS, Azure, GCP). The EC2 Instance ID column is replaced by Cloud Resource ID, and will be deprecated in a future release.

Cloud Asset Metadata Fields in XML Format

See the table below to know which cloud asset metadata tags will appear in your XML reports based on your report template settings.

Cloud Provider	Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
AWS	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID EC2_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID EC2_INFO CLOUD_RESOURCE_METADATA

Azure	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID AZURE_VM_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID AZURE_VM_INFO CLOUD_RESOURCE_METADATA
GCP	CLOUD_RESOURCE_ID EC2_INSTANCE_ID	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA

EC2_INFO includes: PUBLIC_DNS_NAME, IMAGE_ID, VPC_ID, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID

AZURE_VM_INFO includes: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTON_ID, LOCATION, RESOURCE_GROUP_NAME

CLOUD_RESOURCE_METADATA for AWS includes: INSTANCE_ID, PUBLIC_DNS_NAME, PUBLIC_IP_ADDRESS, PRIVATE_IP_ADDRESS, IMAGE_ID, SPOT_INSTANCE, AVAILABILITY_ZONE, VPC_ID, GROUP_ID, GROUP_NAME, LOCAL_HOSTNAME, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID, RESERVATION_ID, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for Azure includes: VM_ID, VM_NAME, PLATFORM, PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_PUBLISHER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for GCP includes: INSTANCE_ID, HOST_NAME, MACHINE_TYPE, MACHINE_STATE, PROJECT_ID, PUBLIC_IP_ADDRESS, VPC_NETWORK, ZONE, PRIVATE_IP_ADDRESS, MAC_ADDRESS

DTD

<platform API server>/api/4.0/fo/report/template/scan/scanreporttemplate_info.dtd

Sample - Create scan template

API request:

```
curl --location --request POST
'https://qualysapi.qualys.com/api/4.0/fo/report/template/scan/?act
ion=create&report_format=xml' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T04:57:23Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>8737800</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Scan template

API request:

```
curl --location --request POST
'https://qualysapi.qualys.com/api/4.0/fo/report/template/scan/?action=upd
ate&report_format=xml&template_id=8708009' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T10:46:08Z</DATETIME>
        <TEXT>Scan Report Template Successfully Updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>8737800</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete Scan template

API request:

```
curl --location
'https://qualysapi.qualys.com/api/4.0/fo/report/template/scan/' \
--header 'X-Requested-With: curl' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Encoded username:passwordstring' \
```

```
--data-urlencode 'template_id=8737800' \
--data-urlencode 'action=delete'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/4.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T10:58:30Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Deleted.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>8737800</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Export Scan template with MITRE A&TTACK details

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/report/template/scan/?action=export&report_f
ormat=xml&template_id=8737800' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "https://
<qualys_base_url>/api/4.0/fo/report/template/scan/scanreporttemplate_info
.dtd">
    <REPORTTEMPLATE>
        <SCANTEMPLATE>
            <TITLE>
                <INFO key="template_id">
                    <![CDATA[3037411]]>
                </INFO>
                <INFO key="title">
                    <![CDATA[API_vapmpdsomiPT]]>
                </INFO>
                <INFO key="owner">
                    <![CDATA[895512]]>
                </INFO>
            </TITLE>
            <TARGET>
                <INFO key="scan_selection">
                    <![CDATA[HostBased]]>
```

```
    </INFO>
    <INFO key="include_trending">
        <![CDATA[0]]>
    </INFO>
    <INFO key="asset_groups">
        <![CDATA[All]]>
    </INFO>
    <INFO key="network">
        <![CDATA[]]>
    </INFO>
    <INFO key="ips">
        <![CDATA[]]>
    </INFO>
    <INFO key="host_with_cloud_agents">
        <![CDATA[]]>
    </INFO>
</TARGET>
<DISPLAY>
    <INFO key="graph_business_risk">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_vuln_over_time">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_text_summary">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_ig_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_categories">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_vulns">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_os">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_services">
        <![CDATA[0]]>
    </INFO>
```

```
<INFO key="graph_top_ports">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
    <![CDATA[]]>
</INFO>
<INFO key="sort_by">
    <![CDATA[host]]>
</INFO>
<INFO key="cvss">
    <![CDATA[all]]>
</INFO>
<INFO key="host_details">
    <![CDATA[0]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[0]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[0]]>
</INFO>
<INFO key="include_text_summary">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_solution">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_compliance">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_exploit">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_malware">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_results">
    <![CDATA[0]]>
</INFO>
```

```
    <INFO key="include_vuln_details_appendix">
        <![CDATA[1]]>
    </INFO>
    <INFO key="exclude_account_id">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_reopened">
        <![CDATA[0]]>
    </INFO>
    <INFO key="metadata_ec2_instances">
        <![CDATA[0]]>
    </INFO>
    <INFO key="cloud_provider_metadata">
        <![CDATA[0]]>
    </INFO>
    <INFO key="mitre_attack_details">
        <![CDATA[1]]>
    </INFO>
</DISPLAY>
<FILTER>
    <INFO key="selective_vulns">
        <![CDATA[complete]]>
    </INFO>
    <INFO key="search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="exclude_qid_option">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="included_os">
        <![CDATA[ALL]]>
    </INFO>
    <INFO key="status_new">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_reopen">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_fixed">
        <![CDATA[0]]>
    </INFO>
    <INFO key="vuln_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="vuln_disabled">
        <![CDATA[0]]>
    </INFO>
    <INFO key="vuln_ignored">
```

```
                    <![CDATA[0]]>
                </INFO>
                <INFO key="potential_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="potential_disabled">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="potential_ignored">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="ig_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_disabled">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="ig_ignored">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="display_non_running_kernels">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_kernel">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                    <![CDATA[0]]>
                </INFO>
                <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                    <![CDATA[ALL]]>
                </INFO>
                <INFO key="vuln_source_qualys">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_source_thirdparty">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="qds_score_min">
                    <![CDATA[]]>
                </INFO>
                <INFO key="qds_score_max">
                    <![CDATA[]]>
                </INFO>
            </FILTER>
            <SERVICESPORTS>
                <INFO key="required_services">
```

```
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="unauthorized_services">
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="services_info">
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="required_ports">
                        <![CDATA[]]>
                    </INFO>
                    <INFO key="unauthorized_ports">
                        <![CDATA[]]>
                    </INFO>
                </SERVICESPORTS>
                <USERACCESS>
                    <INFO key="global">
                        <![CDATA[0]]>
                    </INFO>
                    <INFO key="report_access_users">
                        <![CDATA[]]>
                    </INFO>
                </USERACCESS>
            </SCANTEMPLATE>
    </REPORTTEMPLATE>
```

Sample - Export Scan template with FQDN

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/report/template/scan/?action=export&report_f
ormat=xml&template_id=8737800' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "
<qualys_base_url>/api/4.0/fo/report/template/scan/scanreporttemplate_info
.dtd">
    <REPORTTEMPLATE>
        <SCANTEMPLATE>
            <TITLE>
                <INFO key="template_id">
                    <![CDATA[8737800]]>
                </INFO>
                <INFO key="title">
                    <![CDATA[FQDN_API_Template_FQDNS_API]]>
                </INFO>
                <INFO key="owner">
```

```
            <![CDATA[3766154]]>
        </INFO>
    </TITLE>
    <TARGET>
        <INFO key="scan_selection">
            <![CDATA[HostBased]]>
        </INFO>
        <INFO key="include_trending">
            <![CDATA[0]]>
        </INFO>
        <INFO key="asset_groups">
            <![CDATA[]]>
        </INFO>
        <INFO key="network">
            <![CDATA[]]>
        </INFO>
        <INFO key="ips">
            <![CDATA[10.xx.xx.xx]]>
        </INFO>
        <INFO key="host_with_cloud_agents">
            <![CDATA[]]>
        </INFO>
        <INFO key="fqdns">
            <![CDATA[panzer.qa.qualys.com]]>
        </INFO>
    </TARGET>
    <DISPLAY>
        <INFO key="graph_business_risk">
            <![CDATA[0]]>
        </INFO>
        <INFO key="graph_vuln_over_time">
            <![CDATA[0]]>
        </INFO>
        <INFO key="display_text_summary">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_status">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_potential_status">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_severity">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_potential_severity">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_ig_severity">
            <![CDATA[1]]>
        </INFO>
        <INFO key="graph_top_categories">
            <![CDATA[1]]>
        </INFO>
```

```
<INFO key="graph_top_vulns">
    <![CDATA[1]]>
</INFO>
<INFO key="graph_os">
    <![CDATA[1]]>
</INFO>
<INFO key="graph_services">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_ports">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
    <![CDATA[]]>
</INFO>
<INFO key="sort_by">
    <![CDATA[host]]>
</INFO>
<INFO key="cvss">
    <![CDATA[all]]>
</INFO>
<INFO key="host_details">
    <![CDATA[0]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[0]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[0]]>
</INFO>
<INFO key="include_text_summary">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_solution">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_compliance">
    <![CDATA[1]]>
</INFO>
```

```
        <INFO key="include_vuln_details_exploit">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_malware">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_results">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_appendix">
            <![CDATA[1]]>
        </INFO>
        <INFO key="exclude_account_id">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_reopened">
            <![CDATA[1]]>
        </INFO>
        <INFO key="metadata_ec2_instances">
            <![CDATA[0]]>
        </INFO>
        <INFO key="cloud_provider_metadata">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_vuln_details_detection_logic">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_trurisk_details">
            <![CDATA[1]]>
        </INFO>
    </DISPLAY>
    <FILTER>
        <INFO key="selective_vulns">
            <![CDATA[complete]]>
        </INFO>
        <INFO key="search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="exclude_qid_option">
            <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="included_os">
            <![CDATA[ALL]]>
        </INFO>
        <INFO key="status_new">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_active">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_reopen">
```

```
                    <![CDATA[1]]>
                </INFO>
                <INFO key="status_fixed">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_disabled">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_ignored">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="potential_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="potential_disabled">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="potential_ignored">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_active">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_disabled">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_ignored">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="display_non_running_kernels">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_kernel">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                    <![CDATA[0]]>
                </INFO>
                <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                    <![CDATA[ALL]]>
                </INFO>
                <INFO key="qds_score_min">
                    <![CDATA[]]>
                </INFO>
```

```
            <INFO key="qds_score_max">
                <![CDATA[]]>
            </INFO>
        </FILTER>
        <SERVICESPORTS>
            <INFO key="required_services">
                <![CDATA[]]>
            </INFO>
            <INFO key="unauthorized_services">
                <![CDATA[]]>
            </INFO>
            <INFO key="services_info">
                <![CDATA[]]>
            </INFO>
            <INFO key="required_ports">
                <![CDATA[]]>
            </INFO>
            <INFO key="unauthorized_ports">
                <![CDATA[]]>
            </INFO>
        </SERVICESPORTS>
        <USERACCESS>
            <INFO key="global">
                <![CDATA[1]]>
            </INFO>
            <INFO key="report_access_users">
                <![CDATA[]]>
            </INFO>
        </USERACCESS>
    </SCANTEMPLATE>
</REPORTTEMPLATE>
```

V7.0

api/7.0/fo/report/template/scan/

Perform actions such as create, update, delete and export on the Scan Template.

Scan Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Scan Template	<base_url>/api/7.0/fo/report/template/scan/ Required parameters: action=create report_format=xml	POST
Update Scan Template	<base_url>/api/7.0/fo/report/template/scan/ Required parameters: template_id={value} action=update report_format=xml	PUT

Action	API Endpoint /required parameters	Method
Delete Scan Template	<base_url>/api/7.0/fo/report/template/scan/ Required parameters: template_id={value} action=delete	POST
Export Scan Template	<base_url>/api/7.0/fo/report/template/scan/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Scan Template settings

These parameters (all are optional) are used for a create or update request to define scan template settings. When creating a new template the default value is shown in bold where applicable.

Parameter	Description
Title	The template title and owner.
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .
Target	What target assets to include in the report.
scan_selection={**HostBased**|ScanBased|}	Specify HostBased for Host Based Findings (default for new template) or ScanBased for Scan Based Findings. Choosing Host Based Findings allows you to report on the latest vulnerability data from all of your scans. Choosing Scan Based Findings allows you to run a report based on saved scan results.
fqdns={value}	(Optional) The target FQDN for a vulnerability scan. You must specify at least one target such as IPs, assets groups, or FQDNs. Multiple values are comma-separated. Note: This parameter is only applicable to V4.0 version and later.
include_trending={**0**|1}	Specify 1 to include trending. Choose a timeframe (daily, weekly or monthly) to analyze the vulnerability status for the timeframe selected. This parameter is required only if scan_selection=HostBased.

Parameter	Description
limit_timeframe={**0**|1}	Specify 1 to only include scan results from the specified time frame. This ensures that only vulnerability information gathered in the timeframe that you've specified is included in the report. If unspecified, vulnerability information for hosts that were last scanned prior to the report timeframe may be included. This parameter is required only if scan_selection=HostBased.
selection_type={day|month|weeks|date|none|scans}	Specify whether to include trending information for number of weeks, days or months or a specific date. Specifying none will create a report without any trending information included. Specifying scans will include trending information for the last two detections. This parameter is required only if scan_selection=HostBased.
selection_range={value}	Specify the range for the selection type. Specify a number of units (1|3|5|7|15|30|60|90) for days, weeks or months. Date must be in the format yyyy-mm-dd (2017-04-05), and must be less than or equal to today's date. Trending information since the last number of units or the specified date will be included. This parameter is required only if scan_selection=HostBased.
asset_groups={value}	Specify the name of the asset group(s) to report on. Multiple asset groups are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
asset_group_ids={value}	Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.
network={value}	(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.
ips={value}	Specify the IPs or IP ranges to report on. Multiple IPs or IP ranges are comma separated. This parameter is required only if scan_selection=HostBased.
tag_set_by={name|id}	Specify the name of the tags or the ID of the tags for the hosts you want to report on. Multiple tag names or tag IDs are comma separated.

Parameter	Description
tag_include_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_include={value}	Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
tag_exclude_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation). This parameter is required only if scan_selection=HostBased.
tag_set_exclude={value}	Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.
host_with_cloud_agents={all|scan|agent}	What host findings to include in the report when CA module is enabled. Your options are: all - All data scan - Scan data, i.e. include findings from scans that didn't use Agentless Tracking agent - Agent data, i.e. include findings from the agent when merging is enabled (i.e. Show unified view hosts option in UI under Users > Setup > Cloud Agent Setup)
display_text_summary={**0**|1}	Specify 1 to include the following summary info for the entire report: total vulnerabilities detected, overall security risk, business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.
graph_business_risk={**0**|1}	Specify 1 to include the business risk information. Note that some graphs are only available when trend information is included. Keep in mind that your filter settings will affect the data reflected in your graphs.
graph_vuln_over_time={**0**|1}	Specify 1 to include the vulnerabilities by severity over time.
graph_status={**0**|1}	Specify 1 to include the vulnerabilities by status.

Parameter	Description
graph_potential_status={**0**|1}	Specify 1 to include the potential vulnerabilities by status.
graph_severity={**0**|1}	Specify 1 to include the vulnerabilities by severity.
Display	Display options such as graphs amount of detail.
graph_potential_severity={**0**|1}	Specify 1 to include the potential vulnerabilities by severity.
graph_ig_severity={**0**|1}	Specify 1 to include the information gathered by severity.
graph_top_categories={**0**|1}	Specify 1 to include the top five vulnerable categories.
graph_top_vulns={**0**|1}	Specify 1 to include the ten most prevalent vulnerabilities.
graph_os={**0**|1}	Specify 1 to include the operating systems detected.
graph_services={**0**|1}	Specify 1 to include the services detected.
graph_top_ports={**0**|1}	Specify 1 to include the ports detected.
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
sort_by={host|vuln|os|group|service|port}	Specify how you want to organize the Detailed Results section of your report - by host, vuln (i.e. vulnerability), group (i.e. asset group), service or port.
cvss={**all**|cvssv2|cvssv3|cvssv4}	Specify the CVSS version score you want to display in reports. all - both CVSS versions cvssv2 - CVSS version 2 cvssv3 - CVSS version 3 cvssv4 - CVSS version 4
host_details={0|**1**}	Specify 1 to include identifying information for each host agent like the asset ID and related IPs (IPv4, IPv6 and MAC addresses). This parameter is required only if scan_selection=HostBased and sort_by=host.
metadata_ec2_instances={0|1}	Specify 1 to display “Legacy EC2/Azure Fields” for each EC2 asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
cloud_provider_metadata={**0**|1}	Specify 1 to display “Cloud Provider Metadata Fields” for each cloud asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
qualys_system_ids={0|1}	Specify 1 to include host ID/asset ID in the host-based scan report.

Parameter	Description
include_text_summary={**0**|1}	Specify 1 to include the following summary info for each host, vulnerability, asset group, etc (depending on the sorting method you selected): total vulnerabilities detected, the security risk, the business risk (for reports sorted by asset group), total vulnerabilities by status, total vulnerabilities by severity and top 5 vulnerability categories.
include_vuln_details={**0**|1}	Specify 1 to include additional details for each vulnerability in the report.
include_vuln_details_threat ={**0**|1}	Specify 1 to include a description of the threat.
include_vuln_details_impact ={**0**|1}	Specify 1 to include possible consequences that may occur if the vulnerability is exploited.
include_vuln_details_solutio n={**0**|1}	Specify 1 to include a verified solution to remedy the issue, such as a link to the vendor's patch, Web site, or a workaround.
include_vuln_details_vpatch ={**0**|1}	Specify 1 to include virtual patch information correlated with the vulnerability, obtained from Trend Micro real-time feeds.
include_vuln_details_compli ance={**0**|1}	Specify 1 to include compliance information correlated with the vulnerability.
include_vuln_details_exploit ={**0**|1}	Specify 1 to include exploitability information correlated with the vulnerability, includes references to known exploits and related security resources.
include_vuln_details_malwa re={**0**|1}	Specify 1 to include malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.
include_vuln_details_results ={**0**|1}	Specify 1 to include specific scan test results for each host, when available. We'll also show the date the vulnerability was first detected, last detected and the number of times it was detected.
include_vuln_details_reopen ed={0|1}	Specify 1 to include information related to reopened vulnerabilities.
include_vuln_details_appen dix={**0**|1}	Specify 1 to include more information like IPs in your report target that don't have any scan results, and IPs that were scanned but results are not shown (no vulnerabilities were detected or all vulnerabilities were filtered out).
include_trurisk_details={0|1}	Specify 0 to exclude and 1 to include TruRisk details in the report template. By default, the value is set to 1. **Note**: This parameter is applicable only if: - The scan type is host-based scan (scan_selection= HostBased). - The subscription has Asset Risk Scoring (ARS) enabled.

Parameter	Description
exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.
mitre_attack_details={0|1}	(Optional) Specify 1 to display the MITRE ATT&CK details (MITRE ATT&CK Tactic Name, MITRE ATT&CK Tactic ID, MITRE ATT&CK Technique Name, MITRE ATT&CK Technique ID) in the response, else 0. By default, the value is set to 0. Note: This parameter is only applicable to V3.0 version and later.
Filters	Filter options such as vulnerability status, categories, QIDs, OS.
selective_vulns={**complete**|custom}	Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value}	Specify search list ID or QID. Multiple search list IDs or QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={**0**|1}	Specify 1 to exclude QIDs from the report.
exclude_search_list_ids={value}	Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
included_os={value}	Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.
status_new={0|**1**}	Specify 1 to include vulnerabilities in your report based on the current vulnerability status - New.
status_active={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Active.
status_reopen={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Re-Opened.
status_fixed={0|**1**}	Specify 1 to filter vulnerabilities in your report based on the current vulnerability status - Fixed.
qds_score_min{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS greater than or equal to a QDS score you specify.

Parameter	Description
qds_score_max{value}	(Optional) Use to filter the report data to show only vulnerabilities that have a QDS less than or equal to a QDS score you specify.
vuln_active={0|**1**}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Active.
vuln_disabled={**1**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Disabled.
vuln_ignored={**0**|1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Ignored.
potential_active={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Active.
potential_disabled={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Disabled.
potential_ignored={**0**|1}	Specify 1 to filter potential vulnerabilities in your report based on the state - Ignored.
ig_active={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Active.
ig_disabled={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Disabled.
ig_ignored={**0**|1}	Specify 1 to filter the information gathered in your report based on the state - Ignored.
display_non_running_kernels={**0**|1}	Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={**0**|1}	Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={**0**|1}	Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={**0**|1}	Specify 1 to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host.
exclude_superceded_patches={**0**|1}	Specify 1 to exclude every patch QID which is superceded (replaced) by another patch QID recommended for the same Host.
categories_list={value}	Specify the category name to filter hosts in your report based on various categories. For example, if you're only interested in Windows vulnerabilities make sure you provide the category name for Windows. Multiple category names can be provided using values separated by a comma. Specify ALL to include all categories. See Categories.
Services and Ports	Services and ports to include in report.

Parameter	Description
required_services={value}	Specify the name of a required service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38228 (when a required service is NOT detected). See Identified Services.
unauthorized_services={value}	Specify the name of an unauthorized service. Multiple service names can be provided using values separated by a comma. We'll report QID: 38175 (when an unauthorized service is detected). See Identified Services.
required_ports={value}	Specify required ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82051 (when a required port is NOT detected).
unauthorized_ports={value}	Specify unauthorized ports. Multiple ports can be provided using values separated by a comma. We'll report QID: 82043 (when an unauthorized port is detected).
User Access	Control user access to template and reports generated from template.
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.
report_access_users={value}	Specify the username to share the report with a user who wouldn't already have access to the report. Multiple usernames can be provided using values separated by a comma. Each user you add will be able to view reports generated from this template even if they don't have access to the IPs in the report.

Cloud Asset Metadata Fields in CSV Format

See the table below to know which cloud asset metadata columns will appear in your CSV reports based on your report template settings. Columns will appear in the order shown.

Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
EC2 Instance ID	Cloud Provider	Cloud Provider
Public Hostname	Cloud Provider Service	Cloud Provider Service
Image ID	Cloud Service	Cloud Service
VPC ID	Cloud Resource ID	Cloud Resource ID
Instance State	Cloud Resource Type	Cloud Resource Type
Private Hostname	Cloud Account	Cloud Account
Instance Type	Cloud Image ID	Cloud Image ID
Account ID	Cloud Resource Metadata	Cloud Resource Metadata
Region Code		EC2 Instance ID
Subnet ID		Public Hostname
		Image ID
		VPC ID
		Instance State
		Private Hostname
		Instance Type
		Account ID
		Region Code
		Subnet ID

Important note about the Legacy EC2/Azure Fields in CSV

These fields were originally introduced for AWS cloud assets and will be populated with metadata for your AWS EC2 assets.

For Azure and GCP assets, all Legacy EC2/Azure columns will appear blank in the CSV report, except for the EC2 Instance ID column. We will continue to populate the EC2 Instance ID column for all cloud assets (AWS, Azure, GCP). The EC2 Instance ID column is replaced by Cloud Resource ID, and will be deprecated in a future release.

Cloud Asset Metadata Fields in XML Format

See the table below to know which cloud asset metadata tags will appear in your XML reports based on your report template settings.

Cloud Provider	Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
AWS	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID EC2_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID EC2_INFO CLOUD_RESOURCE_METADATA
Azure	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID AZURE_VM_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID AZURE_VM_INFO CLOUD_RESOURCE_METADATA
GCP	CLOUD_RESOURCE_ID EC2_INSTANCE_ID	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA

EC2_INFO includes: PUBLIC_DNS_NAME, IMAGE_ID, VPC_ID, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID

AZURE_VM_INFO includes: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTON_ID, LOCATION, RESOURCE_GROUP_NAME

CLOUD_RESOURCE_METADATA for AWS includes: INSTANCE_ID, PUBLIC_DNS_NAME, PUBLIC_IP_ADDRESS, PRIVATE_IP_ADDRESS, IMAGE_ID, SPOT_INSTANCE, AVAILABILITY_ZONE, VPC_ID, GROUP_ID, GROUP_NAME, LOCAL_HOSTNAME, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID, RESERVATION_ID, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for Azure includes: VM_ID, VM_NAME, PLATFORM, PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_PUBLISHER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for GCP includes: INSTANCE_ID, HOST_NAME, MACHINE_TYPE, MACHINE_STATE, PROJECT_ID, PUBLIC_IP_ADDRESS, VPC_NETWORK, ZONE, PRIVATE_IP_ADDRESS, MAC_ADDRESS

DTD

<platform API server>/api/7.0/fo/report/template/scan/scanreporttemplate_info.dtd

Sample - Create scan template for Host Based Findings

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=create&report_f
ormat=xml' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/7.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-16T05:16:42Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>10104919</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create scan template for Scan Based Findings

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=create&report_f
ormat=xml' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/7.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-16T05:30:16Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>10104953</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Scan template for Host Base Findings

API request:

```
curl --location
'<qualys_base_url>/api/7.0/fo/report/template/scan/?action=update&report_
format=xml&template_id=10066129' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/7.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-16T05:24:49Z</DATETIME>
        <TEXT>Scan Report Template Successfully Updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>10066129</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update Scan template for Scan Base Findings

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=update&report_f
ormat=xml&template_id=10104970' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
```

```
--header 'Authorization: Bearer <JWT Token>' \
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/7.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-04-16T05:43:34Z</DATETIME>
        <TEXT>Scan Report Template Successfully Updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>10104970</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete Scan template

API request:

```
curl --location
'https://qualysapi.qualys.com/api/7.0/fo/report/template/scan/' \
--header 'X-Requested-With: curl' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic Encoded username:passwordstring' \
--data-urlencode 'template_id=8737800' \
--data-urlencode 'action=delete'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/7.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-17T10:58:30Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Deleted.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>8737800</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Export Scan template with MITRE A&TTACK details

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=export&report_f
ormat=xml&template_id=8737800' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "https://
<qualys_base_url>/api/7.0/fo/report/template/scan/scanreporttemplate_info
.dtd">
    <REPORTTEMPLATE>
        <SCANTEMPLATE>
            <TITLE>
                <INFO key="template_id">
                    <![CDATA[3037411]]>
                </INFO>
                <INFO key="title">
                    <![CDATA[API_vapmpdsomiPT]]>
                </INFO>
                <INFO key="owner">
                    <![CDATA[895512]]>
                </INFO>
            </TITLE>
            <TARGET>
                <INFO key="scan_selection">
                    <![CDATA[HostBased]]>
                </INFO>
                <INFO key="include_trending">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="asset_groups">
                    <![CDATA[All]]>
                </INFO>
                <INFO key="network">
                    <![CDATA[]]>
                </INFO>
                <INFO key="ips">
                    <![CDATA[]]>
                </INFO>
                <INFO key="host_with_cloud_agents">
                    <![CDATA[]]>
                </INFO>
            </TARGET>
            <DISPLAY>
                <INFO key="graph_business_risk">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="graph_vuln_over_time">
                    <![CDATA[0]]>
                </INFO>
```

```
<INFO key="display_text_summary">
    <![CDATA[1]]>
</INFO>
<INFO key="graph_status">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_potential_status">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_potential_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_ig_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_categories">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_vulns">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_os">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_services">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_ports">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
    <![CDATA[]]>
</INFO>
<INFO key="sort_by">
    <![CDATA[host]]>
</INFO>
<INFO key="cvss">
    <![CDATA[all]]>
</INFO>
<INFO key="host_details">
    <![CDATA[0]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[0]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[0]]>
</INFO>
```

```
    <INFO key="include_text_summary">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_threat">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_impact">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_solution">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_vpatch">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_compliance">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_exploit">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_malware">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_results">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_appendix">
        <![CDATA[1]]>
    </INFO>
    <INFO key="exclude_account_id">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_reopened">
        <![CDATA[0]]>
    </INFO>
    <INFO key="metadata_ec2_instances">
        <![CDATA[0]]>
    </INFO>
    <INFO key="cloud_provider_metadata">
        <![CDATA[0]]>
    </INFO>
    <INFO key="mitre_attack_details">
        <![CDATA[1]]>
    </INFO>
</DISPLAY>
<FILTER>
    <INFO key="selective_vulns">
        <![CDATA[complete]]>
    </INFO>
    <INFO key="search_list_ids">
```

```
    <![CDATA[]]>
</INFO>
<INFO key="exclude_qid_option">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_search_list_ids">
    <![CDATA[]]>
</INFO>
<INFO key="included_os">
    <![CDATA[ALL]]>
</INFO>
<INFO key="status_new">
    <![CDATA[1]]>
</INFO>
<INFO key="status_active">
    <![CDATA[1]]>
</INFO>
<INFO key="status_reopen">
    <![CDATA[1]]>
</INFO>
<INFO key="status_fixed">
    <![CDATA[0]]>
</INFO>
<INFO key="vuln_active">
    <![CDATA[1]]>
</INFO>
<INFO key="vuln_disabled">
    <![CDATA[0]]>
</INFO>
<INFO key="vuln_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="potential_active">
    <![CDATA[1]]>
</INFO>
<INFO key="potential_disabled">
    <![CDATA[0]]>
</INFO>
<INFO key="potential_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="ig_active">
    <![CDATA[1]]>
</INFO>
<INFO key="ig_disabled">
    <![CDATA[0]]>
</INFO>
<INFO key="ig_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="display_non_running_kernels">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_non_running_kernel">
```

```
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                    <![CDATA[0]]>
                </INFO>
                <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                    <![CDATA[ALL]]>
                </INFO>
                <INFO key="vuln_source_qualys">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="vuln_source_thirdparty">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="qds_score_min">
                    <![CDATA[]]>
                </INFO>
                <INFO key="qds_score_max">
                    <![CDATA[]]>
                </INFO>
            </FILTER>
            <SERVICESPORTS>
                <INFO key="required_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                    <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                    <![CDATA[]]>
                </INFO>
            </SERVICESPORTS>
            <USERACCESS>
                <INFO key="global">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="report_access_users">
                    <![CDATA[]]>
                </INFO>
            </USERACCESS>
        </SCANTEMPLATE>
```

```
</REPORTTEMPLATE>
```

Sample - Export Scan template with FQDN

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=export&report_f
ormat=xml&template_id=8737800' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Basic Encoded username:passwordstring'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "
<qualys_base_url>/api/7.0/fo/report/template/scan/scanreporttemplate_info
.dtd">
    <REPORTTEMPLATE>
        <SCANTEMPLATE>
            <TITLE>
                <INFO key="template_id">
                    <![CDATA[8737800]]>
                </INFO>
                <INFO key="title">
                    <![CDATA[FQDN_API_Template_FQDNS_API]]>
                </INFO>
                <INFO key="owner">
                    <![CDATA[3766154]]>
                </INFO>
            </TITLE>
            <TARGET>
                <INFO key="scan_selection">
                    <![CDATA[HostBased]]>
                </INFO>
                <INFO key="include_trending">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="asset_groups">
                    <![CDATA[]]>
                </INFO>
                <INFO key="network">
                    <![CDATA[]]>
                </INFO>
                <INFO key="ips">
                    <![CDATA[10.xx.xx.xx]]>
                </INFO>
                <INFO key="host_with_cloud_agents">
                    <![CDATA[]]>
                </INFO>
                <INFO key="fqdns">
                    <![CDATA[panzer.qa.qualys.com]]>
```

```
    </INFO>
</TARGET>
<DISPLAY>
    <INFO key="graph_business_risk">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_vuln_over_time">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_text_summary">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_status">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_potential_status">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_potential_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_ig_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_top_categories">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_top_vulns">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_os">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_services">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_ports">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_custom_footer">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_custom_footer_text">
        <![CDATA[]]>
    </INFO>
    <INFO key="sort_by">
        <![CDATA[host]]>
    </INFO>
    <INFO key="cvss">
        <![CDATA[all]]>
    </INFO>
```

```
<INFO key="host_details">
    <![CDATA[0]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[0]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[0]]>
</INFO>
<INFO key="include_text_summary">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_solution">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_compliance">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_exploit">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_malware">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_results">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_appendix">
    <![CDATA[1]]>
</INFO>
<INFO key="exclude_account_id">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_reopened">
    <![CDATA[1]]>
</INFO>
<INFO key="metadata_ec2_instances">
    <![CDATA[0]]>
</INFO>
<INFO key="cloud_provider_metadata">
    <![CDATA[0]]>
</INFO>
```

```
    <INFO key="include_vuln_details_detection_logic">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_trurisk_details">
        <![CDATA[1]]>
    </INFO>
</DISPLAY>
<FILTER>
    <INFO key="selective_vulns">
        <![CDATA[complete]]>
    </INFO>
    <INFO key="search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="exclude_qid_option">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="included_os">
        <![CDATA[ALL]]>
    </INFO>
    <INFO key="status_new">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_reopen">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_fixed">
        <![CDATA[1]]>
    </INFO>
    <INFO key="vuln_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="vuln_disabled">
        <![CDATA[1]]>
    </INFO>
    <INFO key="vuln_ignored">
        <![CDATA[1]]>
    </INFO>
    <INFO key="potential_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="potential_disabled">
        <![CDATA[1]]>
    </INFO>
    <INFO key="potential_ignored">
        <![CDATA[1]]>
    </INFO>
    <INFO key="ig_active">
```

```
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_disabled">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="ig_ignored">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="display_non_running_kernels">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_kernel">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_non_running_services">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="exclude_superceded_patches">
                    <![CDATA[0]]>
                </INFO>
                <INFO
key="exclude_qids_not_exploitable_due_to_configuration">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="categories_list">
                    <![CDATA[ALL]]>
                </INFO>
                <INFO key="qds_score_min">
                    <![CDATA[]]>
                </INFO>
                <INFO key="qds_score_max">
                    <![CDATA[]]>
                </INFO>
            </FILTER>
            <SERVICESPORTS>
                <INFO key="required_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                    <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                    <![CDATA[]]>
                </INFO>
            </SERVICESPORTS>
            <USERACCESS>
                <INFO key="global">
                    <![CDATA[1]]>
```

```
                    </INFO>
                    <INFO key="report_access_users">
                        <![CDATA[]]>
                    </INFO>
                </USERACCESS>
            </SCANTEMPLATE>
    </REPORTTEMPLATE>
```

Sample - Export Scan template for Host Based Findings with CVSSV4

API request:

```
curl --location
'<qualys_base_url>/api/7.0/fo/report/template/scan/?action=export&report_
format=xml&template_id=10066129' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"<qualys_base_url>/api/7.0/fo/report/template/scan/scanreporttemplate_inf
o.dtd">
<REPORTTEMPLATE>
    <SCANTEMPLATE>
        <TITLE>
            <INFO key="template_id">
                <![CDATA[10066129]]>
            </INFO>
            <INFO key="title">
                <![CDATA[TEST1]]>
            </INFO>
            <INFO key="owner">
                <![CDATA[3766154]]>
            </INFO>
        </TITLE>
        <TARGET>
            <INFO key="scan_selection">
                <![CDATA[HostBased]]>
            </INFO>
            <INFO key="include_trending">
                <![CDATA[0]]>
            </INFO>
            <INFO key="asset_groups">
                <![CDATA[]]>
            </INFO>
            <INFO key="network">
                <![CDATA[-100]]>
            </INFO>
            <INFO key="ips">
                <![CDATA[xx.xxx.xx.xxx-
xx.xxx.xx.xxx,xx.xx.xx.xx,xx.xx.xx.xxx-
xx.xx.xx.xxx,xx.xxx.xx.xxx,xx.xxx.xxx.xx]]>
            </INFO>
```

```
    <INFO key="host_with_cloud_agents">
        <![CDATA[all]]>
    </INFO>
    <INFO key="fqdns">
        <![CDATA[]]>
    </INFO>
</TARGET>
<DISPLAY>
    <INFO key="graph_business_risk">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_vuln_over_time">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_text_summary">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_status">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_potential_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_ig_severity">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_categories">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_vulns">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_os">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_services">
        <![CDATA[0]]>
    </INFO>
    <INFO key="graph_top_ports">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_custom_footer">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_custom_footer_text">
        <![CDATA[]]>
    </INFO>
    <INFO key="sort_by">
```

```
    <![CDATA[host]]>
</INFO>
<INFO key="cvss">
    <![CDATA[cvssv4]]>
</INFO>
<INFO key="host_details">
    <![CDATA[1]]>
</INFO>
<INFO key="host_ag_details">
    <![CDATA[1]]>
</INFO>
<INFO key="qualys_system_ids">
    <![CDATA[1]]>
</INFO>
<INFO key="include_text_summary">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_threat">
    <![CDATA[1]]>
</INFO>
<INFO key="include_vuln_details_impact">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_solution">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_vpatch">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_compliance">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_exploit">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_malware">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_results">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_appendix">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_account_id">
    <![CDATA[0]]>
</INFO>
<INFO key="include_vuln_details_reopened">
    <![CDATA[0]]>
</INFO>
<INFO key="metadata_ec2_instances">
```

```
            <![CDATA[1]]>
        </INFO>
        <INFO key="cloud_provider_metadata">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_detection_logic">
            <![CDATA[0]]>
        </INFO>
        <INFO key="include_trurisk_details">
            <![CDATA[1]]>
        </INFO>
        <INFO key="vuln_detection_source">
            <![CDATA[1]]>
        </INFO>
        <INFO key="trurisk_elimination_status">
            <![CDATA[1]]>
        </INFO>
        <INFO key="mitre_attack_details">
            <![CDATA[1]]>
        </INFO>
        <INFO key="include_vuln_details_deep_scan_results">
            <![CDATA[0]]>
        </INFO>
    </DISPLAY>
    <FILTER>
        <INFO key="selective_vulns">
            <![CDATA[complete]]>
        </INFO>
        <INFO key="search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="exclude_qid_option">
            <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_search_list_ids">
            <![CDATA[]]>
        </INFO>
        <INFO key="included_os">
            <![CDATA[ALL]]>
        </INFO>
        <INFO key="status_new">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_active">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_reopen">
            <![CDATA[1]]>
        </INFO>
        <INFO key="status_fixed">
            <![CDATA[0]]>
        </INFO>
        <INFO key="vuln_active">
            <![CDATA[1]]>
```

```
    </INFO>
    <INFO key="vuln_disabled">
        <![CDATA[0]]>
    </INFO>
    <INFO key="vuln_ignored">
        <![CDATA[0]]>
    </INFO>
    <INFO key="potential_active">
        <![CDATA[0]]>
    </INFO>
    <INFO key="potential_disabled">
        <![CDATA[0]]>
    </INFO>
    <INFO key="potential_ignored">
        <![CDATA[0]]>
    </INFO>
    <INFO key="ig_active">
        <![CDATA[0]]>
    </INFO>
    <INFO key="ig_disabled">
        <![CDATA[0]]>
    </INFO>
    <INFO key="ig_ignored">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_non_running_kernels">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_non_running_kernel">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_non_running_services">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_superceded_patches">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_qids_not_exploitable_due_to_configuration">
        <![CDATA[0]]>
    </INFO>
    <INFO key="categories_list">
        <![CDATA[ALL]]>
    </INFO>
    <INFO key="qds_score_min">
        <![CDATA[]]>
    </INFO>
    <INFO key="qds_score_max">
        <![CDATA[]]>
    </INFO>
    <INFO key="exclude_kpatch_cve">
        <![CDATA[0]]>
    </INFO>
</FILTER>
<SERVICESPORTS>
```

```
                <INFO key="required_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                    <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                    <![CDATA[]]>
                </INFO>
            </SERVICESPORTS>
            <USERACCESS>
                <INFO key="global">
                    <![CDATA[1]]>
                </INFO>
                <INFO key="report_access_users">
                    <![CDATA[]]>
                </INFO>
            </USERACCESS>
        </SCANTEMPLATE>
    </REPORTTEMPLATE>
```

Sample - Export Scan template for Scan Based Findings with CVSSV4

API request:

```
curl --location '
<qualys_base_url>/api/7.0/fo/report/template/scan/?action=export&report_f
ormat=xml&template_id=10066129' \
--header 'X-Requested-With: curl' \
--header 'Authorization: bearer <JWT Token>'
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"<qualys_base_url>/api/7.0/fo/report/template/scan/scanreporttemplate_inf
o.dtd">
<REPORTTEMPLATE>
    <SCANTEMPLATE>
        <TITLE>
            <INFO key="template_id">
                <![CDATA[4462134]]>
            </INFO>
            <INFO key="title">
                <![CDATA[RD scan base]]>
            </INFO>
            <INFO key="owner">
                <![CDATA[1094533]]>
            </INFO>
```

```
</TITLE>
<TARGET>
    <INFO key="scan_selection">
        <![CDATA[ScanBased]]>
    </INFO>
</TARGET>
<DISPLAY>
    <INFO key="display_text_summary">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_potential_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_ig_severity">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_os">
        <![CDATA[1]]>
    </INFO>
    <INFO key="graph_services">
        <![CDATA[1]]>
    </INFO>
    <INFO key="display_custom_footer">
        <![CDATA[0]]>
    </INFO>
    <INFO key="display_custom_footer_text">
        <![CDATA[]]>
    </INFO>
    <INFO key="sort_by">
        <![CDATA[host]]>
    </INFO>
    <INFO key="cvss">
        <![CDATA[cvssv4]]>
    </INFO>
    <INFO key="qualys_system_ids">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_threat">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_impact">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_solution">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_compliance">
        <![CDATA[1]]>
```

```
    </INFO>
    <INFO key="include_vuln_details_exploit">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_malware">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_results">
        <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_appendix">
        <![CDATA[1]]>
    </INFO>
    <INFO key="exclude_account_id">
        <![CDATA[0]]>
    </INFO>
    <INFO key="metadata_ec2_instances">
        <![CDATA[0]]>
    </INFO>
    <INFO key="cloud_provider_metadata">
        <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_detection_logic">
        <![CDATA[1]]>
    </INFO>
</DISPLAY>
<FILTER>
    <INFO key="selective_vulns">
        <![CDATA[complete]]>
    </INFO>
    <INFO key="search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="exclude_qid_option">
        <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_search_list_ids">
        <![CDATA[]]>
    </INFO>
    <INFO key="included_os">
        <![CDATA[ALL]]>
    </INFO>
    <INFO key="status_new">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_active">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_reopen">
        <![CDATA[1]]>
    </INFO>
    <INFO key="status_fixed">
        <![CDATA[0]]>
    </INFO>
```

```
<INFO key="vuln_active">
    <![CDATA[1]]>
</INFO>
<INFO key="vuln_disabled">
    <![CDATA[1]]>
</INFO>
<INFO key="vuln_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="potential_active">
    <![CDATA[1]]>
</INFO>
<INFO key="potential_disabled">
    <![CDATA[1]]>
</INFO>
<INFO key="potential_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="ig_active">
    <![CDATA[1]]>
</INFO>
<INFO key="ig_disabled">
    <![CDATA[1]]>
</INFO>
<INFO key="ig_ignored">
    <![CDATA[0]]>
</INFO>
<INFO key="display_non_running_kernels">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_non_running_kernel">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_non_running_services">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_superceded_patches">
    <![CDATA[0]]>
</INFO>
<INFO key="exclude_qids_not_exploitable_due_to_configuration">
    <![CDATA[0]]>
</INFO>
<INFO key="categories_list">
    <![CDATA[ALL]]>
</INFO>
<INFO key="qds_score_min">
    <![CDATA[]]>
</INFO>
<INFO key="qds_score_max">
    <![CDATA[]]>
</INFO>
<INFO key="exclude_kpatch_cve">
    <![CDATA[0]]>
</INFO>
```

```
            </FILTER>
            <SERVICESPORTS>
                <INFO key="required_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_services">
                    <![CDATA[]]>
                </INFO>
                <INFO key="services_info">
                    <![CDATA[]]>
                </INFO>
                <INFO key="required_ports">
                    <![CDATA[]]>
                </INFO>
                <INFO key="unauthorized_ports">
                    <![CDATA[]]>
                </INFO>
            </SERVICESPORTS>
            <USERACCESS>
                <INFO key="global">
                    <![CDATA[0]]>
                </INFO>
                <INFO key="report_access_users">
                    <![CDATA[]]>
                </INFO>
            </USERACCESS>
        </SCANTEMPLATE>
    </REPORTTEMPLATE>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/7.0/fo/report/template /scan/?action	Active	Active
/api/4.0/fo/report/template /scan/?action	December 2025	June 2027
/api/3.0/fo/report/template /scan/?action	December 2025	December 2026
/api/2.0/fo/report/template /scan/?action	December 2025	December 2026

PCI Scan Template

/api/2.0/fo/report/template/pciscan/

Perform actions such as create, update, delete and export on the PCI Scan Template.

PCI Scan Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create PCI Scan Template	<base_url>/api/2.0/fo/report/template/pciscan/ Required parameters: action=create report_format=xml	POST
Update PCI Scan Template	<base_url>/api/2.0/fo/report/template/pciscan/ Required parameters: template_id={value} action=update report_format=xml	PUT
Delete PCI Scan Template	<base_url>/api/2.0/fo/report/template/pciscan/ Required parameters: template_id={value} action=delete	POST
Export PCI Scan Template	<base_url>/api/2.0/fo/report/template/pciscan/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

PCI Scan Template settings

Go to Scan Template settings. The same parameters used to define PCI Scan Template settings. All parameters (all are optional).

In addition the following parameters are used for PCI Risk Ranking.

Parameter	Description
custom_pci_ranking={**0**|1}}	Specify 1 to enable custom PCI risk ranking. When disabled Qualys will use default PCI ASV risk rankings.
customized_ranking_medium_from={0|1|2|3|4|5|6|7|8|9|10}	By default Qualys uses risk rankings High, Medium, Low. By default for a new template, these are set to the same CVSS scores as required for ASV external scans. You can customize the ASV scores using the scale. When custom PCI risk ranking is enabled, this parameter sets the Medium marker value. Choose between 0 to 10 to set the Medium marker value.
customized_ranking_high_from={0|1|2|3|4|5|6|7|8|9|10}	When custom PCI risk ranking is enabled, this parameter sets the High marker value. Choose between 0 to 10 to set the High marker value.
customized_ranking_comments={value}	When custom PCI risk ranking is enabled, a comment on the custom ranking is required. Enter any string up to 400 characters.
customized_ranking_qid_searchlist_comments={<search list id1/name1>|<SEVERITY>|<comments>,<search list id2/name2>|<SEVERITY>|comments>}	When custom PCI risk ranking is enabled, you can specify custom rankings for QID search lists (i.e. custom rankings per set of vulnerabilities in our KnowledgeBase). Use the format shown. For example: searchlistid1|HIGH|"some comments",searchlistid2|MEDIUM|"some comments"

DTD

<platform API server>/api/2.0/fo/report/template/pciscan/pciscanreporttemplate_info.dtd

Samples

Refer to Scan template examples for create, update, delete and export sample requests. Requests and outputs for PCI Scan template are similar.

Patch Template

/api/2.0/fo/report/template/patch/

Perform actions such as create, update, delete and export on the Patch Template.

Patch Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Patch Template	<base_url>/api/2.0/fo/report/template/patch/ Required parameters: action=create report_format=xml	POST
Update Patch Template	<base_url>/api/2.0/fo/report/template/patch/ Required parameters: template_id={value} action=update report_format=xml	PUT
Delete Patch Template	<base_url>/api/2.0/fo/report/template/patch/ Required parameters: template_id={value} action=delete	POST
Export Patch Template	<base_url>/api/2.0/fo/report/template/patch/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Patch Template settings

These parameters (all are optional) are used for a create or update request to define Patch template settings. When creating a new template the default value is shown in bold where applicable.

Parameter	Description
Title	The template title and owner.
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .

Parameter	Description
Target	What target assets to include in the report.
patch_evaluation={**qidbased**|classic}	Specify classic to choose Classic patch evaluation or specify qidbased to choose QID based patch evaluation.
asset_groups	Asset groups to include in the report. Multiple asset groups are comma separated.
asset_group_ids={value}	Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups.
tag_set_by={name|id}	Specify the name of the tags or the ID of the tags for the hosts you want to report on. Multiple tag names or tag IDs are comma separated.
tag_include_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation).
tag_set_include={value}	Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values.
tag_exclude_selector={ALL|**ANY**}	Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation).
tag_set_exclude={value}	Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values.
network={value}	(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.
ips={value}	IP addresses to include in the report. Multiple IPs are comma separated.
Display	Display options to include in the report.
group_by={HOST|PATCH|OS|AG}	Sort and group the results of the report by any of the following: Host = HOST Patch = PATCH Operating System = OS Asset Group = AG When include_cloud_metadata=1 is specified, then only group_by=HOST is supported.

Parameter	Description
include_cloud_metadata={**0**|1}	(Optional) Specify 1 to include cloud metadata for your cloud assets. Only cloud metadata for AWS is supported at this time. When not specified during a create request, a value of 0 is used. When not specified during an update request, the previous value saved in the template is kept. Notes for update patch template request: - If include_cloud_metadata is set to 0 in the template, then you can change the group_by option to any supported value (HOST, PATCH, OS, AG). - If include_cloud_metadata is set to 1 in the template and you change the group_by option to a value other than HOST during an update request, then we will automatically disable the cloud metadata option and we'll show a notification in the response, letting you know that the option was disabled as a result of the change. - If group_by is set to a value other than HOST in the template and you specify include_cloud_metadata=1 during an update request, then an error will occur because include_cloud_metadata can only have a value of 1 when group_by is set to HOST.
include_table_of_qids_fixed={0|**1**}	Specify 1 to include QIDs that will be fixed by each patch.
include_patch_links={0|**1**}	Specify 1 to include the available links for each patch.
include_patches_from_unspecified_vendors={0|**1**}	Specify 1 to include patches from unspecified vendors.
patch_severity_by={**assigned**|highest}	Specify assigned to display severity which is assigned to the QID for the patch detection. Specify highest to display the severity which is highest across all QIDs found on the host that can be patched.
patch_cvss_score_by={assigned|highest|**none**}	Specify the CVSS version score you want to display in reports. assigned - CVSS score assigned to the QID for the patch detection highest - CVSS score highest across all QIDs found on the host that can be patched. none - Do not display CVSS scores.
cvss={**all**|cvssv2|cvssv3}	Specify the CVSS version score you want to display in reports. all - both CVSS versions cvssv2 - CVSS version 2 cvssv3 - CVSS version 3
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.

Parameter	Description
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.
Filters	Filter options such as vulnerabilities, QIDs, patches.
selective_vulns={**complete**|custom}	Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value}	Specify QID to be included in the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={**0**|1}	Specify 1 to exclude QIDs from the report.
exclude_search_list_ids={value}	Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
display_non_running_kernels={**0**|1}	Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={**0**|1}	Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={**0**|1}	Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={**0**|1}	Specify 1 to exclude vulnerabilities that are not exploitable because there's a specific configuration present on the host.
selective_patches={complete|custom}	Specify complete to show results for any and all patches found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
exclude_patch_qid_option={**0**|1}	Specify 1 to exclude patch QIDs from the report.

Parameter	Description
patch_search_list_ids={value}	Specify patch QID to be included in the report. Multiple patch QIDs can be provided using values separated by a comma. This parameter is required only if selective_patches=custom.
exclude_patch_search_list_ids={value}	Specify patch QID to be excluded from the report. Multiple patch QIDs can be provided using values separated by a comma. This parameter is required only if exclude_patch_qid_option=1.
found_since_days={7|**30**|90|365|NoLimit}	Show only patches for vulnerabilities detected during the specified period of time in days. Specify NoLimit for no time limit.
User Access	Control user access to template and reports generated from template.
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.
report_access_users={value}	Specify the username to share the report with a user who wouldn't already have access to the report. Multiple usernames can be provided using values separated by a comma. Each user you add will be able to view reports generated from this template even if they don't have access to the IPs in the report.

DTD

<platform API server>/api/2.0/fo/report/template/patch/patchreporttemplate_info.dtd

Sample Create Patch Template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -H
Content-Type:text/xml --data-binary
"@/home/sample/cloudmetadata_api/patch_create.xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/?ac
tion=create&report_format=xml"
```

Where patch_create.xml is an XML file that contains the patch template settings:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/pat
chreporttemplate_info.dtd">
<REPORTTEMPLATE>
<PATCHTEMPLATE>
<TITLE>
```

```
<INFO key="title"><![CDATA[My Patch Report]]></INFO>
<INFO key="owner"><![CDATA[225889]]></INFO>
</TITLE>
<TARGET>
<INFO key="patch_evaluation"><![CDATA[qidbased]]></INFO>
<INFO key="asset_groups"><![CDATA[AG1, AG2, AG3]]></INFO>
<INFO key="ips"><![CDATA[]]></INFO>
</TARGET>
<DISPLAY>
<INFO key="group_by"><![CDATA[HOST]]></INFO>
<INFO key="include_table_of_qids_fixed"><![CDATA[0]]></INFO>
<INFO key="include_patch_links"><![CDATA[0]]></INFO>
<INFO
key="include_patches_from_unspecified_vendors"><![CDATA[0]]></INFO
>
<INFO key="patch_severity_by"><![CDATA[assigned]]></INFO>
<INFO key="patch_cvss_score_by"><![CDATA[none]]></INFO>
<INFO key="cvss"><![CDATA[all]]></INFO>
<INFO key="display_custom_footer"><![CDATA[0]]></INFO>
<INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
<INFO key="exclude_account_id"><![CDATA[0]]></INFO>
<INFO key="include_cloud_metadata"><![CDATA[1]]></INFO>
</DISPLAY>
<FILTER>
<INFO key="selective_vulns"><![CDATA[complete]]></INFO>
<INFO key="exclude_qid_option"><![CDATA[0]]></INFO>
<INFO key="display_non_running_kernels"><![CDATA[0]]></INFO>
<INFO key="exclude_non_running_kernel"><![CDATA[0]]></INFO>
<INFO key="exclude_non_running_services"><![CDATA[0]]></INFO>
<INFO
key="exclude_qids_not_exploitable_due_to_configuration"><![CDATA[0
]]></INFO>
<INFO key="selective_patches"><![CDATA[complete]]></INFO>
<INFO key="exclude_patch_qid_option"><![CDATA[0]]></INFO>
<INFO key="found_since_days"><![CDATA[30]]></INFO>
</FILTER>
<USERACCESS>
<INFO key="report_access_users"><![CDATA[]]></INFO>
<INFO key="global"><![CDATA[1]]></INFO>
</USERACCESS>
</PATCHTEMPLATE>
</REPORTTEMPLATE>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T08:06:07Z</DATETIME>
    <TEXT>Patch Report Template(s) Successfully Created.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5084140</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Patch Template

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -H
Content-Type:text/xml --data-binary
"@/home/sample/cloudmetadata_api/patch_update.xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/?ac
tion=update&template_id=5062219&report_format=xml"
```

Where patch_update.xml is an XML file that contains the patch template settings. See "Sample Create Patch Template" for more information.

XML output (Success):

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd
/update/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
    <TEXT>Patch Report Template Successfully Updated</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5062219</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

XML output (Success with Notification):

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd
/update/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
    <TEXT>Patch Report Template Successfully Updated</TEXT>
    <NOTIFICATION>Cloud provider Metadata setting has been turned
off for this template as group by is changed to OS</NOTIFICATION>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5062219</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

XML output (with Error):

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd
/update/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT>parameter include_cloud_metadata has invalid value: 1
(include_cloud_metadata can only be set when group_by is set to
HOST)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Map Template

/api/2.0/fo/report/template/map/

Perform actions such as create, update, delete and export on the Map Template.

Map Template Request

A summary of API Endpoint URLs is provided below.

Action	API Endpoint /required parameters	Method
Create Map Template	<base_url>/api/2.0/fo/report/template/map/ Required parameters: action=create report_format=xml	POST
Update Map Template	<base_url>/api/2.0/fo/report/template/map/ Required parameters: template_id={value} action=update report_format=xml	PUT
Delete Map Template	<base_url>/api/2.0/fo/report/template/map/ Required parameters: template_id={value} action=delete	POST
Export Map Template	<base_url>/api/2.0/fo/report/template/map/ Required parameters: action=export report_format=xml Optional parameter: template_id={value} When unspecified all templates for the report type get exported.	GET

Map Template settings

These parameters (all optional) are used for a create and update requests. When creating a new template the default value is shown in bold where applicable..

Parameter	Description
Title	
title={value}	A string value for the title. Length is maximum 64 characters.
owner={value}	Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See .
global={**0**|1}	Share this report template with other users by making it global. Specify 1 to make it global.

Parameter	Description
Display	
map_sort_by={ipaddress|dns|netbios|router|operatingsystem}	Sort and group the results of the report by any of the following: IP Address = ipaddress DNS = dns NetBIOS = netbios Router = router Operating System = OS
map_related_info_lastscandate={**0**|1}	Specify 1 to include the last scan date.
map_related_info_assetgroups={**0**|1}	Specify 1 to include the asset groups.
map_related_info_authenticationrecords={**0**|1}	Specify 1 to include the authentication records.
map_related_info_discoverymethod={**0**|1}	Specify 1 to include the discovery method.
display_custom_footer={**0**|1}	Specify 1 to include custom text in the report footer.
display_custom_footer_text={value}	Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.
map_exclude_account_id={**0**|1}	Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.
Filters	Filter options to help you specify what to include.
map_included_hosttypes_innetblock={0|**1**}	Specify 1 to filter the report by host types - In Netblock.
map_included_hosttypes_scannable={0|**1**}	Specify 1 to filter the report by host types - Scannable
map_included_hosttypes_live={0|**1**}	Specify 1 to filter the report by host types - Live.
map_included_hosttypes_approved={0|**1**}	Specify 1 to filter the report by host types - Approved.
map_included_hosttypes_outofnetblock={0|**1**}	Specify 1 to filter the report by host types - Not In Netblock.
map_included_hosttypes_notscannable={0|**1**}	Specify 1 to filter the report by host types - Not Scannable.
map_included_hosttypes_notlive={0|**1**}	Specify 1 to filter the report by host types - Not Live.
map_included_hosttypes_rogue={0|**1**}	Specify 1 to filter the report by host types - Rouge.
Included Discovery Methods	Specify at least one.

Parameter	Description
map_idm_tcp={0|**1**}	Specify 1 to filter the report by discovery methods - TCP.
map_idm_udp={0|**1**}	Specify 1 to filter the report by discovery methods - UDP.
map_idm_traceroute={0|**1**}	Specify 1 to filter the report by discovery methods - TraceRoute.
map_idm_other={0|**1**}	Specify 1 to filter the report by discovery methods - Other.
map_idm_dns={0|**1**}	Specify 1 to filter the report by discovery methods - DNS.
map_idm_icmp={0|**1**}	Specify 1 to filter the report by discovery methods - ICMP.
map_idm_auth={0|**1**}	Specify 1 to filter the report by discovery methods - AUTH.
Included Status Levels	Only applicable for differential map reports.
map_included_statuses_added={0|**1**}	Specify 1 to filter the report by statuses - Added.
map_included_statuses_removed={0|**1**}	Specify 1 to filter the report by statuses - Removed.
map_included_statuses_active={0|**1**}	Specify 1 to filter the report by statuses - Active.
dns_exclusions={**none**|DNS|DNS-DNSZone}	Exclude hosts discovered only via: none = None DNS = DNS DNS-DNSZone = DNS and/or DNS Zone Transfer
included_os={value}	Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.

Samples

Refer to Scan template examples for create, update, delete and export sample requests. Requests and outputs for Map template are similar.

About template owner

The user who created the report template is the owner by default. Managers and Unit Managers have the option to specify/change the owner while creating a report template the first time or by updating an existing report template. Use the parameter "owner" to assign a template owner.

Global report templates may be owned by Managers and Unit Managers. Non-global report templates may be owned by Managers, Unit Managers, Scanners and Readers.

Managers / Unit Managers can assign only those users as template owners who are part of their hierarchy and are added in their subscription.

Identified OS

Operating Systems identified by our service as of March 2017 are listed below.

Looking for a more current listing? Sure thing. Just log in to your Qualys account and go to Help > About.

Tip - In API requests replace spaces in OS names with underscores. For example, **Apple IOS** must be specified as **Apple_IOS**

3Com	AIX 4.3
3Com HomeConnect	AIX 4.3.2.0-4.3.3.0
3Com NBX	AIX 4.33
3Com OfficeConnect	AIX 4.3-5.1
3Com SuperStack	AIX 4.x
3Com Switch	AIX 5.1
3Com Wireless Access Point	AIX 5.1-5.2
AB	AIX 5.1-5.3
AB ControlLogix	AIX 5.2
Adic	AIX 5.3
Adic Scalar	AIX 5.3.0.4
Adic Storage	AIX 5.x
Adtran	AIX 6.x
Adtran Device	Alcatel
Adtran NetVanta	Alcatel OmniStack
Adtran TSUIQ	Alcatel OmniSwitch
ADTX	Allied
ADTX ArrayMasStor	Allied Telesyn Switch
AIX	Alteon
AIX 4.2-4.3	Alteon ACE Switch
Alteon Switch	Avaya IP Phone

Altium
Altium Wireless Device
Amazon Linux
AMX
AMX Modero
APC
APC InfraStruXure
APC MasterSwitch
APC Network
APC Network Management Card AOS
APC Smart-UPS
AppCelera
AppCelera ICX
Apple
Apple iOS
Apple Wireless Access Point
Arescom
Arescom Device
Arescom NetDSL
Ascend
Ascend Router
Ascent
Ascent Router
ASUS
ASUS Wireless
ASUS Wireless Access Point
Aten
Aten KVM Switch
ATT NetGate
ATTO Device
AudioCodes
AudioCodes VOIP
Avaya
Avaya Device
Avaya G350
Belkin
Avaya Wireless Access Point
Avocent
Avocent CCM Appliance
Axis
Axis Network Camera
Axis Printer
Axis Storpoint CD
Axis Video Server
Axis Wireless Access Point
Axonix SuperCD
Bay Networks
Bay Networks Router
Bay Networks Switch
Cabletron SmartSTACK
Cabletron Switch
Caldera
Caldera Open Linux
Caldera Open UNIX 7
Caldera Open UNIX 8
Canon
Canon Network Printer
Canon Printer
Cayman3000
CheckPoint FW1 on Solaris
CheckPoint SecurePlatform
Cintech Switch
Cirronet Wireless Access Point
Cisco
Cisco Analog Phone Gateway
Cintech Switch
Cirronet Wireless Access Point
Cisco
Cisco Analog Phone Gateway
Cisco Analog Telephone Adaptor
Cisco Arrowpoint WebNS
Cisco ASA

Belkin Wireless Access Point
BeOS 5
BlueCoat Security Gateway
BlueSocket Embedded Linux 2.4-2.6
BorderWare Firewall
Brocade Device
Brother Printer
BSD
BSD Unix
BSDI BSD
BT Voyager
Buffalo Wireless Access Point
Cabletron
CEKAB Device
CentOS
CentOS
CheckPoint
CheckPoint FW1
Cisco Controller
Cisco File Engine
Cisco Firewall Services Module
Cisco IOS
Cisco IP Phone
Cisco IP/TV Program Manager
Cisco Local Director
Cisco PIX
Cisco VPN
Cisco WGB350
Cisco Wireless Access Point
ClearPath MCP
CNT UltraNet Edge
Cognitive Printer
CometLabs Switch
Compaq
Compaq Insight Manager
Compaq Switch
Cisco Catalyst
Cisco Content Engine
Cisco Content Services Switch
Cisco Content Switching Solution
Cisco Content/File Engine
Cisco
Cisco Analog Phone Gateway
Cisco Analog Telephone Adaptor
Cisco Arrowpoint WebNS
Cisco ASA
Cisco Catalyst
Cisco Content Engine
Cisco Content Services Switch
Cisco Content Switching Solution
Cisco Content/File Engine
Connect2Air Wireless Access Point
ControlLogix ENET
Crossroads Storage Router
Custom Micro Device
CyberGuard Firewall
Datamax I-Class
Datamax Printer
Debian
Dell
Dell Laser
Dell PowerConnect
Dell PowerVault
Dell Remote Access Controller
Digi
Digi One PortServer
Digi One SP
Digi Port Server
Digi One PortServer
Digi One SP
Digi Port Server
Divar Video Camera

Computone Device
Cisco Controller
Cintech Switch
Cirronet Wireless Access Point
D-Link Switch
D-Link Wireless Access Point
Draytek Router
DVD Server
D-Link
D-Link DSL Modem
D-Link Print Server
D-Link Router
Efficient Router
EFI Printer
EMC's Network-Attached Storage Device
Enterasys
Entry-Master Card Access Control System
Epson Printer
ExtendedNet Print Server
Extreme
Extreme Alpine
Extreme Networks Device
Extreme Networks ExtremeWare
Extreme Networks Switch
F5 Networks Big-IP
Fabric OS
FaxPress
Fiery Printer
File Engine
Fortigate
Foundry Networks
FreeBSD
Fujitsu
Fujitsu Blade
Gestetner
Gestetner Printer
Gigafast
Gigafast Wireless Access Point
Gigafast Wireless Access Point
Google Appliance
Hawking Wireless Access Point
Honeyd HoneyPot
HP
HP 3000 MPE
HP AdvanceStack Switch
HP Deskjet Printer
HP Fabric OS
HP Guardian Service Processor
HP iLO
HP Inkjet Printer
HP JetDirect
HP LaserJet
HP OpenVMS
HP ProCurve
HP RILO
HP Surestore Library
HP Switch
HP Tru64
HP-UX
HP-UX 10
HP-UX 10.20
HP-UX 11
Huawei Switch
HVAC controller
IBM
IBM 2210
IBM 4400 Printer
IBM 4690
IBM Infoprint
IBM Mainframe
IBM Network Printer
IBM OS/2

IBM OS/390
IBM OS/400
IBM Printer
IBM Remote Supervisor Adapter
IBM Remote Supervisor Adapter II
IBM Tape Library
IBM Token-Ring Stackable Hub
IBM z/VM
i-data Print Server
Indyme MTS Messaging Telephony Server CU4400
Infinity Embedded Device
Infortrend Serial ATA Storage Subsystem
Intel
Intel NetportExpress Print Server
Intel Switch
Intel Wireless Access Point
Intergy Network Energy Source System
Intermate
Intermate Print Server
Intermate Print Server
Intermec
Intermec EasyLAN Printer
Intermec Wireless Access Point
Inter-Tel IP Phone
IP Phone
IRIX
IRIX 6.2
IRIX 6.5
IRIX behind Firewall or Load Balancer
IronPort
Juniper Networks
Juniper Networks Application Acceleration Platform DX
Juniper Networks JUNOS
Kentrox
Kentrox Q2200 Router
Konica
Konica Minolta
Konica Printer
Kyocera
Kyocera Mita
Kyocera Printer
Lancast
Lancast Media Converter
Lanier
Lanier Printer
Lantronix
Lantronix CoBox
Lantronix ETS32PR
Lantronix MSS100
Lantronix Printer
Leitch
Lexmark
Lexmark Optra
Lexmark Print Server
Lexmark Printer
LinkCom
LinkCom Xpress Print Server
Linksys
Linksys Router
Linksys Wireless
Linux
Linux 1.2.8-1.2.13
Linux 2.0
Linux 2.0.29
Linux 2.0.30+
Linux 2.0.34-38
Linux 2.1.19-2.2.20
Linux 2.2

Linux 2.2.20
Linux 2.4
Linux 2.4.0-2.5.20
Linux 2.4.20-2.4.25
Linux 2.4.20-3
Linux 2.4.22
Linux 2.4.7
Linux 2.4.x
Linux 2.4-2.6
Linux 2.6
Linux 2.x
Linux 3.0
Linux Based MRV LX Series Server
Linux behind
Lucent
Lucent Cajun
Lucent MAX
Lucent Orinoco
Lucent PBX
Lucent Router
Lucent WAP
LynxOS
MacOS
MacOS 10.0.x-10.1.x
MacOS 10.10
MacOS 10.11
MacOS 10.12
MacOS 10.3-10.4
MacOS 8
MacOS 9
MacOS X
magicolor
magicolor 2300 Printer
magicolor 3300 Printer
magicolor Printer
MarkNet Pro Printer
Meditech MAGIC
MGE Uninterruptible Power Supply Systems
Microtest DiscZerver
MiLAN
MiLAN Print Server
MiLAN Switch
MiraPoint
Mitel PBX
Motorola HomeNet WR850G
Moxa
Moxa Async Server
Moxa NPort Serial Server
Multi-Tech
Multi-Tech CommPlete
Multi-Tech MultiVOIP
Muratec MFX Printer
NCR Unix
NEC Projector
Neoteris Instant Virtual Extranet
NetApp
NetApp behind FW1
NetBlazer
NetBSD
NETBuilder Bridge
Netgear
Netgear GSM
Netgear Print Server
Netgear Printer
Netgear Router
Netgear Smart Switch
Netgear Switch
Netgear Wireless Access Point
Netopia
Netopia Router

Netphone
Netphone IP Phone
NetScaler
NetScaler VPN Device
NetScreen
NetScreen 100
NetScreen 50
NetScreen 5XP
NetSilicon Device
Netsilicon Device
NetWare
NetWare 4.11-5.0 SP5
NetWare 5
NetWare 5.0
NetWare 5.1
NetWare 6
NetWare 6.5
NetWare Print Server
Network Camera
Network Print Server
Network Printer
Network Scanner
NGS 500 RouterNIB Network Printer
Nokia
Nokia IPSO
Nokia Wireless Access Point
Nortel
Nortel Device
Nortel Networks BayStack
Nortel Passport
Nortel Router
Nortel Switch
NRG
NRG Network
NRG Printer
Okidata Printer
OkiLAN Print Server
Open Networks Router
OpenBSD
Oracle Enterprise Linux
Oracle Enterprise Linux 4.5
Oracle Enterprise Linux 5.2
ORiNOCO Wireless Access Point
Orinoco Wireless Access Point
Packeteer
Packeteer PacketSeeker
Packeteer PacketShaper
Panasonic Network Camera
Paradyne Device
Perle Jetstream
PocketPro Print Server
Point Six Point Server
Polycom
Polycom Device
Polycom MGC
Polycom VSX
Power Measurement ION Meter
Powerware
Powerware ConnectUPS
Powerware UPS Device
Precidia Device
Primergy RSB
Printronix Printer
Procom NetFORCE
pSOSystem
QNX
Quantum
Quantum NAS SnapServer
Quantum PX506 Tape Library
Quick Eagle Device
RadiSys iRMX
Radware Device

Raptor Firewall
Red Hat
Redline
Redline Networks Processor
Redline Wireless Access Point
Ricoh
RICOH Aficio
Ricoh Aficio
Ricoh Printer
Ringdale Device
RIO Xtreme
RiverStone Networks Router
RoamAbout R2
Rockwell
Rockwell Automation
S3Wireless Wireless Access Point
Savin Printer
Scannex NetBuffer
Schneider Electric Controller
SCO
SCO OpenServer
SCO Unix
SCO UnixWare
SCO UnixWare Firewall
SensaTronics Environmental Monitor
Sentry Remote Power Manager
Shark supercomputer
Sharp Printer
Shore Microsystems Link Protector
Sidewinder G2
Siemens
Siemens 5940 Router
Siemens HiPath 3000
Siemens I-Gate
Siemens IP Phone
Siemens Wireless Access Point
Signature System
Silex Pricom Print Server
SIMATIC NET CP
SMC
SMC Networks SMC8624T
SMC Router
SMC Wireless Access Point
SMC2671 Wireless Access Point
SNAP Ethernet Brain
Snap Server
Solaris
Solaris 10
Solaris 2
Solaris 2.5.1
Solaris 2.5-2.5.1
Solaris 2.6
Solaris 2.6-10
Solaris 2.6-7
Solaris 2.6-8
Solaris 2.7
Solaris 5
Solaris 5.8
Solaris 6-8
Solaris 7
Solaris 7-10
Solaris 8
Solaris 8-10
Solaris 9
Solaris 9-10
Solaris behind
Spectrum24 Wireless Access Point
Stallion EasyServer
StarDot NetCam
Summit Switch
Sun
Sun Cobalt Linux

Sun Lights Out
SUN StorEdge RAID
SuperScript Printer
SuSE
SuSE Linux 10
SuSE Linux 11
SuSE Linux 7
SuSE Linux 8
SuSE Linux 9
Sveasoft Firmware
Symantec Raptor Firewall
Symbol Wireless Access Point
Symon NetLite
SYSTEC CAN-Ethernet Gateway
Tandberg
Tandberg Device
Tandem
Tandem NSK
Tektronix Phaser Printer
Telindus Router
Tenor Switch
TINI
TiVo
TiVo Series
TopLayer Appsafe
Toshiba NWcamera
Transition Networks Device
Trendnet Print Server
Trendware Print Server
Tru64
Tru64 Unix 4.0d
Tru64 Unix 5.x
Tut Modem
TV Program Manager
U.S. Robotics
U.S. Robotics Access point
U.S. Robotics ADSL Wireless Gateway
U.S. Robotics Broadband Router
U.S. Robotics Wireless Access Point
Ubuntu
Ubuntu Linux 10
Ubuntu Linux 11
Ubuntu Linux 7
Ubuntu Linux 8
Ubuntu Linux 9
Ubuntu Linux LTS
Uninterruptible Power Supply Device
UNIX System V
UNIX System V Release 4.2
UNIX SystemUNIX System V 4
Uptime Devices Monitoring System
UptimeDevices Sensorprobe
VAX
VAX VMS 6.1
VAX VMS 6.1 behind Sidewinder G2
VAX VMS 6.2
VAX VMS 7.1
VAX VMS 7.1 behind Sidewinder G2
Verilink WANsuite Router
Vertical Horizon Stack
VirtualAccess LinxpeedPro
VMware
VMWare ESX 3.5
VMWare ESX 4.0
VMWare ESX 4.1
VMware ESX Server
VMWare ESXi 4.0
VMWare ESXi 4.1
VMWare ESXi 5.0
VMWare ESXi 5.0
VxWorks Based Device
WatchGuard Firewall

Web Smart Switch
WebNet uServer
Windows
Windows 10
Windows 2000
Windows 2003
Windows 2008
Windows 2012
Windows 7
Windows 8
Windows 95
Windows 98
Windows CE
Windows Longhorn
Windows ME
Windows NT
Windows NT4
Windows RT
Windows Vista
Windows XP
WKTI RDS Encoder
Xerox
Xerox Device
Xerox DocuColor Printer
Xerox Document Centre
Xerox DocuPrint Printer
Xerox Phaser Printer
Xerox Plotter
Xerox Printer
Xerox WorkCentre
Xerox WorkCentre Printer
XES Printer
XJet Print Server
ZebraNet Print Server
ZOT Print Server

Identified Services

Services identified by our service as of March 2017 are listed below.

Looking for a more current listing? Just log in to your Qualys account and go to Help > About.

Tip - In API requests replace spaces in service names with underscores. For example, Blackberry Attachment must be specified as Blackberry_Attachment

ActiveSync
ADDP
afpovertcp
akak_trojan
amandaidx
aml
Apple_Airport_Management
Applix
Applix_axnet
Applix_TM1_Admin_Server
Applix_TM1_Server
Arkeiad_Network_Backup
ARUGIZER_BACKDOOR
auth
Berlios_Global_Positioning_System_Daemon
BIGFIX_ENTERPRISE_SERVER
BITCOIN
bitkeeper
Blackberry_Attachment
BMC_Patrol

BO2K_backdoor
bofra_worm
bpcd
bpjava_msvc
ca_brightstor
CA_License_Management_Agent
CA_Unicenter_Services
CENTUM_CS_3000
chargen
chargen_udp
CHECKPOINT_FW-1_CLIENT_AUTH_SERVER
chindi
cisco_cnr
CISCO_CNR_AICSERVAGT
Cisco_Secure_ACS
cisco_ta
citadel
Citrix_CMC
Citrix_ICA
CoDeSys
Cognos_Powerplay_Enterprise_Server
Computer_Associates_License_Manager
COREid_Access_Server
crystal_info
Crystal_Reports_App_Server
Crystal_Reports_CMS
cvspserver
daap
dameware
darxite
daytime
daytime_udp
DC Directory Server
dcerpc
dchub
DHCP_or_Bootp_Server
DNS_Server
dtspcd
echo
echo_udp
edonkey_server
EMC_EmailXtender
finger
Forte for Java
ftp
FW1
FW1_NG_Services
gamsoft_telsrv
GCS_SysID
GIOP
girlfriend
gnutella
gopher
h323
healthd
HoneyD_HoneyPot
HP_DATAPROTECT
HP_printer_service
hparray
hpov_alarm
HPOV_BBC
HPOV_CODA
hpov_topmd
hpov_trcsvc
http
http_over_ssl
IBM SolidDB
IBM_DB2_Universal_Database
IBM_TIVOLI_STORAGE_MANAGER
icecast
ident
imap

INDUSOFT
Infopulse_Gatekeeper
ipmi
ipp
irc
ISA_Proxy
isakmp
ISAKMP_over_TCP
iSCSI
iSNS
jabber
Kadmin-4
kazaa
Kerberos-5
l2tp
LANDesk
LANDESK_CBA_PDS
LANDESK_MANAGEMENT_AGENT
LANDESK_MANAGEMENT_AGENT
ldap
ldap_over_ssl
limewire
linuxconf
lpd
managesoft
McAfee_ePolicy_Orchestrator
melange_chat
MERCUR_Control-Service
Micromuse_Netcool_Object_Server
microsoft-ds
Microsoft_Message_Queue_Server
minisql
modbus
MODBUS_UDP
mqseries
msdtc
MSMQ_Ping
msrpc
msrpc-over-http
msrpc_udp
mssql
mssql_monitor
MYDESKTOP
mysql
named_udp
ncp
nessus
netbios_ns
netbios_ssn
netbus
netop
netstat
Netviewer_PC_Duo
nfs
nntp
ntp
ocsp
ocssd
Omniquad_Server
open_vpn
opennap
oracle
Oracle_Express_Server
Oracle_Express_Server_xsagent
Oracle_Express_Server_xsdaemon
oracle_intelligent_agent
ORACLE_RMI
pcanywhere
pen
Polycom_MGC_Management
pop2
pop3

PostgreSQL
pptp
PRORAT_TROJAN
proxy_http
proxy_telnet
psmond
pvserver
Quote_of_the_Day
quote_of_the_day_udp
radius
radius_tcp
radmin
rccmd
RealMedia_EncoderServer
Red_Carpet_Daemon
RELIABLE DATAGRAM SOCKETS OVER TCP
Resonate_CD_Agent
resource_monitor_api
Resource_Monitoring_and_Control
rip
rlogin
RMIRegistry
rpc
rpc_udp
RSA_Auth_Mgr
rsh/rexec
rsyncd
rtsp
SAP_MAXDB
SAP_Protocol
shell
SHOUTcast
skinny
skype
slapper
SMS
smtp
smux
snmp
snmp2
socks4
socks5
SPLASHTOP_REMOTE_DESKTOP
spychat
Spytech_SpyAnywhere
ssdp
ssh
ssh_over_ssl
swagentd
swat
sybase_adaptive_server
Symantec EMS client server
Symantec_AntiVirus
Symantec_AntiVirus_Rtvscan
Symantec_AntiVirus_Rtvscan_UDP
SysGalUR
systat
talk
telnet
telnet_over_ssl
tftp
time
time_udp
timestamp_over_http
trendmicro_officescan
trojan_fireby
unknown
unknown_over_ssl
UPNP
ut_game_queryport
uucp
VMware_Authentication_Daemon

vnc
vnetd
voip_sip
Volume_Manager_Storage_Administrator
VXWORKS_WDBRPC_UDP
watchguard_admin
webshield
win_remote_desktop
winmx
WINS_Replication
Wonderware_InTouch
wsmserver
WSUS_SERVER
x11
X11_Font_Service
xdmcp
xinetd
Xitami
xpilot
XYZFind
Yahoo_Instant_Messenger
yeemp
ZLink

Categories

Vulnerability Categories as defined by our service as of March 2017 are listed below.

Want a current listing? No problem. Just log in to your Qualys account, go to the KnowledgeBase, click the Search button, and open the Category menu.

Looking for category descriptions? We've got you covered. Log in to your Qualys account, go to Help > Online Help and search for Categories and you'll see the article on Vulnerability Categories with all the details.

Tip - In API requests replace spaces in category names with underscores. For example, Amazon Linux must be specified as Amazon_Linux

AIX
Amazon Linux
Backdoors and trojan horses
Brute Force Attack
CentOS
CGI
Cisco
Firewall
Forensics
General remote services
Hardware
HP-UX
Information gathering
Internet Explorer
Database
Debian
DNS and BIND
E-Commerce
Fedora
File Transfer Protocol
Finger
RedHat
RPC
Security Policy
SNMP
Solaris
SMB / NETBIOS
SUSE

Local	TCP/IP
Mail services	Ubuntu
Malware	VMware
News Server	Web Application
NFS	Web Application Firewall
OEL	Web server
Office Application	Windows
Proxy	X-Window

VM Remediation Tickets

List, edit and delete remediation tickets, created using the VM app, in the user's account.

Remediation Tickets overview

Ticket Parameters

View Ticket List

Edit Tickets

Delete Tickets

View Deleted Ticket List

Get Ticket Information

Set Vulnerabilities to Ignore on Hosts

Remediation Tickets overview

Qualys provides fully secure audit trails that track vulnerability status for all detected vulnerabilities. As follow up audits occur, vulnerability status levels - new, active, fixed, and re-opened - are updated automatically and identified in trend reports, giving users access to the most up-to-date security status. Using Remediation Workflow, Qualys automatically updates vulnerability status in remediation tickets, triggering ticket updates and closure in cases where vulnerabilities are verified as fixed.

Ticket information includes

Ticket Due Date - Each ticket has a due date for ticket resolution. The number of days allowed for ticket resolution is set as part of the policy rule configuration. Overdue tickets are those tickets for which the due date for resolution has passed.

Ticket state/status - Several events trigger ticket updates as described earlier. Certain ticket updates result in changes to ticket state/status as indicated below.

Open refers to new and reopened tickets. Tickets are reopened in these cases: 1) when the service detected vulnerabilities for tickets with state/status Resolved or Closed/Fixed, and 2) when users or the service reopened Closed/Ignored tickets.

Resolved refers to tickets marked as resolved by users.

Closed/Fixed refers to tickets with vulnerabilities verified as fixed by the service.

Closed/Ignored refers to tickets ignored by users or the service (based on a user policy). Also, users can ignore vulnerabilities on hosts. If tickets exist for vulnerabilities set to ignore status, the service sets them to Closed/Ignored, and if tickets do not exist for these issues the service adds new tickets and changes them to Closed/Ignored.

Invalid tickets - Tickets are invalid due to the changing status of the IP address or ticket owner. Regarding the IP address, a ticket is marked invalid when the ticket's IP address is removed from the ticket owner's account (applies to Unit Manager, Scanner, or Reader). Regarding the ticket owner, a ticket is marked invalid when the ticket owner's account is inactive, deleted, or the user's role was changed to Contact.

Ticket Parameters

Many ticket parameters are available for making API requests to view, update and delete active tickets and defining tickets to take actions on. Overdue and Invalid tickets are selected automatically, unless otherwise requested.

- All ticket parameters are optional and valid for these requests: ticket_list.php, ticket_edit.php and ticket_delete.php.

- At least one parameter is required.

- Multiple parameters are combined with a logical “and”.

Parameter	Description
ticket_numbers={nnn,nnn-nnn,...}	Tickets with certain ticket numbers. Specify one or more ticket numbers and/or ranges. Use a dash (-) to separate the ticket range start and end. Multiple entries are comma separated.
since_ticket_number={value}	Tickets since a certain ticket number. Specify the lowest ticket number to be selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
until_ticket_number={value}	Tickets until a certain ticket number. Specify the highest ticket number to be selected. Selected tickets will have numbers less than or equal to the ticket number specified.
show_vuln_details={**0**|1}	(Parameter is valid with ticket_list.php request only) By default, vulnerability details are not included in the ticket list XML output. When set to 1, vulnerability details are included. Vulnerability details provide descriptions for the threat posed by the vulnerability, the impact if exploited, the solution provided by Qualys as well as the scan test results (when available).
Ticket Properties	
ticket_assignee={value}	Tickets with a certain assignee. Specify the user login of an active user account.
overdue={**0**|1}	Tickets that are overdue or not overdue. When not specified, overdue and non-overdue tickets are selected. Specify 1 to select only overdue tickets. Specify 0 to select only tickets that are not overdue.
invalid={**0**|1}	Tickets that are invalid or valid. When not specified, both valid and invalid tickets are selected. Specify 1 to select only invalid tickets. Specify 0 to select only valid tickets. You can select invalid tickets owned by other users, not yourself.

Parameter	Description
states={state}	Tickets with certain ticket state/status. Specify one or more state/status codes. A valid value is OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed), or IGNORED (for state/status Closed/Ignored). Multiple entries are comma separated. To select ignored vulnerabilities on hosts, specify: states=IGNORED
Ticket History	
modified_since_datetime={value}	Tickets modified since a certain date/time. Specify a date (required) and time (optional) since tickets were modified. Tickets modified on or after the date/time are selected. date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2006-01-01” or “2006-05-25T23:12:00Z”.
unmodified_since_datetime={value}	Tickets not modified since a certain date/time. Specify a date (required) and time (optional) since tickets were not modified. Tickets not modified on or after the date/time are selected. date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2006-01-01” or “2006-05-25T23:12:00Z”.
Ticket Host Info	
ips={nnn,nnn-nnn,...}	Tickets on hosts with certain IP addresses. Specify one or more IP addresses and/or ranges. Multiple entries are comma separated.
asset_groups={ag1,ag2,...}	Tickets on hosts with IP addresses which are defined in certain asset groups. Specify the title of one or more asset groups. Multiple asset groups are comma separated. The title “All” may be specified to select all IP addresses in the user account.
dns_contains={value}	Tickets on hosts that have a NetBIOS host name which contains a certain text string. Specify a text string to be used. This string may include a maximum of 100 characters (ascii).
netbios_contains={value}	Tickets on hosts that have a NetBIOS host name which contains a certain text string. Specify a text string to be used. This string may include a maximum of 100 characters (ascii).
host_id={value}	Tickets related to a particular asset when the specific HOST_ID is provided.

Parameter	Description
show_host_id={0|1}	When unspecified or show_host_id=0, the Host ID will not appear in the XML output. Specify show_host_id=1 to show the Host ID in the output.
Vulnerability Info	
vuln_severities={1,2,3,4,5}	Tickets for vulnerabilities with certain severity levels. Specify one or more severity levels. Multiple levels are comma separated.
potential_vuln_severities={1,2,3,4,5}	Tickets for potential vulnerabilities with certain severity levels. Specify one or more severity levels. Multiple levels are comma separated.
qids={qid,qid,...}	Tickets for vulnerabilities with certain QIDs (Qualys IDs). Specify one or more QIDs. A maximum of 10 QIDs may be specified. Multiple QIDs are comma separated.
vuln_title_contains={value}	Tickets for vulnerabilities that have a title which contains a certain text string. The vulnerability title is defined in the KnowledgeBase. Specify a text string. This string may include a maximum of 100 characters (ascii).
vuln_details_contains={value}	Tickets for vulnerabilities that have vulnerability details which contain a certain text string. Vulnerability details provide descriptions for threat, impact, solution and results (scan test results, when available). Specify a text string. This string may include a maximum of 100 characters (ascii).
vendor_ref_contains={value}	Tickets for vulnerabilities that have a vendor reference which contains a certain text string. Specify a text string. This string may include a maximum of 100 characters (ascii).

View Ticket List

/msp/ticket_list.php

View remediation tickets and related ticket information in the user's account.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Using an account with more than 1,000 tickets (or potentially more than 1,000 tickets), it is recommended that you write a script that makes multiple ticket_list.php requests until all tickets are retrieved.

A maximum of 1,000 tickets can be returned from a single ticket_list.php request. If this maximum is reached, the function returns a "Truncated after 1,000 records" message at the end of the XML output with the last ticket number included. Using an account with

more than 1,000 tickets (or potentially more than 1,000 tickets), it is recommended that you write a script that makes multiple ticket_list.php requests until all tickets have been retrieved.

Permissions - Managers can view all tickets in the subscription. Unit Managers can view tickets for IP addresses in the user's same business unit. Scanners and Readers can view tickets for IP addresses in the user's own account.

Input Parameters

Click here for ticket list input parameters

Samples

View Open tickets for owner:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
ticket_assignee=comp_ja&states=OPEN
```

View ticket number range:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
ticket_numbers=001800-002800
```

View tickets with severity 5 confirmed vulnerabilities:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
vuln_severities=5
```

View tickets that have been marked as Closed/Fixed or Closed/Ignored since June 1, 2018:

```
https://qualysapi.qualys.com/msp/ticket_list.php?states=CLOSED,IGN
ORED&modified_since_datetime=2018-06-01
```

List all ignored vulnerabilities in the user's account"

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=
All&states=IGNORED
```

View tickets related to SSH vulnerabilities:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
vuln_title_contains=SSH&vuln_details_contains=SSH
```

View Invalid tickets for hosts in the "Desktops" or "Servers" asset groups:

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=
Desktops,Servers&invalid=1
```

View all tickets filtered by Host ID and Show Host ID:

```
https://qualysapi.qualys.com/msp/ticket_list.php?host_id=355311&sh
ow_host_id=1
```

View Overdue tickets assigned to James Adrian (comp_ja) that have not been modified since May 30, 2018 at 16:30:00 (UTC/GMT) for vulnerabilities with a severity level of 3, 4 or 5 and to include vulnerability details in the results:

```
https://qualysapi.qualys.com/msp/ticket_list.php?
unmodified_since_datetime=2018-05-30T16:30:00Z
&vuln_severities=3,4,5&overdue=1&ticket_assignee=comp_ja
&show_vuln_details=1
```

DTD

<platform API server>/ticket_list_output.dtd

Edit Tickets

/msp/ticket_edit.php

Edit remediation tickets in the user's account. Multiple tickets can be edited at one time in bulk. Many ticket parameters are supported for selecting what tickets you'd like to edit.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Editing tickets can be a time intensive task, especially when batch editing many tickets. To ensure best performance, a maximum of 20,000 tickets can be edited in one ticket_edit.php request. It's recommended best practice that you choose to schedule batch updates to occur when ticket processing will least impact user productivity. If the ticket_edit.php request identifies more than 20,000 tickets to be edited, then an error is returned.

Permissions - Managers can edit all tickets in the subscription. Unit Managers can edit tickets for IP addresses in the user's same business unit. Scanners and Readers do not have permissions to edit tickets.

Input Parameters

Click here to view ticket parameters for selecting tickets to edit

The following parameters are used to define the ticket data to be edited. At least one of the following edit parameters is required.

Parameter	Description
change_assignee={value}	(Optional) Used to change the ticket assignee, specified by user login, in all selected tickets. The assignee's account must have a user role other than Contact, and the hosts associated with the selected tickets must be in the user account.
change_state={value}	(Optional) Used to change the ticket state/status to the specified state/status in all selected tickets. A valid value is OPEN (for state/status Open and Open/Reopened), RESOLVED (for state Resolved), or IGNORED (for state/status Closed/Ignored). See "Ticket State/Status Transitions" below for information on valid changes.
add_comment={value}	(Optional) Used to add a comment in all selected tickets. The comment text may include a maximum of 2,000 characters (ascii).
reopen_ignored_days={value}	(Optional) Used to reopen Closed/Ignored tickets in a set number of days. Specify the due date in N days, where N is a number of days from today. A valid value is an integer from 1 to 730. When the due date is reached, the ticket state is changed from Closed/Ignored to Open, assuming the issue still exists, and the ticket is marked as overdue. If the issue was resolved at some point while the ticket was in the Closed/Ignored state, then the ticket state is changed from Closed/Ignored to Closed/Fixed.

Ticket State/Status Transitions

The Qualys remediation workflow feature is a closed loop ticketing system for remediation management and policy compliance. Users may edit tickets to make certain ticket state changes as shown below.

	To State/Status		
From State/Status	**Open**	**Resolved**	**Closed/Ignored**
Open	valid	valid	valid
Resolved	valid	valid	valid
Closed/Ignored	valid	invalid	valid
Closed/Fixed	valid	invalid	valid

Samples

Edit ticket and add comment:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"ticket_numbers=23456&add_comment=Host+patched,+ready+for+re-scan"
```

```
"https://qualysapi.qualys.com/msp/ticket_edit.php?"
```

Edit multiple tickets to change the ticket owner to Alice Cook (acme_ac) for tickets since ticket number #00215555 (tickets with numbers greater than or equal to #00215555) which are marked invalid):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"since_ticket_number=00215555&invalid=1&change_assignee=acme_ac"
"https://qualysapi.qualys.com/msp/ticket_edit.php?"
```

Edit Open tickets on IP addresses in asset groups “New York” and “London” and change the ticket state to Ignored:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"states=OPEN&asset_groups=New+York,London&change_state=IGNORED"
"https://qualysapi.qualys.com/msp/ticket_edit.php?"
```

Edit Open tickets unmodified since August 1, 2017 that are assigned to Tim Burke (acme_tb) and change the ticket assignee to Alice Cook (acme_ac):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"states=OPEN&unmodified_since=2017-08-01&ticket_assignee=acme_tb&c
hange_assignee=acme_ac"
"https://qualysapi.qualys.com/msp/ticket_edit.php?"
```

Reopen all Closed/Ignored tickets on host 10.10.10.120 in 7 days:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"ips=10.10.10.120&reopen_ignored_days=7"
"https://qualysapi.qualys.com/msp/ticket_edit.php?"
```

DTD

<platform API server>/ticket_edit_output.dtd

Delete Tickets

/msp/ticket_delete.php

Delete remediation tickets in the user’s account.Multiple tickets can be deleted at one time in bulk. Many ticket parameters are supported for selecting what tickets you’d like to edit.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Deleting tickets can be a time intensive task, especially when batch deleting many tickets. To ensure best performance, a maximum of 20,000 tickets can be deleted in one ticket_delete.php request. It's recommended best practice that you choose to schedule batch updates to occur when ticket processing will least impact user productivity. If the ticket_delete.php request identifies more than 20,000 tickets to be deleted, then an error is returned.

Permissions - Managers can delete all tickets in the subscription. Unit Managers can delete tickets for IP addresses in their same business unit. Scanners and Readers have no permissions to delete tickets.

Input Parameters

Click here to view ticket parameters for selecting tickets to delete

Samples

Delete certain ticket number:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
ticket_numbers=2487
```

Delete tickets between ticket #001000 and ticket #002500:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
since_ticket_number=1000&until_ticket_number=2500
```

Delete Closed/Fixed tickets owned by James Adrian (comp_ja):

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
states=CLOSED&ticket_assignee=comp_ja
```

Delete tickets on vulnerabilities with an assigned severity level of 1 and potential vulnerabilities with an assigned severity level of 1-3:

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
vuln_severities=1&potential_vuln_severities=1,2,3
```

Delete Overdue tickets assigned to James Adrian (comp_ja) that have not been modified since July 01, 2018 at 12:00:00 (UTC/GMT)

```
https://qualysapi.qualys.com/msp/ticket_delete.php?
unmodified_since_datetime=2018-07-01T12:00:00Z
&overdue=1&ticket_assignee=comp_ja
```

DTD

<platform API server>/ticket_delete_output.dtd

View Deleted Ticket List

/msp/ticket_list_deleted.php

View deleted tickets in the user's account. This function may be run by Managers. The functionality provided allows for real-time integration with third-party applications.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

The XML results returned by the ticket_list_deleted.php function identifies deleted tickets by ticket number and deletion date/time.

A maximum of 1,000 deleted tickets can be returned from a single ticket_list_deleted.php request. If this maximum is reached, the function returns a "Truncated after 1,000 records" message at the end of the XML report with the last ticket number included.

Permissions - Manager user role is required.

Input Parameters

All parameters are optional. At least one parameter is required. Multiple parameters are combined with a logical "and".

Parameter	Description
ticket_numbers={nnn,nnn-nnn,...}	(Optional) Specifies certain ticket numbers. Specify one or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-). Multiple entries are comma separated.
since_ticket_number={value}	(Optional) Specifies tickets since a certain ticket number. Specify the lowest ticket number to be selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
until_ticket_number={value}	(Optional) Specifies tickets until a certain ticket number. Specify the highest ticket number to be selected. Selected tickets will have numbers less than or equal to the ticket number specified.

Parameter	Description
deleted_since_datetime={value}	(Optional) Specifies tickets deleted since a certain date/time. Specify a date (required) and time (optional) to identify this timeframe. Tickets deleted on or after the date/time are selected. date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".
deleted_before_datetime={value}	(Optional) Specifies tickets deleted before a certain date/time. Specify a date (required) and time (optional) to identify this timeframe. Tickets deleted on or before the date/time are selected. date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".

Samples

View tickets deleted in ticket number range:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
ticket_numbers=120-200
```

View tickets deleted since ticket number:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
since_ticket_number=400
```

View tickets deleted since date:

```
https://qualysapi.qualys.com/msp/ticket_list_deleted.php?
deleted_since_datetime=2018-01-01
```

DTD

<platform API server>/ticket_list_deleted_output.dtd

Get Ticket Information

/msp/get_tickets.php

View remediation ticket information from the user's account that can be integrated with third-party applications. Only remediation tickets that the user has permission to view are returned in the resulting ticket information report.

Basic HTTP authentication is required. Session based authentication is not supported using this API.

Qualys recommends that you run the get_tickets.php function two times a day, so that ticket updates due to the latest scan results and user productivity are made available in the ticket information reports.

Permissions - Managers can view all tickets in subscription. Unit Managers can view tickets for IP addresses in their same business unit. Scanners and Readers can view tickets for IP addresses in their own account.

Input Parameters

Parameter	Description
ticket_numbers={nnn,nnn,..}	(Optional) Specifies ticket numbers for which ticket information will be retrieved. Ticket numbers are integers, assigned by the service automatically. A maximum of 1,000 ticket numbers may be specified. Multiple ticket numbers are comma separated. This parameter or since must be specified.
since={value}	(Optional) Specifies the start date/time of the time window for retrieving tickets. Only tickets that have been updated within this time window will be retrieved. The end date/time of the time window for retrieving tickets is the date/time when get_tickets.php is run. The start date/time is specified in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT), like "2005-01-10T02:33:11Z". This parameter or ticket_numbers must be specified.
state={value}	(Optional) Specifies the current state of tickets to be retrieved. A valid value is OPEN, RESOLVED, or CLOSED. If unspecified, tickets with all states are retrieved.
vuln_details={**0**|1}	(Optional) Specifies whether vulnerability details will be retrieved. Vulnerability details include a description of the threat posed by the vulnerability, the impact if it is exploited, a verified solution, and in some cases test results returned by the scanning engine. By default, vulnerability details will not be retrieved. To retrieve vulnerability details, specify vuln_details=1.

Samples

Retrieve remediation tickets that have been updated since July 1, 2018 at 1:00:00 AM (UTC/GMT) and that have any state (Open, Resolved, or Closed):

```
https://qualysapi.qualys.com/msp/get_tickets.php?
  since=2018-07-01T01:00:00Z
```

Retrieve remediation tickets 002737, 002738, and 002740 with vulnerability details:

```
https://qualysapi.qualys.com/msp/get_tickets.php?
  ticket_numbers=002737,002738,002740&vuln_details=1
```

DTD

<platform API server>/remediation_tickets.dtd

Set Vulnerabilities to Ignore on Hosts

/api/2.0/fo/ignore_vuln/index.php

The ignore_vuln/index.php function is used to ignore or restore (un-ignore) vulnerabilities on certain hosts. The ignore status applies to a vulnerability/host pair. Vulnerabilities can be set to ignore on hosts so that they do not appear in automatic scan reports, host information reports, asset search reports as well as other views in the Qualys user interface.

Both Vulnerabilities and Potential Vulnerabilities may be set to the ignore status on hosts in the user's account. Information Gathered issues cannot be set to the ignore status. Note that the following QIDs cannot be set to ignore: 38175 (Unauthorized Service Detected), 82043 (Unauthorized Open Port Detected), 38228 (Required Service Not Detected) and 82051 (Required Port Not Detected).

When making an ignore_vuln/index.php request, you must specify QIDs (up to 10) and target hosts. Host selection parameters allow you to specify hosts by IP address, asset group, asset tag, DNS host name or NetBIOS host name.

Target Hosts

A vulnerability can be set to ignore/restore only on hosts with scan results. If a host was previously scanned and then purged, the scan results are removed and no longer available. In this case an ignore vulnerability request will have no effect until a re-scan populates the host with fresh scan results.

The ignore/restore request applies to the target hosts at the time of the request. For example, if you specify an ignore action on asset groups, the request applies to the IP addresses in the asset groups at the time of the request. Subsequently, if an asset group is updated with new IP addresses, the new IPs are not set to the ignore status.

Ignored Status and Tickets

The ignore/restore actions have an effect on remediation tickets in the user account. When you set the ignore status for vulnerabilities on hosts, the service closes associated remediation tickets with the ticket state/status of Closed/Ignored. If no ticket exists, a new one will be created and closed automatically for tracking purposes as Closed/Ignored. When you restore vulnerabilities on hosts, the service automatically reopens the associated tickets and sets them to Open/Reopened.

The **ticket_list.php** function allows you to list tickets in the user account and this information could be useful for taking actions using **ignore_vuln/index.php**. For example, you could use **ticket_list.php** to find tickets on certain QIDs in the Closed/Ignored state and then use the information returned to make **ignore_vuln/index.php** requests to restore vulnerabilities on certain hosts.

Best Practices for using this API

Qualys recommendes the following best practices when using the Ignore API that helps you to maintain system stability and optimize the performance.

- When you use the IPs parameter, pass a comma-separated list of specific IPs or IP ranges where the QID needs to be ignored. This reduces the response size and avoids resolving large tag sets.

- When you use a new tag, create a new tag and assign only the required hosts to this tag on which the QID needs to be ignored. This ensures targeted execution and minimizes data load on the system.

Permissions

User permissions for the **ignore_vuln/index.php** function are described below.

User Role	Permissions
Manager	Ignore/Restore vulnerabilities and potential vulnerabilities on all hosts in subscription.
Unit Manager	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's business unit.
Scanner	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's account, when a certain remediation policy option is enabled. *
Reader	Ignore/Restore vulnerabilities and potential vulnerabilities on hosts in user's account, when a certain remediation policy option is enabled.*

* Scanners and Readers have permission to ignore/restore vulnerabilities when the option "Allow Scanners and Readers to mark tickets as Closed/Ignored" is enabled in the QualysGuard user interface. A Manager can edit this setting for the subscription. See the QualysGuard online help for information.

Input Parameters

The parameters for **ignore_vuln/index.php** are described below.

The request parameters are below:

Parameter	Description
action=ignore|restore	A flag indicating an ignore or restore request. When unspecified, the action is set to "ignore". Specify "restore" to restore (un-ignore) vulnerabilities.
	Ignore request: Optional
	Restore request: Required
qids={qid,qid,...}	(Required) Specifies the QIDs (Qualys IDs) to ignore/restore. A maximum of 10 QIDs may be specified. Multiple QIDs are comma separated.
comments={value}	(Required) Specify comments for the action. The comments may include a maximum of 255 characters. Comments are stored with ignored vulnerabilities, and are visible to users in the Qualys user interface.
reopen_ignored_days={value}	(Optional) Set to reopen ignored vulnerabilities that are detected after a number of days (1-730). If the ignored vulnerability is reopened by the service, the corresponding ticket's state/status is changed from Closed/Ignored to Open/Reopened. **Note**: If the ignored vulnerability is reopened by the service, the corresponding ticket's due date does not get changed.
reopen_ignored_date={date}	(Optional) Set to reopen ignored vulnerabilities that are detected after a specified date. If the ignored vulnerability is reopened by the service, the corresponding ticket's state/status is changed from Closed/Ignored to Open/Reopened. **Note**: If the ignored vulnerability is reopened by the service, the corresponding ticket's due date does not get changed.

The host parameters mentioned below are optional and mutually exclusive (only one may be specified per request). At least one parameter must be specified.

Parameter	Description
asset_groups={ag1,ag2,...}	(Optional) Selects hosts by asset group. The hosts included in the one or more asset groups provided are selected. A maximum of 5 asset group titles may be specified. The asset group title "All" as defined in the Qualys user interface may be specified. Multiple asset groups are comma separated.
	This parameter or another host selection parameter is required.

Parameter	Description
ips={nnn, nnn-nnn,...}	(Optional) Selects hosts by IP address. Enter one or more IP addresses and/or ranges. Multiple entries are comma separated. The parameter value may include a maximum of 512 characters (ascii).
	This parameter or another host selection parameter is required.
network_id={value}	(Optional) Only valid when the networks feature is enabled. The network ID for the record. **Note:** The default network (Global Default Network) will be assigned to the API, if you do not provide the network id.
	This parameter or another host selection parameter is required.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	This parameter or another host selection parameter is required.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	This parameter or another host selection parameter is required.
tag_set_by={id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
	This parameter or another host selection parameter is required.
tag_include_selector={all|any}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
	This parameter or another host selection parameter is required.
tag_exclude_selector={all|any}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
	This parameter or another host selection parameter is required.

Parameter	Description
use_ip_nt_range_tags_include={0|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to scan all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
	This parameter or another host selection parameter is required.
use_ip_nt_range_tags_exclude={0|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to exclude all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
	This parameter or another host selection parameter is required.
dns_contains={value}	(Optional) Selects hosts by DNS host name. Specify a text string contained in one or more DNS host names. The text string may include a maximum of 100 characters (ascii).
	This parameter or another host selection parameter is required.
netbios_contains={value}	(Optional) Selects hosts by NetBIOS host name. Specify a text string contained in one or more NetBIOS host names. The text string may include a maximum of 100 characters (ascii).
	This parameter or another host selection parameter is required.

Samples

To ignore QID 19070 "MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability" for the hosts in asset group "New York", use a URL like this:

```
https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/index.php?action=ignore&qids=19070&asset_groups=New+York&comments=security+policy
```

To restore (un-ignore) QIDs 90305 and 100035 on IP address 10.10.10.33 and IP range 10.10.10.100-10.10.10.120, use a URL like this:

```
https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/index.php?action=restore&qids=90305,100035&ips=10.10.10.33,10.10.10.100-10.10.10.120&comments=request+by+GStevenson
```

If there are ignored vulnerabilities in your account, you can list all ignored vulnerabilities in the account using the **ticket_list.php** function as shown in the following URL:

```
https://qualysapi.qualys.com/msp/ticket_list.php?asset_groups=All&states=IGNORED
```

DTD

<platform API server>/api/2.0/dtd/fo/ignore_vuln_output.dtd

Compliance

Manage compliance policies, exceptions and reports. Policy Compliance (PC) is required.

Compliance Control List

Compliance Policy List

Compliance Policy - Export

Compliance Policy - Import

Compliance Policy - Merge

Compliance Policy - Manage Asset Groups

Compliance Framework Reports

Compliance Posture Information

PC Posture Streaming APIs

Exceptions

SCAP Cyberscope Report

SCAP ARF Report

SCAP Policy List

PCAS Policies

PCAS Library Policy

Compliance Control List

For API version information, refer to the API Version History section.

V2.0|V3.0|V4.0

V2.0

/api/2.0/fo/compliance/control/?action=list

[GET] [POST]

View a list of compliance controls which are visible to the user. Controls in the XML output are sorted by control ID in ascending order. Optional input parameters support filtering the list.

Using the Qualys user interface, it's possible to customize the list of frameworks at the subscription level. Under PC, go to Policies > Setup > Frameworks to customize the frameworks list. If the frameworks list is customized for your subscription, then the customized list of frameworks will appear in the controls list output returned by a control list API request.

Permissions

Note: The Compliance Control APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Users with PC enabled have the ability to view compliance controls.

Maximum Controls per API Request

The output of the Compliance Control API is paginated. By default, a maximum of 1,000 control records are returned per request. You can customize the page size (i.e. the number of control records) by using the parameter "truncation_limit=2000" for instance. In this case the results will be return with pages of 2,000 records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Parameter	Description
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each control. A valid value is: None - show control ID only Basic (default) - show control ID and basic control information: the control category, sub-category, statement, and technology information All - show control ID, basic control information, and framework mappings
ids={value}	(Optional) Show only certain control IDs and/or ID ranges. Multiple entries are comma separated. One or more control IDs/ranges may be specified. A control ID range entry is specified with a hyphen (for example, 3000-3250). Valid control IDs are required.
id_min={value}	(Optional) Show only controls which have a minimum control ID value. A valid control ID is required.
id_max={value}	(Optional) Show only controls which have a maximum control ID value. A valid control ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See "Date Filters" below.
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See "Date Filters" below.
truncation_limit={value}	(Optional) The maximum number of control records processed per request. When not specified, the truncation limit is set to 1,000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records. You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is being downloaded.

Date Filters

The date/time is specified in YYYY-MM-DD{THH:MM:SSZ] format (UTC/GMT), like "2010-03-01" or "2010-03-01T23:12:00Z"

If you specify a date but no time as for example 2010-03-01, then the service automatically sets the time to 2010-03-01T00:00:00Z (the start of the day).

When date filters are specified using both input parameters for a single API request, both date filters are satisfied (ANDed).

DTD

<platform API server>/api/2.0/fo/compliance/control/control_list_output.dtd

Sample - Control List Output

This sample control list output was produced for CID 1044 with details=Basic.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualyspapi.qualys.com/api/2.0/fo/compliance/control/contr
ol_list_output.dtd">

<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2010-03-16T22:53:05Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>1044</ID>
        <UPDATE_DATE>2010-02-12T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-10-12T00:00:00Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Authorizations (Multi-user
ACL/role)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the
'O7_DICTIONARY_ACCESSIBILITY' setting in init.ora (ORACLE Data
Dictionary)]]></STATEMENT>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>7</ID>
            <NAME>Oracle 9i</NAME>
            <RATIONALE><![CDATA[The "O7_DICTIONARY_ACCESSIBILITY"
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>8</ID>
            <NAME>Oracle 10g</NAME>
            <RATIONALE><![CDATA[The "O7_DICTIONARY_ACCESSIBILITY"
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
```

```
access will be allowed, which is the default for Oracle operations.
Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specified granted.]]></RATIONALE>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>9</ID>
            <NAME>Oracle 11g</NAME>
            <RATIONALE><![CDATA[The "O7_DICTIONARY_ACCESSIBILITY"
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>1045</ID>
        <UPDATE_DATE>2010-03-03T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-10-12T00:00:00Z</CREATED_DATE>
        <CATEGORY>OS Security Settings</CATEGORY>
       <SUB_CATEGORY><![CDATA[System Settings (OSI layers 6-7)]]>
</SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the 'Clipbook' service
(Guidance = Disabled)]]></STATEMENT>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access. As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>2</ID>
            <NAME>Windows 2003 Server</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
```

```
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access.  As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>12</ID>
            <NAME>Windows 2000</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access.  As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
          </TECHNOLOGY>
</CONTROL_LIST_OUTPUT>
```

Updates you'll see once Agent UDC support is available

New Agent UDC Support will be announced soon via the Qualys Technology blog once remaining components are released.

The XML output may include the USE_AGENT_ONLY element for these Windows and Unix control types: Directory Search Control and Directory Integrity Control. This is set to 1 when the "Use agent scan only" option is enabled for the control.

The XML output may include the AUTO_UPDATE element for these Windows and Unix control types: File Integrity Control and Directory Integrity Control. This is set to 1 when the "Auto update expected value" option is enabled for the control.

Option to disable the case-sensitive search in Unix agent UDCs (Directory Search and Directory Integrity) is available. Once the <DISABLE_CASE_SENSITIVE_SEARCH> parameter is enabled (true), the search result lists all possible combinations in the upper and/or lower case file name. By default, this option is disabled (false) which lists result with case-sensitive file name.

Sample - Control List Output when Agent UDC Support is available

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
```

```
    <DATETIME>2018-10-05T10:23:54Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100023</ID>
        <UPDATE_DATE>2018-11-16T06:27:14Z</UPDATE_DATE>
        <CREATED_DATE>2018-11-16T06:27:14Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Directory Integrity Check]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows Directory Integrity
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[test]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <AUTO_UPDATE>1</AUTO_UPDATE>
        <IGNORE_ERROR>0</IGNORE_ERROR>
<CRITICALITY>
         ...
```

Database UDC for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2

You can create custom controls for MSSQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2 databases. To support database controls, we've added new elements to the XML output and DTDs for Control List Output and Policy Export Output.

Sample - Control List API for MS SQL

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=list&details=All&ids=100022"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/">
MSSQLControlAPI.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-05-08T18:31:17Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100022</ID>
        <UPDATE_DATE>2019-05-08T18:31:08Z</UPDATE_DATE>
```

```
        <CREATED_DATE>2019-04-29T20:21:11Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[CustomerData]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[URGENT]]></LABEL>
          <VALUE>5</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[MSSQL Database Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[testComment]]></COMMENT>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <ERROR_SET_STATUS>PASS</ERROR_SET_STATUS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>22</ID>
            <NAME>Microsoft SQL Server 2008</NAME>
            <RATIONALE><![CDATA[select all from
customer]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from
customers;]]></DB_QUERY>
            <DESCRIPTION><![CDATA[select all the rows from
customers]]></DESCRIPTION>

          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Control List API for Oracle

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=list&details=All&ids=100060"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/">
OracleControlAPI.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
```

```
    <DATETIME>2019-05-08T18:32:46Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100060</ID>
        <UPDATE_DATE>2019-05-08T18:32:04Z</UPDATE_DATE>
        <CREATED_DATE>2019-05-03T19:32:18Z</CREATED_DATE>
        <CATEGORY>Database Settings</CATEGORY>
       <SUB_CATEGORY><![CDATA[DB Access Controls]]></SUB_CATEGORY>

<STATEMENT><![CDATA[OracleselectAllCustomerData]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[MINIMAL]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Oracle Database Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[Gather All Data ]]></COMMENT>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <ERROR_SET_STATUS>FAIL</ERROR_SET_STATUS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>7</ID>
            <NAME>Oracle 9i</NAME>
            <RATIONALE><![CDATA[GatherAllData]]></RATIONALE>
           <DB_QUERY><![CDATA[SELECT * FROM Customers WHERE ROWNUM
>= 3;]]></DB_QUERY>
            <DESCRIPTION><![CDATA[select all the
data]]></DESCRIPTION>

          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>8</ID>
            <NAME>Oracle 10g</NAME>
            <RATIONALE><![CDATA[GatherAllData]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from
Customers;]]></DB_QUERY>
            <DESCRIPTION><![CDATA[select all the
data]]></DESCRIPTION>

          </TECHNOLOGY>
          ...
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Control List API for Sybase

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=list&details=All&ids=100947"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
    <REQUEST>
        <DATETIME>2020-03-21T05:29:10Z</DATETIME>
        <USER_LOGIN>quays_sp1</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/contr
ol/</RESOURCE>
        <PARAM_LIST>
            <PARAM>
                <KEY>action</KEY>
                <VALUE>list</VALUE>
            </PARAM>
            <PARAM>
                <KEY>ids</KEY>
                <VALUE>100947</VALUE>
            </PARAM>
            <PARAM>
                <KEY>echo_request</KEY>
                <VALUE>1</VALUE>
            </PARAM>
        </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
        <DATETIME>2020-03-21T05:29:10Z</DATETIME>
        <CONTROL_LIST>
            <CONTROL>
                <ID>100947</ID>
                <UPDATE_DATE>2020-03-20T15:05:35Z</UPDATE_DATE>
                <CREATED_DATE>2020-03-18T05:50:27Z</CREATED_DATE>
                <CATEGORY>Access Control Requirements</CATEGORY>
                <SUB_CATEGORY>
                    <![CDATA[Account Creation/User Management]]>
                </SUB_CATEGORY>
                <STATEMENT>
```

```
                    <![CDATA[sybase db udc]]>
                </STATEMENT>
                <CRITICALITY>
                    <LABEL>
                        <![CDATA[UNDEFINED]]>
                    </LABEL>
                    <VALUE>0</VALUE>
                </CRITICALITY>
                <CHECK_TYPE>
                    <![CDATA[Sybase Database Check]]>
                </CHECK_TYPE>
                <COMMENT>
                    <![CDATA[]]>
                </COMMENT>
                <IGNORE_ERROR>0</IGNORE_ERROR>
                <ERROR_SET_STATUS></ERROR_SET_STATUS>
                <TECHNOLOGY_LIST>
                    <TECHNOLOGY>
                        <ID>69</ID>
                        <NAME>Sybase ASE 15</NAME>
                        <RATIONALE>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
t.free_space as free_space_pages,
case t.status when 1 then 'LAST CHANCE' else 'OTHER' end as status,
t.proc_name, suser_name(t.suid) as owner
from syssegments s, systhresholds t
where t.segment = s.segment]]>
                        </RATIONALE>
                        <DB_QUERY>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
            t.free_space as free_space_pages,
          case t.status when 1 then 'LAST CHANCE' else 'OTHER' end
as status,
            t.proc_name, suser_name(t.suid) as owner
            from syssegments s, systhresholds t
            where t.segment = s.segment]]>
                        </DB_QUERY>
                        <DESCRIPTION>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
            t.free_space as free_space_pages,
          case t.status when 1 then 'LAST CHANCE' else 'OTHER' end
as status,
            t.proc_name, suser_name(t.suid) as owner
```

```
            from syssegments s, systhresholds t
            where t.segment = s.segment]]>
                        </DESCRIPTION>
                    </TECHNOLOGY>
                    <TECHNOLOGY>
                        <ID>116</ID>
                        <NAME>SAP Adaptive Server Enterprise
16</NAME>
                        <RATIONALE>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
t.free_space as free_space_pages,
case t.status when 1 then 'LAST CHANCE' else 'OTHER' end as status,
t.proc_name, suser_name(t.suid) as owner
from syssegments s, systhresholds t
where t.segment = s.segment]]>
                        </RATIONALE>
                        <DB_QUERY>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
            t.free_space as free_space_pages,
          case t.status when 1 then 'LAST CHANCE' else 'OTHER' end
as status,
            t.proc_name, suser_name(t.suid) as owner
            from syssegments s, systhresholds t
            where t.segment = s.segment]]>
                        </DB_QUERY>
                        <DESCRIPTION>
                            <![CDATA[select db_name() as dbname,
s.name as segment_name,
            t.free_space as free_space_pages,
          case t.status when 1 then 'LAST CHANCE' else 'OTHER' end
as status,
            t.proc_name, suser_name(t.suid) as owner
            from syssegments s, systhresholds t
            where t.segment = s.segment]]>
                        </DESCRIPTION>
                    </TECHNOLOGY>
                </TECHNOLOGY_LIST>
            </CONTROL>
        </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Control List API for PostgreSQL/Pivotal Greenplum

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&details=All&ids=101335"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML output:

```
XML output:
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-10-15T16:59:13Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>101335</ID>
        <UPDATE_DATE>2020-10-14T20:11:29Z</UPDATE_DATE>
        <CREATED_DATE>2020-10-14T19:46:01Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>

<STATEMENT><![CDATA[prePostGreSQL_selectStatement]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[URGENT]]></LABEL>
          <VALUE>5</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[PostgreSQL Database
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[comments]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <ERROR_SET_STATUS></ERROR_SET_STATUS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>114</ID>
            <NAME>PostgreSQL 9.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
```

```
            <ID>143</ID>
            <NAME>PostgreSQL 10.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>192</ID>
            <NAME>PostgreSQL 11.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>201</ID>
            <NAME>Pivotal Greenplum 5.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>228</ID>
            <NAME>PostgreSQL 12.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>230</ID>
            <NAME>Pivotal Greenplum 6.x</NAME>
            <RATIONALE><![CDATA[Rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select name, setting from
pg_catalog.pg_settings where
name='log_min_duration_statement']]></DB_QUERY>
            <DESCRIPTION><![CDATA[Description]]></DESCRIPTION>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
```

```
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Control List API for IBM DB2

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&ids=100010"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-06-22T11:14:08Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100010</ID>
        <UPDATE_DATE>2021-06-22T08:24:27Z</UPDATE_DATE>
        <CREATED_DATE>2021-06-22T08:24:27Z</CREATED_DATE>
        <CATEGORY>Database Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[DB Access
Controls]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[db2 statement]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[DB2 Database Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[comment for db2 udc]]></COMMENT>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <ERROR_SET_STATUS>FAIL</ERROR_SET_STATUS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>40</ID>
            <NAME>IBM DB2 9.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
          </TECHNOLOGY>
```

```
          <TECHNOLOGY>
            <ID>93</ID>
            <NAME>IBM DB2 10.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>142</ID>
            <NAME>IBM DB2 11.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Control List API for File Content Check

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d
"action=list&echo_request=1&ids=100006,100000,100026&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/">
control_list.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <REQUEST>
    <DATETIME>2019-10-14T21:17:21Z</DATETIME>
    <USER_LOGIN>username</USER_LOGIN>
<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/contr
ol/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
```

```
        <KEY>action</KEY>
        <VALUE>list</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ids</KEY>
        <VALUE>100006,100000,100026</VALUE>
      </PARAM>
<PARAM>
        <KEY>details</KEY>
        <VALUE>All</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2019-10-14T21:17:21Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100000</ID>
        <UPDATE_DATE>2019-10-10T21:54:35Z</UPDATE_DATE>
        <CREATED_DATE>2019-10-08T19:16:02Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[preFCCUDC]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[min]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows File Content
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>
            <PATH_TYPE><![CDATA[Use file search]]></PATH_TYPE>
            <FILE_QUERY><![CDATA[QWEB*]]></FILE_QUERY>
            <BASE_DIR><![CDATA[c:\]]></BASE_DIR>
            <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>

<FILE_NAME_MATCH><![CDATA[preTest2.txt]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
```

```
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
            <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
            <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>
            <DATA_TYPE>String List</DATA_TYPE>
           <DESCRIPTION><![CDATA[FileContentChech]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>53</ID>
            <NAME>Windows 2012 Server</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                   <DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>75</ID>
            <NAME>Windows Server 2012 R2</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                   <DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>100006</ID>
        <UPDATE_DATE>2019-10-14T19:06:55Z</UPDATE_DATE>
        <CREATED_DATE>2019-10-09T22:00:50Z</CREATED_DATE>
        <CATEGORY>Database Settings</CATEGORY>
       <SUB_CATEGORY><![CDATA[DB Access Controls]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[min]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows File Content
Check]]></CHECK_TYPE>
```

```
        <COMMENT><![CDATA[]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>
            <PATH_TYPE><![CDATA[Use Registry key]]></PATH_TYPE>
            <REG_HIVE><![CDATA[HKEY_CLASSES_ROOT
(HKCR)]]></REG_HIVE>
            <REG_KEY><![CDATA[TestKey\user]]></REG_KEY>
            <REG_VALUE_NAME><![CDATA[preName]]></REG_VALUE_NAME>
            <FILE_PATH><![CDATA[]]></FILE_PATH>
            <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
            <DATA_TYPE>String List</DATA_TYPE>
            <DESCRIPTION><![CDATA[reg key]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>53</ID>
            <NAME>Windows 2012 Server</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
<OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>75</ID>
            <NAME>Windows Server 2012 R2</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>100026</ID>
        <UPDATE_DATE>2019-10-11T20:12:48Z</UPDATE_DATE>
        <CREATED_DATE>2019-10-11T20:12:48Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
```

```
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>

<STATEMENT><![CDATA[pre_fcc_file_path_regexwith$]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[min]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows File Content
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>
         <PATH_TYPE><![CDATA[Use file path]]></PATH_TYPE>
<FILE_PATH><![CDATA[C:\user\PreTest\pretestfile1.txt]]></FILE_PATH
>
           <FILE_QUERY><![CDATA[pre\$]]></FILE_QUERY>
           <DATA_TYPE>String List</DATA_TYPE>
           <DESCRIPTION><![CDATA[pre\$]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>2</ID>
            <NAME>Windows 2003 Server</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
```

```
            <TECHNOLOGY>
              <ID>12</ID>
              <NAME>Windows 2000</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>18</ID>
              <NAME>Windows Vista</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>21</ID>
              <NAME>Windows 2008 Server</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
<OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>37</ID>
              <NAME>Windows 7</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
```

```
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>53</ID>
    <NAME>Windows 2012 Server</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>54</ID>
    <NAME>Windows 8</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>72</ID>
    <NAME>Windows 8.1</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>75</ID>
    <NAME>Windows Server 2012 R2</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
```

```
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>91</ID>
            <NAME>Windows 10</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>106</ID>
            <NAME>Windows 2016 Server</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>144</ID>
            <NAME>Windows Embedded 7</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>145</ID>
            <NAME>Windows Embedded 8</NAME>
```

```
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>146</ID>
            <NAME>Windows Embedded 8.1</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>180</ID>
            <NAME>Windows 2019 Server</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

List Unix File Content Custom Controls when Evaluate as string is enabled

You have an option in Unix File Content custom controls to evaluate scan results as a string instead of string list. Once the <EVALUATE_AS_STRING> parameter is enabled (1), the scan result is evaluated as a single string. By default the option is disabled (0).

Sample: List FC UDC when Evaluate as string is enabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&ids=102090&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/contro
l_list_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-04-06T11:14:08Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>102090</ID>
        <UPDATE_DATE>2021-04-01T11:59:40Z</UPDATE_DATE>
        <CREATED_DATE>2021-04-01T11:59:40Z</CREATED_DATE>
        <CATEGORY>Web Application Services</CATEGORY>
        <SUB_CATEGORY><![CDATA[Web Server/Tier
Settings]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[FC_New Option Enabled _With String
list]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[URGENT]]></LABEL>
          <VALUE>5</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix File Content
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[String list]]></COMMENT>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>1</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>

<FILE_PATH><![CDATA[/home/testscan/samram]]></FILE_PATH>
            <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
            <DATA_TYPE>String List</DATA_TYPE>
            <EVALUATE_AS_STRING>1</EVALUATE_AS_STRING>
           <DESCRIPTION><![CDATA[with string list]]></DESCRIPTION>
```

```
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
        ...
```

Sample - List DS UDCs when case sensitive search is disabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&ids=102154&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-07-21T12:14:26Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>102154</ID>
        <UPDATE_DATE>2021-07-21T07:02:43Z</UPDATE_DATE>
        <CREATED_DATE>2021-07-07T06:38:30Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[DS UDC case sensitive with new
option]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[MINIMAL]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix Directory Search Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[DI UDC case sensitive disabled]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <SCAN_PARAMETERS>
            <BASE_DIR><![CDATA[/home/qa]]></BASE_DIR>
            <SHOULD_DESCEND><![CDATA[true]]></SHOULD_DESCEND>
            <DEPTH_LIMIT><![CDATA[10]]></DEPTH_LIMIT>
            <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
            <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
            <PERMISSIONS>
                <SPECIAL>
                    <USER>any</USER>
                    <GROUP>any</GROUP>
                    <DELETION>any</DELETION>
                </SPECIAL>
```

```
                    <USER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </USER>
                    <GROUP>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </GROUP>
                    <OTHER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </OTHER>
                </PERMISSIONS>
                <PERM_COND><![CDATA[all]]></PERM_COND>
                <TYPE_MATCH><![CDATA[d,f,l,p,b,c,s,D]]></TYPE_MATCH>
                <USER_OWNER><![CDATA[Any User]]></USER_OWNER>
                <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>
                <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[true]]></DISABLE_CASE_SENSITIVE_S
EARCH>
                <DATA_TYPE>String List</DATA_TYPE>
                <DESCRIPTION><![CDATA[/home/qa desc]]></DESCRIPTION>
            </SCAN_PARAMETERS>
            ...
        </CONTROL_LIST>
      </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

V3.0

/api/3.0/fo/compliance/control/?action=list

[GET] [POST]

View a list of compliance controls which are visible to the user. Controls in the XML output are sorted by control ID in ascending order. Optional input parameters support filtering the list.

Using the Qualys user interface, it's possible to customize the list of frameworks at the subscription level. Under PC, go to Policies > Setup > Frameworks to customize the frameworks list. If the frameworks list is customized for your subscription, then the customized list of frameworks will appear in the controls list output returned by a control list API request.

Permissions

Note: The Compliance Control APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Users with PC enabled have the ability to view compliance controls.

Maximum Controls per API Request

The output of the Compliance Control API is paginated. By default, a maximum of 1,000 control records are returned per request. You can customize the page size (i.e. the number of control records) by using the parameter "truncation_limit=2000" for instance. In this case the results will be return with pages of 2,000 records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each control. A valid value is: None - show control ID only Basic (default) - show control ID and basic control information: the control category, sub-category, statement, and technology information All - show control ID, basic control information, and framework mappings
ids={value}	(Optional) Show only certain control IDs and/or ID ranges. Multiple entries are comma separated. One or more control IDs/ranges may be specified. A control ID range entry is specified with a hyphen (for example, 3000-3250). Valid control IDs are required.
id_min={value}	(Optional) Show only controls which have a minimum control ID value. A valid control ID is required.
id_max={value}	(Optional) Show only controls which have a maximum control ID value. A valid control ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See "Date Filters" below.

Parameter	Description
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See "Date Filters" below.
truncation_limit={value}	(Optional) The maximum number of control records processed per request. When not specified, the truncation limit is set to 1,000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records. You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is being downloaded.

Date Filters

The date/time is specified in YYYY-MM-DD{THH:MM:SSZ] format (UTC/GMT), like "2010-03-01" or "2010-03-01T23:12:00Z"

If you specify a date but no time as for example 2010-03-01, then the service automatically sets the time to 2010-03-01T00:00:00Z (the start of the day).

When date filters are specified using both input parameters for a single API request, both date filters are satisfied (ANDed).

DTD

<platform API server>/api/3.0/fo/compliance/control/control_list_output.dtd

Sample - Control List Output

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u
"yyyuser:Yuser@123#" -d "action=list"
"https://<qualys_base_url>/api/3.0/fo/compliance/control/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/3.0/fo/compliance/control/control_l
ist_output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2024-09-11T09:26:14Z</DATETIME>
```

```
    <CONTROL_LIST>
      <CONTROL>
      <ID>1044</ID>
        <UPDATE_DATE>2021-04-14T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-10-12T00:00:00Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Authorizations (Multi-user
ACL/role)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the
&apos;O7_DICTIONARY_ACCESSIBILITY&apos; setting in
init.ora]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[CRITICAL]]></LABEL>
          <VALUE>4</VALUE>
        </CRITICALITY>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>7</ID>
            <NAME>Oracle 9i</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>8</ID>
            <NAME>Oracle 10g</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
```

```
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>9</ID>
            <NAME>Oracle 11g</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>99</ID>
            <NAME>Oracle 12c</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
```

```
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>175</ID>
            <NAME>Oracle 18c</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>310</ID>
            <NAME>Oracle 12c Multitenant</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>311</ID>
            <NAME>Oracle 18c Multitenant</NAME>
            <RATIONALE><![CDATA[The 'O7_DICTIONARY_ACCESSIBILITY'
setting allows control/restrictions to be placed on the user's
```

```
SYSTEM privileges. If this parameter is set to TRUE, SYS schema
access will be allowed, which is the default for Oracle operations.
 Restricting this system privilege with a setting of FALSE will
allow users or roles granted SELECT ANY TABLE access to objects in
the normal schema, but disallow access to objects in the SYS
schema, unless access is specifically granted.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[FALSE]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>1045</ID>
        <UPDATE_DATE>2018-10-12T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-10-12T00:00:00Z</CREATED_DATE>
        <CATEGORY>OS Security Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[System Settings (OSI layers 6-
7)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the &apos;Clipbook&apos;
service (startup type)]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access.  As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
```

```
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>2</ID>
            <NAME>Windows 2003 Server</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access.  As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>12</ID>
            <NAME>Windows 2000</NAME>
            <RATIONALE><![CDATA[The 'Clipbook' service is used to
transfer Clipboard information across the LAN and is sent in clear
text.  The authentication required is a holdover from the 16-bit
'Network Dynamic Data Exchange' protocol, which is a 'network'
password among systems sharing the LAN, with a default set allow
READ for EVERYONE that has network access.  As this Windows service
is not required for any other system operations and increases
system vulnerability it should be disabled unless there is a
demonstrated need for its use set by the business.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
```

```
      <ID>1074</ID>
        <UPDATE_DATE>2022-03-10T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-10-17T00:00:00Z</CREATED_DATE>
        <CATEGORY>OS Security Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[Database Settings (non-Access
Control/Logging)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[The current list of ORACLE accounts
that not having &apos;Maximum Tablespace Quotas&apos; set to
&apos;unlimited&apos;]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[CRITICAL]]></LABEL>
          <VALUE>4</VALUE>
        </CRITICALITY>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>7</ID>
            <NAME>Oracle 9i</NAME>
            <RATIONALE><![CDATA[Through 'tablespace quotas,'
Oracle can limit the [collective] amount of disk storage made
available to objects in a schema.  This permits selective control
of the space consumed by those objects according to the schema
type.  Quotas should be set for each tablespace, which can
eliminate resource-contention/denial-of-service conditions, such
as having 'online comment' fields repeatedly filled in by a
malicious user's script, eventually consuming enough disk space to
cause the database to freeze.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>is contained in</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>8</ID>
            <NAME>Oracle 10g</NAME>
            <RATIONALE><![CDATA[Through 'tablespace quotas,'
Oracle can limit the [collective] amount of disk storage made
available to objects in a schema.  This permits selective control
of the space consumed by those objects according to the schema
type.  Quotas should be set for each tablespace, which can
eliminate resource-contention/denial-of-service conditions, such
as having 'online comment' fields repeatedly filled in by a
malicious user's script, eventually consuming enough disk space to
cause the database to freeze.]]></RATIONALE>
            <DATAPOINT>
```

```
                <CARDINALITY>is contained in</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>9</ID>
            <NAME>Oracle 11g</NAME>
            <RATIONALE><![CDATA[Through 'tablespace quotas,'
Oracle can limit the [collective] amount of disk storage made
available to objects in a schema.  This permits selective control
of the space consumed by those objects according to the schema
type.  Quotas should be set for each tablespace, which can
eliminate resource-contention/denial-of-service conditions, such
as having 'online comment' fields repeatedly filled in by a
malicious user's script, eventually consuming enough disk space to
cause the database to freeze.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>is contained in</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>99</ID>
            <NAME>Oracle 12c</NAME>
            <RATIONALE><![CDATA[Through 'tablespace quotas,'
Oracle can limit the [collective] amount of disk storage made
available to objects in a schema.  This permits selective control
of the space consumed by those objects according to the schema
type.  Quotas should be set for each tablespace, which can
eliminate resource-contention/denial-of-service conditions, such
as having 'online comment' fields repeatedly filled in by a
malicious user's script, eventually consuming enough disk space to
cause the database to freeze.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>is contained in</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
```

```
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
       <CONTROL>
        <ID>1331</ID>
        <UPDATE_DATE>2024-04-18T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-12-07T00:00:00Z</CREATED_DATE>
        <CATEGORY>OS Security Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[Network Settings (OSI Layers 2-
5)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the &apos;TCP packet
numbering sequence randomization&apos; (TCP_STRONG)
setting]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>4</ID>
            <NAME>Solaris 9.x</NAME>
            <RATIONALE><![CDATA[The 'sequence randomization' for
TCP packet numbering was designed to prevent malicious users from
crafting TCP packets, that could appear to be part of a pre-
existing TCP sequence from one host, while slipping in their own
packets from another.  (RFC 793 provides specifics on TCP design.)
 As various spoofing and hijacking attacks have been based upon the
ability to predict the sequence numbers of TCP packets, the method
outlined in RFC1948, using a strong algorithm to randomize TCP
sequence numbers, is the most secure option available for
protecting the packet sequence and should be applied as
appropriate to business needs.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[2]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>10</ID>
            <NAME>Solaris 10.x</NAME>
            <RATIONALE><![CDATA[The 'sequence randomization' for
TCP packet numbering was designed to prevent malicious users from
crafting TCP packets, that could appear to be part of a pre-
existing TCP sequence from one host, while slipping in their own
```

```
packets from another.  (RFC 793 provides specifics on TCP design.)
 As various spoofing and hijacking attacks have been based upon the
ability to predict the sequence numbers of TCP packets, the method
outlined in RFC1948, using a strong algorithm to randomize TCP
sequence numbers, is the most secure option available for
protecting the packet sequence and should be applied as
appropriate to business needs.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[2]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>46</ID>
            <NAME>Solaris 11.x</NAME>
            <RATIONALE><![CDATA[The 'sequence randomization' for
TCP packet numbering was designed to prevent malicious users from
crafting TCP packets, that could appear to be part of a pre-
existing TCP sequence from one host, while slipping in their own
packets from another.  (RFC 793 provides specifics on TCP design.)
 As various spoofing and hijacking attacks have been based upon the
ability to predict the sequence numbers of TCP packets, the method
outlined in RFC1948, using a strong algorithm to randomize TCP
sequence numbers, is the most secure option available for
protecting the packet sequence and should be applied as
appropriate to business needs.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[2]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>1332</ID>
        <UPDATE_DATE>2019-03-12T00:00:00Z</UPDATE_DATE>
        <CREATED_DATE>2007-12-07T00:00:00Z</CREATED_DATE>
        <CATEGORY>OS Security Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[Performance Monitoring  (All OSI
Layers)]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[Status of the &apos;Graphical User
```

```
Interface (GUI)&amp;apos; startup environment]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[MEDIUM]]></LABEL>
          <VALUE>2</VALUE>
        </CRITICALITY>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>3</ID>
            <NAME>Red Hat Enterprise Linux 3/4</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>4</ID>
            <NAME>Solaris 9.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to exist.
 (S99dtlogin)]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>5</ID>
            <NAME>HPUX 11.iv1</NAME>
```

```
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY/>
                  <OPERATOR>re</OPERATOR>
                  <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[(^DESKTOP=$|161803399999999|31415926535897
9)]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
           </TECHNOLOGY>
           <TECHNOLOGY>
             <ID>11</ID>
             <NAME>Red Hat Enterprise Linux 5.x</NAME>
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY/>
                  <OPERATOR>eq</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
           </TECHNOLOGY>
           <TECHNOLOGY>
             <ID>13</ID>
             <NAME>HPUX 11.iv2</NAME>
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
```

```
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>re</OPERATOR>
                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[(^DESKTOP=$|161803399999999|31415926535897
9)]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>14</ID>
            <NAME>Solaris 8.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to exist.
 (S99dtlogin)]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>15</ID>
            <NAME>SUSE Linux Enterprise 9/10</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
```

```
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>25</ID>
            <NAME>CentOS 4.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>26</ID>
            <NAME>CentOS 5.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>27</ID>
            <NAME>Debian GNU/Linux 5.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
```

```
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>matches</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>33</ID>
            <NAME>Oracle Enterprise Linux 4.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>34</ID>
            <NAME>Oracle Enterprise Linux 5.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[3]]></DEFAULT_VALUE>
```

```
                </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>35</ID>
              <NAME>AIX 6.x</NAME>
             <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY/>
                  <OPERATOR>eq</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[2]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>36</ID>
              <NAME>HPUX 11.iv3</NAME>
             <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY/>
                  <OPERATOR>re</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>38</ID>
              <NAME>SUSE Linux Enterprise 11.x</NAME>
             <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
```

```
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>43</ID>
            <NAME>CentOS 6.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>44</ID>
            <NAME>Oracle Enterprise Linux 6.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
```

```
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>45</ID>
            <NAME>Red Hat Enterprise Linux 6.x</NAME>
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>52</ID>
            <NAME>AIX 7.x</NAME>
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>eq</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[2]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>81</ID>
            <NAME>Red Hat Enterprise Linux 7.x</NAME>
            <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
```

```
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>94</ID>
            <NAME>SUSE Linux Enterprise 12.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>96</ID>
            <NAME>Ubuntu 14.x</NAME>
           <RATIONALE><![CDATA[The graphical user interface (GUI)
is set up through the kernel and provides windowing system, such as
GNOME or KDE, which can be used to conduct host operations.  As the
X-windows services used for supporting the GUI operations have
been compromised by a number of exploits, use of the GUI and its
associated processes should be disabled or restricted and used
only where a clear business need is determined to
exist.]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY/>
                <OPERATOR>ge</OPERATOR>
```

```
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[0]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
        </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

V4.0

/api/4.0/fo/compliance/control/?action=list

[GET] [POST]

View a list of compliance controls which are visible to the user. Controls in the XML output are sorted by control ID in ascending order. Optional input parameters support filtering the list.

Using the Qualys user interface, it's possible to customize the list of frameworks at the subscription level. Under PC, go to Policies > Setup > Frameworks to customize the frameworks list. If the frameworks list is customized for your subscription, then the customized list of frameworks will appear in the controls list output returned by a control list API request.

Permissions

Note: The Compliance Control APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

Users with PC enabled have the ability to view compliance controls.

Maximum Controls per API Request

The output of the Compliance Control API is paginated. By default, a maximum of 1,000 control records are returned per request. You can customize the page size (i.e. the number of control records) by using the parameter "truncation_limit=2000" for instance. In this case the results will be return with pages of 2,000 records.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each control. A valid value is: None - show control ID only Basic (default) - show control ID and basic control information: the control category, sub-category, statement, and technology information All - show control ID, basic control information, and framework mappings
ids={value}	(Optional) Show only certain control IDs and/or ID ranges. Multiple entries are comma separated. One or more control IDs/ranges may be specified. A control ID range entry is specified with a hyphen (for example, 3000-3250). Valid control IDs are required.
id_min={value}	(Optional) Show only controls which have a minimum control ID value. A valid control ID is required.
id_max={value}	(Optional) Show only controls which have a maximum control ID value. A valid control ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See “Date Filters” below.

Parameter	Description
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See "Date Filters" below.
truncation_limit={value}	(Optional) The maximum number of control records processed per request. When not specified, the truncation limit is set to 1,000 host records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records. You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is being downloaded.

Date Filters

The date/time is specified in YYYY-MM-DD{THH:MM:SSZ] format (UTC/GMT), like "2010-03-01" or "2010-03-01T23:12:00Z"

If you specify a date but no time as for example 2010-03-01, then the service automatically sets the time to 2010-03-01T00:00:00Z (the start of the day).

When date filters are specified using both input parameters for a single API request, both date filters are satisfied (ANDed).

DTD

<platform API server>/api/4.0/fo/compliance/control/control_list_output.dtd

Sample - Control List Output

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"quaylys_username:Password@" -d
"action=list&details=All&ids=100019"
"https://<qualys_base_url>/api/4.0/fo/compliance/control/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM "https://
<qualys_base_url>/api/4.0/fo/compliance/control/control_list_outpu
t.dtd">
    <CONTROL_LIST_OUTPUT>
        <RESPONSE>
```

```
            <DATETIME>2025-06-02T05:12:46Z</DATETIME>
            <CONTROL_LIST>
                <CONTROL>
                    <ID>100019</ID>
                   <UPDATE_DATE>2025-05-05T09:36:52Z</UPDATE_DATE>
                    <CREATED_DATE>2025-05-
05T09:14:23Z</CREATED_DATE>
                  <CATEGORY>Access Control Requirements</CATEGORY>
                    <SUB_CATEGORY>
                        <![CDATA[Authentication/Passwords]]>
                    </SUB_CATEGORY>
                    <STATEMENT>
                        <![CDATA[File Content Check-Manager]]>
                    </STATEMENT>
                    <CRITICALITY>
                        <LABEL>
                            <![CDATA[URGENT]]>
                        </LABEL>
                        <VALUE>5</VALUE>
                    </CRITICALITY>
                    <CHECK_TYPE>
                        <![CDATA[Unix File Content Check]]>
                    </CHECK_TYPE>
                    <COMMENT>
                        <![CDATA[]]>
                    </COMMENT>
                    <IS_ACTIVE>0</IS_ACTIVE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>
                        <FILE_PATH>
                            <![CDATA[c:/windows/notepad.exe]]>
                        </FILE_PATH>
                        <FILE_QUERY>
                            <![CDATA[.*]]>
                        </FILE_QUERY>
                        <DATA_TYPE>Line List</DATA_TYPE>
                        <EVALUATE_AS_STRING>0</EVALUATE_AS_STRING>
                        <DESCRIPTION>
                            <![CDATA[Test description]]>
                        </DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGY_LIST>
                        <TECHNOLOGY>
                            <ID>4</ID>
                            <NAME>Solaris 9.x</NAME>
```

```
                        <RATIONALE>
                            <![CDATA[Error]]>
                        </RATIONALE>
                        <DATAPOINT>
                          <CARDINALITY>match any</CARDINALITY>
                            <OPERATOR>re</OPERATOR>
                            <DEFAULT_VALUES total="1">
                                <DEFAULT_VALUE>
                                    <![CDATA[0]]>
                                </DEFAULT_VALUE>
                            </DEFAULT_VALUES>
                        </DATAPOINT>
                    </TECHNOLOGY>
                    <TECHNOLOGY>
                        <ID>10</ID>
                        <NAME>Solaris 10.x</NAME>
                        <RATIONALE>
                            <![CDATA[Error]]>
                        </RATIONALE>
                        <DATAPOINT>
                          <CARDINALITY>match any</CARDINALITY>
                            <OPERATOR>re</OPERATOR>
                            <DEFAULT_VALUES total="1">
                                <DEFAULT_VALUE>
                                    <![CDATA[0]]>
                                </DEFAULT_VALUE>
                            </DEFAULT_VALUES>
                        </DATAPOINT>
                    </TECHNOLOGY>
                </TECHNOLOGY_LIST>
            </CONTROL>
        </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/compliance/control/?action=list	Active	Active

API Version	EOS	EOL
/api/3.0/fo/compliance/control/?action=list	December 2025	December 2026
/api/2.0/fo/compliance/control/?action=list	December 2025	December 2026

Compliance Policy List

For API version information, refer to the API Version History section.

V2.0|V3.0|V4.0

V2.0

/api/2.0/fo/compliance/policy/?action=list

[GET] [POST]

View a list of compliance policies visible to the user. Policies in the XML output are sorted by compliance policy ID in ascending order. Optional input parameters support filtering the policy list output.

Maximum Policies per API Request

A maximum of 1,000 compliance policy records can be processed per request. If the requested list identifies more than 1,000 policies, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of policy records.

Permissions

Note: The Compliance APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

User Role	Permissions
Manager	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Auditor	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Unit Manager	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user's business unit, and groups created by any user in the same business unit.
Scanner	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.
Reader	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.

User Permissions — Asset Group Information

Asset group information included in the policy list output includes the following, as defined for each asset group: asset group ID, title, and assigned IP addresses. Users are granted permission to view asset group information assigned to policies when the user has permission to view the asset groups.

For example, when a user makes a request for a compliance policy list and the user does not have permission to view asset groups that are assigned to the target policies, then the asset group information does not appear in the policy list output. The asset group IDs are not listed under the <POLICY> section, and the asset group title and assigned IP addresses are not listed under the <GLOSSARY> section.

In a case where a user makes a request for a compliance policy list and the user does not have permission to see one or more asset groups assigned to a target policy, the following information is provided in the compliance policy list output:

<POLICY> section. The attribute "has_hidden_data=1" is returned in the <POLICY> section in the <ASSET_GROUP_IDS> element. This indicates that the user does not have permission to see one or more asset groups in the policy. When this attribute is present, only the asset group IDs that the user has permission to see, if any, are listed in the <ASSET_GROUP_IDS> element.

<GLOSSARY> section. Asset group information is not displayed for asset groups assigned to compliance policies that the user does not have permission to see.

<WARNING_LIST> section. A warning message is returned for informational purposes. This indicates that at least one of the compliance policies in the output has one or more asset groups that the user does not have permission to see.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show requested amount of information for each policy. A valid value is: None — show policy ID only Basic (default) — show policy ID and title, date/time when the policy was created and last modified, asset groups included, asset tags included, controls included, whether the Evaluate Now option was selected, whether the policy is locked, and glossary of compliance policy data in the output. All — show the basic policy information, plus a technology list for each control, IP list for each asset group, and a user list

Parameter	Description
ids={value}	(Optional) Show only certain policy IDs and/or ID ranges. One or more policy IDs/ranges may be specified. Multiple entries are comma separated. A policy ID range entry is specified with a hyphen (for example, 160-165). Valid policy IDs are required.
id_min={value}	(Optional) Show only policies which have a minimum policy ID value. A valid policy ID is required.
id_max={value}	(Optional) Show only policies which have a maximum policy ID value. A valid policy ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See Date Filters.
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See Date Filters.

DTD

<platform API server>/api/2.0/fo/compliance/policy/policy_list_output.dtd

Sample - Compliance Policy List

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -D
headers.15
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=list"
```

XML output:

```
<POLICY_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-11-03T21:15:29Z</DATETIME>
    <POLICY_LIST>
      <POLICY>
        <ID>18948</ID>
        <TITLE><![CDATA[XP policy]]></TITLE>
        <CREATED>
          <DATETIME>2017-10-19T18:37:15Z</DATETIME>
          <BY>quays_as</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2017-10-26T23:31:57Z</DATETIME>
          <BY>quays_as</BY>
        </LAST_MODIFIED>
        <LAST_EVALUATED>
          <DATETIME>2017-11-03T08:40:44Z</DATETIME>
        </LAST_EVALUATED>
        <STATUS><![CDATA[active]]></STATUS>
```

```
        <IS_LOCKED>0</IS_LOCKED>
        <EVALUATE_NOW><![CDATA[yes]]></EVALUATE_NOW>
        <ASSET_GROUP_IDS>6065</ASSET_GROUP_IDS>
        <TAG_SET_INCLUDE>
          <TAG_ID>7588415</TAG_ID>
        </TAG_SET_INCLUDE>
        <TAG_INCLUDE_SELECTOR>ANY</TAG_INCLUDE_SELECTOR>
        <INCLUDE_AGENT_IPS>1</INCLUDE_AGENT_IPS>
        <CONTROL_LIST>
          <CONTROL>
            <ID>1045</ID>
            <STATEMENT><![CDATA[Status of the 'Clipbook' service
(startup type)]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[SERIOUS]]></LABEL>
              <VALUE>3</VALUE>
            </CRITICALITY>
          </CONTROL>
          <CONTROL>
            <ID>1048</ID>
            <STATEMENT><![CDATA[Status of the 'Shutdown: Clear
virtual memory pagefile' setting]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[CRITICAL]]></LABEL>
              <VALUE>4</VALUE>
            </CRITICALITY>
          </CONTROL>
        </CONTROL_LIST>
      </POLICY>
    </POLICY_LIST>
    <GLOSSARY>
      <ASSET_GROUP_LIST>
        <ASSET_GROUP>
          <ID>6065</ID>
          <TITLE><![CDATA[Windows XP]]></TITLE>
        </ASSET_GROUP>
      </ASSET_GROUP_LIST>
      <ASSET_TAG_LIST>
        <TAG>
          <TAG_ID>7588415</TAG_ID>
          <TAG_NAME>windows XP</TAG_NAME>
        </TAG>
      </ASSET_TAG_LIST>
    </GLOSSARY>
  </RESPONSE>
</POLICY_LIST_OUTPUT>
```

V3.0

/api/3.0/fo/compliance/policy/?action=list

[GET] [POST]

View a list of compliance policies visible to the user. Policies in the XML output are sorted by compliance policy ID in ascending order. Optional input parameters support filtering the policy list output.

Maximum Policies per API Request

A maximum of 1,000 compliance policy records can be processed per request. If the requested list identifies more than 1,000 policies, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of policy records.

Permissions

Note: The Compliance APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

User Role	Permissions
Manager	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Auditor	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Unit Manager	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user's business unit, and groups created by any user in the same business unit.
Scanner	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.
Reader	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.

User Permissions — Asset Group Information

Asset group information included in the policy list output includes the following, as defined for each asset group: asset group ID, title, and assigned IP addresses. Users are granted permission to view asset group information assigned to policies when the user has permission to view the asset groups.

For example, when a user makes a request for a compliance policy list and the user does not have permission to view asset groups that are assigned to the target policies, then the asset group information does not appear in the policy list output. The asset group IDs are not listed under the <POLICY> section, and the asset group title and assigned IP addresses are not listed under the <GLOSSARY> section.

In a case where a user makes a request for a compliance policy list and the user does not have permission to see one or more asset groups assigned to a target policy, the following information is provided in the compliance policy list output:

<POLICY> section. The attribute "has_hidden_data=1" is returned in the <POLICY> section in the <ASSET_GROUP_IDS> element. This indicates that the user does not have permission to see one or more asset groups in the policy. When this attribute is present, only the asset group IDs that the user has permission to see, if any, are listed in the <ASSET_GROUP_IDS> element.

<GLOSSARY> section. Asset group information is not displayed for asset groups assigned to compliance policies that the user does not have permission to see.

<WARNING_LIST> section. A warning message is returned for informational purposes. This indicates that at least one of the compliance policies in the output has one or more asset groups that the user does not have permission to see.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show requested amount of information for each policy. A valid value is: None — show policy ID only Basic (default) — show policy ID and title, date/time when the policy was created and last modified, asset groups included, asset tags included, controls included, whether the Evaluate Now option was selected, whether the policy is locked, and glossary of compliance policy data in the output. All — show the basic policy information, plus a technology list for each control, IP list for each asset group, and a user list

Parameter	Description
ids={value}	(Optional) Show only certain policy IDs and/or ID ranges. One or more policy IDs/ranges may be specified. Multiple entries are comma separated. A policy ID range entry is specified with a hyphen (for example, 160-165). Valid policy IDs are required.
id_min={value}	(Optional) Show only policies which have a minimum policy ID value. A valid policy ID is required.
id_max={value}	(Optional) Show only policies which have a maximum policy ID value. A valid policy ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See Date Filters.
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See Date Filters.

DTD

<platform API server>/api/3.0/fo/compliance/policy/policy_list_output.dtd

Sample - Compliance Policy List

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"username:Password#" -d "action=list&details=Basic&ids=5744989"
"https://qualysapi.qualys.com/api/3.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/3.0/fo/compliance/policy/policy_
list_output.dtd">
<POLICY_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-06-30T06:26:19Z</DATETIME>
        <POLICY_LIST>
            <POLICY>
                <ID>5744989</ID>
                <TITLE>
                    <![CDATA[One UDC]]>
                </TITLE>
                <CREATED>
                    <DATETIME>2025-06-25T15:04:04Z</DATETIME>
                    <BY>ctxta</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2025-06-27T11:57:34Z</DATETIME>
                    <BY>ctxta</BY>
```

```
                </LAST_MODIFIED>
                <LAST_EVALUATED>
                    <DATETIME>2025-06-30T06:01:44Z</DATETIME>
                </LAST_EVALUATED>
                <STATUS>
                    <![CDATA[active]]>
                </STATUS>
                <IS_LOCKED>0</IS_LOCKED>
                <EVALUATE_NOW>
                    <![CDATA[yes]]>
                </EVALUATE_NOW>

<ASSET_GROUP_IDS>10898081,10919108,10926154,10996581,11000130,1100
0163-
11000164,11024194,11035730,11072689,11076105,11080595,11080756,110
81917,11111120</ASSET_GROUP_IDS>
                <CONTROL_LIST>
                    <CONTROL>
                        <ID>1071</ID>
                        <STATEMENT>
                          <![CDATA[Status of the 'Minimum Password
Length' setting]]>
                        </STATEMENT>
                        <CRITICALITY>
                            <LABEL>
                                <![CDATA[URGENT]]>
                            </LABEL>
                            <VALUE>5</VALUE>
                        </CRITICALITY>
                        <STATUS>
                            <![CDATA[Active]]>
                        </STATUS>
                    </CONTROL>
                    <CONTROL>
                        <ID>100000</ID>
                        <STATEMENT>
                            <![CDATA[CitiJSONUDC2]]>
                        </STATEMENT>
                        <CRITICALITY>
                            <LABEL>
                                <![CDATA[URGENT]]>
                            </LABEL>
                            <VALUE>5</VALUE>
                        </CRITICALITY>
                        <STATUS>
                            <![CDATA[Active]]>
```

```
                </STATUS>
            </CONTROL>
        </CONTROL_LIST>
    </POLICY>
</POLICY_LIST>
<GLOSSARY>
    <ASSET_GROUP_LIST>
        <ASSET_GROUP>
            <ID>10898081</ID>
            <TITLE>
                <![CDATA[IBMDB2]]>
            </TITLE>
            <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
        <ASSET_GROUP>
            <ID>10919108</ID>
            <TITLE>
                <![CDATA[Inflobox AG]]>
            </TITLE>
            <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
        <ASSET_GROUP>
            <ID>10926154</ID>
            <TITLE>
                <![CDATA[ip agent merge case]]>
            </TITLE>
            <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
        <ASSET_GROUP>
            <ID>11081917</ID>
            <TITLE>
                <![CDATA[pyscand ag3]]>
            </TITLE>
            <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
        <ASSET_GROUP>
            <ID>11111120</ID>
            <TITLE>
                <![CDATA[Windows AG nEw]]>
            </TITLE>
            <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
        <ASSET_GROUP>
            <ID>10996581</ID>
            <TITLE>
```

```
            <![CDATA[dtest AG]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11000130</ID>
        <TITLE>
            <![CDATA[Windows AG]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11000163</ID>
        <TITLE>
            <![CDATA[Vcenter]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11000164</ID>
        <TITLE>
            <![CDATA[VMagentPCIP]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11024194</ID>
        <TITLE>
            <![CDATA[PC Only Ip]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11035730</ID>
        <TITLE>
            <![CDATA[1.1.1.1]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
    </ASSET_GROUP>
    <ASSET_GROUP>
        <ID>11072689</ID>
        <TITLE>
            <![CDATA[red hat 8]]>
        </TITLE>
        <NETWORK_ID>0</NETWORK_ID>
```

```
                    </ASSET_GROUP>
                    <ASSET_GROUP>
                        <ID>11076105</ID>
                        <TITLE>
                            <![CDATA[pyscand ag2]]>
                        </TITLE>
                        <NETWORK_ID>0</NETWORK_ID>
                    </ASSET_GROUP>
                    <ASSET_GROUP>
                        <ID>11080595</ID>
                        <TITLE>
                            <![CDATA[windows and unix agent ip]]>
                        </TITLE>
                        <NETWORK_ID>0</NETWORK_ID>
                    </ASSET_GROUP>
                    <ASSET_GROUP>
                        <ID>11080756</ID>
                        <TITLE>
                            <![CDATA[RDS]]>
                        </TITLE>
                        <NETWORK_ID>0</NETWORK_ID>
                    </ASSET_GROUP>
                </ASSET_GROUP_LIST>
            </GLOSSARY>
        </RESPONSE>
    </POLICY_LIST_OUTPUT>
```

V4.0

/api/4.0/fo/compliance/policy/?action=list

[GET] [POST]

View a list of compliance policies visible to the user. Policies in the XML output are sorted by compliance policy ID in ascending order. Optional input parameters support filtering the policy list output.

Maximum Policies per API Request

A maximum of 1,000 compliance policy records can be processed per request. If the requested list identifies more than 1,000 policies, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of policy records.

Permissions

Note: The Compliance APIs are available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

User Role	Permissions
Manager	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Auditor	View all compliance policies in subscription. View asset group information for all asset groups assigned to policies.
Unit Manager	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user's business unit, and groups created by any user in the same business unit.
Scanner	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.
Reader	View all compliance policies in subscription. View asset group information for asset groups assigned to policies, when the user has permission to view these asset groups. This user can view groups assigned to the user account, and groups created by the user.

User Permissions — Asset Group Information

Asset group information included in the policy list output includes the following, as defined for each asset group: asset group ID, title, and assigned IP addresses. Users are granted permission to view asset group information assigned to policies when the user has permission to view the asset groups.

For example, when a user makes a request for a compliance policy list and the user does not have permission to view asset groups that are assigned to the target policies, then the asset group information does not appear in the policy list output. The asset group IDs are not listed under the <POLICY> section, and the asset group title and assigned IP addresses are not listed under the <GLOSSARY> section.

In a case where a user makes a request for a compliance policy list and the user does not have permission to see one or more asset groups assigned to a target policy, the following information is provided in the compliance policy list output:

<POLICY> section. The attribute "has_hidden_data=1" is returned in the <POLICY> section in the <ASSET_GROUP_IDS> element. This indicates that the user does not have permission to see one or more asset groups in the policy. When this attribute is present, only the asset group IDs that the user has permission to see, if any, are listed in the <ASSET_GROUP_IDS> element.

<GLOSSARY> section. Asset group information is not displayed for asset groups assigned to compliance policies that the user does not have permission to see.

<WARNING_LIST> section. A warning message is returned for informational purposes. This indicates that at least one of the compliance policies in the output has one or more asset groups that the user does not have permission to see.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
details={**Basic**|All|None}	(Optional) Show requested amount of information for each policy. A valid value is: None — show policy ID only Basic (default) — show policy ID and title, date/time when the policy was created and last modified, asset groups included, asset tags included, controls included, whether the Evaluate Now option was selected, whether the policy is locked, and glossary of compliance policy data in the output. All — show the basic policy information, plus a technology list for each control, IP list for each asset group, and a user list
ids={value}	(Optional) Show only certain policy IDs and/or ID ranges. One or more policy IDs/ranges may be specified. Multiple entries are comma separated. A policy ID range entry is specified with a hyphen (for example, 160-165). Valid policy IDs are required.
id_min={value}	(Optional) Show only policies which have a minimum policy ID value. A valid policy ID is required.
id_max={value}	(Optional) Show only policies which have a maximum policy ID value. A valid policy ID is required.
updated_after_datetime={value}	(Optional) Show only controls updated after a certain date/time. See Date Filters.
created_after_datetime={value}	(Optional) Show only controls created after a certain date/time. See Date Filters.

DTD

<platform API server>/api/4.0/fo/compliance/policy/policy_list_output.dtd

Sample - Compliance Policy List

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "username:password@" -d
"action=list&details=Basic&ids=1538419"
"https://<qualys_base_url>/api/4.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_LIST_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/compliance/policy/policy_list_outpu
t.dtd">
<POLICY_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2025-07-11T10:13:20Z</DATETIME>
    <POLICY_LIST>
      <POLICY>
        <ID>1538419</ID>
        <TITLE><![CDATA[PC-33757]]></TITLE>
        <CREATED>
          <DATETIME>2025-07-07T05:40:23Z</DATETIME>
          <BY>quays_ca7</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2025-07-10T07:05:28Z</DATETIME>
          <BY>quays_ca7</BY>
        </LAST_MODIFIED>
        <LAST_EVALUATED>
          <DATETIME>2025-07-10T07:06:34Z</DATETIME>
        </LAST_EVALUATED>
        <STATUS><![CDATA[active]]></STATUS>
        <IS_LOCKED>0</IS_LOCKED>
        <EVALUATE_NOW><![CDATA[yes]]></EVALUATE_NOW>
        <ASSET_GROUP_IDS>54114745</ASSET_GROUP_IDS>
        <CONTROL_LIST>
          <CONTROL>
            <ID>1071</ID>
            <STATEMENT><![CDATA[Status of the 'Minimum Password Length'
setting]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <STATUS><![CDATA[Active]]></STATUS>
          </CONTROL>
          <CONTROL>
            <ID>1073</ID>
            <STATEMENT><![CDATA[Status of the 'Maximum Password Age'
setting (expiration) / Accounts having the 'password never expires' flag
set]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <STATUS><![CDATA[Inactive]]></STATUS>
          </CONTROL>
          <CONTROL>
            <ID>100017</ID>
            <STATEMENT><![CDATA[File Directory
Existence_Manager]]></STATEMENT>
```

```
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <STATUS><![CDATA[Inactive]]></STATUS>
          </CONTROL>
          <CONTROL>
            <ID>100018</ID>
            <STATEMENT><![CDATA[File/Directory Permission-
Manager]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <STATUS><![CDATA[Active]]></STATUS>
          </CONTROL>
          <CONTROL>
            <ID>100021</ID>
            <STATEMENT><![CDATA[Unix Directory Search Check-
Manager]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <STATUS><![CDATA[Active]]></STATUS>
          </CONTROL>
        </CONTROL_LIST>
      </POLICY>
    </POLICY_LIST>
    <GLOSSARY>
      <ASSET_GROUP_LIST>
        <ASSET_GROUP>
          <ID>54114745</ID>
          <TITLE><![CDATA[10.11.70.160]]></TITLE>
          <NETWORK_ID>0</NETWORK_ID>
        </ASSET_GROUP>
      </ASSET_GROUP_LIST>
    </GLOSSARY>
  </RESPONSE>
</POLICY_LIST_OUTPUT>
```

Sample - View Response Progress Updates

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With: Curl" -X "POST" -d
"action=list" "<qualys_base_url>/api/4.0/fo/compliance/policy/">
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/4.0/fo/compliance/policy/policy_list_output.dtd">
<POLICY_LIST_OUTPUT>
```

```
  <RESPONSE>
    <DATETIME>2026-05-28T09:44:19Z</DATETIME>
<!-- Loading policy tags: 9/581 processed -->
<!-- Loading policy tags: 22/581 processed -->
<!-- Loading policy tags: 33/581 processed -->
<!-- Loading policy tags: 44/581 processed -->
<!-- Loading policy tags: 52/581 processed -->
<!-- Loading policy tags: 62/581 processed -->
<!-- Loading policy tags: 74/581 processed -->
<!-- Loading policy tags: 84/581 processed -->
<!-- Loading policy tags: 96/581 processed -->
<!-- Loading policy tags: 106/581 processed -->
<!-- Loading policy tags: 119/581 processed -->
<!-- Loading policy tags: 128/581 processed -->
<!-- Loading policy tags: 138/581 processed -->
<!-- Loading policy tags: 154/581 processed -->
<!-- Loading policy tags: 169/581 processed -->
<!-- Loading policy tags: 179/581 processed -->
<!-- Loading policy tags: 191/581 processed -->
<!-- Loading policy tags: 203/581 processed -->
<!-- Loading policy tags: 214/581 processed -->
<!-- Loading policy tags: 227/581 processed -->
<!-- Loading policy tags: 242/581 processed -->
<!-- Loading policy tags: 253/581 processed -->
<!-- Loading policy tags: 262/581 processed -->
<!-- Loading policy tags: 270/581 processed -->
<!-- Loading policy tags: 281/581 processed -->
<!-- Loading policy tags: 295/581 processed -->
<!-- Loading policy tags: 308/581 processed -->
<!-- Loading policy tags: 318/581 processed -->
<!-- Loading policy tags: 329/581 processed -->
<!-- Loading policy tags: 342/581 processed -->
<!-- Loading policy tags: 355/581 processed -->
<!-- Loading policy tags: 362/581 processed -->
<!-- Loading policy tags: 371/581 processed -->
<!-- Loading policy tags: 378/581 processed -->
<!-- Loading policy tags: 386/581 processed -->
<!-- Loading policy tags: 393/581 processed -->
<!-- Loading policy tags: 401/581 processed -->
<!-- Loading policy tags: 408/581 processed -->
<!-- Loading policy tags: 415/581 processed -->
<!-- Loading policy tags: 423/581 processed -->
<!-- Loading policy tags: 430/581 processed -->
<!-- Loading policy tags: 438/581 processed -->
<!-- Loading policy tags: 445/581 processed -->
<!-- Loading policy tags: 452/581 processed -->
<!-- Loading policy tags: 459/581 processed -->
<!-- Loading policy tags: 467/581 processed -->
<!-- Loading policy tags: 474/581 processed -->
<!-- Loading policy tags: 481/581 processed -->
<!-- Loading policy tags: 488/581 processed -->
<!-- Loading policy tags: 495/581 processed -->
<!-- Loading policy tags: 502/581 processed -->
<!-- Loading policy tags: 509/581 processed -->
```

```
<!-- Loading policy tags: 517/581 processed -->
<!-- Loading policy tags: 524/581 processed -->
<!-- Loading policy tags: 531/581 processed -->
<!-- Loading policy tags: 538/581 processed -->
<!-- Loading policy tags: 546/581 processed -->
<!-- Loading policy tags: 553/581 processed -->
<!-- Loading policy tags: 561/581 processed -->
<!-- Loading policy tags: 568/581 processed -->
<!-- Loading policy tags: 575/581 processed -->
<!-- Loading policy tags: 581/581 processed -->
    <POLICY_LIST>
      <POLICY>
        <ID>195889</ID>
        <TITLE><![CDATA[CIS_1 Centos 6]]></TITLE>
        <CREATED>
          <DATETIME>2023-11-07T11:38:00Z</DATETIME>
          <BY>quays_fd4</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2024-01-08T13:43:29Z</DATETIME>
          <BY>quays_fd4</BY>
        </LAST_MODIFIED>
        <LAST_EVALUATED>
          <DATETIME>2023-11-26T23:39:22Z</DATETIME>
        </LAST_EVALUATED>
        <STATUS><![CDATA[active]]></STATUS>
        <IS_LOCKED>0</IS_LOCKED>
        <EVALUATE_NOW><![CDATA[no]]></EVALUATE_NOW>
        <TAG_SET_INCLUDE>
          <TAG_ID>29749348</TAG_ID>
        </TAG_SET_INCLUDE>
        <TAG_INCLUDE_SELECTOR>ANY</TAG_INCLUDE_SELECTOR>
        <CONTROL_LIST>
.
.
.
.
.
.
.
.
.
.
.
.
.
            <TAG_ID>42670845</TAG_ID>
            <TAG_NAME><![CDATA[dtest tag]]></TAG_NAME>
          </TAG>
          <TAG>
            <TAG_ID>42670846</TAG_ID>
            <TAG_NAME><![CDATA[dtest tag 2]]></TAG_NAME>
          </TAG>
          <TAG>
```

```
            <TAG_ID>42670847</TAG_ID>
            <TAG_NAME><![CDATA[dtest tag 3]]></TAG_NAME>
          </TAG>
        </ASSET_INCLUDE_TAG_LIST>
      </ASSET_TAG_LIST>
    </GLOSSARY>
  </RESPONSE>
</POLICY_LIST_OUTPUT>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/compliance/policy/?action=list	Active	Active
/api/3.0/fo/compliance/policy/?action=list	December 2025	December 2026
/api/2.0/fo/compliance/policy/?action=list	December 2025	December 2026

Compliance Policy - Export

For API version information, refer to the API Version History section.

V2.0|V3.0|V4.0

V2.0

/api/2.0/fo/compliance/policy/?action=export

[GET] [POST]

Export compliance policies from your account to an XML file. Service provided controls are exported and you can choose to also export user defined controls. The output also includes an appendix with human readable look-ups for control descriptions, giving you explanation on the various aspects of control description and evaluation.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=export	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id={value} or title={value}	(Required) The ID or the title of the policy you want to export.
show_user_controls={**0**|1}	(Optional) Set to 1 to include user-defined controls (UDCs) in the XML output. For Qualys Custom Controls you'll see the UDC ID for each control in the output.When not specified, UDCs are not included. Interested in Qualys Custom Controls? Log in to Qualys, go to Help > Online Help and search for "custom controls".
show_appendix={**0**|1}	(Optional) Set to 1 to show the appendix section in the XML output. When unspecified, the appendix section is not included in the output.

Sample - Export Policy

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=export&id=853744"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0 encoding=UTF-8" ?>
```

```
<DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2/fo/compliance/policy/policy_ex
port_output.dtd">
<POLICY>
    <TITLE><![CDATA[My Policy]]></TITLE>
    <EXPORTED><![CDATA[2013-07-17T18:19:57Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Default section]]></HEADING>
            <CONTROLS total="20">
                <CONTROL>
                    <ID>1111</ID>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>1</ID>
                            <NAME>Windows XP desktop</NAME>
                            <EVALUATE
checksum="74378d12a39f82721a3cb156dee58c663a650a9ce422bd311b5e5443
c2a20f14">&lt;CTRL&gt;&lt;NOT&gt;&lt;DP&gt;&lt;K&gt;auth.general.l
ogintext&lt;/K&gt;&lt;OP&gt;re&lt;/OP&gt;&lt;V&gt;&lt;![CDATA[^(\s
*|314159265358979|161803399999999)$]]&gt;&lt;/V&gt;&lt;/DP&gt;&lt;
/NOT&gt;&lt;/CTRL&gt;</EVALUATE>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                </CONTROL>
        </SECTION>
    </SECTIONS>
</POLICY>
```

Sample - Export Policy with Appendix with lookups for control descriptions

API request:

```
curl -u "USERNAME:PASSWORD" GET -H "X-Requested-With: curl" -X
"POST" -d "action=export&id=5438&show_appendix=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/">showA
pp.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-09-09T09:07:13Z</DATETIME>
   <POLICY>
    <TITLE><![CDATA[Solaris]]></TITLE>
    <EXPORTED><![CDATA[2017-09-09T09:07:12Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="4">
        <TECHNOLOGY>
            <ID>4</ID>
            <NAME>Solaris 9.x</NAME>
        </TECHNOLOGY>
...
   <SECTION>
            <NUMBER>3</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="4"/>
        </SECTION>
    </SECTIONS>
    <!--Note : Remove APPENDIX section if you wish to import this
     XML as policy.-->
    <APPENDIX>
        <OP_ACRONYMS><OP id="lt">less than</OP>
                     <OP id="gt">greater than</OP>
                     <OP id="le">less than or equal to</OP>
                     <OP id="ge">greater than or equal to</OP>
                     <OP id="ne">not equal to</OP>
                    <OP id="xeq">list OR string list</OP>
                     <OP id="eq">equal to</OP>
                     <OP id="in">in</OP>
                     <OP id="xre">regular expression list</OP>
                     <OP id="re">regular expression</OP>
                     <OP id="range">in range</OP></OP_ACRONYMS>
        <DATA_POINT_ACRONYMS>
            <DP>
                <K id="auth.useraccount.legacy-plus-
accounts"><![CDATA[The following List String value(s) <B>X</B>
indicate the current list of accounts defined within the
<B>/etc/group
</B>, <B>/etc/shadow</B>, and/or <B>/etc/passwd</B> files having a
```

```
<B>plus-sign '+'</B> preceding them.]]></K>
                <FV id="161803399999999"><![CDATA[Setting not
found]]></FV>
               <FV id="314159265358979"><![CDATA[File not
found]]></FV>
            </DP>
            <DP>
                <K id="auth.useraccount.minimum-password-length">
                 <![CDATA[This Integer value <B>X</B> indicates the
                   current status of the <B>PASSLENGTH 'minimum
password
                   length'</B> setting within the
<B>/etc/default/passwd
                   </B> file.]]></K>
                <FV id="161803399999999"><![CDATA[Setting not
found]]></FV>
               <FV id="314159265358979"><![CDATA[File not
found]]></FV>
            </DP>
     ...
    </DATA_POINT_ACRONYMS>
    </APPENDIX>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Sample - Export Library Policy to XML

You can export a library compliance policy from your account to an XML file. Just like with user created policies you must specify the input parameter show_user_controls=1 to include UDCs in the output. When the policy includes a Qualys Custom Control you'll see the UDC ID for the control in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=export&ids=991742279&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<POLICY>
    <TITLE><![CDATA[Library Policy with 2 UDC v.2.0]]></TITLE>
    <EXPORTED><![CDATA[2017-04-17T15:02:56Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="2">
        <TECHNOLOGY>
```

```
            <ID>2</ID>
            <NAME>Windows 2003 Server</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>12</ID>
            <NAME>Windows 2000</NAME>
        </TECHNOLOGY>
        </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="1">
                <USER_DEFINED_CONTROL>
                    <ID>100005</ID>
                    <UDC_ID>55449d95-1877-7ee5-829a-
4eededacb04f</UDC_ID>
                    <CHECK_TYPE>Registry Value
Existence</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                        <NAME><![CDATA[Access Control
Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1007</ID>

<NAME><![CDATA[Authentication/Passwords]]></NAME>
                    </SUB_CATEGORY>
...
```

Updates you'll see once Agent UDC support is available

New Agent UDC Support will be announced soon via the Qualys Technology blog once remaining components are released.

The XML output may include the USE_AGENT_ONLY element for these Windows and Unix control types: Directory Search Control and Directory Integrity Control. This is set to 1 when the "Use agent scan only" option is enabled for the control.

The XML output may include the AUTO_UPDATE element for these Windows and Unix control types: File Integrity Control and Directory Integrity Control. This is set to 1 when the "Auto update expected value" option is enabled for the control.

Sample - Export Policy when Agent UDC Support is available

API request:

```
curl -u username:password -H "X-Requested-With: curl" -d
"action=export&id=1448425&show_user_controls=1&show_appendix=0"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/">UDCWI
ND.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-10-05T10:41:43Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Windows_Linux_UDC_Policy]]></TITLE>
    <EXPORTED><![CDATA[2018-10-05T10:41:43Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="3">
        <TECHNOLOGY>
            <ID>45</ID>
            <NAME>Red Hat Enterprise Linux 6.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>52</ID>
            <NAME>AIX 7.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>81</ID>
            <NAME>Red Hat Enterprise Linux 7.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[ddd]]></HEADING>
            <CONTROLS total="4">
                <USER_DEFINED_CONTROL>
                    <ID>100041</ID>
                    <UDC_ID>929a8c4e-5057-e3f3-8225-
e92d4076f499</UDC_ID>
                    <CHECK_TYPE>Unix Directory Search
Check</CHECK_TYPE>
```

```
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                        <NAME><![CDATA[Access Control
Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1010</ID>
                        <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[Directory
Search]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
...
```

Sample: Export Policy when Case Sensitive Search is disabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=export&id=4034697&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML Output:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-07-22T08:33:50Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Suse 11 DI and DS check]]></TITLE>
    <EXPORTED><![CDATA[2021-07-22T08:33:48Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="2">
        <TECHNOLOGY>
            <ID>38</ID>
            <NAME>SUSE Linux Enterprise 11.x</NAME>
        </TECHNOLOGY>
...
```

```
                <USER_DEFINED_CONTROL>
                    <ID>100550</ID>
                    <UDC_ID>74d487e1-6c1c-5de7-8063-a878edc046d7</UDC_ID>
                    <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                      <NAME><![CDATA[Access Control Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1010</ID>
                        <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[Basic Directory Search Check-
UNIX_edited]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[MEDIUM]]></LABEL>
                        <VALUE>2</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[Directory Search Check]]></COMMENT>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                    <SCAN_PARAMETERS>

<BASE_DIR><![CDATA[/etc/123/yyy/eeee/lll]]></BASE_DIR>
                       <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>
...
                        <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>
                        <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                        <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE
_SEARCH>
                        <DATA_TYPE>String List</DATA_TYPE>
                        <DESCRIPTION><![CDATA[Directory Search
Check]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    ...
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
            </CONTROLS>
        </SECTION>
    </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Database UDCs for MS SQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2

You can create custom controls for MSSQL, Oracle, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2 databases. To support database controls, we've added new elements to the XML output and DTDs for Control List Output and Policy Export Output.

Sample - Policy API

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=export&id=1358790&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/">
PolicyExportAPI.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
   <RESPONSE>
    <DATETIME>2019-05-21T18:49:06Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Objects_Check]]></TITLE>
    <EXPORTED><![CDATA[2019-05-21T18:49:06Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
      ...
        <USER_DEFINED_CONTROL>
                    <ID>100338</ID>
                    <UDC_ID>e9ff3da7-9d0c-4a64-8055-
e49a3f88f838</UDC_ID>
                    <CHECK_TYPE>Oracle Database Check</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>5</ID>
                        <NAME><![CDATA[Services]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1024</ID>
                        <NAME><![CDATA[Support]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[STMT:SELECT * FROM
user_tables;]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[MEDIUM]]></LABEL>
```

```
                        <VALUE>2</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[SELECT * FROM
user_tables]]></COMMENT>
                    <IGNORE_ERROR>1</IGNORE_ERROR>
                    <ERROR_SET_STATUS>PASS</ERROR_SET_STATUS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>8</ID>
                            <NAME>Oracle 10g</NAME>

<EVALUATE><CTRL><AND><OR><DP><K>custom.oracle_query.1661091</K><OP
>xre</OP><CD>matches</CD><FV set="1">No data
found</FV><DT>5</DT><V><![CDATA[.*]]></V><DBCOL><![CDATA[STATUS]]>
</DBCOL></DP></OR><DP><K>custom.oracle_query.1661091</K><L>0</L><O
P>eq</OP><DT>4</DT><CD>match
all</CD><V>2</V><DBCOL>NUM_ROWS</DBCOL></DP></AND></CTRL></EVALUAT
E>
                            <RATIONALE><![CDATA[rat:SELECT * FROM
user_tables]]></RATIONALE>
                            <DB_QUERY><![CDATA[SELECT * FROM
user_tables;]]></DB_QUERY>
                          <DESCRIPTION><![CDATA[des:SELECT * FROM
user_tables]]></DESCRIPTION>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
 ...
      </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Sample - Export Policy for File Content Check

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=export&id=1758961&show_user_controls=1"
"<qualys_base_url>/api/2.0/fo/compliance/policy/">
FCCWin_Policy_Export.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
```

```
<RESPONSE>
    <DATETIME>2019-10-14T21:21:45Z</DATETIME>
<POLICY>

<TITLE><![CDATA[SamplePolicyWithFileContentSearchUDCs]]></TITLE>
    <EXPORTED><![CDATA[2019-10-14T21:21:45Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>75</ID>
            <NAME>Windows Server 2012 R2</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="3">
                <USER_DEFINED_CONTROL>
                    <ID>100006</ID>
                    <UDC_ID>98e7dde1-412d-4a95-8262-
b7bd168ebad8</UDC_ID>
                    <CHECK_TYPE>Windows File Content
Check</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>8</ID>
                        <NAME><![CDATA[Database Settings]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1044</ID>
                       <NAME><![CDATA[DB Access Controls]]></NAME>
                    </SUB_CATEGORY>

<STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[min]]></LABEL>
                        <VALUE>1</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>
```

```
                        <PATH_TYPE><![CDATA[Use Registry
key]]></PATH_TYPE>
                        <REG_HIVE><![CDATA[HKEY_CLASSES_ROOT
(HKCR)]]></REG_HIVE>
                       <REG_KEY><![CDATA[TestKey\user]]></REG_KEY>

<REG_VALUE_NAME><![CDATA[preName]]></REG_VALUE_NAME>
                        <FILE_PATH><![CDATA[]]></FILE_PATH>
                        <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
                        <DATA_TYPE>String List</DATA_TYPE>
                        <DESCRIPTION><![CDATA[reg
key]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>75</ID>
                            <NAME>Windows Server 2012 R2</NAME>

<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1007110</K><L
>0</L><CD>contains</CD><OP>xre</OP><V><![CDATA[.*]]></V></DP></CTR
L></EVALUATE>

<RATIONALE><![CDATA[rationale]]></RATIONALE>
                            <DATAPOINT>
                               <CARDINALITY>contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
                <USER_DEFINED_CONTROL>
                    <ID>100000</ID>
                    <UDC_ID>b24df689-0714-7045-833a-
987f04cdab15</UDC_ID>
                    <CHECK_TYPE>Windows File Content
Check</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                        <NAME><![CDATA[Access Control
Requirements]]></NAME>
```

```
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1010</ID>
                        <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[preFCCUDC]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[min]]></LABEL>
                        <VALUE>1</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>
                        <PATH_TYPE><![CDATA[Use file
search]]></PATH_TYPE>
                        <FILE_QUERY><![CDATA[QWEB*]]></FILE_QUERY>
                        <BASE_DIR><![CDATA[c:\]]></BASE_DIR>
                        <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>

<FILE_NAME_MATCH><![CDATA[preTest2.txt]]></FILE_NAME_MATCH>

<FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>

<DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                       <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                        <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                        <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>
                        <DATA_TYPE>String List</DATA_TYPE>

<DESCRIPTION><![CDATA[FileContentChech]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>75</ID>
                            <NAME>Windows Server 2012 R2</NAME>

<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1007020</K><L
>0</L><CD>contains</CD><OP>xre</OP><V><![CDATA[true]]></V></DP></C
TRL></EVALUATE>

<RATIONALE><![CDATA[rationale]]></RATIONALE>
                            <DATAPOINT>
```

```
                                <CARDINALITY>contains</CARDINALITY>
                                 <OPERATOR>xre</OPERATOR>
                                 <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
                                 </DEFAULT_VALUES>
                             </DATAPOINT>
                         </TECHNOLOGY>
                     </TECHNOLOGIES>
                     <REFERENCE_LIST/>
                 </USER_DEFINED_CONTROL>
                 <USER_DEFINED_CONTROL>
                     <ID>100026</ID>
                     <UDC_ID>d908b3f9-59f9-fb70-801c-
29d04fb12511</UDC_ID>
                     <CHECK_TYPE>Windows File Content
Check</CHECK_TYPE>
             <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                     <CATEGORY>
                         <ID>3</ID>
                         <NAME><![CDATA[Access Control
Requirements]]></NAME>
                     </CATEGORY>
                     <SUB_CATEGORY>
                         <ID>1010</ID>
                         <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                     </SUB_CATEGORY>

<STATEMENT><![CDATA[pre_fcc_file_path_regexwith$]]></STATEMENT>
                     <CRITICALITY>
                         <LABEL><![CDATA[min]]></LABEL>
                         <VALUE>1</VALUE>
                     </CRITICALITY>
                     <COMMENT><![CDATA[]]></COMMENT>
                     <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                     <AUTO_UPDATE>0</AUTO_UPDATE>
                     <IGNORE_ERROR>0</IGNORE_ERROR>
<IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                     <SCAN_PARAMETERS>
                         <PATH_TYPE><![CDATA[Use file
path]]></PATH_TYPE>

<FILE_PATH><![CDATA[C:\user\PreTest\pretestfile1.txt]]></FILE_PATH
>
                         <FILE_QUERY><![CDATA[pre\$]]></FILE_QUERY>
```

```
                            <DATA_TYPE>String List</DATA_TYPE>
                          <DESCRIPTION><![CDATA[pre\$]]></DESCRIPTION>
                        </SCAN_PARAMETERS>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>75</ID>
                                <NAME>Windows Server 2012 R2</NAME>

<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1008003</K><L
>0</L><CD>contains</CD><OP>xre</OP><V><![CDATA[.*]]></V></DP></CTR
L></EVALUATE>

<RATIONALE><![CDATA[ration]]></RATIONALE>
                                <DATAPOINT>
                                   <CARDINALITY>contains</CARDINALITY>
                                    <OPERATOR>xre</OPERATOR>
                                    <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                    </DEFAULT_VALUES>
                                </DATAPOINT>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                        <REFERENCE_LIST/>
                    </USER_DEFINED_CONTROL>
                </CONTROLS>
            </SECTION>
        </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Sample - Export policy with UDCs into XML file showing remediation information

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=export&id=1801961&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-22T16:47:24Z</DATETIME>
```

```
<POLICY>
    <TITLE><![CDATA[RHEL_8]]></TITLE>
    <EXPORTED><![CDATA[2020-04-22T16:47:24Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>217</ID>
            <NAME>Red Hat Enterprise Linux 8.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="2">
       ...
        <SECTION>
            <NUMBER>2</NUMBER>
            <HEADING><![CDATA[UDC]]></HEADING>
            <CONTROLS total="6">
                <USER_DEFINED_CONTROL>
                    <ID>100028</ID>
                    <UDC_ID>c50922a1-1482-df3f-83e2-
bb96c99ffc48</UDC_ID>
                    <CHECK_TYPE>Unix File/Directory
Permission</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                        <NAME><![CDATA[Access Control
Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1007</ID>

<NAME><![CDATA[Authentication/Passwords]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[Basic File/Directory
Permission-UNIX-RHEL_8]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[Basic File/Directory
Permission]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
```

```
                    <SCAN_PARAMETERS>

<FILE_PATH><![CDATA[/etc/profile]]></FILE_PATH>
                        <DATA_TYPE>String</DATA_TYPE>
                        <DESCRIPTION><![CDATA[File/Directory
Permission]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>217</ID>
                         <NAME>Red Hat Enterprise Linux 8.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_permission.1007079</K><OP>re</O
P><V><![CDATA[.*]]></V></DP></CTRL></EVALUATE>
                          <RATIONALE><![CDATA[Basic File/Directory
Permission-UNIX]]></RATIONALE>
                           <REMEDIATION><![CDATA[]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>re</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
                <USER_DEFINED_CONTROL>
                    <ID>100029</ID>
                    <UDC_ID>9da2c628-fb7d-50cf-8230-
6f3ff59172a8</UDC_ID>
                    <CHECK_TYPE>Unix File/Directory
Existence</CHECK_TYPE>
            <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                        <NAME><![CDATA[Access Control
Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1007</ID>

<NAME><![CDATA[Authentication/Passwords]]></NAME>
                    </SUB_CATEGORY>
```

```
                    <STATEMENT><![CDATA[Basic File/Directory
Existence-UNIX-RHEL_8]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[File/Directory Existence -
this is in comment section]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>

<FILE_PATH><![CDATA[/etc/profile]]></FILE_PATH>
                        <DATA_TYPE>Boolean</DATA_TYPE>
                       <DESCRIPTION><![CDATA[test]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>217</ID>
                          <NAME>Red Hat Enterprise Linux 8.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_dir_exist.1007080</K><L>2</L><V
>false</V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[File/Directory
Existence-this is in rationale section under default
value]]></RATIONALE>
                           <REMEDIATION><![CDATA[]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>no op</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE>true</DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
          ...
        </SECTION>
    </SECTIONS>
</POLICY>
  </RESPONSE>
```

```
</POLICY_EXPORT_OUTPUT>
...
```

Sample: Export policy with Unix File Content Controls when Evaluate as string is enabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=export&id=3721621&show_user_controls=1"
"<qualys_base_url>/api/2.0/fo/compliance/policy/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
export_output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-04-06T11:56:11Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Multiline CHeck Oracle asset]]></TITLE>
    <EXPORTED><![CDATA[2021-04-06T11:56:11Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="2">
        <TECHNOLOGY>
            <ID>79</ID>
            <NAME>Oracle Enterprise Linux 7.x</NAME>
            ...
                    <CRITICALITY>
                        <LABEL><![CDATA[URGENT]]></LABEL>
                        <VALUE>5</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[FC UDC]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>1</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>1</IGNORE_ITEM_NOT_FOUND>
                   <SCAN_PARAMETERS>
<FILE_PATH><![CDATA[/home/testscan/samram]]></FILE_PATH>
                        <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
                        <DATA_TYPE>Line List</DATA_TYPE>
                        <EVALUATE_AS_STRING>1</EVALUATE_AS_STRING>
                        <DESCRIPTION><![CDATA[New option enabled
with line list]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
```

```
<TECHNOLOGIES total="2">
    <TECHNOLOGY>
        <ID>79</ID>
      <NAME>Oracle Enterprise Linux 7.x</NAME>
       ...
```

DTD

<platform API server>/api/2.0/fo/compliance/policy/policy_export_output.dtd

V3.0

/api/3.0/fo/compliance/policy/?action=export

[GET] [POST]

Export compliance policies from your account to an XML file. Service provided controls are exported and you can choose to also export user defined controls. The output also includes an appendix with human readable look-ups for control descriptions, giving you explanation on the various aspects of control description and evaluation.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=export	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id={value} or title={value}	(Required) The ID or the title of the policy you want to export.
show_user_controls={**0**|1}	(Optional) Set to 1 to include user-defined controls (UDCs) in the XML output. For Qualys Custom Controls you'll see the UDC ID for each control in the output.When not specified, UDCs are not included. Interested in Qualys Custom Controls? Log in to Qualys, go to Help > Online Help and search for "custom controls".
show_appendix={**0**|1}	(Optional) Set to 1 to show the appendix section in the XML output. When unspecified, the appendix section is not included in the output.

Sample - Export Policy

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"username:Password#" -d
"action=export&id=5744989&show_user_controls=1"
"https://https://qualysapi.qualys.com/api/3.0/fo/compliance/policy
/"> Policy_export_V3sample.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://https://qualysapi.qualys.com/api/3.0/fo/compliance/policy
/policy_export_output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2025-06-27T12:02:10Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[One UDC]]></TITLE>
    <EXPORTED><![CDATA[2025-06-27T12:02:10Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>80</ID>
            <NAME>CentOS 7.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="2">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[UDC]]></HEADING>
            <CONTROLS total="1">
                <USER_DEFINED_CONTROL>
                    <ID>100000</ID>
                    <UDC_ID>3e8fada3-8bc3-f557-8115-
c567323d327a</UDC_ID>
                    <CHECK_TYPE>Unix File/Directory
Existence</CHECK_TYPE>

<IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>2</ID>
                        <NAME><![CDATA[Web Application
Services]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1028</ID>
                        <NAME><![CDATA[Web Server/Tier
```

```
Settings]]></NAME>
                    </SUB_CATEGORY>
                   <STATEMENT><![CDATA[CitiJSONUDC2]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[URGENT]]></LABEL>
                        <VALUE>5</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                  <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>

<FILE_PATH><![CDATA[/etc/profile]]></FILE_PATH>
                        <DATA_TYPE>Boolean</DATA_TYPE>
                        <DESCRIPTION><![CDATA[NA]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>80</ID>
                            <NAME>CentOS 7.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_dir_exist.4211083</K><L>2</L><V
>true</V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[RA]]></RATIONALE>
                           <REMEDIATION><![CDATA[]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>no op</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE>true</DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
            </CONTROLS>
        </SECTION>
        <SECTION>
            <NUMBER>2</NUMBER>
            <HEADING><![CDATA[SDC]]></HEADING>
            <CONTROLS total="1">
                <CONTROL>
```

```
                        <ID>1071</ID>
                        <CRITICALITY>
                            <LABEL><![CDATA[URGENT]]></LABEL>
                            <VALUE>5</VALUE>
                        </CRITICALITY>

<IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>80</ID>
                                <NAME>CentOS 7.x</NAME>

<EVALUATE><CTRL><DP><K>rh06.secman.system.logindefs-min-password-
length</K><OP>ge</OP><V>0</V><FV set="1">161803399999999</FV><FV
set="1">314159265358979</FV></DP></CTRL></EVALUATE>
                                <REMEDIATION/>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                    </CONTROL>
                </CONTROLS>
            </SECTION>
        </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

DTD

<platform API server>/api/3.0/fo/compliance/policy/policy_export_output.dtd

V4.0

/api/4.0/fo/compliance/policy/?action=export

[GET] [POST]

Export compliance policies from your account to an XML file. Service provided controls are exported and you can choose to also export user defined controls. The output also includes an appendix with human readable look-ups for control descriptions, giving you explanation on the various aspects of control description and evaluation.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=export	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
id={value} or title={value}	(Required) The ID or the title of the policy you want to export.
show_user_controls={**0**|1}	(Optional) Set to 1 to include user-defined controls (UDCs) in the XML output. For Qualys Custom Controls you'll see the UDC ID for each control in the output.When not specified, UDCs are not included. Interested in Qualys Custom Controls? Log in to Qualys, go to Help > Online Help and search for "custom controls".
show_appendix={**0**|1}	(Optional) Set to 1 to show the appendix section in the XML output. When unspecified, the appendix section is not included in the output.

Sample - Export Policy

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"quaylys_username:Password@" -d
"action=export&id=5744989&show_user_controls=1"
"https://<qualys_base_url>/api/4.0/fo/compliance/policy/">
Policy_export_id_1.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://<qualys_base_url>/api/4.0/fo/compliance/policy/policy_exp
ort_output.dtd">
<POLICY_EXPORT_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-06-25T15:29:46Z</DATETIME>
        <POLICY>
            <TITLE>
                <![CDATA[One UDC]]>
            </TITLE>
            <EXPORTED>
                <![CDATA[2025-06-25T15:29:46Z]]>
            </EXPORTED>
            <COVER_PAGE>
```

```
                <![CDATA[]]>
            </COVER_PAGE>
            <STATUS>
                <![CDATA[active]]>
            </STATUS>
            <TECHNOLOGIES total="1">
                <TECHNOLOGY>
                    <ID>80</ID>
                    <NAME>CentOS 7.x</NAME>
                </TECHNOLOGY>
            </TECHNOLOGIES>
            <SECTIONS total="1">
                <SECTION>
                    <NUMBER>1</NUMBER>
                    <HEADING>
                        <![CDATA[UDC]]>
                    </HEADING>
                    <CONTROLS total="1">
                        <USER_DEFINED_CONTROL>
                            <ID>100000</ID>
                            <UDC_ID>3e8fada3-8bc3-f557-8115-
c567323d327a</UDC_ID>
                            <CHECK_TYPE>Unix File/Directory
Existence</CHECK_TYPE>
                            <IS_CONTROL_DISABLE>
                                <![CDATA[0]]>
                            </IS_CONTROL_DISABLE>
                            <CATEGORY>
                                <ID>2</ID>
                                <NAME>
                                    <![CDATA[Web Application
Services]]>
                                </NAME>
                            </CATEGORY>
                            <SUB_CATEGORY>
                                <ID>1028</ID>
                                <NAME>
                                    <![CDATA[Web Server/Tier
Settings]]>
                                </NAME>
                            </SUB_CATEGORY>
                            <STATEMENT>
                                <![CDATA[CitiJSONUDC2]]>
                            </STATEMENT>
                            <CRITICALITY>
                                <LABEL>
```

```
                                    <![CDATA[URGENT]]>
                                </LABEL>
                                <VALUE>5</VALUE>
                            </CRITICALITY>
                            <COMMENT>
                                <![CDATA[]]>
                            </COMMENT>
                            <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                            <AUTO_UPDATE>0</AUTO_UPDATE>
                            <IGNORE_ERROR>0</IGNORE_ERROR>

<IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                            <SCAN_PARAMETERS>
                                <FILE_PATH>
                                    <![CDATA[/etc/profile]]>
                                </FILE_PATH>
                                <DATA_TYPE>Boolean</DATA_TYPE>
                                <DESCRIPTION>
                                    <![CDATA[NA]]>
                                </DESCRIPTION>
                            </SCAN_PARAMETERS>
                            <TECHNOLOGIES total="1">
                                <TECHNOLOGY>
                                    <ID>80</ID>
                                    <NAME>CentOS 7.x</NAME>
                                    <EVALUATE>
                                        <CTRL>
                                            <DP>

<K>custom.file_dir_exist.4211083</K>
                                                    <L>2</L>
                                                    <V>true</V>
                                            </DP>
                                        </CTRL>
                                    </EVALUATE>
                                    <RATIONALE>
                                        <![CDATA[RA]]>
                                    </RATIONALE>
                                    <REMEDIATION>
                                        <![CDATA[]]>
                                    </REMEDIATION>
                                    <DATAPOINT>
                                        <CARDINALITY>no
cd</CARDINALITY>
                                        <OPERATOR>no op</OPERATOR>
                                        <DEFAULT_VALUES total="1">
```

```
<DEFAULT_VALUE>true</DEFAULT_VALUE>
                                                    </DEFAULT_VALUES>
                                                </DATAPOINT>
                                            </TECHNOLOGY>
                                        </TECHNOLOGIES>
                                        <REFERENCE_LIST/>
                                        <IS_ACTIVE>1</IS_ACTIVE>
                                    </USER_DEFINED_CONTROL>
                                </CONTROLS>
                            </SECTION>
                        </SECTIONS>
                    </POLICY>
                </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

DTD

<platform API server>/api/4.0/fo/compliance/policy/policy_export_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/4.0/fo/compliance/policy/?action=export	Active	Active
/api/3.0/fo/compliance/policy/?action=export	December 2025	December 2026
/api/2.0/fo/compliance/policy/?action=export	December 2025	December 2026

Compliance Policy - Import

For API version information, refer to the API Version History section.

V2.0|V3.0|V4.0

V2.0

/api/2.0/fo/compliance/policy/?action=import

[POST]

Import a compliance policy, defined in an XML file, into your account. We'll include all the service-provided controls from your XML file. You have the option to also include user-defined controls.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=import	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
xml_file	(Required) The file containing the policy details.
title={value}	(Required) The title of the new policy.
create_user_controls={**0**|1}	(Optional) When not specified, user-defined controls are not created when you import a policy. Specify 1 to include UDCs from the XML file.

Sample - Import policy

API request:

```
curl -H "X-Requested-With: Curl Sample" -H "Content-type:
text/xml" --data-binary @policy.xml -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=import&title=My+Policy"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
   <RESPONSE>
      <DATETIME>2017-09-15T21:32:40Z</DATETIME>
      <TEXT>Successfully imported compliance policy</TEXT>
```

```
      <ITEM_LIST>
         <ITEM>
         <KEY>ID</KEY>
         <VALUE>136992</VALUE>
      </ITEM>
      <ITEM>
         <KEY>TITLE</KEY>
         <VALUE>My Policy</VALUE>
      </ITEM>
   </ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

Sample - Import policy with UDCs having remediation information using xml file

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -H
Content-Type:text/xml --data-binary
"@UDC_with_Remedy_20200422.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=import&title=Policy1&create_user_controls=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-22T22:51:16Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1867541</VALUE>
      </ITEM>
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>Policy1</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V3.0

/api/3.0/fo/compliance/policy/?action=import

[POST]

Import a compliance policy, defined in an XML file, into your account. We'll include all the service-provided controls from your XML file. You have the option to also include user-defined controls.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=import	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
xml_file	(Required) The file containing the policy details.
title={value}	(Required) The title of the new policy.
create_user_controls={**0**|1}	(Optional) When not specified, user-defined controls are not created when you import a policy. Specify 1 to include UDCs from the XML file.

Sample - Import policy

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"username:Password#" -H Content-type:text/xml --data-binary
"@/home/location/Policy_V3sample.xml"
"https://<qualys_base_url>/api/3.0/fo/compliance/policy/?action=im
port&title=V3sample"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-06-27T12:04:53Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5757988</VALUE>
      </ITEM>
```

```
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>V3sample</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

V4.0

/api/4.0/fo/compliance/policy/?action=import

[POST]

Import a compliance policy, defined in an XML file, into your account. We'll include all the service-provided controls from your XML file. You have the option to also include user-defined controls.

Permissions - If you're not a Manager, the permission to Manage PC module must be turned on in your account.

Input Parameters

Parameter	Description
action=import	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
xml_file	(Required) The file containing the policy details.
title={value}	(Required) The title of the new policy.
create_user_controls={**0**|1}	(Optional) When not specified, user-defined controls are not created when you import a policy. Specify 1 to include UDCs from the XML file.

Sample - Import policy

API request:

```
curl -k -s -S -H 'X-Requested-With:curl demo2' -u
"quaylys_username:Password@" -H Content-type:text/xml --data-
binary "<file_directory_path>/compliance/policy_import_api.xml"
"https://<qualys_base_url>/api/4.0/fo/compliance/policy/?action=im
port&title=UDC_inactive_create_v4&create_user_controls=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/4.0/simple_return.dtd">
```

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-06-02T13:23:31Z</DATETIME>
        <TEXT>Successfully imported compliance policy</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1464127</VALUE>
            </ITEM>
            <ITEM>
                <KEY>TITLE</KEY>
                <VALUE>UDC_inactive_create_v4</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/2.0/fo/compliance/policy/?action=import	Active	Active
/api/3.0/fo/compliance/policy/?action=import	December 2025	December 2026
/api/4.0/fo/compliance/policy/?action=import	December 2025	December 2026

Compliance Policy - Merge

/api/2.0/fo/compliance/policy/?action=merge

[POST]

Merge combines two compliance policies using Qualys Policy Compliance (PC). You can merge specific parts of a new policy into an existing one as defined by the parameter options given under input parameters. The merged changes can also be previewed before saving. This API is available to Managers and Auditors.

For example, if you imported a policy from our library (Policy A) and configured it to add asset groups, controls, and sections. Later, an updated version of this policy (Policy B) with new controls and technologies may be released. In this scenario, you can use the Policy Merge API to add the new controls and technologies from Policy B into Policy A (your existing policy) without losing the asset groups, controls, and sections you added.

Input Parameters

The policy merge input parameters provide flexibility in merging different parts of a new policy (Policy B) into an existing one (Policy A). For example, you can update controls with revised definitions, replace asset groups, and add new technologies and controls. By default, no changes are applied to your existing policy unless the required parameters (see below) are specified:

Parameter	Description
action=merge	(Required)
id={value}	(Required) ID of the policy that will be updated with merged content (let's call this Policy A).
merge_policy_id={value} -or- policy XML data	(Required) Policy with the content that will be merged into Policy A (let's call this Policy B). You can specify a policy ID using "merge_policy_id" or policy XML data. To upload XML data, use this syntax: --data-binary @path_to_xml_file.xml
	These options are mutually exclusive: policy XML data and merge_policy_id. You must provide only one of the above options. If both options are provided, the API will return an error.
replace_cover_page={**0**|1}	(Optional) Set replace_cover_page=1 to replace the cover page in Policy A with the cover page in Policy B.
replace_asset_groups={**0**|1}	(Optional) Set replace_asset_groups=1 to replace asset groups in Policy A with asset groups in Policy B.
	These options are mutually exclusive: add_new_asset_groups and replace_asset_groups. You must provide only one of the above options. If both options are provided, the API will return an error.
add_new_asset_groups={**0**|1}	(Optional) Set add_new_asset_groups=1 to add new asset groups, i.e. add asset groups from Policy B if they are not already present in Policy A.

Parameter	Description
add_new_technologies={**0**|1}	(Optional) Set add_new_technologies=1 to add new technologies and to add technologies from Policy B if they are not already in Policy A. This will also add the technology within all controls already specified in the policy for which this technology is relevant. For example, consider a policy to have 20 controls, of which ten controls are applicable for centOS v4.0. You can add this technology to the policy to reflect these ten controls.
add_new_controls={**0**|1}	(Optional) Set add_new_controls=1 to add new controls, i.e. addcontrols from Policy B if they are not already in Policy A.
update_section_heading={**0**|1}	(Optional) Set update_section_heading=1 to replace the section heading in Policy A with the one in Policy B, based on section number (applies only to common sections). This parameter must be specified with: add_new_controls or update_existing_controls.
update_existing_controls={**0**|1}	(Optional) Set update_existing_controls=1 to replace the common controls in Policy A with the ones in Policy B. These are controls that exist in both policies. (Controls will not be removed). This setting currently updates the following properties of a control: — Status in terms of enabling or disabling the control — Criticality — Reference text — Control evaluation Operator and Value — Set/Unset Fixed values
preview_merge={**0**|1}	(Optional) Set preview_merge= 1 to view the changes merged into Policy A without saving them.

DTD

<platform API server>/api/2.0/fo/compliance/policy/policy_merge_result_output.dtd"

Policy Merge Request 1 - preview merged policy

Policy ID 15993 (Policy A) will be updated with content merged from policy ID 15994 (Policy B) and the XML output will show the merged policy in preview mode. Policy changes will not be saved in Policy 15993 since the request includes "preview_merge=1".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?
action=merge&id=15993&merge_policy_id=15994&replace_cover_page=1&a
dd_new_asset_groups=1&add_new_technologies=1&update_section_headin
g=1&add_new_controls=1&update_existing_controls=1&preview_merge=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE POLICY_MERGE_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
merge_result_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-04-24T05:28:04Z</DATETIME>
    <POLICY_MERGE_RESULT>
      <NOTE>Policy changes were not merged or saved since the
request had preview_merge=1.</NOTE>
      <NEW_COVER_PAGE><![CDATA[My Cover Page]]></NEW_COVER_PAGE>
      <ASSET_GROUPS_ADDED>
        <ASSET_GROUP>
          <ID>424422</ID>
          <NAME><![CDATA[<script>alert("xss");</script>]]></NAME>
        </ASSET_GROUP>
        <ASSET_GROUP>
          <ID>424577</ID>
          <NAME><![CDATA[10.10.32.26]]></NAME>
        </ASSET_GROUP>
      </ASSET_GROUPS_ADDED>
      <TECHNOLOGIES_ADDED>
        <TECHNOLOGY>
          <ID>1</ID>
          <NAME>Windows XP desktop</NAME>
        </TECHNOLOGY>
      </TECHNOLOGIES_ADDED>
      <SECTIONS_UPDATED>
        <SECTION>
          <ID>1</ID>
          <HEADING><![CDATA[First section]]></HEADING>
        </SECTION>
        <SECTION>
          <ID>2</ID>
          <HEADING><![CDATA[Second section]]></HEADING>
        </SECTION>
      </SECTIONS_UPDATED>
      <SECTIONS>
        <SECTION>
          <ID>1</ID>
          <CONTROLS_UPDATED>
            <CONTROL>
              <ID>1061</ID>
            </CONTROL>
          </CONTROLS_UPDATED>
        </SECTION>
        <SECTION>
```

```
            <ID>2</ID>
            <CONTROLS_ADDED>
              <CONTROL>
                <ID>1045</ID>
              </CONTROL>
              <CONTROL>
                <ID>1048</ID>
              </CONTROL>
            </CONTROLS_ADDED>
          </SECTION>
        </SECTIONS>
      </POLICY_MERGE_RESULT>
    </RESPONSE>
</POLICY_MERGE_RESULT_OUTPUT>
```

Policy Merge Request 2 - save merged policy

Policy ID 15993 (Policy A) will be updated with content merged from policy ID 15994 (Policy B). The merged policy will be saved in policy 15993.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?
action=merge&id=15993&merge_policy_id=15994&replace_cover_page=1&a
dd_new_asset_groups=1&add_new_technologies=1&update_section_headin
g=1&add_new_controls=1&update_existing_controls=1&preview_merge=0"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_MERGE_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
merge_result_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-04-24T05:31:26Z</DATETIME>
    <POLICY_MERGE_RESULT>
      <NOTE>Policy changes have been merged successfully.</NOTE>
      <NEW_COVER_PAGE><![CDATA[My Cover Page]]></NEW_COVER_PAGE>
      <ASSET_GROUPS_ADDED>
        <ASSET_GROUP>
          <ID>424422</ID>
...
    </POLICY_MERGE_RESULT>
  </RESPONSE>
</POLICY_MERGE_RESULT_OUTPUT>
```

Policy Merge Request 3 - pass policy XML, preview merged policy

Policy ID 15993 (Policy A) will be updated with content merged from the policy defined in the file "path_to_policy_xml_file.xml." The merged changes will not be saved in policy 15993 since the request includes "preview_merge=1".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -H
"Content-type: text/xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?
action=merge&id=15993&replace_cover_page=1&replace_asset_groups=1&
add_new_technologies=1&update_section_heading=1&add_new_controls=1
&update_existing_controls=1&preview_merge=1" --data-binary
@/home/aamin/PC_XML/path_to_policy_xml_file.xml>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_MERGE_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_
merge_result_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-04-24T05:38:26Z</DATETIME>
    <POLICY_MERGE_RESULT>
      <NOTE>Policy changes were not merged or saved since the
request had preview_merge=1.</NOTE>
      <NEW_COVER_PAGE><![CDATA[My Cover Page]]></NEW_COVER_PAGE>
      <SECTIONS_UPDATED>
        <SECTION>
          <ID>1</ID>
          <HEADING><![CDATA[First section]]></HEADING>
        </SECTION>
        <SECTION>
          <ID>2</ID>
          <HEADING><![CDATA[Second section]]></HEADING>
        </SECTION>
      </SECTIONS_UPDATED>
      <SECTIONS>
        <SECTION>
          <ID>1</ID>
          <CONTROLS_UPDATED>
            <CONTROL>
              <ID>1061</ID>
            </CONTROL>
          </CONTROLS_UPDATED>
        </SECTION>
        <SECTION>
```

```
          <ID>2</ID>
          <CONTROLS_ADDED>
            <CONTROL>
              <ID>1045</ID>
            </CONTROL>
            <CONTROL>
              <ID>1048</ID>
            </CONTROL>
          </CONTROLS_ADDED>
        </SECTION>
      </SECTIONS>
    </POLICY_MERGE_RESULT>
  </RESPONSE>
</POLICY_MERGE_RESULT_OUTPUT>
```

Compliance Policy - Manage Asset Tags

/api/2.0/fo/compliance/policy/

[POST]

Add, remove, and set asset tags for a policy. You must have permission to modify the policy you want to update.

Add asset tags to policy

Use this action to add asset tags to the policy. When specified, we will check whether the asset tags specified in the request are already associated with the policy and only add the asset tags that are new to the policy.

Parameter	Description
action=add_asset_tags	(Required)
id={value}	(Required) Policy ID for the policy you want to update.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_set_include={tag id|name}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={tag id|name}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=add_asset_tags"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2022-01-19T06:35:40Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Removing asset tags from policy

Use this action to remove asset tags from the policy.

Parameter	Description
action=remove_asset_tags	(Required) Note: With the remove_asset_tags action, you must set either tag_set_include or tag_set_exclude parameter, or both the parameters.
id={value}	(Required) Policy ID for the policy you want to update.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_set_include={tag id|name}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={tag id|name}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=remove_asset_tags"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2022-01-19T06:35:40Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Set asset tags for policy

Use this action to overwrite the asset tags for a policy. Any assigned asset tags not specified in the request will be removed from the policy.

Parameter	Description
action=set_asset_tags	(Required)
id={value}	(Required) Policy ID for the policy you want to update.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_by={**id**|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.

Parameter	Description
tag_set_include={tag id|name}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={tag id|name}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action
=set_asset_tags"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2022-01-19T06:28:30Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Compliance Policy - Manage Asset Groups

/api/2.0/fo/compliance/policy/

[POST]

Add, remove and set asset groups for a policy. You must have permission to modify the policy you want to update.

Add asset group IDs to policy

Parameter	Description
action=add_asset_group_ids	(Required)
id={value}	Policy ID for the policy you want to update.
asset_group_ids={value}	Asset groups IDs for the asset groups you want to add to the policy specified in "id". Multiple IDs are comma separated. Each asset group must have at least 1 assigned IP address.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -X POST -d
"id=43400&asset_group_ids=649737,649736"
"https://qualysapi.qualys.com//api/2.0/fo/compliance/policy/?actio
n=add_asset_group_ids"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-09-11T09:06:17Z</DATETIME>
    <TEXT>Compliance Policy successfully modified.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>43400</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Remove asset group IDs from policy

Parameter	Description
action=remove_asset_group_ids	(Required)
id={value}	Policy ID for the policy you want to update.
asset_group_ids={value}	Asset groups IDs for the asset groups you want to delete from the policy specified in "id". Multiple IDs are comma separated.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -X POST -d
"id=43400&asset_group_ids=649737,649736"
"https://qualysapi.qualys.com//api/2.0/fo/compliance/policy/?actio
n=remove_asset_group_ids"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-09-11T09:06:17Z</DATETIME>
    <TEXT>Compliance Policy successfully modified.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>43400</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Set asset group IDs for policy

Use this action to reset the asset groups for a specified policy. Any assigned asset groups not specified in this request will be removed.

Parameter	Description
action=set_asset_group_ids	(Required)
id={value}	Policy ID for the policy you want to update.
asset_group_ids={value}	Asset groups IDs for the asset groups you want to assign to the policy specified in "id". Multiple IDs are comma separated. Each asset group must have at least 1 assigned IP address.
evaluate_now={**0**|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.

API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -X POST -d
"id=43400&asset_group_ids=649737,649736"
"https://qualysapi.qualys.com//api/2.0/fo/compliance/policy/?
action=set_asset_group_ids"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-09-11T09:07:43Z</DATETIME>
    <TEXT>Compliance Policy successfully modified.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>43400</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Compliance Framework Reports

The Compliance Framework Reports APIs help in providing the required data and for managing compliance framework reports. The following are the list of APIs:

GET Preferred Framework List API

GET Policies List API

GET Asset Groups List API

GET Asset Tags List API

GET Asset Sources List API

Create Compliance Framework Report API

GET Report Generation Status API

Download Compliance Framework Report API

GET Preferred Framework List API

/pcrs/1.0/mandate/list

[GET]

With this API, you can get a list of preferred compliance frameworks configured for a subscription, including the count of top-level requirements for each mandate.

Sample - List compliance frameworks configured for a subscription

API request:

```
curl -X GET "<gateway_base_url>/pcrs/1.0/mandate/list" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
[
  {
    "id": 1,
    "name": "PCI DSS v4.0",
    "requirementsCount": 12
  },
  {
    "id": 2,
    "name": "HIPAA",
    "requirementsCount": 8
  }
]
```

GET Policies List API

/pcrs/1.0/policy/list

[GET]

With this API, you can get a list of all active policies associated for a subscription.

Sample - List all active policies associated for a subscription

API request:

```
curl -X GET "<gateway_base_url>/pcrs/1.0/policy/list" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
[
  {
    "id": 101,
    "title": "CIS Microsoft Windows Server 2019 Benchmark v1.2.1"
  },
  {
    "id": 102,
    "title": "CIS Red Hat Enterprise Linux 8 Benchmark v2.0.0"
  }
]
```

GET Asset Groups List API

/pcrs/1.0/assetGroup/list

[GET]

With this API, you can get a list of asset groups associated to a subscription.

Note: This API to run the user subscription must be AGMS enabled.

Sample - List all asset groups associated to a subscription

API request:

```
curl -X GET "<gateway_base_url>/pcrs/1.0/assetGroup/list" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
[
  {
    "id": 1001,
    "name": "Production Servers"
```

```
  },
  {
    "id": 1002,
    "name": "Development Environment"
  }
]
```

GET Asset Tags List API

/pcrs/1.0/assetTag/list

[GET]

With this API, you can get a hierarchical list of asset tags for the subscription.

Sample - List hierarchical list of asset tags for the subscription

API request:

```
curl -X GET "<gateway_base_url>/pcrs/1.0/assetTag/list" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
[
  {
    "id": 2001,
    "name": "Environment",
    "isFavorite": false,
    "children": [
      {
        "id": 2002,
        "name": "Production",
        "isFavorite": false,
        "children": []
      }
    ]
  }
]
```

GET Asset Sources List API

/pcrs/1.0/mandate/report/sources

[GET]

With this API, you can get all available asset source options for report creation.

Sample - List all available asset source options for report creation

API request:

```
curl -X GET "<gateway_base_url>/pcrs/1.0/mandate/report/sources" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
[
  "All Assets In Policy",
  "Asset Groups",
  "Asset Tags"
]
```

Create Compliance Framework Report API

/pcrs/1.0/mandate/report

[POST]

With this API, you can create a new mandate report.

Note: Maximum 3 mandate IDs and 10 policies can be selected for generating the compliance framework report.

Input Parameters

Parameter	Description
mandateIds	(Required) Enter the list of mandate IDs.
policyIds	(Required) Enter the policyID.
selectionType	(Required) Select the type of asset source (from sources API).
assetGroupIds	(Optional) Enter the asset group ID. Required if assetSource is "Asset Groups".
tagsetInputParam	(Optional) Enter the tag set. Required if assetSource is "Asset Tags".
title	(Required) Enter a title for the report.
reportFormat	(Required) Type of output format (JSON or HTML. By default, report type is JSON).

Sample - Generate framework based report

API request:

```
curl -X 'POST' \
  '<gateway_base_url>/pcrs/1.0/mandate/report' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -H "Authorization: <bearer_token>" \
  -d '{
  "title": "report 1 via api",
  "reportFormat": "HTML",
  "selectionType": "All Assets In Policy",
  "filters": {
    "mandateIds": [
      10482,4966,2741
    ],
    "policyIds": [
      1919419,2296420,1965419,1943420,1949423
    ]
    },
  "schedule": {
    "scheduleType": "ONDEMAND"
  }
}'
```

JSON Response:

```
{
  "reportId": 4036133,
  "message": "Report generation is in progress"
}
```

Sample - Generate framework based report using asset groups

API request:

```
curl -X 'POST' \
  '<gateway_base_url>/pcrs/1.0/mandate/report' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -H "Authorization: <bearer_token>" \
  -d '{
  "title": "report 1 via api",
  "reportFormat": "HTML",
  "selectionType": "Asset Groups",
  "filters": {
    "mandateIds": [
      10482,4966,2741
    ],
```

```
    "policyIds": [
      1919419,2296420,1965419,1943420,1949423
    ],
    "assetGroupIds" : [1111, 2222]
   },
  "schedule": {
    "scheduleType": "ONDEMAND"
  }
}'
```

JSON Response:

```
{
  "reportId": 4035396,
  "message": "Report generation is in progress"
}
```

Sample - Generate framework based report using asset tags

API request:

```
curl -X 'POST' \
  '<gateway_base_url>/pcrs/1.0/mandate/report' \
  -H 'accept: */*' \
  -H 'Content-Type: application/json' \
  -H "Authorization: <bearer_token>" \
  -d '{
  "title": "report 1 via api",
  "reportFormat": "HTML",
  "selectionType": "Asset Tags",
  "filters": {
    "mandateIds": [
      10482,4966,2741
    ],
    "policyIds": [
      1919419,2296420,1965419,1943420,1949423
    ],

"tagsetInputParam":{"includeTagResolution":"Any","excludeTagResolu
tion":"Any","includeTagIds":[143936447,143968096,143968094,1439680
92],"excludeTagIds":[]}},
  "schedule": {
    "scheduleType": "ONDEMAND"
  }
}'
```

JSON Response:

```
{
  "reportId": 4038574,
  "message": "Report generation is in progress"
}
```

GET Report Generation Status API

/pcrs/1.0/mandate/report/status

[GET]

With this API, you can get the generation status of compliance framework reports.

Input Parameters

Parameter	Description
reportDataId	(Required) Enter the report data ID from create API.

Sample - Generate report status

API request:

```
curl -X GET
"<gateway_base_url>/pcrs/1.0/mandate/report/status?reportDataId=98
765" \
  -H "Authorization: <bearer_token>" \
  -H "Accept: application/json"
```

JSON Response:

```
{
  "status": 2,
  "percentageCompleted": 75
}
```

Download Compliance Framework Report API

/pcrs/1.0/mandate/report/download/html

[GET]

With this API, you can download the compliance framework report in HTML format.

Input Parameters

Parameter	Description
reportDataId	(Required) Enter the report data ID.

Sample - Download mandate based report

API request:

```
curl -X GET
"<gateway_base_url>/pcrs/1.0/mandate/report/download/html?reportDa
taId=98765" \
  -H "Authorization: <bearer_token>" \
  -o mandate_report.zip
```

Response:

Report is downloaded.

Compliance Posture Information

The Policy Compliance APIs help you gain the essential insight into the compliance posture of the hosts within your account. Qualys PC provides you with the following two types of APIs to fetch posture data:

- PC Posture Information APIs

- PC Posture Streaming APIs

Depending on the size of your posture data, you may choose to use the PC Posture Information APIs or the PC Posture Streaming APIs.

We recommend that you leverage the Posture Streaming APIs if you want to download more than 1 million postures, as they provide you a faster way to retrieve larger amount of posture information. The Posture Streaming APIs also has the ability to filter data based on the desired input entered by the user. If your posture information is expected to be less than 1 million, use the PC Posture Information APIs.

Refer the following KB article for recommendations on retrieving compliance posture information:

Compliance Posture Data Retrieval Best Practices

PC Posture Information APIs

/api/2.0/fo/compliance/posture/info/?action=list

[GET] [POST]

Each compliance posture info record includes a compliance posture ID and other attributes. Optional input parameters support filtering the posture info record output.

Each compliance posture info record in the output includes:

Output	Description
Compliance Posture ID	The service assigns a unique value to each compliance posture info record.
Host ID	Identifies a host.
Control ID	Identifies a technical control.
Technology ID	Identifies a technology.
Instance	Identifies a technology instance, when applicable.
Compliance Status	Passed, Failed or Error. An error, only assigned to a custom control, indicates control evaluation failed (and the ignore errors configuration option for the control was not selected).
Evaluation Date	The last posture evaluation date.
First Fail Date	The first scan date when the control was reported as Fail. If the previous status was Pass then this is the date the status changed from Pass to Fail.
Last Fail Date	The most recent scan date when the control was reported as Fail.

Output	Description
First Pass Date	The first scan date when the control was reported as Pass. If the previous status was Fail then this is the date the status changed from Fail to Pass.
Last Pass Date	The most recent scan date when the control was reported as Pass.
Previous Status	The compliance status (Pass or Fail) for each control before the most recent compliance scan.
Exception	Identifies an exception assignee and status, if an exception has been created.

The user has the ability to select the amount of information to include in the posture information output. By default, basic posture information is included: the posture ID, host ID, control ID, technology ID, technology instance (when applicable), and the compliance status. If an exception has been created, this full exception information is also included: the exception assignee and status, the date/time when the exception was created, when it was last modified, the user who took these actions on the exception, and the date when the exception is set to expire. A glossary of compliance posture information identifies: basic host information and basic control information.

Use the details input parameter to select another level of detail to be included in the policy information output.

By default, the posture information output shows posture information for all hosts (IP addresses) in asset groups assigned to the selected policy, provided the user has permission to view the hosts themselves. If you have a sub-account like a Unit Manager, Scanner or Reader, the posture information output only includes hosts that the account has permission to see.

Best Practices

You can reduce the amount of data being retrieved by only pulling the data that is required for the downstream processes. For example, only download the delta of the changes in posture since the last pull. This can be done using optional input parameters which allow you to set filters to restrict the posture information output to postures info records with certain IP addresses, host IDs, compliance control IDs, compliance posture IDs, posture info records with changes in status since a specified date, and posture info records with a certain compliance status (Passed, Failed or Error).

The optional glossary in the compliance posture information output includes:

Output	Description
User List	List of users who created, modified, or added comments to exceptions in compliance posture info records which are included in the posture information output. For a policy that was edited, the user who most recently edited the exception is listed.
Host List	List of hosts in compliance posture info records which are included in the posture information output. This basic host information is included: host ID, IP address, and tracking method. When details=All is specified, this additional information is included: last vulnerability scan date/time, last compliance scan date/time.
Control List	List of controls in compliance posture info records which are included in the posture information output. When details=All is specified, this additional information is included: rationale information and technology information for each control.
Technology List	List of technologies for controls in compliance posture info records which are included in the posture list output. This information is included only when details=All is specified.
Evidence List	List of evidence information for control data points.

Maximum Postures per API Request

The output of the Compliance Posture Info API is paginated when your API request identifies a single policy to report on using the "policy_id" input parameter. In this case, a maximum of 5,000 posture info records are returned per request by default. You can customize the page size (i.e. the number of posture info records) by using the parameter "truncation_limit=10000" for instance if you want to return pages with 10,000 records.

Permissions

Note: The Posture Info API is available as part of one of the following subscription combinations only:

- PC and API add-on
- PC, SCA, and API add-on
- VMDR, SCA, and API add-on

All users have permission view posture information for hosts (IP addresses) in asset groups assigned to the selected policy, when the hosts are available to the user based on user account settings.

User Role	Permissions
Manager	View compliance postures for all hosts (IP addresses) in asset groups assigned to the selected policy.
Auditor	View compliance postures for all hosts (IP addresses) in asset groups assigned to the selected policy.

User Role	Permissions
Unit Manager	View compliance postures for all hosts (IP addresses) in asset groups assigned to the selected policy, when the hosts are included in the user's business unit.
Scanner	View compliance postures for all hosts (IP addresses) in asset groups assigned to the selected policy, when the hosts are included in the user's account.
Reader	View compliance postures for all hosts (IP addresses) in asset groups assigned to the selected policy, when the hosts are included in the user's account.

User Permissions: Asset Group IPs

All users have permission to view posture information for all hosts (IP addresses) in the asset groups assigned to the selected policy provided they have permission to view the hosts themselves. This permission is granted even when users do not have permission to view the asset groups assigned to the policy.

For example, when a user makes a request for compliance posture information for "Policy A" and this policy has one assigned asset group "Hong Kong", and the user does not have permission to view this asset group, then the user does have permission to view compliance posture info records for all the IP addresses in the asset group "Hong Kong" provided the IP addresses in the group "Hong Kong" are visible to the user.

Input Parameters

Parameter	Description
action=list	(Required)
policy_id={value}	(policy_id or policy_ids is required) Show compliance posture info records for a specified policy. A valid policy ID is required.
	The parameters policy_id and policy_ids cannot be specified in the same request.
policy_ids={value}	(policy_id or policy_ids is required) Show compliance posture info records for multiple policies - up to 10 policies may be requested. Provide a comma-separated list of valid policy IDs. When this parameter is specified, all posture data is downloaded (and the "truncation_limit" parameter is invalid).
	The parameters policy_id and policy_ids cannot be specified in the same request. When policy_ids is specified, truncation_limit is invalid. For CSV output, policy_id must be specified (and policy_ids is invalid).
echo_request={**0**|1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.
output_format={value}	(Optional) The output format. A valid value is: xml (default), csv (posture data and metadata, i.e. summary and warning data), csv_no_metadata (posture data only, no metadata). For CSV output, you can include only one policy. For this reason, policy_id is required.
details={**Basic**|All|None|Light}	(Optional) Show a certain amount of information for each compliance posture info record. A valid value is: None - show posture info and minimum exception information (assignee and status) if appropriate Basic (default) - show posture info, full exception information if appropriate, and a minimum glossary (basic info for hosts and controls) Light - show posture info, exception info if appropriate, and a limited glossary (host info and last scan date/time, control ID, and evidence info All - show posture info (including the percentage of controls that passed for each host), exception info if appropriate, posture summary (the number of assets, controls, and control instances evaluated) and a glossary (host info and last scan date/time), control info, technology info, evidence info When hide_evidence=1 is specified in the same request as details=All or details=Light, then evidence info will not be shown in the output.

Parameter	Description
hide_evidence={**0**|1}	(Optional when details=All or details=Light) Set to 1 to hide the evidence information in the output. When set to 0 or unspecified, evidence information is shown in the output.
show_extended_evidence={**0**|1}	(Optional when details=All or details=Light) Set to 1 to show extended evidence information in the output. When set to 0 or when unspecified, extended evidence information is not shown in the output. Note: You cannot specify show_extended_evidence=1 in the same request as hide_evidence=1. This will result in an Error. Extended evidence is a part of the evidence data and it's shown only when evidence data is shown.
include_dp_name={value}	(Optional) Show the name and ID for each data point in the XML output. This is useful for uniquely identifying data points.
show_remediation_info={**0**|1}	(Optional) Set to 1 to show remediation information in the XML or CSV output. By default, the output does not include the remediation information. When not specified, the remediation information is not included in the output.
cause_of_failure={**0**|1}	(Optional) Set flag to 1 to display the cause of failure of Directory Integrity Monitoring UDCs (user defined controls). When set to 0 or unspecified, cause of failure is not displayed for these UCDs. When set to 1 and Directory Integrity Monitoring UDC control failed assessment, cause of failure info is shown in XML response, i.e. added, removed directories, directories where content changed, permissions changed etc.
truncation_limit={value}	(Optional) The parameter is valid only when the API request is for a single policy and the policy_id parameter is specified. By default, a limit of 5,000 posture info records are returned per request (when "policy_id" is specified). You may specify a value less than the default (1-4999) or greater than the default (5001-1000000) to configure the number records returned per request. If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records. You can specify truncation_limit=0 for no truncation limit. This means that the output is not paginated and all the records are returned in a single output. WARNING: This can generate very large output and processing large XML files can consume a lot of resources on the client side. In this case it is recommended to use the pagination logic and parallel processing. The previous page can be processed while the next page is being downloaded.
ips={value}	(Optional) Show only compliance posture info records for compliance hosts which have certain IP addresses/ranges. One or more IP addresses/ranges may be specified. Multiple IPs/ranges are comma separated.

Parameter	Description
host_ids={value}	(Optional) Show only compliance posture info records for compliance hosts which have certain host IDs and/or ID ranges. One or more host IDs/ranges may be specified. Multiple entries are comma separated. A host ID range entry is specified with a hyphen (for example, 123-125). Valid host IDs are required.
control_ids={value}	(Optional) Show only compliance posture info records for controls which have certain control IDs and/or ranges. One or more control IDs/ranges may be specified. Multiple entries are comma separated. An control ID range entry is specified with a hyphen (for example, 1200-1300). Valid control IDs are required.
ids={value}	(Optional) Show only compliance posture info records for certain compliance posture IDs and/or ID ranges. One or more posture IDs/ranges may be specified. Multiple entries are comma separated. A posture ID range entry is specified with a hyphen (for example, 1-10). Valid posture IDs are required.
id_min={value}	(Optional) Show only compliance posture info records which have a minimum ID value. A valid posture ID is required.
id_max={value}	(Optional) Show only compliance posture info records which have a maximum ID value. A valid posture ID is required.
status_changes_since={date}	(Optional) Show compliance posture info records when the compliance status was changed since a certain date and time (optional). If the policy itself was changed, a warning message is generated. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2008-05-01” or “2008-05-01T23:12:00Z”.
evaluation_date={date}	(Optional) Show compliance posture info records when the posture evaluation date is equal to or greater than a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-04-01” or “2021-04-01T23:12:00Z”.
asset_group_ids={value}	(Optional) Show only hosts in certain asset groups. Provide a comma-separated list of asset group IDs for the asset groups you want to download compliance posture data for. The asset groups specified do not need to be assigned to the one or more policies requested. Posture data will be returned as long as there are common hosts specified by “asset_group_ids” and asset groups that are assigned to the policies requested.
status={Passed|Failed|Error}	(Optional) Show only compliance posture info records which have a posture status of Passed, Failed or Error. By default, records with the status Passed, Failed and Error are listed.

Parameter	Description
criticality_labels={value}	(Optional) Show only compliance posture info records for controls which have certain criticality labels. One or more criticality labels (e.g. SERIOUS, CRITICAL, URGENT) may be specified. Multiple entries are comma separated. Note - This parameter is not available to VMDR SCA customers using this API. This is because SCA customers do not have access to the Controls tab in the UI.
	The parameters criticality_labels and criticality_values cannot be specified in the same request.
criticality_values={value}	(Optional) Show only compliance posture info records for controls which have certain criticality values. One or more criticality values (0-5) may be specified. Multiple entries are comma separated.
	The parameters criticality_labels and criticality_values cannot be specified in the same request.
tag_set_by={id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={all|**any**}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={all|**any**}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
filter_hosts={**0**|1}	(Optional) A Manager or Auditor user can specify filter_hosts=1 to improve performance. The API will skip calling the tag resolution service and directly check the host IDs for the policy. The default value is 0.

DTD

<platform API server>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd

Sample - Posture Info filtered by evaluation date

In this example, we're filtering the output by an evaluation date of 2021-03-05. The XML output will only include info records with an evaluation date equal to or greater than March 5, 2021.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&policy_id=3318470&details=Basic&output_format=xml&evaluation
_date=2021-03-05"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-04-07T21:59:40Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>10911451</ID>
        <HOST_ID>3077710</HOST_ID>
        <CONTROL_ID>1071</CONTROL_ID>
        <TECHNOLOGY_ID>43</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
03T07:12:32Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-04-05T20:36:21Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-03T07:12:32Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2021-04-05T20:36:22Z</LAST_PASS_DATE>
      </INFO>
      <INFO>
        <ID>10911452</ID>
        <HOST_ID>3077710</HOST_ID>
        <CONTROL_ID>1113</CONTROL_ID>
        <TECHNOLOGY_ID>43</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
03T07:12:32Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-04-05T20:36:21Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2020-11-03T07:12:32Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2021-04-05T20:36:22Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
        <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
      </INFO>
      <INFO>
        <ID>10911479</ID>
        <HOST_ID>4640713</HOST_ID>
        <CONTROL_ID>1048</CONTROL_ID>
        <TECHNOLOGY_ID>21</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
```

```
        <POSTURE_MODIFIED_DATE>2020-11-
03T07:12:33Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-03-05T21:35:00Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-03T07:12:33Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2021-03-05T21:35:00Z</LAST_PASS_DATE>
      </INFO>
      <INFO>
        <ID>10911480</ID>
        <HOST_ID>4640713</HOST_ID>
        <CONTROL_ID>1071</CONTROL_ID>
        <TECHNOLOGY_ID>21</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
03T07:12:33Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-03-05T21:35:00Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-03T07:12:33Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2021-03-05T21:35:00Z</LAST_PASS_DATE>
      </INFO>
...
```

Sample - Posture Info with Data Point Name

Sample API request to uniquely identify Data Points using Name and ID.

API request:

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -d headers.15
'https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/?action=
list&policy_id=15472&details=All&include_dp_name=1'
```

XML Response:

```
...
 <DPD_LIST>
        <DPD>
          <LABEL>:dp_1</LABEL>
          <ID>136</ID>
          <NAME><![CDATA[secman.system.clearpageonshut]]></NAME>
         <DESC><![CDATA[This Integer value <B>X</B> indicates the current
status of the setting <B>Shutdown: Clear virtual memory pagefile</B> using
the registry key path
<B>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\Memory Management\ClearPageFileAtShutdown</B>.  A value of
<B>0</B> indicates the setting is <B>Disabled</B>; a value of <B>1</B>
indicates the setting is <B>Enabled</B>.]]></DESC>
        </DPD>
...
<DPD>
```

```
            <LABEL>:dp_3</LABEL>
            <ID>1001035</ID>
            <NAME><![CDATA[custom.win_group_membership.1001035]]></NAME>
            <DESC><![CDATA[IIS_IUSR]]></DESC>
          </DPD>
...
```

Sample - Posture Info with database controls

This applies to database UDCs for Oracle, MSSQL, Sybase, PostgreSQL/Pivotal Greenplum, SAP IQ, and IBM DB2.

When the Posture API output includes database controls, the values returned for the database controls are shown in a tabular format. You'll see these elements in the output: Header (H), Row (R) and Column (C).

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=list&policy_id=1303776&details=All&include_dp_name=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/">
PostureInfo.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-05-03T19:24:32Z</DATETIME>
    <INFO_LIST>
      <INFO>
...
          <DPV_LIST>
            <DPV lastUpdated="2019-05-03T00:33:14Z">
              <LABEL>:dp_2</LABEL>
              <V>
                <H>
                  <C><![CDATA[CustomerID]]></C>
                  <C><![CDATA[CustomerName]]></C>
                  <C><![CDATA[ContactName]]></C>
                  <C><![CDATA[Address]]></C>
                  <C><![CDATA[City]]></C>
                  <C><![CDATA[PostalCode]]></C>
                  <C><![CDATA[Country]]></C>
                </H>
                <R>
                  <C><![CDATA[1]]></C>
                  <C><![CDATA[Alfreds Futterkiste]]></C>
                  <C><![CDATA[Maria Anders]]></C>
                  <C><![CDATA[Obere Str. 57]]></C>
                  <C><![CDATA[Berlin]]></C>
                  <C><![CDATA[12209]]></C>
```

```
                  <C><![CDATA[Germany]]></C>
                </R>
                <R>
                  <C><![CDATA[2]]></C>
                  <C><![CDATA[Ana Trujillo Emparedados y helados]]></C>
                  <C><![CDATA[Ana Trujillo]]></C>
                  <C><![CDATA[Avda. de la Constitucion 2222]]></C>
                  <C><![CDATA[Mexico D.F.]]></C>
                  <C><![CDATA[05021]]></C>
                  <C><![CDATA[Mexico]]></C>
                </R>
                <R>
                  <C><![CDATA[3]]></C>
                  <C><![CDATA[Antonio Moreno Taqueria]]></C>
                  <C><![CDATA[Antonio Moreno]]></C>
                  <C><![CDATA[Mataderos 2312]]></C>
                  <C><![CDATA[Mexico D.F.]]></C>
                  <C><![CDATA[05023]]></C>
                  <C><![CDATA[Mexico]]></C>
                </R>
...
          </GLOSSARY>
  </RESPONSE>
</POSTURE_INFO_LIST_OUTPUT>
```

Sample - Posture Info for File Content Check

API request:

```
curl -u "<username>:<password>" -H "Content-type: text/xml" -X "POST" -d
"action=list&echo_request=1&policy_id=1758961&details=All&include_dp_name
=1" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/">
posture_info_result.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <REQUEST>
    <DATETIME>2019-10-14T21:19:57Z</DATETIME>
    <USER_LOGIN>rey_pt11</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info
/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>list</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
```

```
      </PARAM>
      <PARAM>
        <KEY>policy_id</KEY>
        <VALUE>1758961</VALUE>
      </PARAM>
      <PARAM>
        <KEY>details</KEY>
        <VALUE>All</VALUE>
      </PARAM>
      <PARAM>
        <KEY>include_dp_name</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2019-10-14T21:19:57Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>34544283</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100006</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2019-10-14T21:15:46Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2019-10-14T21:15:46Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2019-10-14T21:15:46Z</LAST_PASS_DATE>
        <EVIDENCE>
<BOOLEAN_EXPR><![CDATA[:dp_2 contains $tp_2]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_2</LABEL>
              <V fileName="c:\Agent\user\test2.txt"><![CDATA[QWEB]]></V>
              <TM_REF>@tm_1</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>34544284</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100000</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2019-10-14T21:15:46Z</EVALUATION_DATE>
```

```
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2019-10-14T21:15:46Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2019-10-14T21:15:46Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
        <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_1 contains $tp_1]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_1</LABEL>
              <V fileName="C:\preTest2.txt"><![CDATA[QWEB]]></V>
              <TM_REF>@tm_2</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>34544285</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100026</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2019-10-14T21:15:46Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2019-10-14T21:15:46Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2019-10-14T21:15:46Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_3 contains $tp_2]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_3</LABEL>
              <V
fileName="C:\user\PreTest\pretestfile1.txt"><![CDATA[pre$]]></V>
              <TM_REF>@tm_3</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
    </INFO_LIST>
    <SUMMARY>
      <TOTAL_ASSETS>1</TOTAL_ASSETS>
      <TOTAL_CONTROLS>3</TOTAL_CONTROLS>
      <CONTROL_INSTANCES>
        <TOTAL>3</TOTAL>
        <TOTAL_PASSED>2</TOTAL_PASSED>
        <TOTAL_FAILED>1</TOTAL_FAILED>
        <TOTAL_ERROR>0</TOTAL_ERROR>
        <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
      </CONTROL_INSTANCES>
```

```
    </SUMMARY>
    <GLOSSARY>
      <HOST_LIST>
        <HOST>
          <ID>7368441</ID>
          <IP>10.115.74.93</IP>
          <TRACKING_METHOD>AGENT</TRACKING_METHOD>
          <DNS><![CDATA[win-890blrmesc6]]></DNS>
          <NETBIOS><![CDATA[WIN-890BLRMESC6]]></NETBIOS>
          <OS><![CDATA[Windows Server 2012 R2 Standard 64 bit
Edition]]></OS>
          <QG_HOSTID>3031a534-6b78-4c4c-aacd-db56257c155f</QG_HOSTID>
          <ASSET_ID>689027</ASSET_ID>
          <LAST_VULN_SCAN_DATETIME>2019-10-
14T19:18:12Z</LAST_VULN_SCAN_DATETIME>
          <LAST_COMPLIANCE_SCAN_DATETIME>2019-10-
14T20:21:07Z</LAST_COMPLIANCE_SCAN_DATETIME>
          <PERCENTAGE><![CDATA[66.67% (2 of 3)]]></PERCENTAGE>
        </HOST>
      </HOST_LIST>
      <CONTROL_LIST>
        <CONTROL>
          <ID>100006</ID>
          <STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[min]]></LABEL>
            <VALUE>1</VALUE>
          </CRITICALITY>
          <RATIONALE_LIST>
            <RATIONALE>
              <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
              <TEXT><![CDATA[rationale]]></TEXT>
            </RATIONALE>
          </RATIONALE_LIST>
        </CONTROL>
        <CONTROL>
          <ID>100000</ID>
          <STATEMENT><![CDATA[preFCCUDC]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[min]]></LABEL>
            <VALUE>1</VALUE>
          </CRITICALITY>
          <RATIONALE_LIST>
            <RATIONALE>
              <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
              <TEXT><![CDATA[rationale]]></TEXT>
            </RATIONALE>
          </RATIONALE_LIST>
        </CONTROL>
        <CONTROL>
          <ID>100026</ID>
          <STATEMENT><![CDATA[pre_fcc_file_path_regexwith$]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[min]]></LABEL>
```

```
            <VALUE>1</VALUE>
          </CRITICALITY>
          <RATIONALE_LIST>
            <RATIONALE>
              <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
              <TEXT><![CDATA[ration]]></TEXT>
            </RATIONALE>
          </RATIONALE_LIST>
        </CONTROL>
      </CONTROL_LIST>
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <ID>75</ID>
          <NAME><![CDATA[Windows Server 2012 R2]]></NAME>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
      <DPD_LIST>
        <DPD>
          <LABEL>:dp_1</LABEL>
          <ID>1007020</ID>
          <NAME><![CDATA[custom.win_file_content_check.1007020]]></NAME>
          <DESC><![CDATA[FileContentChech]]></DESC>
</DPD>
        <DPD>
          <LABEL>:dp_2</LABEL>
          <ID>1007110</ID>
          <NAME><![CDATA[custom.win_file_content_check.1007110]]></NAME>
          <DESC><![CDATA[reg key]]></DESC>
        </DPD>
        <DPD>
          <LABEL>:dp_3</LABEL>
          <ID>1008003</ID>
          <NAME><![CDATA[custom.win_file_content_check.1008003]]></NAME>
          <DESC><![CDATA[pre\$]]></DESC>
        </DPD>
      </DPD_LIST>
      <TP_LIST>
        <TP>
          <LABEL>$tp_1</LABEL>
          <V><![CDATA[true]]></V>
        </TP>
        <TP>
          <LABEL>$tp_2</LABEL>
          <V><![CDATA[.*]]></V>
        </TP>
      </TP_LIST>
      <TM_LIST>
        <TM>
          <LABEL>@tm_1</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
```

```
        </TM>
        <TM>
          <LABEL>@tm_2</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
        </TM>
        <TM>
          <LABEL>@tm_3</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
        </TM>
      </TM_LIST>
    </GLOSSARY>
  </RESPONSE>
</POSTURE_INFO_LIST_OUTPUT>
```

Sample - Posture Info with Extended Evidence parameter

This sample includes 2 INFO records. One record has data for Extended Evidence, and the other record has data for Statistics and Extended Statistics Error.

API request:

```
curl -H "X-Requested-With:curl" -u "<username>:<password>" -d
"action=list&policy_id=1055704&details=All&output_format=xml&show_extende
d_evidence=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-04-28T11:08:05Z</DATETIME>
    <POLICY>
<ID>1055704</ID>    <DATETIME>2022-04-28T11:08:05Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>10461454</ID>
        <HOST_ID>2573671</HOST_ID>
        <CONTROL_ID>1071</CONTROL_ID>
        <TECHNOLOGY_ID>80</TECHNOLOGY_ID>
        <INSTANCE><![CDATA[os]]></INSTANCE>
        <STATUS>Failed</STATUS>
```

```
        <POSTURE_MODIFIED_DATE>2022-04-
27T08:57:38Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2022-05-02T06:21:45Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2022-04-27T08:57:38Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2022-05-02T06:21:45Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2022-04-21T12:05:56Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2022-04-21T12:05:56Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[(:dp_2 in #fv_2 or :dp_2 < $tp_1
)]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2022-04-28T10:03:33Z">
              <LABEL>:dp_2</LABEL>
              <V><![CDATA[5]]></V>
            </DPV>
          </DPV_LIST>
          <EXTENDED_EVIDENCE><![CDATA[Row 1:File name,Setting,Value
Row 2:/etc/login.defs,PASS_MIN_LEN,5
]]></EXTENDED_EVIDENCE>
          <STATISTICS><![CDATA[]]></STATISTICS>

<EXTENDED_STATISTICS_ERROR><![CDATA[]]></EXTENDED_STATISTICS_ERROR>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>10479751</ID>
        <HOST_ID>2573673</HOST_ID>
        <CONTROL_ID>100002</CONTROL_ID>
        <TECHNOLOGY_ID>81</TECHNOLOGY_ID>
        <INSTANCE><![CDATA[os]]></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2022-04-
28T10:09:39Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2022-05-02T06:21:45Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2022-04-28T10:09:39Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2022-05-02T06:21:45Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_8 matches $tp_5]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2022-04-28T10:03:26Z">
              <LABEL>:dp_8</LABEL>
              <V><![CDATA[No data found]]></V>
            </DPV>
          </DPV_LIST>
          <EXTENDED_EVIDENCE><![CDATA[]]></EXTENDED_EVIDENCE>
          <STATISTICS><![CDATA[Search duration: 63 seconds
]]></STATISTICS>
          <EXTENDED_STATISTICS_ERROR><![CDATA[Error Code 28:Base directory
not foundcan't lstat target of '/usr/lib/debug/usr/.dwz ->
/usr/lib/debug/.dwz' (No such file or directory),can't lstat target of
```

'/usr/lib/systemd/system/dbus-org.freedesktop.network1.service -> /usr/lib/systemd/system/systemd-networkd.service' (No such file or directory),can't lstat target of '/usr/lib/modules/3.10.0-327.el7.x86_64/build -> /usr/src/kernels/3.10.0-327.el7.x86_64' (No such file or directory),can't lstat target of '/usr/lib/modules/3.10.0-327.el7.x86_64/source -> /usr/src/kernels/3.10.0-327.el7.x86_64' (No such file or directory),can't lstat target of '/usr/share/gdb/auto-load/bin -> /usr/share/gdb/auto-load/usr/bin' (No such file or directory),can't lstat target of '/usr/share/gdb/auto-load/lib -> /usr/share/gdb/auto-load/usr/lib' (No such file or directory),can't lstat target of '/usr/share/gdb/auto-load/sbin -> /usr/share/gdb/auto-load/usr/sbin' (No such file or directory),can't lstat target of '/usr/share/PackageKit/icons -> /usr/share/pixmaps/comps' (No such file or directory)
]]></EXTENDED_STATISTICS_ERROR>
</EVIDENCE>
</INFO>
...

PC Posture Streaming APIs

The PC Posture Streaming APIs help you have posture data continuously streamed for one host ID at a time for all the specified host IDs for which posture information is available. You can process the data concurrently, which helps you save time and achieve optimum results within a short span of time.

You must use the compliance posture streaming APIs in the following sequence:

- **Get Policy List (optional):** Use the Get Policy List API to fetch the list of policies against which you want to evaluate the compliance posture of your assets.

If you have a list of policy IDs, you can directly use the Resolve Host IDs API.

- **Resolve Host IDs:** Use the policy IDs received from Get Policy List API as the input parameter for Resolve Host IDs. You can specify a maximum of 10 comma-separated policy IDs.

- **Get Posture Info:** Use the host IDs received from Resolve Host IDs as the input parameter to get the posture info in JSON stream.

Note: By default, for each of these APIs, you can send a maximum of 25 API requests per Qualys PC subscription in a 60-second timeframe.

To customize the rate limits as per your requirement, contact your Technical Account Manager or Qualys support.

Before you start, you must authenticate to receive the token needed for the PC Posture API requests. The API Gateway is responsible for authenticating the user who accesses the Posture Streaming APIs to get the posture details.

Input parameters for Auth API:

- username

- password

- token

URL for Auth API: https://gateway.<assigned URL>/auth

```
headers = {'Content-Type': 'application/x-www-form-urlencoded'}
authUrl= 'https://gateway.<assigned URL>/auth'
data = {'username':'username',
'password':'password','token':true}authResp=requests.post(authUrl,
data=data, headers=headers, verify=False)
token=authResp.content.decode('utf-8')
```

Note: Provide the URL, user ID, and password that have been assigned to you. For token, the value can be 'true' or 'True'.

Get Policy List

For API version information, refer to API Version History section.

V1.0 | V2.0

V1.0

/pcrs/1.0/posture/policy/list?lastEvaluationDate=<evaluation date>

[GET]

List all policy IDs as per the last evaluation date specified.

Input Parameters

Parameter	Description
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The format for date and time is YYYY-MM-DD or YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).

Sample JSON output response - Get Policy List

Get Policy List without lastEvaluationDate

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/policy/list -H "accept: */*" -H "Authorization:
Bearer <token>"
```

JSON Response:


```
{
    "subscriptionId": "<SUBSCRIPTION ID>",
    "policyList": [
        {
            "id": "<POLICY ID>",
            "title": "VMWARE 5.5 AND 6.0",
            "createdBy": "<USER NAME>",
            "createdDate": "2018-01-19T07:52:11Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2018-02-01T09:32:33Z",
            "lastEvaluatedDate": "2019-12-19T06:38:46Z",
            "status": "inactive",
            "locked": 0
        },
        {
            "id": "<POLICY ID>",
            "title": "Windows Server 2012",
```

```
                "createdBy": "<USER NAME>",
                "createdDate": "2018-02-02T06:22:16Z",
                "modifiedBy": "<USER NAME>",
                "modifiedDate": "2018-02-22T10:06:25Z",
                "lastEvaluatedDate": "2019-12-19T06:39:05Z",
                "status": "inactive",
                "locked": 0
            },
            {
                "id": "<POLICY ID>",
                "title": "Policy for HPUX",
                "createdBy": "<USER NAME>",
                "createdDate": "2018-04-23T07:14:16Z",
                "modifiedBy": "<USER NAME>",
                "modifiedDate": "2018-04-23T07:15:12Z",
                "lastEvaluatedDate": "2019-12-19T06:37:51Z",
                "status": "inactive",
                "locked": 0
            },

        ....
         ]
    }
```


Get Policy List with lastEvaluationDate

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/policy/list?lastEvaluationDate=2022-02-15T06:04:46Z
-H "accept: */*" -H "Authorization: Bearer <token>"
```

JSON Response:


```
    {
        "subscriptionId": "<SUBSCRIPTION ID>",
        "policyList": [

            {
                "id": "<POLICY ID>",
                "title": "ALL",
                "createdBy": "<USER NAME>",
                "createdDate": "2021-04-08T05:46:39Z",
                "modifiedBy": "<USER NAME>",
                "modifiedDate": "2021-06-16T11:38:54Z",
                "lastEvaluatedDate": "2022-02-17T13:11:19Z",
                "status": "inactive",
                "locked": 0
            },
            {
                "id": "<POLICY ID>",
                "title": "udc_sp",
                "createdBy": "<USER NAME>",
                "createdDate": "2021-04-20T17:40:32Z",
                "modifiedBy": "<USER NAME>",
```

```
                "modifiedDate": "2021-04-20T17:44:48Z",
                "lastEvaluatedDate": "2022-02-17T13:11:08Z",
                "status": "inactive",
                "locked": 0
            },
            {
                "id": "<POLICY ID>",
                "title": "10.115.95.138_agent_fromHostPolicy",
                "createdBy": "<USER NAME>",
                "createdDate": "2021-05-19T23:30:25Z",
                "modifiedBy": "<USER NAME>",
                "modifiedDate": "2021-05-19T23:31:53Z",
                "lastEvaluatedDate": "2022-02-17T12:59:33Z",
                "status": "inactive",
                "locked": 0
            },
            .....
        ]
    }
```

V2.0

/pcrs/2.0/posture/policy/list?lastEvaluationDate=<evaluation date>

[GET]

List all policy IDs as per the last evaluation date specified.

Input Parameters

Parameter	Description
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The format for date and time is YYYY-MM-DD or YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
requireTagInfo	(Optional) Specify '1' to retrieve tag information details for a policy, else specify '0'.

Sample JSON output response - Get Policy List

Get Policy List without lastEvaluationDate

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/policy/list -H "accept: */*" -H "Authorization:
Bearer <token>"
```

JSON Response:


```
{
    "subscriptionId": "<SUBSCRIPTION ID>",
    "policyList": [
        {
            "id": "<POLICY ID>",
            "title": "VMWARE 5.5 AND 6.0",
            "createdBy": "<USER NAME>",
            "createdDate": "2018-01-19T07:52:11Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2018-02-01T09:32:33Z",
            "lastEvaluatedDate": "2019-12-19T06:38:46Z",
            "status": "inactive",
            "locked": 0
        },
        {
            "id": "<POLICY ID>",
            "title": "Windows Server 2012",
            "createdBy": "<USER NAME>",
            "createdDate": "2018-02-02T06:22:16Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2018-02-22T10:06:25Z",
            "lastEvaluatedDate": "2019-12-19T06:39:05Z",
            "status": "inactive",
            "locked": 0
        },
        {
            "id": "<POLICY ID>",
            "title": "Policy for HPUX",
            "createdBy": "<USER NAME>",
            "createdDate": "2018-04-23T07:14:16Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2018-04-23T07:15:12Z",
            "lastEvaluatedDate": "2019-12-19T06:37:51Z",
            "status": "inactive",
            "locked": 0
        },

       ....
        ]
}
```


Get Policy List with lastEvaluationDate

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/policy/list?lastEvaluationDate=2022-02-15T06:04:46Z
-H "accept: */*" -H "Authorization: Bearer <token>"
```

JSON Response:


```
{
    "subscriptionId": "<SUBSCRIPTION ID>",
    "policyList": [
```

```
        {
            "id": "<POLICY ID>",
            "title": "ALL",
            "createdBy": "<USER NAME>",
            "createdDate": "2021-04-08T05:46:39Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2021-06-16T11:38:54Z",
            "lastEvaluatedDate": "2022-02-17T13:11:19Z",
            "status": "inactive",
            "locked": 0
        },
        {
            "id": "<POLICY ID>",
            "title": "udc_sp",
            "createdBy": "<USER NAME>",
            "createdDate": "2021-04-20T17:40:32Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2021-04-20T17:44:48Z",
            "lastEvaluatedDate": "2022-02-17T13:11:08Z",
            "status": "inactive",
            "locked": 0
        },
        {
            "id": "<POLICY ID>",
            "title": "10.115.95.138_agent_fromHostPolicy",
            "createdBy": "<USER NAME>",
            "createdDate": "2021-05-19T23:30:25Z",
            "modifiedBy": "<USER NAME>",
            "modifiedDate": "2021-05-19T23:31:53Z",
            "lastEvaluatedDate": "2022-02-17T12:59:33Z",
            "status": "inactive",
            "locked": 0
        },
       .....
    ]
}
```


Display tag information for a specific policy ID

Request:

```
curl --location
'<gateway_base_url>/pcrs/2.0/posture/policy/list?lastEvaluationDate=20
21-09-30T07%3A25%3A58Z&requireTagInfo=1' \
--header 'Authorization: Bearer <Bearer Token>'
```

JSON Response:


```
{
  "subscriptionId": 4427355,
  "policyList": [
    {
      "id": 6367495,
```

```
      "title": "AssetTagPolicy-1",
      "createdBy": "neaxmn",
      "createdDate": "2026-04-01T05:55:37Z",
      "modifiedBy": "neaxmn",
      "modifiedDate": "2026-04-01T06:16:05Z",
      "lastEvaluatedDate": "2026-04-01T06:16:19Z",
      "tagsetId": "7d5fccf2-dee3-4783-80ac-a2cd5ee493ed",
      "status": "active",
      "locked": 0,
      "includeAgentIp": null,
      "tagInfo": {
        "includeTags": [
          {
            "id": 152244404,
            "name": "pyscand_1.1.1.1_ag"
          },
          {
            "id": 152245230,
            "name": "OCA"
          },
          {
            "id": 154079256,
            "name": "CaponeAG"
          }
        ],
        "excludeTags": [
          {
            "id": 153227435,
            "name": "StaleDataAssestGroupWindows12andCentos7"
          },
          {
            "id": 156570542,
            "name": "dtest"
          }
        ],
        "includeTagsScope": "ANY",
        "excludeTagsScope": "ALL"
      }
    }
  ]
}
```


API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/pcrs/2.0/posture/policy/list	Active	Active
/pcrs/1.0/posture/policy/list	November 2026	May 2027

Resolve Host IDs

For API version information, refer to the API Version History section.

V 1.0 |V 2.0 |V 3.0 | V 4.0 | V 5.0

Note: The V5.0, V4.0, and V3.0 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions V1.0 or V2.0. If you want to enable V5.0, V4.0, and V3.0 to support SCA Asset data, contact your Technical Account Manager (TAM).

V 1.0

API URL:

/pcrs/1.0/posture/hostids?policyId=policyId1, policyId2

[GET]

List all Host IDs for the specified policies.

For the Resolve Host IDs API, you must use the token that is returned by the authentication request. You can include a maximum of 10 policies in one API request.

Input Parameters

Parameter	Description
policyId	(Required) Policy IDs for compliance evaluation.
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=YYYY-MM-DD For example: llastScanDate=2022-05-25 Or, lastScanDate=2022-05-25T18:48:16Z

Sample JSON output response - Resolve Host IDs

Resolve Host IDs with single policy ID

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/hostids?policyId=<POLICY ID> -H "accept: */*" -H
"Authorization: <token>"
```

Response:

```
[
    {
        "policyId": "<POLICY ID>",
        "subscriptionId": "SUBSCRIPTION ID",
        "hostIds": [
            "<HOST ID>"
        ]
    }
      ]
```

Resolve Host IDs with multiple policy IDs

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/hostids?policyId=xxx,xxx -H "accept: */*" -H
"Authorization: <token>"
```

Response:

```
[
  {
        "policyId": "<POLICY ID>",
        "subscriptionId": "<SUBSCRIPTION ID>",
        "hostIds": [
            "<HOST ID>"
        ]
    },
    {
        "policyId": "<POLICY ID>",
        "subscriptionId": "SUBSCRIPTION ID",
        "hostIds": [
            "<HOST ID>"
        ]
    }
]
```

Resolve Host IDs based on the specified date

Request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/hostids?policyId=4677689&lastScanDate=2022-05-25 -H
"accept: */*" -H "Authorization: <token>"
```

Response:

```
    [
        {
            "policyId": "4677689",
```

```
            "subscriptionId": "<SUBSCRIPTION ID>",
            "hostIds": [
                "<HOST ID 1>",
                "<HOST ID 2>",
                "<HOST ID 3>",
                "<HOST ID 4>",
                "<HOST ID 5>",
            ]
        }
    ]
```

V 2.0

API URL:

/pcrs/2.0/posture/hostids?policyId=policyId1, policyId2

[GET]

List all Host IDs for the specified policies.

For the Resolve Host IDs API, you must use the token that is returned by the authentication request. You can include a maximum of 10 policies in one API request.

Input Parameters

Parameter	Description
policyId	(Required) The ID of the policy for which you want to resolve hosts. You can specify a single policy or multiple/all the policies in your subscription using comma-separated values.
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=YYYY-MM-DD For example: lastScanDate=2022-05-25 Or, lastScanDate=2022-05-25T18:48:16Z

Sample JSON output response - Resolve Host IDs

Resolve Host IDs with single policy ID

Request:

```
curl -X GET
<qualys_base_url>/pcrs/2.0/posture/hostids?policyId=POLICY ID-H
```

```
"accept:*/*"-H "Authorization: Bearer token"
```

Response:

```
[
{
"policyId": "<POLICY ID>",
"subscriptionId": "SUBSCRIPTION ID",
"hostIds": [
"<HOST ID>"
]
}
]
```

Resolve Host IDs with multiple policy IDs

Request:

```
curl -X GET <qualys_base_url>/pcrs/2.0/posture/hostids?policyId=xxx,xxx-H
"accept: */*"-H"Authorization: Bearer token"
```

Response:

```
[
{
"policyId": "
<POLICY ID>",
"subscriptionId": "
    <SUBSCRIPTION ID>",
"hostIds": [
"
        <HOST ID>"
]
},
{
"policyId": "
            <POLICY ID>",
"subscriptionId": "SUBSCRIPTION ID",
"hostIds": [
"
                <HOST ID>"
]
}
```

Resolve Host IDs based on the specified date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/2.0/posture/hostids?policyId=4677689&lastScanDate=
2022-05-25-H "accept: */*"-H"Authorization: token"
```

Response:

```
[
    {
        "policyId": "4677689",
```

```
            "subscriptionId": "<SUBSCRIPTION ID>",
            "hostIds": [
                "<HOST ID 1>",
                "<HOST ID 2>",
                "<HOST ID 3>",
                "<HOST ID 4>",
                "<HOST ID 5>",
            ]
        }
    ]
```

V 3.0

API URL:

/pcrs/3.0/posture/hostids?policyId=policyId1, policyId2

[GET]

The V3.0 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions V1.0 or V2.0. If you want to enable V3.0 to support SCA Asset data, contact your Technical Account Manager (TAM).

This new version (/pcrs/3.0/posture/hostids) of this API enables to resolve hostIDs:

- With posture modified (failed or passed) on or after the specified date.
- For all the policies or specific policies in your subscription without any limit on the number of policies.

Note:

- Previously, the policyID parameter was required in the API, but it is now optional. If a policy ID is not provided in the API request, the hosts are resolved for all policies within the subscription.
- For the Resolve Host IDs API, you must use the token that is returned by the authentication request.
- This version of the API can be executed only by the Manager user.

Input Parameters

Parameter	Description
policyId	(Optional) The ID of the policy for which you want to resolve hosts. You can specify a single policy or multiple/all the policies in your subscription using comma-separated values. **Note:** If no Policy ID is provided in the API request, then the hosts are resolved for all the policies in the subscription.
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.

Parameter	Description
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=YYYY-MM-DD For example: lastScanDate=2022-05-25 Or, lastScanDate=2022-05-25T18:48:16Z
statusChangedSince	(Optional) Specify the date to resolve the hosts with posture modified (failed or passed) on or after the specified date.

Sample JSON output response - Resolve Host IDs

Resolve Host IDs with single policy ID

Request:

```
curl -X GET <qualys_base_url>/pcrs/3.0/posture/hostids?policyId=POLICY
ID-H "accept:*/*"-H "Authorization: Bearer token"
```

Response:

```
[
{
"policyId": "<POLICY ID>",
"subscriptionId": "SUBSCRIPTION ID",
"hostIds": [
"<HOST ID>"
]
}
]
```

Resolve Host IDs with multiple policy IDs

Request:

```
curl -X GET <qualys_base_url>/pcrs/3.0/posture/hostids?policyId=xxx,xxx-H
"accept: */*"-H"Authorization: Bearer token"
```

Response:

```
[
{
"policyId": "<POLICY ID>",
"subscriptionId": "<SUBSCRIPTION ID>",
"hostIds": [
"<HOST ID>"
]
},
{
```

```
"policyId": "<POLICY ID>",
"subscriptionId": "SUBSCRIPTION ID",
"hostIds": [
"<HOST ID>"
]
}
]
```

Resolve Host IDs based on the specified date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/3.0/posture/hostids?policyId=4677689&lastScanDate=
2022-05-25-H "accept: */*"-H"Authorization: token"
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "<SUBSCRIPTION ID>",
        "hostIds": [
            "<HOST ID 1>",
            "<HOST ID 2>",
            "<HOST ID 3>",
            "<HOST ID 4>",
            "<HOST ID 5>",
        ]
    }
]
```

Sample JSON output response - Resolve Host IDs based on specific posture modification date

Request:

```
curl -X GET
https://gateway/pcrs/3.0/posture/hostids?policyId=<Policy_ID>&
statusChangedSince= <Date> -H "accept: */*" -H "Authorization: "
```

Response:

```
[
    {
        "policyId": <Policy_ID>,
        "subscriptionId": <Subscription_id>,
        "hostIds": [
            <Host_IDs>,
            <Host_IDs>,
            <Host_IDs>,
        ]
```

```
    }
]
```

V 4.0

API URL:

/pcrs/4.0/posture/hostids?policyId=policyId1, policyId2

[GET]

The V4.0 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions V1.0 or V2.0. If you want to enable V4.0 to support SCA Asset data, contact your Technical Account Manager (TAM).

This new version (/pcrs/4.0/posture/hostids) of this API enables to resolve hostIDs:

- With posture modified (failed or passed) on or after the specified date.
- For all the policies or specific policies in your subscription without any limit on the number of policies.

Note:

- Previously, the policyID parameter was required in the API, but it is now optional. If a policy ID is not provided in the API request, the hosts are resolved for all policies within the subscription.
- For the Resolve Host IDs API, you must use the token that is returned by the authentication request.
- This version of the API can be executed only by the Manager user.

Input Parameters

Parameter	Description
policyId	(Optional) The ID of the policy for which you want to resolve hosts. You can specify a single policy or multiple/all the policies in your subscription using comma-separated values. **Note:** If no Policy ID is provided in the API request, then the hosts are resolved for all the policies in the subscription.
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.

Parameter	Description
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=YYYY-MM-DD For example: lastScanDate=2022-05-25 Or, lastScanDate=2022-05-25T18:48:16Z
statusChangedSince	(Optional) Specify the date to resolve the hosts with posture modified (failed or passed) on or after the specified date.

Sample JSON output response - Resolve Host IDs

Resolve Host IDs with single policy ID

Request:

```
curl -X GET <qualys_base_url>/pcrs/4.0/posture/hostids?policyId=POLICY
ID-H "accept:*/*"-H "Authorization: Bearer Token "
```

Response:

```
[
  {
    "policyId": "<POLICY ID>",
    "subscriptionId": "SUBSCRIPTION ID",
    "hostIds": [
      "<HOST ID>"
    ]
  }
]
```

Resolve Host IDs with multiple policy IDs

Request:

```
curl -X GET <qualys_base_url>/pcrs/4.0/posture/hostids?policyId=xxx,xxx-H
"accept: */*"-H"Authorization: Bearer Token "
```

Response:

```
[
  {
    "policyId": "<POLICY ID>",
    "subscriptionId": "<SUBSCRIPTION ID>",
    "hostIds": [
      "<HOST ID>"
    ]
  },
  {
```

```
    "policyId": "<POLICY ID>",
    "subscriptionId": "SUBSCRIPTION ID",
    "hostIds": [
      "<HOST ID>"
    ]
  }
]
```

Resolve Host IDs based on the specified date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/4.0/posture/hostids?policyId=4677689&lastScanDate=
2022-05-25-H "accept: */*"-H"Authorization:Bearer Token "
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "<SUBSCRIPTION ID>",
        "hostIds": [
            "<HOST ID 1>",
            "<HOST ID 2>",
            "<HOST ID 3>",
            "<HOST ID 4>",
            "<HOST ID 5>",
        ]
    }
]
```

Sample JSON output response - Resolve Host IDs based on specific posture modification date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/4.0/posture/hostids?policyId=<Policy_ID>&
statusChangedSince= <Date>
-H "accept: */*" -H "Authorization: Bearer Token"
```

Response:

```
[
    {
        "policyId": <Policy_ID>,
        "subscriptionId": <Subscription_id>,
        "hostIds": [
            <Host_IDs>,
            <Host_IDs>,
            <Host_IDs>,
        ]
    }
]
```

V 5.0

API URL:

/pcrs/5.0/posture/hostids?policyId=policyId1, policyId2

[GET]

The V5.0 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions V1.0 or V2.0. If you want to enable V5.0 to support SCA Asset data, contact your Technical Account Manager (TAM).

This new version (/pcrs/5.0/posture/hostids) of this API enables to resolve hostIDs:

- With posture modified (failed or passed) on or after the specified date.
- For all the policies or specific policies in your subscription without any limit on the number of policies.

Note:

- Previously, the policyID parameter was required in the API, but it is now optional. If a policy ID is not provided in the API request, the hosts are resolved for all policies within the subscription.
- For the Resolve Host IDs API, you must use the token that is returned by the authentication request.
- This version of the API can be executed only by the Manager user.

Input Parameters

Parameter	Description
policyId	(Optional) The ID of the policy for which you want to resolve hosts. You can specify a single policy or multiple/all the policies in your subscription using comma-separated values. **Note:** If no Policy ID is provided in the API request, then the hosts are resolved for all the policies in the subscription.
Request header: Authorization	(Required) JWT encrypted token. **Note:** Provide the token received from the Authorization API as the input.
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=`YYYY-MM-DD` For example: lastScanDate=`2022-05-25` Or, lastScanDate=`2022-05-25T18:48:16Z`

Parameter	Description
statusChangedSince	(Optional) Specify the date to resolve the hosts with posture modified (failed or passed) on or after the specified date.
assetDeploymentType	(Optional) Filter by asset deployment type: ON-PREM, CLOUD, or ALL.
assetState	(Optional) Filter by asset state: TERMINATED, ACTIVE, or ALL.

Asset Filter Changes

1. The API supports filtering by assetDeploymentType (CLOUD, ON-PREM, ALL).

a. Cloud Assets

i. Identified using integration with connectors (AWS, Azure, GCP).

ii. Deployment type is automatically classified as CLOUD.

b. On-Premises Assets

i. Identified by IP, hostname, or agent installation within corporate datacenters.

ii. Assets not mapped to a cloud provider are categorized as ON-PREM.

iii. For On-Prem assets, state information is not tracked. If assetDeploymentType=ON-PREM is selected, the assetState (see below) filter is ignored.

2. The API supports filtering by assetState (ACTIVE, TERMINATED, ALL). Each cloud provider (AWS, Azure, GCP) exposes multiple lifecycle states, such as, RUNNING, STOPPED, DEALLOCATED, and TERMINATED.To keep API usage consistent, we normalize them into three categories:

a. ACTIVE - Hosts that are not decommissioned are considered active.

b. TERMINATED - Host is permanently deleted or decommissioned, not expected to return.

c. ALL - Includes every state, for broader queries.

Sample JSON output response - Resolve Host IDs

Resolve Host IDs with single policy ID

Request:

```
curl -X GET <qualys_base_url>/pcrs/5.0/posture/hostids?policyId=POLICY
ID-H "accept:*/*"-H "Authorization: Bearer Token "
```

Response:

```
[
  {
    "policyId": "<POLICY ID>",
    "subscriptionId": "SUBSCRIPTION ID",
```

```
    "hostIds": [
      "<HOST ID>"
    ]
  }
]
```

Resolve Host IDs with multiple policy IDs

Request:

```
curl -X GET <qualys_base_url>/pcrs/5.0/posture/hostids?policyId=xxx,xxx-H
"accept: */*"-H"Authorization: Bearer Token "
```

Response:

```
[
  {
    "policyId": "<POLICY ID>",
    "subscriptionId": "<SUBSCRIPTION ID>",
    "hostIds": [
      "<HOST ID>"
    ]
  },
  {
    "policyId": "<POLICY ID>",
    "subscriptionId": "SUBSCRIPTION ID",
    "hostIds": [
      "<HOST ID>"
    ]
  }
]
```

Resolve Host IDs based on the specified date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2022-05-25-H "accept: */*"-H"Authorization:Bearer Token "
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "<SUBSCRIPTION ID>",
        "hostIds": [
            "<HOST ID 1>",
            "<HOST ID 2>",
            "<HOST ID 3>",
            "<HOST ID 4>",
            "<HOST ID 5>",
        ]
    }
]
```

Sample JSON output response - Resolve Host IDs based on specific posture modification date

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=<Policy_ID>&
statusChangedSince= <Date>
-H "accept: */*" -H "Authorization: Bearer Token"
```

Response:

```
[
    {
        "policyId": <Policy_ID>,
        "subscriptionId": <Subscription_id>,
        "hostIds": [
            <Host_IDs>,
            <Host_IDs>,
            <Host_IDs>,
        ]
    }
]
```

Sample - Retrieve all active cloud assets for a given policy

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08-25&assetDeploymentType=CLOUD&assetState=ACTIVE ' \-H 'accept:
*/*' -H 'Authorization: Bearer <AuthToken>
```

Response:

```
[
 {
  "policyId": "4677689",
        "subscriptionId": "41",
        "hostIds": [
            "924781",
            "724905"
        ]
    }
]
```

Sample - Retrieve cloud assets that are permanently decommissioned

Request:

```
curl -X GET
```

```
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08- 25&assetDeploymentType=CLOUD&assetState=TERMINATED ' \
-H 'accept: */*' -H 'Authorization: Bearer <AuthToken>’
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "41",
        "hostIds": [
            "504718”
        ]
    }
]
```

Sample - For On-Premises assets, state is not tracked

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08-25&assetDeploymentType=ON-PREM' \
-H 'accept: */*' -H 'Authorization: Bearer <AuthToken>’
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "41",
        "hostIds": [
            "3001",
            "3002",
            "3003"
        ]
    }
]
```

Sample - deploymentType and assetState fields are omitted

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08- 25 ' \
-H 'accept: */*' -H 'Authorization: Bearer <AuthToken>’
```

Response:

```
[
```

```
    {
        "policyId": "4677689",
        "subscriptionId": "41",
        "hostIds": [
            "924781",
            "724905",
            "504718",
        ]
    }
]
```

Sample - deploymentType is set to ALL and assetState is ACTIVE

Request:

```
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08- 25&assetDeploymentType=ALL&assetState=ACTIVE ' \
-H 'accept: */*' -H 'Authorization: Bearer <AuthToken>’
OR
curl -X GET
<qualys_base_url>/pcrs/5.0/posture/hostids?policyId=4677689&lastScanDate=
2025-08- 25&assetState=ACTIVE ' \
-H 'accept: */*' -H 'Authorization: Bearer <AuthToken>’
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "41",
        "hostIds": [
            "924781",
            "724905",
            "3001",
            "3002",
            "3003"
        ]
    }
]
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/pcrs/5.0/posture/hostids?	Active	Active
/pcrs/4.0/posture/hostids?	Active	Active
/pcrs/3.0/posture/hostids?	Active	Active
/pcrs/2.0/posture/hostids?	Active	Active
/pcrs/1.0/posture/hostids?	November 2026	May 2027

Get Posture Info

For API version information, refer to the API Version History section.

V1.0 |V2.0 |V3.0|V4.0|V5.0

Note: The V3 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions V1 or V2.

V1.0

Note: Execute this API only after successful execution of Resolve Host Ids API. If you encounter any errors while executing the Resolve Host Ids API, then rectify them before executing this API.

API URL:

/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=1&lastEvaluationDate=2021-12-23

[POST]

Get continuous posture information for all the specified hosts for each policy ID included in the API.

To get posture information, you must use the host IDs retrieved in the Resolve Host IDs API request.

Input Parameters

Parameter	Description
evidenceRequired	Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note:** Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	Default value is 1, which indicates that the output will be compressed. If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
Request Body	Output of the Resolve Host ID and the JWT token.
Request header: Authorization	(Required) JWT encrypted token. **Note:** The token received from the Authorization API and the token used in the second API need to be the input here.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
lastScanDate	(Optional) Compliance posture information on the date on which an asset was last scanned. The formats for date are: lastScanDate=2021-12-17 Or, lastScanDate=2021-12-17T18:48:16Z

Parameter	Description
lastScanDateFrom, lastScanDateTo	(Optional) Compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.
statusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)

Sample JSON output response - Get Posture Info (single policy ID)

Get posture Info With lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0&lastEvaluationDate=2021-12-23" -H "accept: */*" -H "Authorization:
Bearer <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION
ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON Output

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
       "controlStatement": "Status of the 'banner motd' configuration
command on the device",
      "rationale": "The 'Message of the Day (banner motd)' command is
used to provide a warning banner displayed when a connection to the
device is made BEFORE a user successfully authenticates to the device.
The Message of the Day banner can be used to provide an acceptable use
policy or warning prior to login notifying that all user activity may
be monitored and potential legal consequences may result from
```

```
unauthorized use.  Run this check periodically to ensure content of the
banner displayed is in compliance with the requirements and
expectations driven by internal standards and/or policies.",
        "remediation": "Execute following commands to set desired
banner message:\n1. configure terminal\n2. banner motd 'delimiting-
character' 'message' 'delimiting-character'\n3. exit\n\nc",
        "controlReference": null,
        "technologyId": xxx,
        "status": "Error",
        "previousStatus": "Error",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-21T11:28:21Z",
        "lastPassDate": "2021-12-21T11:29:22Z",
        "postureModifiedDate": "2021-12-22T12:56:41Z",
        "lastEvaluatedDate": "2021-12-23T05:32:40Z",
        "created": "2022-02-21T13:10:13Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco::7.0%283%29i2%282%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-22T12:49:59Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xxx,
            "name": "Cisco NX-OS"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 1,
        "totalBatches": 1
    }
```


GET Get Posture Info Without lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=0 and compressionRequired=0

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0" -H "accept: */*" -H "Authorization: <token>" -H "Content-Type:
```

```
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\
"]}]"
```

JSON Response:


```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL ID>,
        "technologyId": xx,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:54:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":  "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "xxx",
        "customerId": "xxx",
        "assetId": "xxx",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": null,
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
```

```
                    ]
                },
                "unexpected": {
                    "value": [
                        "0"
                    ]
                }
            }
        },
        {
            "id": xxx,
            "instance": "os",
            "policyId": "<POLICY ID>",
            "policyTitle": "<POLICY TITLE>",
            "netBios": "<NETBIOS>",
            "controlId": "<CONTROL ID>",
            "technologyId": "<TECHNOLOGY ID>",
            "status": "Passed",
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-25T07:21:13Z",
            "lastPassDate": "2021-10-29T07:52:41Z",
            "postureModifiedDate": "2021-10-25T07:21:11Z",
            "lastEvaluatedDate": "2021-10-29T07:52:41Z",
            "created": "2021-10-29T07:54:26Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "xxxx",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Windows Server 2012 R2"
            },
            "criticality": {
                "label": "URGENT",
                "value": 5
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info Without lastEvaluationDate, Without Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=0 & compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=1" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-
Type: application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\
"]}]"
```

JSON Output (Compressed)

```
‹        íÝ]sÚHÅñ¯ââ:Îê!ÁÝ¬íUœIì8©š©©)
²CD2S©|÷•p2Ž_ÖôÁý€ÿ»d.~é´8:ýÛçÆ ßè„í(ÈÒfð¬1OËî¸—
7:ÚxÖ¸,†ƒÞß‡Õ6Í(ŠÓ${Öè-ãrR
ëÇÂ0Kž5Ê¼÷~\
‹‹ùviõHµ6-öñª;æýz?"üã MOî<s>LËÿtÃýnY¿lõÐ°{û‘ùFõ?}(
¢p7
v£äM?¢° Æ¿~ýÁû¶j×[%QSþ:ÿ?ål'-ýÁù
ïÿß]†ßvyð±;œU[ÝÙôæ~{"¼Þèî--N Ô?¼¯^¸>DY«?ÚÍêh_V?‡Áó0|ž-Ï›QµM9éö>
ÆGyù¾¨÷uøªz´ú,:ãÙpXÿiï²~½Ë¼ó¯¢3ô&Å´8/;Ÿ-ã~ñiúÇ4Ÿ|Ì'?DAu&Q§óW«Ù©öÐ×G½WŒ
úùÇéŸÃêéVõèŸÿ-ÞS}
\í}œ—
ŸŠÉ‡úM6,Æ???ÙÕ¯ùó°8ëwöóóîlXî¼¼z²þÍ‹ÑåpPŸ7/ªÃuÒëŽo©ìMØêÄíN'ÌÔlZ£|r:?Ì_
©?giž-»ÙYÔÚM³óóÝ,l&»Ažeaë¼?¦çßýÔüÝEIPí»z´>Ê«‡Â´aiý¾¯OÉFçê ¯OËñÕ¯ñîêHí
œÌÔN}¤vŽ£Æ—ú ?"ƒ^w8(ç?7ìžåÃêöŽß?îýô¢Úq}&TûhV?W't?ŸS¹:v½îlšÿr^Ÿ¸ÕÙuõè—
g7€…*°(lE ÀÜ€Eò´C€ìvrp|øËéÉµ¯x9_±î+Å¾~t_Gû‡§G×¼¢åx5—
àõðÿëW»Ÿ×?ÏÜæõ€œû¶°y†ßfx—
?¼àµ'áësc4N«Or¾§âbÐû¶å×ÔÖ¨ßþOe9œÍÊ|g\";çÅl\£8wÏ†ùNYìLòêùüc¾sYý¢Õáîï\'l
ü^½‡Ù8ÿë2ïÍO°Ï×û
ª'¿Ü²?ñ_Sæ~ØþÑmŸÿ|ðòÍ5íd¹¡³uƒ×ÑÉÉëõ‹ ·:Õ¹ÖŒãÎü'êß'·ÇW{ûoû»çâf5Þ €Oàü¼
ü*ðèÛAÛ©
\;l-âLêª}—@aC>À0óÏ°•Á †0T¶-Æ0„!
Ý&Žvð0C.¼Âp›.¾úª]?MBÄw¾›d,1^K#†Ì,aC…aìŸa0Â †
Ã¦Ã&
aCªbÁpÁ—ÿ\àª63t^×Õo÷mý—éwÙ°.û„÷\öñŸë©h·a¡
ma„5Èõ¤-æ›0„¡ÂÐ ×"'ëªv0ôtdb ëI‰õ …,Â-Aª'‹P^B
```

Get Posture Info Without lastEvaluationDate, With Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
1" -H "accept: */*" -H "Authorization: <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)

```
‹        í?sÛFš@ÿ
```

```
JµöÎˆ ¼€|"%yâÄr  SvR"ÌNQ$LaC4 ÚÖÌä¿o7HJ¼
ša‹"qR•*YÂµÑ}ú,ßùõß'^ÿ¤mµª¦Ó¬™?=ñü(îú=÷¤}D'?=C¯wÿFlS«VífÝùëI/ðã0ÊßY-
SÿëIìöîü`
'íšâ7âñ$Ç¸îF'Û—ÇÝ/^0‰:k?ùä…Qü°ë
/°±<-øÕ°»ú›d#¹ËìWU³j‰æiµ~c6ÛU«mÙ?Ÿí¶UKnU¯¶kÖß"{ŠâIè^}ï"çö3iÍyù¥;œˆ-Ö6]
>n/tåFë?ÔÚõ†ÜàNœX'ÓhÕ?-š(í±ØØ2+-
Uiš•ZUl ‡ÝÞïž?¸rã»@ëÍµø-xm?2?ÊŸÎÇòzc·ý?A{äõÂ
>Åí¯žß¾FÿŒÜð‹?þ³jZÕvXm·¿5jmq„¾/K½Œúî—
èóPü¹!~ûyð?&Y¦G÷Ýøk þ./òÄ<yø÷»îHžóoÃà¶;4.ÜOÝÉ06ÞMÿ(ï<⁋ž¬7oEquz]?µ¤œ?
«Ñ®‹²p''šDq0rÃ /9S×všnÓ<un«Ø¦óéÓ©cÕê§¦Õ¼u¬Æ§®Õü´°WruÕ°)Ž-
~+ëQ<ý•ÕlÕ?¼îÇ*yÒžVqY-ýémü<-)£"””!KÊx_=ùC>A/özÝ¡'û
»·îPìpþþÍÍ›ó³·âÀ²&^cÔÄÆ¢B÷Ý¤©üûÄý6v{âÙ?”?-
ý›?áEÝÛ¡Û7^7?óOþ3~|o,þû7ÿÒŸmjånúÞt&·?¸÷†ÄÆ§`â÷óvYÚ8)Ç0týx~-¿ž,^êÉ?D'öâ
Iw8ÿû´fô½PÜa Þ¿öFú½é¯e'u''ûã'Ù\E›šÿz+-*VªV£
VÀ
```


Get Posture Info Without lastEvaluationDate, With Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequir
ed=0" -H "accept: */*" -H "Authorization: <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"xxx\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output:

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
```

```
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "xxx",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
           "expectedValues": "\nAttribute not found\n------------ OR -
-----------\nUnable to retrieve password policy\n------------ OR -----
-------\nequal to\n1",
            "currentValues": [
                "0"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:PCDEV",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
```

```
            "firstPassDate": "2021-10-25T07:21:13Z",
            "lastPassDate": "2021-10-29T07:52:41Z",
            "postureModifiedDate": "2021-10-25T07:21:11Z",
            "lastEvaluatedDate": "2021-10-29T07:52:41Z",
            "created": "2021-10-29T07:55:27Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:39:55Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "SERIOUS",
                "value": 3
            },
            "evidence": {
                "expectedValues": "\nGrantees not found\n------------ OR -
----------\nmatches regular expression list\n.*",
                "currentValues": [
                    "Grantees not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null
            },
            "causeOfFailure": null
        }
    ]
```


Sample JSON output response - Get Posture Info (multiple policy IDs)

Get Posture Info with lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequir
ed=0&lastEvaluationDate=2021-12-27T15:35:22Z" -H "accept: /" -H
"Authorization: Bearer <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<Policy_ID>\",\"subscriptionId\":\"<Subscription_ID>
\",\"hostIds\":[\"<Host_ID1>\"]},{\"policyId\":\"policyId1\",\"subscri
```

```
ptionId\":\"<Subscription_ID\",\"hostIds\":[\"<HOST_ID1>\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL_ID,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
       "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting
a 'minimum password length' requirement.  Each character that is added
to the password length squares the difficulty of breaking the password
via 'brute force,' which attempts using every combination possible
within the password symbol set-space, in order to discover a user's
password.  While no 'minimum length' can be guaranteed secure, eight
(8) is commonly considered to be the minimum for most application
access, along with requiring other password security factors, such as
increasing the size of the symbol set-space by requiring mixed-cases,
along with other forms of password variability creation, increases the
difficulty of breaking any password by brute-force attack.",
       "remediation": "To establish the recommended configuration via
GP, set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-12T13:12:26Z",
        "lastPassDate": "2021-12-27T15:35:22Z",
        "postureModifiedDate": "2021-10-12T13:12:26Z",
        "lastEvaluatedDate": "2021-12-27T15:35:22Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "DNS Hostname",
        "os": xx,
        "osCpe": "cpe:/o:microsoft:windows_2003_server::sp2::",
        "domainName": "<DOMAIN NAME>",
        "dns": "client5-25-244.root.vuln.qa.qualys.com",
        "qgHostid": xx,
        "networkId": xx,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-27T15:31:18Z",
        "customerUuid": "xx",
        "customerId": "xx",
```

```
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "Windows 2003 Server"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": xx
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n0",
            "currentValues": [
                "1"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null,
        "currentBatch": xx,
        "totalBatches": xx
    },
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL_ID>,
        "controlStatement": "Status of the
'net.ipv4.conf.all.send_redirects' setting within the
'/etc/sysctl.conf' file",
        "rationale": "The 'net.ipv4.conf.all.send_redirects' network
parameter (/etc/sysctl.conf) allows ICMP routing redirection.  If the
system is not going to be used as a firewall or gateway to pass network
traffic, and this parameter is not disabled, malicious users may
attempt to spoof source addresses or redirect traffic to a host with a
network sniffer, so this value should be set according to the needs of
the business.",
        "remediation": "Set the following parameters in the
/etc/sysctl.conf file:\n\n# net.ipv4.conf.all.send_redirects = 0\n\nOR
\nRun the following commands to set the active kernel parameters:\n#
sysctl -w net.ipv4.conf.all.send_redirects=0\n# sysctl -w
net.ipv4.route.flush=1",
        "controlReference": null,
        "technologyId": 80,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-02-11T12:54:23Z",
        "lastPassDate": "2022-02-11T12:54:23Z",
        "postureModifiedDate": "2022-02-11T12:54:23Z",
        "lastEvaluatedDate": "2022-02-11T12:54:23Z",
        "created": "2022-02-24T14:21:06Z",
```

```
            "hostId": xx,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
            "domainName": "<DOMAIN NAME>",
            "dns": null,
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2022-02-11T12:47:29Z",
            "customerUuid": "xx",
            "customerId": "xx",
            "assetId": xx,
            "technology": {
                "id": xx,
                "name": "CentOS 7.x"
            },
            "criticality": {
                "label": "CRITICAL",
                "value": 4
            },
            "evidence": {
                "expectedValues": "\nSetting not found\n------------ OR --
----------\nFile not found\n------------ OR ------------\nmatches
regular expression list\n.*",
                "currentValues": [
                    "Setting not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null
            },
            "causeOfFailure": null,
            "currentBatch": 1,
            "totalBatches": 1
        }
    ]
```


Get Posture Info without lastEvaluationDate, without evidence, without compression, without lastScanDate

User Input: evidenceRequired=0 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-
Type: application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
,{\"policyId\":\"policyId1\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\
"]}]"
```

JSON Output:

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:38:14Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": null,
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
```

```
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "xxxx",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "CRITICAL",
        "value": 4
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": 19235413,
    "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-28T16:53:06Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-28T16:53:06Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:15Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
```

```
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:53:14Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info without lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request**:**

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequir
ed=0" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-
Type: application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
,{\"policyId\":\"policyId1\",\"subscriptionId\":\"xx\",\"hostIds\":[\"
xx\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
```

```
        "created": "2021-10-29T08:40:38Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nFilter 2 not found: ^[\\*\\.\\d]\n---
--------- OR ------------\nFilter 1 not found: show clock detail\n----
-------- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "show clock detail:08:26:29.074 pdt Thu Oct 14 2021"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-28T16:53:06Z",
        "lastPassDate": "2021-10-29T08:39:07Z",
        "postureModifiedDate": "2021-10-28T16:53:06Z",
        "lastEvaluatedDate": "2021-10-29T08:39:07Z",
        "created": "2021-10-29T08:40:46Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
```

```
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": {
               "expectedValues": "\nSet status to PASS if no data found\n-
----------- OR ------------\nmatches regular expression list\n.*",
                "currentValues": [
                    "Error Code 35:Failed to execute database query"
                ],
                "actualValues": null,
                "directoryFimUdc": null
            },
            "causeOfFailure": null
        }
    ]
```


Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

User input: evidenceRequired=0 & compressionRequired=1 & lastScanDate=yyyy-mm-dd:Thh:mm:ssZ

Request:

```
Curl-X POST
"https://<qualys_base_url>/pcrs/1.0/posture/postureInfo?evidenceRequir
ed=0&compressionRequired=1&lastEvaluationDate=2021-12-
17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z" -H
"accept: */*" -H
"Content-Type: application/json" -d "
[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

JSON output:


```
    [
        {
            "id": <HOST INSTANCE ID>,
            "instance": "os",
```

```
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
        "osCpe": null,
       "domainName": "<DOMAIN NAME>",
        "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-23T12:59:04Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 217,
            "name": "Red Hat Enterprise Linux 8.x"
```

```
            },
            "criticality": {
                "label": "CRITICAL",
                "value": 4
            },
            "evidence": null,
            "causeOfFailure": null,
            "currentBatch": 8,
            "totalBatches": 12
        },
    ]
```

Get Posture Info without evidence, without compression, with statusChangedSince

Request:

```
curl -X POST
"https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0&statusChangedSince=2021-12-23" -H "accept: */*" -H
"Authorization: Bearer <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONID>\"
,\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON output:

```
[
    {
        "id": 24705485,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "pcas_win16_redhat7 tech",
        "netBios": "<NETBIOS>",
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
       "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting
a 'minimum password length' requirement.  Each character that is added
to the password length squares the difficulty of breaking the password
via 'brute force,' which attempts using every combination possible
within the password symbol set-space, in order to discover a user's
password.  While no 'minimum length' can be guaranteed secure, eight
(8) is commonly considered to be the minimum for most application
access, along with requiring other password security factors, such as
increasing the size of the symbol set-space by requiring mixed-cases,
along with other forms of password variability creation, increases the
difficulty of breaking any password by brute-force attack.",
       "remediation": "To establish the recommended configuration via
GP, set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": 106,
        "status": "Passed",
```

```
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2022-11-09T12:50:12Z",
            "lastPassDate": "2022-12-06T06:42:21Z",
            "postureModifiedDate": "2022-11-09T12:50:12Z",
            "lastEvaluatedDate": "2022-12-06T06:42:21Z",
            "created": "2022-12-07T07:35:56Z",
            "hostId": <HOST ID>,
            "CLOUD_RESOURCE_ID": null,
            "ip": "xx.xx.xx.xxx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2016:1607::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "<DNS>",
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2022-08-23T04:57:05Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": <ASSET ID>,
            "technology": {
                "id": 106,
                "name": "Windows 2016 Server"
            },
            "criticality": {
                "label": "high updated",
                "value": 5
            },
            "evidence": {
               "expectedValues": "\nAttribute not found\n------------ OR -
----------\ngreater than or equal to\n0",
                "currentValues": [
                    "6"
                ],
                "actualValues": null,
                "directoryFimUdc": null
            },
            "causeOfFailure": null,
            "currentDataSizeKB": "2.41",
            "totalDataSizeKB": "2.41",
            "currentBatch": 1,
            "totalBatches": 1
        },
    ]
```


V2.0

API URL:

<qualys_base_url>/pcrs/2.0/posture/postureInfo?

[POST] [GET]

Input Parameters

Parameter	Description
Authentication Token (Bearer Token)	(Required) Specify the authentication token that is returned by the authentication request.
evidenceRequired	(Optional) Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note:** Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	(Required) Default value is 1, which indicates that the output will be compressed. If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
Request Body	(Required) Output of the Resolve Host ID and the JWT token.
Request header: Authorization	(Required) JWT encrypted token. **Note:** The token received from the Authorization API and the token used in the second API need to be the input here.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
lastScanDate	(Optional) Compliance posture information on the date on which an asset was last scanned. The formats for date are: lastScanDate=2021-12-17 Or, lastScanDate=2021-12-17T18:48:16Z
lastScanDateFrom, lastScanDateTo	(Optional) Compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.

Parameter	Description
statusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)
excludeInactiveControl	(Optional) Default value is 0, which indicates that inactive controls data is retrieved for the host posture. If you want to exclude inactive control data then, change the value to 1.

Sample - Get Extended Evidence for a Control

Using this V2 API URL you can retrieve extended evidence and last updated date information for the hosts. The evidence for a control includes the expected and actual values for the control on the host. The extended evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result. To retrieve the extended information in the API response, specify the following input parameters.

API Request

<qualys_base_url>/pcrs/2.0/posture/postureInfo?compressionRequired=0&evidenceRequired=1

Json Output


```
{
"id": xx,
"instance": "os",
"policyId": 725886,
"policyTitle": "AllTech_policy",
"netBios": null,
"controlId": xx,
"controlStatement": "Status of the 'Minimum Password
Length' setting",
"rationale":
"Among the several characteristics that make'user identification' via
password a secure and workable solution
is setting a 'minimum password length' requirement. Each
character that is added to the password length squares the
difficulty of breaking the password via 'brute force,' which
attempts using every combination possible within the password
symbol set-space, in order to discover a user's password. While no
'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along
with requiring other password security factors, such as increasing
the size of the symbol set-space by requiring mixed-cases, along
with other forms of password variability creation, increases the
```

```
difficulty of breaking any password by brute-force attack.",
"remediation": "To specify password length requirements for
new accounts, edit the file \"/etc/login.defs\" and add or correct
the following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\"
and also another PAM module (such as \"pam_cracklib\") during a
password change operation, then the most restrictive must be
satisfied.",
"controlReference": null,
"technologyId": 80,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-07-04T13:58:08Z",
"lastFailDate": "2024-01-23T12:56:18Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-07-04T13:58:08Z",
"lastEvaluatedDate": "2024-01-23T12:56:18Z",
"created": "2024-02-02T13:02:57Z",
"hostId": xx,
"ip": "xx.xx.xx.xxx",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2023-07-04T13:59:25Z",
"customerUuid": "xx-xx-xx-xx-xx",
"customerId": "xx",
"assetId": xx,
"technology": {
"id": 80,"name": "CentOS 7.x"
},
"criticality": {
"label": "URGENT",
"value": 5
},
"evidence": {
"expectedValues": "\ngreater than or equal to\n9",
"currentValues": [
"5"
],
"actualValues": null,
"directoryFimUdc": null,
"lastUpdated": "2023-07-04T13:59:25Z",
"extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n"
}
```

Sample - Exclude Inactive Control Data

You can include/exclude inactive controls (SDC, UDC) from the host compliance posture information in the API response. Inactive controls are the controls removed or deactivated from a policy.

API Request

<qualys_base_url>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compressionRequired=0&excludeInactiveControl=1

JSON Output


```
{
"id": xx,
"instance": "oracle19cdb:1:1527:ora19csu",
"policyId": xx,
"policyTitle": "Oracle_DB_UDC",
"netBios": null,
"controlId": 100432,
"controlStatement": "Oracle_DB_UDC_3",
"rationale": "rationle",
"remediation": "Remediation",
"controlReference": null,
"technologyId": 312,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-06-08T09:52:13Z",
"lastFailDate": "2023-08-24T10:00:05Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-06-08T09:52:13Z",
"lastEvaluatedDate": "2023-08-24T10:00:05Z",
"created": "2024-01-30T06:54:04Z",
"hostId": xx,
"ip": "xx.xx.xx.xx",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2024-01-05T10:24:32Z",
"customerUuid": "xx-xx-xx-xx-xx",
"customerId": "xx",
"assetId": xx,
"technology": {
"id": 312,
"name": "Oracle 19c Multitenant"
},
"criticality": {
"label": "SERIOUS",
"value": 3
},
```

```
"evidence": {
"expectedValues": "\nSet status to PASS if no data found",
"currentValues": [
"GRANTEE|:|GRANTED_ROLE",
"APPQOSSYS|:|DBA",
"UDC_SENSITIVE_SCAN|:|DBA",
"QUALYS_SCAN|:|DBA"
],
"actualValues": null,
"directoryFimUdc": null
},
"causeOfFailure": {
"missing": {
"logic": null,
"value": [
"------------ OR ------------",
"Set status to PASS if no data found"
]
},
"unexpected": {
"value": [
"DBA,DBA,DBA",
"APPQOSSYS,UDC_SENSITIVE_SCAN,QUALYS_SCAN"
]
}
},
"currentDataSizeKB": "1.47",
"totalDataSizeKB": "4.59",
"currentBatch": 1,
"totalBatches": 1,
"CLOUD_RESOURCE_ID": null
}
```


Sample - Retrieve Compliance Posture Information along with Control Status

API response now displays the status of the controls on a host as passed when an exception has been created and approved. The controls on which the exception has been approved are displayed as Passed*. Exception is a way to temporarily change the status of a control on a host from Failed to PassedE (passed with an exception). To learn about what is exceptions refer to Exceptions- The Basics.

API Request

```
https://<qualys_base_url>/pcrs/2.0/posture/postureInfo?compressionRequired=0' \ --header 'accept: */*'
\ --header 'Authorization: Bearer <Auth Token>' \ --header 'Content-Type: application/json'
\ --data '[  {  "policyId": "xx",  "subscriptionId": "xx",  "hostIds": [  "xx"  ]
} ]'
```

JSON Response


```
{
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "LinuxAllAssetScan_withAssetTag",
```

```
            "netBios": null,
            "controlId": xx,
            "controlStatement": "File_content_check_udc-2",
            "rationale": "rationale",
            "remediation": null,
            "category": "Access Control Requirements",
            "subCategory": "Authentication/Passwords",
            "controlReference": null,
            "technologyId": 43,
            "status": "Passed*",
            "previousStatus": "Error",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "",
            "lastPassDate": "",
            "postureModifiedDate": "2024-07-10T15:10:32Z",
            "lastEvaluatedDate": "2024-08-25T17:36:31Z",
            "created": "2024-08-29T10:58:49Z",
            "hostId": xx,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": null,
            "domainName": null,
            "dns": null,
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2024-06-10T17:08:52Z",
            "customerUuid": "xx-xx-xx-xx-xx",
            "customerId": "xx",
            "assetId": xx,
            "technology":
    {             "id": 43,             "name": "CentOS 6.x"          }
    ,
            "criticality":
    {             "label": "MEDIUM",             "value": 2          }
    ,
            "evidence": null,
            "causeOfFailure": null,
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "1.14",
            "totalDataSizeKB": "1.14",
            "currentBatch": 1,
            "totalBatches": 1,
            "CLOUD_RESOURCE_ID": null
        }
```


Sample - Retrieve Compliance Posture Information along with Control Category and Sub-Category

Two new fields in the API response to display control category and sub-category.

- category -Displays control category set on a particular control.

- SubCategory - Displays control Subcategory set on a particular control.

API Request

```
https://<qualys_base_url>/pcrs/2.0/posture/postureInfo?compressionRequired=0' \ --header
'accept: */*'
\ --header 'Authorization: Bearer <Auth Token>'
\ --header 'Content-Type: application/json'
\ --data '[    {        "policyId": "xx",        "subscriptionId": "xx",        "hostIds": [            "xx"        ]
} ]'
```

JSON Response


```
{
  "id": xx,
  "instance": "os",
  "policyId": xx,
  "policyTitle": "LinuxAllAssetScan_withAssetTag",
  "netBios": null,
  "controlId": xx,
  "controlStatement": "File_content_check_udc-2",
  "rationale": "rationale",
  "remediation": null,
  "category": "Access Control Requirements",
  "subCategory": "Authentication/Passwords",
  "controlReference": null,
  "technologyId": 43,
  "status": "Passed*",
  "previousStatus": "Error",
  "firstFailDate": "",
  "lastFailDate": "",
  "firstPassDate": "",
  "lastPassDate": "",
  "postureModifiedDate": "2024-07-10T15:10:32Z",
  "lastEvaluatedDate": "2024-08-25T17:36:31Z",
  "created": "2024-08-29T10:58:49Z",
  "hostId": xx,
  "ip": "xx.xx.xx.xx",
  "trackingMethod": "IP",
  "os": null,
  "osCpe": null,
  "domainName": null,
  "dns": null,
  "qgHostid": null,
  "networkId": 0,
  "networkName": "Global Default Network",
  "complianceLastScanDate": "2024-06-10T17:08:52Z",
  "customerUuid": "xx-xx-xx-xx-xx",
  "customerId": "xx",
  "assetId": xx,
  "technology": {
    "id": 43,
    "name": "CentOS 6.x"
  },
  "criticality": {
```

```
    "label": "MEDIUM",
    "value": 2
  },
  "evidence": null,
  "causeOfFailure": null,
  "userDefinedAttributesList": null,
  "currentDataSizeKB": "1.14",
  "totalDataSizeKB": "1.14",
  "currentBatch": 1,
  "totalBatches": 1,
  "CLOUD_RESOURCE_ID": null
}
```

Sample JSON output response - Get Posture Info (single policy ID)

Get posture Info With lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

API Request

```
curl -X POST "https://gateway.<assigned URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&lastEvaluationDate=2021-12-23" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-Type: application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON Output

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "controlStatement": "Status of the 'banner motd' configuration command on the device",
        "rationale": "The 'Message of the Day (banner motd)' command is used to provide a warning banner displayed when a connection to the device is made BEFORE a user successfully authenticates to the device.  The Message of the Day banner can be used to provide an acceptable use policy or warning prior to login notifying that all user activity may be monitored and potential legal consequences may result from unauthorized use.  Run this check periodically to ensure content of the banner displayed is in compliance with the requirements and expectations driven by internal standards and/or policies.",
        "remediation": "Execute following commands to set desired banner message:\n1. configure terminal\n2. banner motd 'delimiting-character' 'message' 'delimiting-character'\n3. exit\n\nc",
        "controlReference": null,
        "technologyId": xxx,
        "status": "Error",
        "previousStatus": "Error",
        "firstFailDate": "",
```

```
        "lastFailDate": "",
        "firstPassDate": "2021-12-21T11:28:21Z",
        "lastPassDate": "2021-12-21T11:29:22Z",
        "postureModifiedDate": "2021-12-22T12:56:41Z",
        "lastEvaluatedDate": "2021-12-23T05:32:40Z",
        "created": "2022-02-21T13:10:13Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco::7.0%283%29i2%282%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-22T12:49:59Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xxx,
            "name": "Cisco NX-OS"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 1,
        "totalBatches": 1
    }
```

GET Get Posture Info Without lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=0 and compressionRequired=0

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Response:

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": <POLICY TITLE>,
```

```
    "netBios": <NETBIOS>,
    "controlId": <CONTROL ID>,
    "technologyId": xx,
    "status": "Failed",
    "previousStatus": "Failed",
    "firstFailDate": "2021-10-25T07:21:13Z",
    "lastFailDate": "2021-10-29T07:52:41Z",
    "firstPassDate": "",
    "lastPassDate": "",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T07:52:41Z",
    "created": "2021-10-29T07:54:26Z",
    "hostId": <HOST ID>,
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe":  "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:57:58Z",
    "customerUuid": "xxx",
    "customerId": "xxx",
    "assetId": "xxx",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "SERIOUS",
        "value": 3
    },
    "evidence": null,
    "causeOfFailure": {
        "missing": {
            "logic": null,
            "value": [
                "1",
                "Attribute not found",
                "Unable to retrieve password policy"
            ]
        },
        "unexpected": {
            "value": [
                "0"
            ]
        }
    }
},
{
    "id": xxx,
    "instance": "os",
```

```
            "policyId": "<POLICY ID>",
            "policyTitle": "<POLICY TITLE>",
            "netBios": "<NETBIOS>",
            "controlId": "<CONTROL ID>",
            "technologyId": "<TECHNOLOGY ID>",
            "status": "Passed",
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-25T07:21:13Z",
            "lastPassDate": "2021-10-29T07:52:41Z",
            "postureModifiedDate": "2021-10-25T07:21:11Z",
            "lastEvaluatedDate": "2021-10-29T07:52:41Z",
            "created": "2021-10-29T07:54:26Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "xxxx",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Windows Server 2012 R2"
            },
            "criticality": {
                "label": "URGENT",
                "value": 5
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info Without lastEvaluationDate, Without Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=0 & compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)

```
‹        íÝ]sÚHÅñ¯ââ:Îê!ÁÝ¬í?UœIì8©š©©)
²CD2S©|÷•p2Ž_ÖôÁý€ÿ»d?~é´8:ýÛçÆ ßè„í(ÈÒfð¬1OËî¸—
7:PÚxÖ¸,†ƒÞß‡Õ6Í(ŠÓ${Öè-ãrR
ëÇÂ0Kž5Ê¼÷~\
‹‹ùviõHµP6-öñª;æýz?"üã MOî<s>LËÿtÃýnY¿lõÐ°{û'ùFõ?}(
¢p7
v£äMP¢° Æ¿~ýÁû¶j×[%QSþ:ÿ?ål'-ýÁù
ïÿß]†ßvyð±;œU[ÝÙôæ~{"¼Þèî--N Ô?¼¯^¸>DY«?ÚÍêh_V?‡Áó0|ž-Ï›QµM9éö>
ÆGyù¾¨÷uºªz´ú,:ãÙpXÿïï²~½Ë¼ó¯¢3ô&Å´8/;Ÿ-ã~ñiúÇ4Ÿ|Ì'?DAu&Q§óW«Ù©öÐ×G½WŒ
úùÇéŸÃêéVõèŸÿ-ÞS}
\í}œ—
ŸŠÉ‡úM6,Æ???ÙÕ¯ùó°8ëwöóóîlXî¼¼z²þÍ‹ÑåpPŸ7/ªÃuÒëŽo©ìMØêÄíN'ÌP lZ£|r:?Ì_
©?giž-»ÙYÔÚM³óóÝ,l&»Ažeaë¼?¦çßýÔüÝEIPí»z´>P«‡Â´PiÝ¾¯OÉFçê ¯OËñÕ¯ñîêHí
œÌP N}¤vŽ£Æ—ú ?"ƒ^w8(ç?7ìžåÃêöŽß?îýô¢Úq}&TûhV?W't?ŸS¹:v½îlšÿr^Ÿ¸ÕÙuõè—
g7€…*°(lE ÀÜ€Eò´C€ìvrp|øËéÉµ¯x9_±î+Å¾~t_Gû‡§G×¼¢åx5—
àõðÿëW»Ÿ×?ÏÜæõ€œû¶°y†ßfx—
?¼àµ'áësc4N«Or¾§âbÐû¶å×PÖ¨ßþOe9œÍÊ|g\";çÅl\£8wÏ†ùNYìLòêùüc¾sYý¢Õáîï\'l
ü^½‡Ù8ÿë2ïÍO°Ï×û
ª'¿Ü²?ñ_Sæ~ØþÑmŸÿ|ðòÍ5íd¹¡³uƒ×ÑÉËëõ‹ ·:Õ¹ÖŒãÎü'êß'·ÇW{ûoû»çâf5Þ €Oàü¼
ü*ðèÛAÛ©
\;l-âLêP}—@aC>À0óÏ°•Á †0T¶-Æ0„!
Ý&Pvð0C.¼Âp›.¾úª]?MBÄw¾›d,1^K#†Ì,aC…aìŸa0Â †
Ã¦Ã&
aCPbÁpÁ—ÿ\àP63tˆ×Õo÷mý—éwÙ°.û„÷\öñŸë©h·a¡
ma„5Èõ¤-æ›0„¡ÂÐ ×"'ëPv0ôtdb ëI‰õ …,Â-Aª'‹PˆB
```

Get Posture Info Without lastEvaluationDate, With Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compressionRequired=1" -H
"accept: */*" -H "Authorization: <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output (Compressed)

```
‹        í?sÛFš@ÿ
JµöÎˆ ¼€|"%yâÄr  SvR"ÌNQ$LaC4 ÚÖÌä¿o7HJ¼
ša‹"qR•*YÂµÑ}ú,ßùõß'^ÿ¤mµª¦Ó¬™?=ñü(îú=÷¤}D'?=C¯wÿFlS«VífÝùëI/ðã0ÊßY-
SÿëIìöîü`
'íšâ7âñ$Ç¸îF'Û—ÇÝ/^0‰:k?ùä…Qü°ë
/°±<-øÕ°»ú›d#¹ËìWU³j2æiµ~c6ÛU«mÙ?Ÿí¶UKnU¯¶kÖß"{ŠâIè^}ï"çö3iÍyù¥;œˆ-Ö6]
>n/tåFë?ÔÚõ†ÜàNœX'ÓhÕ?-š(í±ØØ2+-
Uiš•ZUl ‡ÝÞïž?¸rã»@ëÍµø-xm?2?ÊŸÎÇòzc·ý?A{äõÂ
>Åí¯žß¾FÿŒÜð‹?þ³jZÕvXm·¿5jmq„¾/K½ŒÚû—
èóPü¹!~ûyð?&Y¦G÷Ýøk þ./òÄ<yø÷»îHžóoÃà¶;4.ÜOÝÉ06ÞMÿ(ï<P¶ž¬7oEquz]?µ¤œ?
«Ñ®‹²p''šDq0rÃ /9S×všnÓ<un«Ó¦óéÓ©cÕê§¦Õ¼u¬Æ§®Õü´°WruÕ°)Ž-
~+ëQ<ý•ÕlÕ?¼îÇ*yÒžVqY-ýémü<-)£"""!KÊx_=ùC>A/özÝ¡'û
»·îPìpþÞÍÍ›ó³·âÀ²&^cÔÄÆ¢B÷Ý¤©üûÄý6v{âÙ?"?-
ý›?áEÝÛ¡Û7^7?óOþ3~|o,þû7ÿÒŸmjånúÞt&·?¸÷†ÄÆ§`â÷óvYÚ8)Ç0týx~-¿ž,^êÉ?D'öâ
Iw8ÿû´fô½PÜa Þ¿öFú½é¯e'u''ûã'Ù\E›šÿz+-*VªV£
VÀ
```

Get Posture Info Without lastEvaluationDate, With Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"xxx\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output:


```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
```

```
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\nUnable to retrieve password policy\n------------ OR ----------
--\nequal to\n1",
            "currentValues": [
                "0"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:PCDEV",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-25T07:21:13Z",
        "lastPassDate": "2021-10-29T07:52:41Z",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:27Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
```

```
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nGrantees not found\n------------ OR ----
--------\nmatches regular expression list\n.*",
            "currentValues": [
                "Grantees not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null
    }
]
```

Sample JSON output response - Get Posture Info (multiple policy IDs)

Get Posture Info with lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0&lastEvaluationDate=2021-12-27T15:35:22Z" -H "accept: /" -H
"Authorization: Bearer <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<Policy_ID>\",\"subscriptionId\":\"<Subscription_ID>\",
\"hostIds\":[\"<Host_ID1>\"]},{\"policyId\":\"policyId1\",\"subscriptionI
d\":\"<Subscription_ID\",\"hostIds\":[\"<HOST_ID1>\"]}]"
```

JSON Output:

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL_ID,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
```

identification' via password a secure and workable solution is setting a 'minimum password length' requirement. Each character that is added to the password length squares the difficulty of breaking the password via 'brute force,' which attempts using every combination possible within the password symbol set-space, in order to discover a user's password. While no 'minimum length' can be guaranteed secure, eight (8) is commonly considered to be the minimum for most application access, along with requiring other password security factors, such as increasing the size of the symbol set-space by requiring mixed-cases, along with other forms of password variability creation, increases the difficulty of breaking any password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP, set the following UI path to 14 or more character(s):\n\n\tComputer Configuration\\Policies\\Windows Settings\\Security Settings\\Account Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-12T13:12:26Z",
        "lastPassDate": "2021-12-27T15:35:22Z",
        "postureModifiedDate": "2021-10-12T13:12:26Z",
        "lastEvaluatedDate": "2021-12-27T15:35:22Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "DNS Hostname",
        "os": xx,
        "osCpe": "cpe:/o:microsoft:windows_2003_server::sp2::",
        "domainName": "<DOMAIN NAME>",
        "dns": "client5-25-244.root.vuln.qa.qualys.com",
        "qgHostid": xx,
        "networkId": xx,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-27T15:31:18Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "Windows 2003 Server"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": xx
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n0",
            "currentValues": [
                "1"
            ],
            "actualValues": null,

```
            "directoryFimUdc": null
        },
        "causeOfFailure": null,
        "currentBatch": xx,
        "totalBatches": xx
    },
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL_ID>,
        "controlStatement": "Status of the
'net.ipv4.conf.all.send_redirects' setting within the '/etc/sysctl.conf'
file",
        "rationale": "The 'net.ipv4.conf.all.send_redirects' network
parameter (/etc/sysctl.conf) allows ICMP routing redirection.  If the
system is not going to be used as a firewall or gateway to pass network
traffic, and this parameter is not disabled, malicious users may attempt
to spoof source addresses or redirect traffic to a host with a network
sniffer, so this value should be set according to the needs of the
business.",
        "remediation": "Set the following parameters in the
/etc/sysctl.conf file:\n\n# net.ipv4.conf.all.send_redirects = 0\n\nOR
\nRun the following commands to set the active kernel parameters:\n#
sysctl -w net.ipv4.conf.all.send_redirects=0\n# sysctl -w
net.ipv4.route.flush=1",
        "controlReference": null,
        "technologyId": 80,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-02-11T12:54:23Z",
        "lastPassDate": "2022-02-11T12:54:23Z",
        "postureModifiedDate": "2022-02-11T12:54:23Z",
        "lastEvaluatedDate": "2022-02-11T12:54:23Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-02-11T12:47:29Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
```

```
            "id": xx,
            "name": "CentOS 7.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------ OR ------------\nmatches regular
expression list\n.*",
            "currentValues": [
                "Setting not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null,
        "currentBatch": 1,
        "totalBatches": 1
    }
]
```


Get Posture Info without lastEvaluationDate, without evidence, without compression, without lastScanDate

User Input: evidenceRequired=0 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
```

```
    "lastEvaluatedDate": "2021-10-18T06:17:29Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
    "domainName": "<DOMAIN NAME>",
    "dns": null,
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-14T09:37:38Z",
    "customerUuid": "<CUSTOMER UUID>",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Cisco ASA 9.x"
    },
    "criticality": {
        "label": "MEDIUM",
        "value": 2
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": xx,
    "instance": "os",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
```

```
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "CRITICAL",
        "value": 4
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": xx,
    "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-28T16:53:06Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-28T16:53:06Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:15Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "<CUSTOMER UUID>",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Microsoft SQL Server 2016"
    },
    "criticality": {
        "label": "MEDIUM",
        "value": 2
    },
```

```
        "evidence": null,
        "causeOfFailure": null
    }
]
```

Get Posture Info without lastEvaluationDate, with evidence, without compression, without lastScanDate

User input: evidenceRequired=1 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
]"
```

JSON Output:

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:40:38Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
```

```
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nFilter 2 not found: ^[\\*\\.\\d]\n------
------ OR ------------\nFilter 1 not found: show clock detail\n----------
-- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "show clock detail:08:26:29.074 pdt Thu Oct 14 2021"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-28T16:53:06Z",
        "lastPassDate": "2021-10-29T08:39:07Z",
        "postureModifiedDate": "2021-10-28T16:53:06Z",
        "lastEvaluatedDate": "2021-10-29T08:39:07Z",
        "created": "2021-10-29T08:40:46Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
        "criticality": {
```

```
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nSet status to PASS if no data found\n---
--------- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "Error Code 35:Failed to execute database query"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null
    }
]
```


Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

User input: evidenceRequired=0 & compressionRequired=1 & lastScanDate=yyyy-mm-dd:Thh:mm:ssZ

Request:

```
Curl-X POST
"https://qualysapi.qualys.com/pcrs/2.0/posture/postureInfo?evidenceRequir
ed=0&compressionRequired=1&lastEvaluationDate=2021-12-
17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z" -H
"accept: */*" -H
"Content-Type: application/json" -d "
[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

JSON output:


```
[
    {
        "id": <HOST INSTANCE ID>,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
```

```
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
        "osCpe": null,
       "domainName": "<DOMAIN NAME>",
        "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-23T12:59:04Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 217,
            "name": "Red Hat Enterprise Linux 8.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 8,
        "totalBatches": 12
    },
]
```


Get Posture Info without evidence, without compression, with statusChangedSince

Request:

```
curl -X POST
"https://gateway.<assigned
```

```
URL>/pcrs/2.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0&statusChangedSince=2021-12-23" -H "accept: */*" -H "Authorization:
Bearer <token>" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONID>\",\"
hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON output:


```
[
    {
        "id": 24705485,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "pcas_win16_redhat7 tech",
        "netBios": "<NETBIOS>",
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": 106,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-11-09T12:50:12Z",
        "lastPassDate": "2022-12-06T06:42:21Z",
        "postureModifiedDate": "2022-11-09T12:50:12Z",
        "lastEvaluatedDate": "2022-12-06T06:42:21Z",
        "created": "2022-12-07T07:35:56Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": null,
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2016:1607::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "<DNS>",
        "qgHostid": null,
```

```
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-08-23T04:57:05Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 106,
            "name": "Windows 2016 Server"
        },
        "criticality": {
            "label": "high updated",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\ngreater than or equal to\n0",
            "currentValues": [
                "6"
            ],
            "actualValues": null,
            "directoryFimUdc": null
        },
        "causeOfFailure": null,
        "currentDataSizeKB": "2.41",
        "totalDataSizeKB": "2.41",
        "currentBatch": 1,
        "totalBatches": 1
    },
]
```


V3.0

API URL: <qualys_base_url>/pcrs/3.0/posture/postureInfo?

[POST] [GET]

Note: The V3 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions v1 or v2.

This version (/pcrs/3.0/posture/postureInfo) of the API enables you to:

- View cloud metadata in the API response.
- Retrieve the posture information based on the current posture status (passe/failed/error).
- Retrieve the posture information based on the previous status (passed/failed/error) of the posture.
- Retrieve posture information based on the following criticality categories:
  - UNDEFINED (0)
  - MINIMAL (1)
  - MEDIUM (2)
  - SERIOUS (3)

- CRITICAL (4)
- URGENT (5)

Input Parameters

Parameter	Description
Authentication Token (Bearer Token)	(Required) Specify the authentication token that is returned by the authentication request.
evidenceRequired	(Optional) Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note:** Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	(Required) Default value is 1, which indicates that the output will be compressed. If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
Request Body	(Required) Output of the Resolve Host ID and the JWT token.
Request header: Authorization	(Required) JWT encrypted token. **Note:** The token received from the Authorization API and the token used in the second API need to be the input here.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
lastScanDate	(Optional) Compliance posture information on the date on which an asset was last scanned. The formats for date are: lastScanDate=2021-12-17 Or, lastScanDate=2021-12-17T18:48:16Z
lastScanDateFrom, lastScanDateTo	(Optional) Compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.

Parameter	Description
statusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)
excludeInactiveControl	(Optional) Default value is 0, which indicates that inactive controls data is retrieved for the host posture. If you want to exclude inactive control data then, change the value to 1.
cloudMetaDataRequired	(Optional) This parameter allows you to retrieve cloud metadata. Specify "1" to retrieve cloud metadata information in the API response. Specify "0" to not retrieve cloud metadata information in the API response. **Note:** Cloud metadata is returned as null in the response for the postures that do not have cloud metadata.
status	(Optional) This parameter lets you retrieve posture information based on the current posture status. Possible values are Passed, Failed, and Error. You can provide multiple comma-separated values.
previousStatus	(Optional) This parameter lets you retrieve posture information based on the previous posture status. Possible values are Passed, Failed, and Error. You can provide a single value at a time.

Parameter	Description
criticalityValues	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated values. When set to 0, posture information with criticality level UNDEFINED is retrieved. When set to 1, posture information with criticality level MINIMAL is retrieved. When set to 2, posture information with criticality level MEDIUM is retrieved. When set to 3, posture information with criticality level SERIOUS is retrieved. When set to 4, posture information with criticality level CRITICAL is retrieved. When set to 6, posture information with criticality level URGENT is retrieved. **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.
criticalityLabels	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated crticality labels. Possible values are: - UNDEFINED - MINIMAL - MEDIUM - SERIOUS - CRITICAL - URGENT **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.

Sample - Get Extended Evidence for a Control and Control description

You can retrieve extended evidence and last updated date information for the hosts. The evidence for a control includes the expected and actual values for the control on the host. The extended evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result. You can also view a control description under the evidence section for the particular host posture. To retrieve the extended information in the API response, specify the following input parameters.

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=
1&compressionRequired=0"
-H "accept: */*"
-H "Authorization: Bearer Token"
-H "Content-Type: application/json"-d "[{\"policyId\":\"POLICY
ID\",\"subscriptionId\":\"SUBSCRIPTION ID\",\"hostIds\":[\"HOST
ID1\",\"HOST ID2\"]}]"
```

JSON Output


```
  {
        "id": 20245394,
        "instance": "os",
        "policyId": 1455112,
        "policyTitle": "Linux_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN
<required value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\" and also
another PAM module (such as \"pam_cracklib\") during a password change
operation, then the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T10:40:30Z",
        "lastPassDate": "2024-11-15T01:22:58Z",
        "postureModifiedDate": "2024-11-06T10:40:30Z",
        "lastEvaluatedDate": "2024-11-15T01:22:58Z",
        "created": "2025-02-05T06:01:09Z",
        "hostId": 6396397,
        "ip": "10.11.70.111",
```

```
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos:6.6:::",
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T10:42:29Z",
        "customerUuid": "e57ba830-15e4-714c-8243-6d1740d3577e",
        "customerId": "2309240",
        "assetId": 50568616,
        "technology": {
            "id": 43,
            "name": "CentOS 6.x"
        },
        "criticality": {
            "label": "urg_updated",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------ OR ------------\ngreater than or
equal to\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2024-11-06T10:42:29Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN setting as defined within the
/etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.88",
        "totalDataSizeKB": "2.88",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
```


Sample - Exclude Inactive Control Data

You can include/exclude inactive controls (SDC, UDC) from the host compliance posture information in the API response. Inactive controls are the controls removed or deactivated from a policy.

API Request

```
https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=1
&compressionRequired=0&excludeInactiveControl=1
```

JSON Output


```
"id": xx,
"instance": "oracle19cdb:1:1527:ora19csu",
"policyId": xx,
"policyTitle": "Oracle_DB_UDC",
"netBios": null,
"controlId": 100432,
"controlStatement": "Oracle_DB_UDC_3",
"rationale": "rationle",
"remediation": "Remediation",
"controlReference": null,
"technologyId": 312,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-06-08T09:52:13Z",
"lastFailDate": "2023-08-24T10:00:05Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-06-08T09:52:13Z",
"lastEvaluatedDate": "2023-08-24T10:00:05Z",
"created": "2024-01-30T06:54:04Z",
"hostId": xx,
"ip": "xx.xx.xx.xx",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2024-01-05T10:24:32Z",
"customerUuid": "xx-xx-xx-xx-xx",
"customerId": "xx",
"assetId": xx,
"technology": {
"id": 312,
"name": "Oracle 19c Multitenant"
},
"criticality": {
"label": "SERIOUS",
"value": 3
},
"evidence": {
"expectedValues": "\nSet status to PASS if no data found",
"currentValues": [
"GRANTEE|:|GRANTED_ROLE",
"APPQOSSYS|:|DBA",
"UDC_SENSITIVE_SCAN|:|DBA",
"QUALYS_SCAN|:|DBA"
],
"actualValues": null,
"directoryFimUdc": null
```

```
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
},
"causeOfFailure": {
"missing": {
"logic": null,
"value": [
"------------ OR ------------",
"Set status to PASS if no data found"
]
},
"unexpected": {
"value": [
"DBA,DBA,DBA",
"APPQOSSYS,UDC_SENSITIVE_SCAN,QUALYS_SCAN"
]
}
},
"currentDataSizeKB": "1.47",
"totalDataSizeKB": "4.59",
"currentBatch": 1,
"totalBatches": 1,
"CLOUD_RESOURCE_ID": null
}
```


Sample - Retrieve Compliance Posture Information along with Control Status

API response now displays the status of the controls on a host as passed when an exception has been created and approved. The controls on which the exception has been approved are displayed as Passed*. Exception is a way to temporarily change the status of a control on a host from Failed to PassedE (passed with an exception). To learn about what is exceptions refer to Exceptions- The Basics.

API Request

https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?compressionRequired=0' \ --header 'accept: */*' \ --header 'Authorization: `Bearer Token`' \ --header 'Content-Type: application/json' \ --data '[{ "policyId": "xx", "subscriptionId": "xx", "hostIds": ["xx"] }]'

JSON Response


```
{
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "LinuxAllAssetScan_withAssetTag",
        "netBios": null,
        "controlId": xx,
        "controlStatement": "File_content_check_udc-2",
        "rationale": "rationale",
        "remediation": null,
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
```

```
            "status": "Passed*",
            "previousStatus": "Error",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "",
            "lastPassDate": "",
            "postureModifiedDate": "2024-07-10T15:10:32Z",
            "lastEvaluatedDate": "2024-08-25T17:36:31Z",
            "created": "2024-08-29T10:58:49Z",
            "hostId": xx,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": null,
            "domainName": null,
            "dns": null,
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2024-06-10T17:08:52Z",
            "customerUuid": "xx-xx-xx-xx-xx",
            "customerId": "xx",
            "assetId": xx,
            "technology":
{               "id": 43,               "name": "CentOS 6.x"           }
,
            "criticality":
{               "label": "MEDIUM",               "value": 2           }
,
            "evidence": null,
            "causeOfFailure": null,
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "1.14",
            "totalDataSizeKB": "1.14",
            "currentBatch": 1,
            "totalBatches": 1,
            "CLOUD_RESOURCE_ID": null
        }
```


Sample - Retrieve Compliance Posture Information along with Control Category and Sub-Category

Two new fields in the API response to display control category and sub-category.

- category -Displays control category set on a particular control.
- SubCategory - Displays control Subcategory set on a particular control.

API Request

```
https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?compressionRequire
d=0' \ --header 'accept: */*' \ --header 'Authorization: Bearer Token' \ -
-header 'Content-Type: application/json' \ --data '[     {
"policyId": "5657103",          "subscriptionId": "xx",          "hostIds":
[               "xx"          ]      } ]'
```

JSON Response


```
{
  "id": xx,
  "instance": "os",
  "policyId": xx,
  "policyTitle": "LinuxAllAssetScan_withAssetTag",
  "netBios": null,
  "controlId": xx,
  "controlStatement": "File_content_check_udc-2",
  "rationale": "rationale",
  "remediation": null,
  "category": "Access Control Requirements",
  "subCategory": "Authentication/Passwords",
  "controlReference": null,
  "technologyId": 43,
  "status": "Passed*",
  "previousStatus": "Error",
  "firstFailDate": "",
  "lastFailDate": "",
  "firstPassDate": "",
  "lastPassDate": "",
  "postureModifiedDate": "2024-07-10T15:10:32Z",
  "lastEvaluatedDate": "2024-08-25T17:36:31Z",
  "created": "2024-08-29T10:58:49Z",
  "hostId": xx,
  "ip": "xx.xx.xx.xx",
  "trackingMethod": "IP",
  "os": null,
  "osCpe": null,
  "domainName": null,
  "dns": null,
  "qgHostid": null,
  "networkId": 0,
  "networkName": "Global Default Network",
  "complianceLastScanDate": "2024-06-10T17:08:52Z",
  "customerUuid": "xx-xx-xx-xx-xx",
  "customerId": "xx",
  "assetId": xx,
  "technology": {
    "id": 43,
    "name": "CentOS 6.x"
  },
  "criticality": {
    "label": "MEDIUM",
    "value": 2
  },
  "evidence": null,
  "causeOfFailure": null,
  "userDefinedAttributesList": null,
  "currentDataSizeKB": "1.14",
  "totalDataSizeKB": "1.14",
  "currentBatch": 1,
  "totalBatches": 1,
```

```
  "CLOUD_RESOURCE_ID": null
}
```

Sample JSON output response - Get Posture Info (single policy ID)

Get posture Info With lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=
0&compressionRequired=0&lastEvaluationDate=2021-12-23"-H "accept: */*"-H
"Authorization: Bearer Token"-H "Content-Type: application/json"-d
"[{\"policyId\":\"POLICY ID\",\"subscriptionId\":\"SUBSCRIPTION
ID\",\"hostIds\":[\"HOST ID1\",\"HOST ID2\"]}]"
```

JSON Output

```
[
{
"id": xxx,
"instance": "os",
"policyId": "<POLICY ID>",
"controlId": "<CONTROL ID>",
"controlStatement": "Status of the 'banner motd' configuration command on
the device",
"rationale": "The 'Message of the Day (banner motd)' command is used to
provide a warning banner displayed when a
connection to the device is made BEFORE a user successfully authenticates
to the device. The Message of the Day banner can be used to provide an
acceptable use policy or warning prior to login notifying that all user
activity may be monitored and potential legal consequences may result from
unauthorized use. Run this check periodically to ensure content of the
banner displayed is in compliance with the requirements and expectations
driven by internal standards and/or policies.",
"remediation": "Execute following commands to set desired
banner message:\n1. configure terminal\n2. banner motd
'delimiting-character' 'message' 'delimiting-character'\n3.
exit\n\nc",
"controlReference": null,
"technologyId": xxx,
"status": "Error",
"previousStatus": "Error",
"firstFailDate": "",
"lastFailDate": "",
"firstPassDate": "2021-12-21T11:28:21Z",
"lastPassDate": "2021-12-21T11:29:22Z",
"postureModifiedDate": "2021-12-22T12:56:41Z",
"lastEvaluatedDate": "2021-12-23T05:32:40Z",
"created": "2022-02-21T13:10:13Z",
"hostId": "<HOST ID>",
"ip": "xx.xx.xx.xxx",
"trackingMethod": "IP",
"os": null,
```

```
"osCpe": "cpe:/o:cisco::7.0%283%29i2%282%29:::",
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2021-12-22T12:49:59Z",
"customerUuid": "<CUSTOMER UUID>",
"customerId": "<CUSTOMER ID>",
"assetId": "<ASSET ID>",
"technology": {
"id": xxx,
"name": "Cisco NX-OS"
},
"criticality": {
"label": "CRITICAL",
"value": 4
},
"evidence": null,
"causeOfFailure": null,
"currentBatch": 1,
"totalBatches": 1
}
```

GET Get Posture Info Without lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=0 and compressionRequired=0

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Response:

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL ID>,
        "technologyId": xx,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
```

```
    "created": "2021-10-29T07:54:26Z",
    "hostId": <HOST ID>,
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe":  "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:57:58Z",
    "customerUuid": "xxx",
    "customerId": "xxx",
    "assetId": "xxx",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "SERIOUS",
        "value": 3
    },
    "evidence": null,
    "causeOfFailure": {
        "missing": {
            "logic": null,
            "value": [
                "1",
                "Attribute not found",
                "Unable to retrieve password policy"
            ]
        },
        "unexpected": {
            "value": [
                "0"
            ]
        }
    }
},
{
    "id": xxx,
    "instance": "os",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T07:52:41Z",
```

```
            "postureModifiedDate": "2021-10-25T07:21:11Z",
            "lastEvaluatedDate": "2021-10-29T07:52:41Z",
            "created": "2021-10-29T07:54:26Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "xxxx",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Windows Server 2012 R2"
            },
            "criticality": {
                "label": "URGENT",
                "value": 5
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info Without lastEvaluationDate, Without Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=0 & compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)


```
‹        íÝ]sÚHÅñ¯ââ:Îê!ÁÝ¬í¤UœIì8©š©©)
²CÐ2S©|÷•p2Ž_ÖôÁý€ÿ»d‡~é´8:ýÛçÆ ßè„í(ÈÒfð¬1OËî¸—
7:ÞÚxÖ¸,†ƒÞß‡Õ6Í(ŠÓ${Öè-ãrR
ëÇÂ0Kž5Ê¼÷~\
‹‹ùviõHµ‡6-öñª;æýz?"üã ̃MOî<s>LËÿtÃýnY¿lõÐ°{û'ùFõ?}(
¢p7
v£äM?¢° Æ¿~ýÁû¶j×[%Q§þ:ÿ?ål’-ýÁù
ïÿß]†ßvyð±;œU[ÝÙôæ~{"¼Þèî--N Ô?¼¯^¸>DY«?ÚÍêh_V?‡Áó0|ž-Ï›QµM9éö>
ÆGyù¾¨÷uøªz´ú,:ãÙpXÿiï²~½Ë¼ó¯¢3ô&Å´8/;Ÿ-ã~ñiúÇ4Ÿ|Ì'?DAu&Q§óW«Ù©öÐ×G½WŒúùÇ
éŸÃêéVõèŸÿ-ÞS}
\í}œ—
```

```
ŸŠÉ‡úM6,Æ???ÙÕ¯ùó°8ëwöóóîlXî¼¼z²þÍ‹ÑåpPŸ7/ªÃuÒëŽo©ìMØêÄíN'Ì0lZ£|r:?Ì_©?g
iž-»ÙYÔÚM³óóÝ,l&»Ažeaë¼?¦çßýÔüÝEIPí»z´>Ê«‡Â´0iý¾¯OÉFçê ¯OËñÕ¯ñîêHíœÌ0N}¤
vŽ£Æ—ú ?"ƒ^w8(ç?7ìžåÃêöŽß?îýô¢Úq}&TûhV?W't?ŸS¹:v½îlšÿr^Ÿ¸ÕÙuõè—g7€…*°(lE
ÀÜ€Eò´C€ìvrp|øËéÉµ¯x9_±î+Å¾~t_Gû‡$G×¼¢åx5—àõðÿëW»Ÿ×?ÏÜæõ€œû¶°y†ßfx—
?¼àµ'áësc4Ñ«Or¾$âbÐû¶å×0Ö¨ßþOe9œÍÊ|g\";çÅl\£8wÏ†ùNYìLòêùüc¾sYý¢Õáîï\'lü^½
‡Ù8ÿë2ïÍO°Ï×û
ª'¿Ü²?ñ_Sæ~ØþÑmŸÿ|ðòÍ5íd¹¡³uƒ×ÑÉÉëõ‹ ·:Õ¹ÖŒãÎü'êß'·ÇW{ûoû»çâf5Þ €Oàü¼ü*ð
èÛAÛ©
\;l-âLê0}—@aC>À0óÏ°•Á †0T¶-Æ0„!
Ý&Ãvð0C.¼Âp›.¾úª]?MBÄw¾›d,1^K#†Ì,aC…aìŸa0Â †
Ã¦Ã&
aC0bÁpÁ—ÿ\à0163tˆ×Õo÷mý—éwÙ°.û„÷\öñŸë©h·a¡
ma„5Èõ¤-æ›0„¡ÂÐ ×"'ë0v0ôtdb ëI‰õ …,Â-Aª'‹PˆB
```

Get Posture Info Without lastEvaluationDate, With Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)

```
‹        í?sÛFš@ÿ
Jµöî^ ¼€|"%yâÄr  SvR"ÌNQ$LaC4 ÚÖÌä¿o7HJ¼
ša‹"qR•*YÂµÑ}ú,ßùõß'^ÿ¤mµª¦Ó¬™?=ñü(îú=÷¤}D'?=C¯wÿFlS«VífÝùëI/ðã0ÊßY-
SÿëIìöîü`
'íšâ7âñ$Ç¸îF'Û—ÇÝ/^0‰:k?ùä…Qü°ë
/°±<-øÕ°»ú›d#¹ËìWU³j2æiµ~c6ÛU«mÙ?Ÿí¶UKnU¯¶kÖß"{ŠâIè^}ï"çö3iÍyù¥;œ^-Ö6]>n/
tåFë?ÔÚõ†ÜàNœX'ÓhÕ?-š(i±ØØ2+-Uiš•ZUl ‡ÝÞïž?¸rã»@ëÍµø-xm?2?ÊŸÎÇòzc·ý?A{äõÂ
>Åí¯žß¾FÿŒÜð‹ ?þ³jZÕvXm·¿5jmq„¾/K½Œúî—
èóPü¹!~ûyð?&Y¦G÷Ýøk þ./òÄ<yø÷»îHžóoÃà¶;4.ÜOÝÉ06ÞMÿ(ï<?ž¬7oEquz]?µ¤œ?«Ñ®
‹²p''šDq0rÃ /9S×všnÓ<un«Ó¦óéÓ©cÕê$¦Õ¼u¬Æ$®Õü´°WruÕ°)Ž-
~+ëQ<ý•ÕlÕ?¼îÇ*yÒžVqY-ýémü<-)£"””!KÊx_=ùC>A/özÝ¡'û
»·îPìpÞþÍÍ›ó³·âÀ²&ˆcÔÄÆ¢B÷Ý¤©üûÄý6v{âÙ?"?-
ý›?áEÝÛ¡Û7^7?óOþ3~|o,þû7ÿÒŸmjånúÞt&·?¸÷†ÄÆ$`â÷óvYÚ8)Ç0týx~-¿ž,^êÉ?D'öâIw8
ÿû´fô½PÜa Þ¿öFú½é¯e'u''ûã'Ù\E›šÿz+-*VªV£
VÀ
```

Get Posture Info Without lastEvaluationDate, With Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
```

```
"[{\"policyId\":\"xxx\",\"xxx\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output:


```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\nUnable to retrieve password policy\n------------ OR ----------
--\nequal to\n1",
            "currentValues": [
                "0"
            ],
            "actualValues": null,
            "directoryFimUdc": null
```

```
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:PCDEV",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-25T07:21:13Z",
        "lastPassDate": "2021-10-29T07:52:41Z",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:27Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
```

```
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nGrantees not found\n------------ OR ----
--------\nmatches regular expression list\n.*",
            "currentValues": [
                "Grantees not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    }
]
```


Sample JSON output response - Get Posture Info (multiple policy IDs)

Get Posture Info with lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0&lastEvaluationDate=2021-12-27T15:35:22Z" -H "accept: /" -H
"Authorization: Bearer Token" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<Policy_ID>\",\"subscriptionId\":\"<Subscription_ID>\",
\"hostIds\":[\"<Host_ID1>\"]},{\"policyId\":\"policyId1\",\"subscriptionI
d\":\"<Subscription_ID\",\"hostIds\":[\"<HOST_ID1>\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL_ID,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
```

```
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-12T13:12:26Z",
        "lastPassDate": "2021-12-27T15:35:22Z",
        "postureModifiedDate": "2021-10-12T13:12:26Z",
        "lastEvaluatedDate": "2021-12-27T15:35:22Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "DNS Hostname",
        "os": xx,
        "osCpe": "cpe:/o:microsoft:windows_2003_server::sp2::",
        "domainName": "<DOMAIN NAME>",
        "dns": "client5-25-244.root.vuln.qa.qualys.com",
        "qgHostid": xx,
        "networkId": xx,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-27T15:31:18Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "Windows 2003 Server"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": xx
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n0",
            "currentValues": [
                "1"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "currentBatch": xx,
```

```
        "totalBatches": xx
    },
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL_ID>,
        "controlStatement": "Status of the
'net.ipv4.conf.all.send_redirects' setting within the '/etc/sysctl.conf'
file",
        "rationale": "The 'net.ipv4.conf.all.send_redirects' network
parameter (/etc/sysctl.conf) allows ICMP routing redirection.  If the
system is not going to be used as a firewall or gateway to pass network
traffic, and this parameter is not disabled, malicious users may attempt
to spoof source addresses or redirect traffic to a host with a network
sniffer, so this value should be set according to the needs of the
business.",
        "remediation": "Set the following parameters in the
/etc/sysctl.conf file:\n\n# net.ipv4.conf.all.send_redirects = 0\n\nOR
\nRun the following commands to set the active kernel parameters:\n#
sysctl -w net.ipv4.conf.all.send_redirects=0\n# sysctl -w
net.ipv4.route.flush=1",
        "controlReference": null,
        "technologyId": 80,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-02-11T12:54:23Z",
        "lastPassDate": "2022-02-11T12:54:23Z",
        "postureModifiedDate": "2022-02-11T12:54:23Z",
        "lastEvaluatedDate": "2022-02-11T12:54:23Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-02-11T12:47:29Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "CentOS 7.x"
        },
        "criticality": {
```

```
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------ OR ------------\nmatches regular
expression list\n.*",
            "currentValues": [
                "Setting not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "currentBatch": 1,
        "totalBatches": 1
    }
]
```


Get Posture Info without lastEvaluationDate, without evidence, without compression, without lastScanDate

User Input: evidenceRequired=0 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}]"
```

JSON Output:


```
    [
        {
            "id": xx,
            "instance": "os",
            "policyId": "<POLICY ID>",
            "policyTitle": "<POLICY TITLE>",
            "netBios": "<NETBIOS>",
            "controlId": "<CONTROL ID>",
            "technologyId": "<TECHNOLOGY ID>",
            "status": "Passed",
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-14T11:19:31Z",
            "lastPassDate": "2021-10-18T06:17:29Z",
            "postureModifiedDate": "2021-10-14T11:19:30Z",
            "lastEvaluatedDate": "2021-10-18T06:17:29Z",
            "created": "2021-10-29T08:38:14Z",
```

```
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
    "domainName": "<DOMAIN NAME>",
    "dns": null,
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-14T09:37:38Z",
    "customerUuid": "<CUSTOMER UUID>",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Cisco ASA 9.x"
    },
    "criticality": {
        "label": "MEDIUM",
        "value": 2
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": xx,
    "instance": "os",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "xx-xx-xx-xx-xx",
```

```
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "CRITICAL",
        "value": 4
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": 19235413,
    "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-28T16:53:06Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-28T16:53:06Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:15Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "<CUSTOMER UUID>",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Microsoft SQL Server 2016"
    },
    "criticality": {
        "label": "MEDIUM",
        "value": 2
    },
    "evidence": null,
    "causeOfFailure": null
```

```
        }
    ]
```

Get Posture Info without lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request**:**

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
]"
```

JSON Output:

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:40:38Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
```

```
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nFilter 2 not found: ^[\\*\\.\\d]\n------
------ OR ------------\nFilter 1 not found: show clock detail\n----------
-- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "show clock detail:08:26:29.074 pdt Thu Oct 14 2021"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-28T16:53:06Z",
        "lastPassDate": "2021-10-29T08:39:07Z",
        "postureModifiedDate": "2021-10-28T16:53:06Z",
        "lastEvaluatedDate": "2021-10-29T08:39:07Z",
        "created": "2021-10-29T08:40:46Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
```

```
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nSet status to PASS if no data found\n---
---------- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "Error Code 35:Failed to execute database query"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    }
]
```

Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

User input**:** evidenceRequired=0 & compressionRequired=1 & lastScanDate=yyyy-mm-dd:Thh:mm:ssZ

Request**:**

```
Curl-X POST
"https://qualysapi.qualys.com/pcrs/1.0/posture/postureInfo?evidenceRequir
ed=0&compressionRequired=1&lastEvaluationDate=2021-12-
17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z" -H
"accept: */*" -H
"Content-Type: application/json" -d "
[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

JSON output:

```
[
    {
        "id": <HOST INSTANCE ID>,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
```

```
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
        "osCpe": null,
       "domainName": "<DOMAIN NAME>",
        "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-23T12:59:04Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 217,
            "name": "Red Hat Enterprise Linux 8.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 8,
        "totalBatches": 12
    },
]
```


Get Posture Info without evidence, without compression, with statusChangedSince

Request:

```
curl -X POST
"https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0&statusChangedSince=2021-12-23" -H "accept: */*" -H "Authorization:
Bearer Token" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONID>\",\"
hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON output:


```
[
    {
        "id": 24705485,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "pcas_win16_redhat7 tech",
        "netBios": "<NETBIOS>",
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": 106,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-11-09T12:50:12Z",
        "lastPassDate": "2022-12-06T06:42:21Z",
        "postureModifiedDate": "2022-11-09T12:50:12Z",
        "lastEvaluatedDate": "2022-12-06T06:42:21Z",
        "created": "2022-12-07T07:35:56Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": null,
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2016:1607::x64:",
```

```
            "domainName": "<DOMAIN NAME>",
            "dns": "<DNS>",
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2022-08-23T04:57:05Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": <ASSET ID>,
            "technology": {
                "id": 106,
                "name": "Windows 2016 Server"
            },
            "criticality": {
                "label": "high updated",
                "value": 5
            },
            "evidence": {
                "expectedValues": "\nAttribute not found\n------------ OR ---
---------\ngreater than or equal to\n0",
                "currentValues": [
                    "6"
                ],
                "actualValues": null,
                "directoryFimUdc": null
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            },
            "causeOfFailure": null,
            "currentDataSizeKB": "2.41",
            "totalDataSizeKB": "2.41",
            "currentBatch": 1,
            "totalBatches": 1
        },
    ]
```


Sample - Retrieve Cloud Metadata

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=
0&compressionRequired=0&cloudMetaDataRequired=1" -H "accept: */*" -H
"Authorization: Bearer Token" -H "Content-Type:application/json" -d
"[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST
ID1>\",\"<HOST ID2>\"]}]"
```

JSON Output


```
[    {
            "id": xx,
            "instance": "os",
            "policyId": xx,
            "policyTitle": "CPS -Test",
```

```
        "netBios": "INSTANCE-xx-xx",
        "controlId": xx,
       "controlStatement": "Status of the 'Trivial File Transfer Protocol
(TFTP)' service",
      "rationale": "The 'TFTP' service is both a command and TCP protocol
that is normally used only for booting diskless workstations, getting or
saving network component configuration files, or as a 'kickstart' type
host configuration from a network-based template.  The connection
initiation and data transfer is all done in clear text without requiring
credentials of any kind.  As a malicious user with a 'sniffer' running on
the network, could easily capture the data and/or reproduce the same
operation, simply by knowing the name of the file(s) and the source
address(es), this process should be disabled/restricted according to the
needs of the business.",
        "remediation": "Review \"/etc/inetd.conf\" file to check whether
tftp service's configuration in line with business needs and
organization's security policies.\n\nExample: To disable the tftp
service,\n\nRemove or comment out any tftp lines in /etc/inetd.conf: \n#
tftp stream tcp nowait root internal",
        "category": "Services",
        "subCategory": "Guidelines/Procedures (Services)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:20:49Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xx-xx-xx-xx-xxx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
```

```
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.98",
        "totalDataSizeKB": "27.09",
        "currentBatch": 1,
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "xx",
            "cloudResourceType": "Instance",
            "cloudAccountId": "xx",
            "cloudImageId": null,
            "cloudResourceMetadata": "{'Public IP
Address':'xx.xxx.xx.xxx', 'Private IP Address':'xx.xxx.x.xx', 'Machine
Type':'e2-medium', 'Zone':'null', 'ProjectId':'qlys-devqa-qweb',
'State':'RUNNING', 'Network':'N/A', 'MAC Address':'null'}"
        },
        "CLOUD_RESOURCE_ID": "xxx"
    }
]
```


Sample - Retrieve Posture Information Based on Current Posture Status - passed

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=0&compressio
nRequired=0&status=Passed" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-
Type:application/json" -d "[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST
ID2>\"]}]"
```

JSON Output


```
[        {
        "id": xx,
        "instance": "os",
        "policyId": 1438626,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xxxxxx-xxxxx",
        "controlId": xx,
```

```
        "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
protocol, most commonly used for accessing remote computers via a command
line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
clear text including any uid/password input, so if a telnet session is
used for privileged communication(s)/host configuration purposes, the
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
       "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xxx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxxxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxx",
        "customerId": "xx",
        "assetId": xxx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
```

```
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"

        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxx"
    }
]
```

Sample - Retrieve Posture Information Based on Previous status-passed

API Request

curl -X POST "https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&previousStatus=Passed" -H "accept: */*" -H "Authorization: `Bearer Token`" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output

```
[        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xx-xx",
        "controlId": xx,
       "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
protocol, most commonly used for accessing remote computers via a command
line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
clear text including any uid/password input, so if a telnet session is
used for privileged communication(s)/host configuration purposes, the
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
       "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
```

```
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxxxx",
        "customerId": "xxxx",
        "assetId": 42078290,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxxx"
    }
]
```

Sample - Retrieve Posture Information Based on Criticality Value: 2

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=0&compressio
nRequired=0& criticalityValues=2" -H "accept: */*" -H "Authorization: Bearer Token" -H
"Content-Type:application/json" -d "[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST
ID2>\"]}]"
```

JSON Output


```
[
        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
based facsimile service that can take system documents and send these out
to a fax-recipient via a hardware modem and analog phone line.  (One
reported public exploit uses the Windows Picture and Fax Viewer
(SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
can potentially compromise sensitive system documents, by transmitting
information to unauthorized recipients and can be activated remotely, this
capability should be restricted/set according to the needs of the
business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xxx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
"cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
```

```
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2024-11-06T09:12:22Z",
            "customerUuid": "xx-xx-xx-xx-xxxx",
            "customerId": "xx",
            "assetId": xx,
            "technology": {
                "id": 21,
                "name": "Windows 2008 Server"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": {
                "expectedValues": "\nAutomatic (2)\n------------ OR ---------
        ---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
        (3)\n------------ OR ------------\nKey not found\n------------ OR -------
        -----\nDisabled (4)",
                "currentValues": [
                    "Key not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null,
        "description": "The following Integer value X indicates the current value
        of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
                "lastUpdated": "2024-11-06T09:12:22Z",
                "extendedEvidence": "Row 1:Service Name,Registry Key,Start
        Value,Delayed Start\nRow
        2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
            },
            "causeOfFailure": null,
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "2.34",
            "totalDataSizeKB": "7.61",
            "currentBatch": 1,
            "totalBatches": 1,
            "CLOUD_RESOURCE_ID": null
        }
        ]
```


Sample - Retrieve Posture Information Based on Criticality Label: Medium

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/3.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0& criticalityLabels= MEDIUM" -H "accept: */*" -H "Authorization: Bearer Token" -H
"Content-Type:application/json" -d "[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST
ID2>\"]}]"
```

JSON Output


```
[
            {
            "id": xx,
```

```
        "instance": "os",
        "policyId": xx,
        "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
based facsimile service that can take system documents and send these out
to a fax-recipient via a hardware modem and analog phone line.  (One
reported public exploit uses the Windows Picture and Fax Viewer
(SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
can potentially compromise sensitive system documents, by transmitting
information to unauthorized recipients and can be activated remotely, this
capability should be restricted/set according to the needs of the
business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
"cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T09:12:22Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxx",
        "customerId": "xxx",
        "assetId": xxx,
        "technology": {
            "id": 21,
            "name": "Windows 2008 Server"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nAutomatic (2)\n------------ OR ---------
```

```
---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
(3)\n------------ OR ------------\nKey not found\n------------ OR -------
-----\nDisabled (4)",
            "currentValues": [
                "Key not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-11-06T09:12:22Z",
            "extendedEvidence": "Row 1:Service Name,Registry Key,Start
Value,Delayed Start\nRow
2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.34",
        "totalDataSizeKB": "7.61",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
]
```


V4.0

API URL: <qualys_base_url>/pcrs/4.0/posture/postureInfo?

[POST] [GET]

Note: The V4 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions v1 or v2.

This version (/pcrs/4.0/posture/postureInfo) of the API enables you to:

- View cloud metadata in the API response.
- Retrieve the posture information based on the current posture status (passe/failed/error).
- Retrieve the posture information based on the previous status (passed/failed/error) of the posture.
- Retrieve posture information based on the following criticality categories:
  - UNDEFINED (0)
  - MINIMAL (1)
  - MEDIUM (2)
  - SERIOUS (3)
  - CRITICAL (4)
  - URGENT (5)

Input Parameters

Parameter	Description
Authentication Token (Bearer Token)	(Required) Specify the authentication token that is returned by the authentication request.
evidenceRequired	(Optional) Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note:** Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	(Required) Default value is 1, which indicates that the output will be compressed. If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
Request Body	(Required) Output of the Resolve Host ID and the JWT token.
Request header: Authorization	(Required) JWT encrypted token. **Note:** The token received from the Authorization API and the token used in the second API need to be the input here.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
lastScanDate	(Optional) Compliance posture information on the date on which an asset was last scanned. The formats for date are: lastScanDate=2021-12-17 Or, lastScanDate=2021-12-17T18:48:16Z
lastScanDateFrom, lastScanDateTo	(Optional) Compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.

Parameter	Description
statusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)
excludeInactiveControl	(Optional) Default value is 0, which indicates that inactive controls data is retrieved for the host posture. If you want to exclude inactive control data then, change the value to 1.
cloudMetaDataRequired	(Optional) This parameter allows you to retrieve cloud metadata. Specify "1" to retrieve cloud metadata information in the API response. Specify "0" to not retrieve cloud metadata information in the API response. **Note:** Cloud metadata is returned as null in the response for the postures that do not have cloud metadata.
status	(Optional) This parameter lets you retrieve posture information based on the current posture status. Possible values are Passed, Failed, and Error. You can provide multiple comma-separated values.
previousStatus	(Optional) This parameter lets you retrieve posture information based on the previous posture status. Possible values are Passed, Failed, and Error. You can provide a single value at a time.

Parameter	Description
criticalityValues	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated values. When set to 0, posture information with criticality level UNDEFINED is retrieved. When set to 1, posture information with criticality level MINIMAL is retrieved. When set to 2, posture information with criticality level MEDIUM is retrieved. When set to 3, posture information with criticality level SERIOUS is retrieved. When set to 4, posture information with criticality level CRITICAL is retrieved. When set to 6, posture information with criticality level URGENT is retrieved. **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.
criticalityLabels	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated crticality labels. Possible values are: - UNDEFINED - MINIMAL - MEDIUM - SERIOUS - CRITICAL - URGENT **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.

Sample - Get Extended Evidence for a Control and Control description

You can retrieve extended evidence and last updated date information for the hosts. The evidence for a control includes the expected and actual values for the control on the host. The extended evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result. You can also view a control description under the evidence section for the particular host posture. To retrieve the extended information in the API response, specify the following input parameters.

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compre
ssionRequired=0"
-H "accept: */*"
-H "Authorization: Bearer Token"
-H "Content-Type: application/json"-d "[{\"policyId\":\"POLICY
ID\",\"subscriptionId\":\"SUBSCRIPTION ID\",\"hostIds\":[\"HOST
ID1\",\"HOST ID2\"]}]"
```

JSON Output


```
  {
        "id": 20245394,
        "instance": "os",
        "policyId": 1455112,
        "policyTitle": "Linux_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN
<required value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\" and also
another PAM module (such as \"pam_cracklib\") during a password change
operation, then the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T10:40:30Z",
        "lastPassDate": "2024-11-15T01:22:58Z",
        "postureModifiedDate": "2024-11-06T10:40:30Z",
        "lastEvaluatedDate": "2024-11-15T01:22:58Z",
        "created": "2025-02-05T06:01:09Z",
        "hostId": 6396397,
        "ip": "10.11.70.111",
```

```
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos:6.6:::",
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T10:42:29Z",
        "customerUuid": "e57ba830-15e4-714c-8243-6d1740d3577e",
        "customerId": "2309240",
        "assetId": 50568616,
        "technology": {
            "id": 43,
            "name": "CentOS 6.x"
        },
        "criticality": {
            "label": "urg_updated",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------ OR ------------\ngreater than or
equal to\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2024-11-06T10:42:29Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN setting as defined within the
/etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.88",
        "totalDataSizeKB": "2.88",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
```


Sample - Exclude Inactive Control Data

You can include/exclude inactive controls (SDC, UDC) from the host compliance posture information in the API response. Inactive controls are the controls removed or deactivated from a policy.

API Request

```
<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compres
sionRequired=0&excludeInactiveControl=1
```

JSON Output


```
"id": xx,
"instance": "oracle19cdb:1:1527:ora19csu",
"policyId": xx,
"policyTitle": "Oracle_DB_UDC",
"netBios": null,
"controlId": 100432,
"controlStatement": "Oracle_DB_UDC_3",
"rationale": "rationle",
"remediation": "Remediation",
"controlReference": null,
"technologyId": 312,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-06-08T09:52:13Z",
"lastFailDate": "2023-08-24T10:00:05Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-06-08T09:52:13Z",
"lastEvaluatedDate": "2023-08-24T10:00:05Z",
"created": "2024-01-30T06:54:04Z",
"hostId": xx,
"ip": "xx.xx.xx.xx",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2024-01-05T10:24:32Z",
"customerUuid": "xx-xx-xx-xx-xx",
"customerId": "xx",
"assetId": xx,
"technology": {
"id": 312,
"name": "Oracle 19c Multitenant"
},
"criticality": {
"label": "SERIOUS",
"value": 3
},
"evidence": {
"expectedValues": "\nSet status to PASS if no data found",
"currentValues": [
"GRANTEE|:|GRANTED_ROLE",
"APPQOSSYS|:|DBA",
"UDC_SENSITIVE_SCAN|:|DBA",
"QUALYS_SCAN|:|DBA"
],
"actualValues": null,
"directoryFimUdc": null
```

```
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
},
"causeOfFailure": {
"missing": {
"logic": null,
"value": [
"------------ OR ------------",
"Set status to PASS if no data found"
]
},
"unexpected": {
"value": [
"DBA,DBA,DBA",
"APPQOSSYS,UDC_SENSITIVE_SCAN,QUALYS_SCAN"
]
}
},
"currentDataSizeKB": "1.47",
"totalDataSizeKB": "4.59",
"currentBatch": 1,
"totalBatches": 1,
"CLOUD_RESOURCE_ID": null
}
```


Sample - Retrieve Compliance Posture Information along with Control Status

API response now displays the status of the controls on a host as passed when an exception has been created and approved. The controls on which the exception has been approved are displayed as Passed*. Exception is a way to temporarily change the status of a control on a host from Failed to PassedE (passed with an exception). To learn about what is exceptions refer to Exceptions- The Basics.

API Request

<qualys_base_url>/pcrs/4.0/posture/postureInfo?compressionRequired=0' \ --header 'accept: */*' \ --header 'Authorization: `Bearer Token`' \ --header 'Content-Type: application/json' \ --data '[{ "policyId": "xx", "subscriptionId": "xx", "hostIds": ["xx"] }]'

JSON Response


```
{
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "LinuxAllAssetScan_withAssetTag",
        "netBios": null,
        "controlId": xx,
        "controlStatement": "File_content_check_udc-2",
        "rationale": "rationale",
        "remediation": null,
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
```

```
            "status": "Passed*",
            "previousStatus": "Error",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "",
            "lastPassDate": "",
            "postureModifiedDate": "2024-07-10T15:10:32Z",
            "lastEvaluatedDate": "2024-08-25T17:36:31Z",
            "created": "2024-08-29T10:58:49Z",
            "hostId": xx,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": null,
            "domainName": null,
            "dns": null,
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2024-06-10T17:08:52Z",
            "customerUuid": "xx-xx-xx-xx-xx",
            "customerId": "xx",
            "assetId": xx,
            "technology":
{               "id": 43,               "name": "CentOS 6.x"           }
,
            "criticality":
{               "label": "MEDIUM",               "value": 2           }
,
            "evidence": null,
            "causeOfFailure": null,
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "1.14",
            "totalDataSizeKB": "1.14",
            "currentBatch": 1,
            "totalBatches": 1,
            "CLOUD_RESOURCE_ID": null
        }
```


Sample - Retrieve Compliance Posture Information along with Control Category and Sub-Category

Two new fields in the API response to display control category and sub-category.

- category -Displays control category set on a particular control.
- SubCategory - Displays control Subcategory set on a particular control.

API Request

```
<qualys_base_url>/pcrs/4.0/posture/postureInfo?compressionRequired=0' \ -
-header 'accept: */*' \ --header 'Authorization: Bearer Token' \ --header
'Content-Type: application/json' \ --data '[     {          "policyId":
"5657103",          "subscriptionId": "xx",          "hostIds": [
"xx"          ]     } ]'
```

JSON Response

```
{
  "id": xx,
  "instance": "os",
  "policyId": xx,
  "policyTitle": "LinuxAllAssetScan_withAssetTag",
  "netBios": null,
  "controlId": xx,
  "controlStatement": "File_content_check_udc-2",
  "rationale": "rationale",
  "remediation": null,
  "category": "Access Control Requirements",
  "subCategory": "Authentication/Passwords",
  "controlReference": null,
  "technologyId": 43,
  "status": "Passed*",
  "previousStatus": "Error",
  "firstFailDate": "",
  "lastFailDate": "",
  "firstPassDate": "",
  "lastPassDate": "",
  "postureModifiedDate": "2024-07-10T15:10:32Z",
  "lastEvaluatedDate": "2024-08-25T17:36:31Z",
  "created": "2024-08-29T10:58:49Z",
  "hostId": xx,
  "ip": "xx.xx.xx.xx",
  "trackingMethod": "IP",
  "os": null,
  "osCpe": null,
  "domainName": null,
  "dns": null,
  "qgHostid": null,
  "networkId": 0,
  "networkName": "Global Default Network",
  "complianceLastScanDate": "2024-06-10T17:08:52Z",
  "customerUuid": "xx-xx-xx-xx-xx",
  "customerId": "xx",
  "assetId": xx,
  "technology": {
    "id": 43,
    "name": "CentOS 6.x"
  },
  "criticality": {
    "label": "MEDIUM",
    "value": 2
  },
  "evidence": null,
  "causeOfFailure": null,
  "userDefinedAttributesList": null,
  "currentDataSizeKB": "1.14",
  "totalDataSizeKB": "1.14",
  "currentBatch": 1,
  "totalBatches": 1,
  "CLOUD_RESOURCE_ID": null
}
```

Sample JSON output response - Get Posture Info (single policy ID)

Get posture Info With lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=0&lastEvaluationDate=2021-12-23"-H "accept: */*"-H
"Authorization: Bearer Token"-H "Content-Type: application/json"-d
"[{\"policyId\":\"POLICY ID\",\"subscriptionId\":\"SUBSCRIPTION
ID\",\"hostIds\":[\"HOST ID1\",\"HOST ID2\"]}]"
```

JSON Output


```
[
{
"id": xxx,
"instance": "os",
"policyId": "<POLICY ID>",
"controlId": "<CONTROL ID>",
"controlStatement": "Status of the 'banner motd' configuration command on
the device",
"rationale": "The 'Message of the Day (banner motd)' command is used to
provide a warning banner displayed when a
connection to the device is made BEFORE a user successfully authenticates
to the device. The Message of the Day banner can be used to provide an
acceptable use policy or warning prior to login notifying that all user
activity may be monitored and potential legal consequences may result from
unauthorized use. Run this check periodically to ensure content of the
banner displayed is in compliance with the requirements and expectations
driven by internal standards and/or policies.",
"remediation": "Execute following commands to set desired
banner message:\n1. configure terminal\n2. banner motd
'delimiting-character' 'message' 'delimiting-character'\n3.
exit\n\nc",
"controlReference": null,
"technologyId": xxx,
"status": "Error",
"previousStatus": "Error",
"firstFailDate": "",
"lastFailDate": "",
"firstPassDate": "2021-12-21T11:28:21Z",
"lastPassDate": "2021-12-21T11:29:22Z",
"postureModifiedDate": "2021-12-22T12:56:41Z",
"lastEvaluatedDate": "2021-12-23T05:32:40Z",
"created": "2022-02-21T13:10:13Z",
"hostId": "<HOST ID>",
"ip": "xx.xx.xx.xxx",
"trackingMethod": "IP",
"os": null,
"osCpe": "cpe:/o:cisco::7.0%283%29i2%282%29:::",
"dns": null,
```

```
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2021-12-22T12:49:59Z",
"customerUuid": "<CUSTOMER UUID>",
"customerId": "<CUSTOMER ID>",
"assetId": "<ASSET ID>",
"technology": {
"id": xxx,
"name": "Cisco NX-OS"
},
"criticality": {
"label": "CRITICAL",
"value": 4
},
"evidence": null,
"causeOfFailure": null,
"currentBatch": 1,
"totalBatches": 1
}
```

GET Get Posture Info Without lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=0 and compressionRequired=0

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Response:

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL ID>,
        "technologyId": xx,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:54:26Z",
        "hostId": <HOST ID>,
```

```
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe":  "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:57:58Z",
    "customerUuid": "xxx",
    "customerId": "xxx",
    "assetId": "xxx",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "SERIOUS",
        "value": 3
    },
    "evidence": null,
    "causeOfFailure": {
        "missing": {
            "logic": null,
            "value": [
                "1",
                "Attribute not found",
                "Unable to retrieve password policy"
            ]
        },
        "unexpected": {
            "value": [
                "0"
            ]
        }
    }
},
{
    "id": xxx,
    "instance": "os",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T07:52:41Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T07:52:41Z",
```

```
            "created": "2021-10-29T07:54:26Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "xxxx",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Windows Server 2012 R2"
            },
            "criticality": {
                "label": "URGENT",
                "value": 5
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info Without lastEvaluationDate, Without Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=0 & compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)


```
‹        íÝ]sÚHÅñ¯ââ:Îê!ÁÝ¬í¤UœIì8©š©©)
²CÐ2S©|÷•p2Ž_ÖôÁý€ÿ»d‡~é´8:ýÛçÆ ßè„í(ÈÒfð¬1OËî¸—
7:ÐÚxÖ¸,†ƒÞß‡Õ6Í(ŠÓ${Öè-ãrR
ëÇÂ0Kž5Ê¼÷~\
‹‹ùviõHµ‡6-öñª;æýz?"üã MOî<s>LËÿtÃýnY¿lõÐ°{û'ùFõ?}(
¢p7
v£äM9¢° Æ¿~ýÁû¶j×[%Q§þ:ÿ?ål'-ýÁù
ïÿß]†ßvyð±;œU[ÝÙôæ~{"¼ÞèÎ--N Ô?¼¯^¸>DY«?ÚÍêh_V?‡Áó0|ž-Ï›QµM9éö>
ÆGyù¾¨÷uøªz´ú,:ãÙpXÿiï²~½Ë¼ó¯¢3ô&Å´8/;Ÿ-ã~ñiúÇ4Ÿ|Ì'?DAu&Q§óW«Ù©öÐ×G½WŒúùÇ
éŸÃêéVõèŸÿ-ÞS}
\í}œ—
ŸŠÉ‡úM6,Æ???ÙÕ¯ùó°8ëwöóóîlXî¼¼z²þÍ‹ÑåpPŸ7/ªÃuÒëŽo©ìMØêÄíN'ÌÔlZ£|r:?Ì_©?g
iž-»ÙYÔÚM³óóÝ,l&»Ažeaë¼?¦çßýÔüÝEIPí»z´>Ê«‡Â´Ðiý¾¯OÉFçê ¯OËñÕ¯ñîêHíœÌÔN}¤
```

```
vŽ£Æ—ú ?”ƒ^w8(ç?7ìžåÃêöŽß?îýô¢Úq}&TûhV?W't?ŸS¹:v½îlšÿr^Ÿ¸ÕÙuõè—g7€…*°(lE
ÀÜ€Eò´C€ìvrp|øËéÉµ¯x9_±î+Å¾~t_Gû‡§G×¼¢åx5—àõðÿëW»Ÿ×?ÏÜæõ€œû¶°y†ßfx—
?¼àµ’áësc4Ñ«Or¾§âbÐû¶å×¤Ö¨¨ßþOe9œÍÊ|g\”;çÅl\£8wÏ†ùNYìLòêùüc¾sYý¢Õáîï\‘lü^½
‡Ù8ÿë2ïÍO°Ï×û
ª'¿Ü²?ñ_Sæ~ØþÑmŸÿ|ðòÍ5íd¹¡³uƒ×ÑÉÉëõ‹ ·:Õ¹ÖŒãÎü‘êß‘·ÇW{ûoû»çâf5Þ €Oàü¼ü*ð
èÛAÛ©
\;l-âLêâ}—@aC>À0óÏ°•Á †0T¶-Æ0„!
Ý&Ãvð0C.¼Âp›.¾úª]?MBÄw¾›d,1^K#†Ì,aC…aìŸa0Â †
Ã¦Ã&
aCâbÁpÁ—ÿ\àâ63tˆ×Õo÷mý—éwÙ°.û„÷\öñŸë©h·a¡
ma„5Èõ¤-æ›0„¡ÂÐ ×"’ëâv0ôtdb ëI‰õ …,Â-Aª'‹PˆB
```

Get Posture Info Without lastEvaluationDate, With Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)

```
‹        í?sÛFš@ÿ
Jµöî^ ¼€|"%yâÄr  SvR"ÌNQ$LaC4 ÚÖÌä¿o7HJ¼
ša‹"qR•*YÂµÑ}ú,ßùõß'^ÿ¤mµª¦Ó¬™?=ñü(îú=÷¤}D'?=C¯wÿFlS«VífÝùëI/ðã0ÊßY-
SÿëIìöîü`
’íšâ7âñ$Ç¸îF‘Û—ÇÝ/^0‰:k?ùä…Qü°ë
/°±<-øÕ°»ú›d#¹ËìWU³j2æiµ~c6ÛU«mÙ?Ÿí¶UKnU¯¶kÖß"{ŠâIè^}ï"çö3iÍyù¥;œˆ-Ö6]>n/
tåFë?ÔÚõ†ÜàNœX‘ÓhÕ?-š(í±ØØ2+-Uiš•ZUl ‡ÝÞïž?¸rã»@ëÍµø-xm?2?ÊŸÎÇòzc·ý?A{äõÂ
>Åí¯žß¾FÿŒÜð‹ ?þ³jZÕvXm·¿5jmq„¾/K½Œúî—
èóPü¹!~ûyð?&Y¦G÷Ýøk þ./òÄ<yø÷»îHžóoÃà¶;4.ÜOÝÉ06ÞMÿ(ï<?ž¬7oEquz]?µ¤œ?«Ñ®
‹²p’’šDq0rÃ /9S×všnÓ<un«Ó¦óéÓ©cÕê§¦Õ¼u¬Æ§®Õü´°WruÕ°)Ž-
~+ëQ<ý•ÕlÕ?¼îÇ*yÒžVqY-ýémü<-)£"””!KÊx_=ùC>A/özÝ¡'û
»·îPìpþþÍÍ›ó³·âÀ²&ˆcÔÄÆ¢B÷Ý¤©üûÄý6v{âÙ?”?-
ý›?áEÝÛ¡Û7^/?óOþ3~|o,þû7ÿÒŸmjånúÞt&·?¸÷†ÄÆ§`â÷óvYÚ8)Ç0týx~-¿ž,^êÉ?D‘öâIw8
ÿû´fô½PÜa Þ¿öFú½é¯e‘u'‘ûã'Ù\E›šÿz+-*VªV£
VÀ
```

Get Posture Info Without lastEvaluationDate, With Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"xxx\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output:


```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\nUnable to retrieve password policy\n------------ OR ----------
--\nequal to\n1",
            "currentValues": [
                "0"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
```

```
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:PCDEV",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-25T07:21:13Z",
        "lastPassDate": "2021-10-29T07:52:41Z",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:27Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
```

```
        },
        "evidence": {
            "expectedValues": "\nGrantees not found\n------------ OR ----
--------\nmatches regular expression list\n.*",
            "currentValues": [
                "Grantees not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    }
]
```

Sample JSON output response - Get Posture Info (multiple policy IDs)

Get Posture Info with lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0&lastEvaluationDate=2021-12-27T15:35:22Z" -H "accept: /" -H
"Authorization: Bearer Token" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<Policy_ID>\",\"subscriptionId\":\"<Subscription_ID>\",
\"hostIds\":[\"<Host_ID1>\"]},{\"policyId\":\"policyId1\",\"subscriptionI
d\":\"<Subscription_ID\",\"hostIds\":[\"<HOST_ID1>\"]}]"
```

JSON Output:

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL_ID,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
```

```
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-12T13:12:26Z",
        "lastPassDate": "2021-12-27T15:35:22Z",
        "postureModifiedDate": "2021-10-12T13:12:26Z",
        "lastEvaluatedDate": "2021-12-27T15:35:22Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "DNS Hostname",
        "os": xx,
        "osCpe": "cpe:/o:microsoft:windows_2003_server::sp2::",
        "domainName": "<DOMAIN NAME>",
        "dns": "client5-25-244.root.vuln.qa.qualys.com",
        "qgHostid": xx,
        "networkId": xx,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-27T15:31:18Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "Windows 2003 Server"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": xx
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n0",
            "currentValues": [
                "1"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "currentBatch": xx,
        "totalBatches": xx
    },
    {
        "id": xx,
```

```
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL_ID>,
        "controlStatement": "Status of the
'net.ipv4.conf.all.send_redirects' setting within the '/etc/sysctl.conf'
file",
        "rationale": "The 'net.ipv4.conf.all.send_redirects' network
parameter (/etc/sysctl.conf) allows ICMP routing redirection.  If the
system is not going to be used as a firewall or gateway to pass network
traffic, and this parameter is not disabled, malicious users may attempt
to spoof source addresses or redirect traffic to a host with a network
sniffer, so this value should be set according to the needs of the
business.",
        "remediation": "Set the following parameters in the
/etc/sysctl.conf file:\n\n# net.ipv4.conf.all.send_redirects = 0\n\nOR
\nRun the following commands to set the active kernel parameters:\n#
sysctl -w net.ipv4.conf.all.send_redirects=0\n# sysctl -w
net.ipv4.route.flush=1",
        "controlReference": null,
        "technologyId": 80,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-02-11T12:54:23Z",
        "lastPassDate": "2022-02-11T12:54:23Z",
        "postureModifiedDate": "2022-02-11T12:54:23Z",
        "lastEvaluatedDate": "2022-02-11T12:54:23Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-02-11T12:47:29Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "CentOS 7.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": {
```

```
            "expectedValues": "\nSetting not found\n------------ OR -----
    -------\nFile not found\n------------ OR ------------\nmatches regular
    expression list\n.*",
            "currentValues": [
                "Setting not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "currentBatch": 1,
        "totalBatches": 1
    }
]
```

Get Posture Info without lastEvaluationDate, without evidence, without compression, without lastScanDate

User Input**:** evidenceRequired=0 & compressionRequired=0

Request**:**

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}]"
```

JSON Output**:**

```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:38:14Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
```

```
    "dns": null,
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-14T09:37:38Z",
    "customerUuid": "<CUSTOMER UUID>",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Cisco ASA 9.x"
    },
    "criticality": {
        "label": "MEDIUM",
        "value": 2
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": xx,
    "instance": "os",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "xx-xx-xx-xx-xx",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
```

```
            "criticality": {
                "label": "CRITICAL",
                "value": 4
            },
            "evidence": null,
            "causeOfFailure": null
        },
        {
            "id": 19235413,
            "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
            "policyId": "<POLICY ID>",
            "policyTitle": "<POLICY TITLE>",
            "netBios": "<NETBIOS>",
            "controlId": "<CONTROL ID>",
            "technologyId": "<TECHNOLOGY ID>",
            "status": "Passed",
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-28T16:53:06Z",
            "lastPassDate": "2021-10-29T08:38:10Z",
            "postureModifiedDate": "2021-10-28T16:53:06Z",
            "lastEvaluatedDate": "2021-10-29T08:38:10Z",
            "created": "2021-10-29T08:38:15Z",
            "hostId": "<HOST ID>",
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:53:14Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info without lastEvaluationDate, with evidence, without compression, without lastScanDate

User input: evidenceRequired=1 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:40:38Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
```

```
            "expectedValues": "\nFilter 2 not found: ^[\\*\\.\\d]\n------
------ OR ------------\nFilter 1 not found: show clock detail\n----------
-- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "show clock detail:08:26:29.074 pdt Thu Oct 14 2021"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-28T16:53:06Z",
        "lastPassDate": "2021-10-29T08:39:07Z",
        "postureModifiedDate": "2021-10-28T16:53:06Z",
        "lastEvaluatedDate": "2021-10-29T08:39:07Z",
        "created": "2021-10-29T08:40:46Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Microsoft SQL Server 2016"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nSet status to PASS if no data found\n---
```

```
--------- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "Error Code 35:Failed to execute database query"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    }
]
```

Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

User input**:** evidenceRequired=0 & compressionRequired=1 & lastScanDate=yyyy-mm-dd:Thh:mm:ssZ

Request**:**

```
Curl-X POST
"<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=1&lastEvaluationDate=2021-12-
17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z" -H
"accept: */*" -H
"Content-Type: application/json" -d "
[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

JSON output:

```
[
    {
        "id": <HOST INSTANCE ID>,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
```

```
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
        "osCpe": null,
       "domainName": "<DOMAIN NAME>",
        "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-23T12:59:04Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 217,
            "name": "Red Hat Enterprise Linux 8.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 8,
        "totalBatches": 12
    },
]
```


Get Posture Info without evidence, without compression, with statusChangedSince

Request:

```
curl -X POST
"https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0&statusChangedSince=2021-12-23" -H "accept: */*" -H "Authorization:
Bearer Token" -H "Content-Type: application/json" -d
```

```
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONID>\",\"
hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON output:


```
[
    {
        "id": 24705485,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "pcas_win16_redhat7 tech",
        "netBios": "<NETBIOS>",
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": 106,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-11-09T12:50:12Z",
        "lastPassDate": "2022-12-06T06:42:21Z",
        "postureModifiedDate": "2022-11-09T12:50:12Z",
        "lastEvaluatedDate": "2022-12-06T06:42:21Z",
        "created": "2022-12-07T07:35:56Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": null,
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2016:1607::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "<DNS>",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-08-23T04:57:05Z",
```

```
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": <ASSET ID>,
            "technology": {
                "id": 106,
                "name": "Windows 2016 Server"
            },
            "criticality": {
                "label": "high updated",
                "value": 5
            },
            "evidence": {
                "expectedValues": "\nAttribute not found\n------------ OR ---
---------\ngreater than or equal to\n0",
                "currentValues": [
                    "6"
                ],
                "actualValues": null,
                "directoryFimUdc": null
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            },
            "causeOfFailure": null,
            "currentDataSizeKB": "2.41",
            "totalDataSizeKB": "2.41",
            "currentBatch": 1,
            "totalBatches": 1
        },
    ]
```


Sample - Retrieve Cloud Metadata

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=0&cloudMetaDataRequired=1" -H "accept: */*" -H
"Authorization: Bearer Token" -H "Content-Type:application/json" -d
"[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST
ID1>\",\"<HOST ID2>\"]}]"
```

JSON Output


```
[    {
            "id": xx,
            "instance": "os",
            "policyId": xx,
            "policyTitle": "CPS -Test",
            "netBios": "INSTANCE-xx-xx",
            "controlId": xx,
           "controlStatement": "Status of the 'Trivial File Transfer Protocol
    (TFTP)' service",
          "rationale": "The 'TFTP' service is both a command and TCP protocol
    that is normally used only for booting diskless workstations, getting or
    saving network component configuration files, or as a 'kickstart' type
```

```
host configuration from a network-based template.  The connection
initiation and data transfer is all done in clear text without requiring
credentials of any kind.  As a malicious user with a 'sniffer' running on
the network, could easily capture the data and/or reproduce the same
operation, simply by knowing the name of the file(s) and the source
address(es), this process should be disabled/restricted according to the
needs of the business.",
        "remediation": "Review \"/etc/inetd.conf\" file to check whether
tftp service's configuration in line with business needs and
organization's security policies.\n\nExample: To disable the tftp
service,\n\nRemove or comment out any tftp lines in /etc/inetd.conf: \n#
tftp stream tcp nowait root internal",
        "category": "Services",
        "subCategory": "Guidelines/Procedures (Services)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:20:49Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xx-xx-xx-xx-xxx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
```

```
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.98",
        "totalDataSizeKB": "27.09",
        "currentBatch": 1,
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "xx",
            "cloudResourceType": "Instance",
            "cloudAccountId": "xx",
            "cloudImageId": null,
            "cloudResourceMetadata": "{'Public IP
    Address':'xx.xxx.xx.xxx', 'Private IP Address':'xx.xxx.x.xx', 'Machine
    Type':'e2-medium', 'Zone':'null', 'ProjectId':'qlys-devqa-qweb',
    'State':'RUNNING', 'Network':'N/A', 'MAC Address':'null'}"
        },
        "CLOUD_RESOURCE_ID": "xxx"
    }
]
```


Sample - Retrieve Posture Information Based on Current Posture Status - passed

API Request

curl -X POST "<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&status=Passed" -H "accept: */*" -H "Authorization: `Bearer Token`" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[        {
        "id": xx,
        "instance": "os",
        "policyId": 1438626,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xxxxxx-xxxxx",
        "controlId": xx,
       "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
    protocol, most commonly used for accessing remote computers via a command
    line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
    clear text including any uid/password input, so if a telnet session is
    used for privileged communication(s)/host configuration purposes, the
```

```
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
       "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xxx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxxxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxx",
        "customerId": "xx",
        "assetId": xxx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
------ OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
```

```
            "extendedEvidence": "Row 1:\n"

        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxx"
    }
]
```


Sample - Retrieve Posture Information Based on Previous status-passed

API Request

curl -X POST "<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&previousStatus=Passed" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[       {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xx-xx",
        "controlId": xx,
        "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
protocol, most commonly used for accessing remote computers via a command
line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
clear text including any uid/password input, so if a telnet session is
used for privileged communication(s)/host configuration purposes, the
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
       "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
```

```
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxxxx",
        "customerId": "xxxx",
        "assetId": 42078290,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxxx"
    }
]
```


Sample - Retrieve Posture Information Based on Criticality Value: 2

API Request

curl -X POST "<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0& criticalityValues=2" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[
        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
    based facsimile service that can take system documents and send these out
    to a fax-recipient via a hardware modem and analog phone line.  (One
    reported public exploit uses the Windows Picture and Fax Viewer
    (SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
    can potentially compromise sensitive system documents, by transmitting
    information to unauthorized recipients and can be activated remotely, this
    capability should be restricted/set according to the needs of the
    business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xxx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
    "cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T09:12:22Z",
        "customerUuid": "xx-xx-xx-xx-xxxx",
```

```
            "customerId": "xx",
            "assetId": xx,
            "technology": {
                "id": 21,
                "name": "Windows 2008 Server"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": {
                "expectedValues": "\nAutomatic (2)\n------------ OR ---------
        ---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
        (3)\n------------ OR ------------\nKey not found\n------------ OR -------
        -----\nDisabled (4)",
                "currentValues": [
                    "Key not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null,
        "description": "The following Integer value X indicates the current value
        of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
                "lastUpdated": "2024-11-06T09:12:22Z",
                "extendedEvidence": "Row 1:Service Name,Registry Key,Start
        Value,Delayed Start\nRow
        2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
            },
            "causeOfFailure": null,
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "2.34",
            "totalDataSizeKB": "7.61",
            "currentBatch": 1,
            "totalBatches": 1,
            "CLOUD_RESOURCE_ID": null
        }
        ]
```


Sample - Retrieve Posture Information Based on Criticality Label: Medium

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0& criticalityLabels= MEDIUM" -H "accept: */*" -H "Authorization: Bearer Token" -H
"Content-Type:application/json" -d "[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST
ID2>\"]}]"
```

JSON Output


```
[
            {
            "id": xx,
            "instance": "os",
            "policyId": xx,
            "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
```

```
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
based facsimile service that can take system documents and send these out
to a fax-recipient via a hardware modem and analog phone line.  (One
reported public exploit uses the Windows Picture and Fax Viewer
(SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
can potentially compromise sensitive system documents, by transmitting
information to unauthorized recipients and can be activated remotely, this
capability should be restricted/set according to the needs of the
business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
"cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T09:12:22Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxx",
        "customerId": "xxx",
        "assetId": xxx,
        "technology": {
            "id": 21,
            "name": "Windows 2008 Server"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nAutomatic (2)\n------------ OR ---------
---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
(3)\n------------ OR ------------\nKey not found\n------------ OR -------
-----\nDisabled (4)",
```

```
            "currentValues": [
                "Key not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
        "description": "The following Integer value X indicates the current value
        of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-11-06T09:12:22Z",
            "extendedEvidence": "Row 1:Service Name,Registry Key,Start
        Value,Delayed Start\nRow
        2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.34",
        "totalDataSizeKB": "7.61",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
]
```


Sample - Retrieve compliance posture information

API Request

```
curl --location
'<qualys_base_url>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequir
ed=0&clou
 dMetaDataRequired=1' \
--header 'accept: */*' \
--header 'Authorization: Bearer <JWT TOKEN>' \
--header 'Content-Type: application/json' \ --data '[
  {
    "policyId": "1438442",
    "subscriptionId": "822838",
    "hostIds": [
      "4783735",
      "4980343"
    ]
  }
]'
```

JSON Output


```
[
    {
        "id": <id>,
        "instance": "os",
        "policyId": <policy_id>,
        "policyTitle": "GCP policy-Neha",
        "netBios": "NEW-SPIN123",
        "controlId": <control_id>,
        "controlStatement": "Status of the 'Minimum Password Length'
        setting",
        "rationale": "Among the several characteristics that make 'user
```

identification' via password a secure and workable solution is setting a 'minimum password length' requirement. Each character that is added to the password length squares the difficulty of breaking the password via 'brute force,' which attempts using every combination possible within the password symbol set-space, in order to discover a user's password. While no 'minimum length' can be guaranteed secure, eight (8) is commonly considered to be the minimum for most application access, along with requiring other password security factors, such as increasing the size of the symbol set-space by requiring mixed cases, along with other forms of password variability creation, increases the difficulty of breaking any password by brute-force attack.",
        "remediation": "To specify password length requirements for new accounts, edit the file
\"/etc/login.defs\" and add or correct the following lines:
\n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program
consults \"/etc/login.defs\" and also another PAM module (such as
\"pam_cracklib\") during a
password change operation, then the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 81,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-03-23T07:10:02Z",
        "lastPassDate": "2025-03-23T07:10:02Z",
        "postureModifiedDate": "2025-03-23T07:10:02Z",
        "lastEvaluatedDate": "2025-03-23T07:10:02Z",
        "created": "2025-04-16T12:24:23Z",
        "hostId": 4783735,
        "ip": "10.xxx.x.19",
        "trackingMethod": "AGENT",
        "os": null,
        "osCpe": null,
        "domainName": "121.xxx.xxx.34.bc.googleusercontent.com",
        "dns": "121.xxx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "c4b0cde6-9017-4340-933e-afbbc71556b4",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "93f7ad53-1590-e3ac-83cd-322b91180e13",
        "customerId": "1337821",
        "assetId": 41157957,
        "technology": {
            "id": 81,
            "name": "Red Hat Enterprise Linux 7.x"
        },
        "criticality": {
            "label": "URGENT",
            "value": 5

```
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------
OR ------------\ngreater than or equal to\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2025-04-20T08:52:58Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN
setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "3.39",
        "totalDataSizeKB": "3.39",
        "currentBatch": 1,
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "3654664005469669138",
            "cloudResourceType": "Instance",
            "cloudAccountId": "175127636344",
            "cloudImageId": null,
            "cloudResourceMetadata": {
                "publicIpAddress": "34.136.202.121",
                "privateIpAddress": "10.128.0.19",
                "machineType": "custom-1-1024",
                "zone": null,
                "projectId": "qlys-devqa-qweb",
                "state": "STOPPED",
                "network": "N/A",
                "macAddress": null
            }
        },
        "CLOUD_RESOURCE_ID": "3654664005469669138"
    },
    .......
    {
        "id": 19029079,
        "instance": "os",
        "policyId": 1438442,
        "policyTitle": "GCP policy-Neha",
        "netBios": "INSTANCE-20250423-173020",
        "controlId": 1131,
       "controlStatement": "Status of the 'Trivial File Transfer Protocol
(TFTP)' service",
       "rationale": "The 'TFTP' service is both a command and TCP protocol
```

```
that is normally used only
for booting diskless workstations, getting or saving network component
configuration files, or as a
'kickstart' type host configuration from a network-based template.  The
connection initiation and
data transfer is all done in clear text without requiring credentials of
any kind.  As a malicious user
with a 'sniffer' running on the network, could easily capture the data
and/or reproduce the same
operation, simply by knowing the name of the file(s) and the source
address(es), this process should
be disabled/restricted according to the needs of the business.",
        "remediation": "Review \"/etc/inetd.conf\" file to check whether
tftp service's configuration in line
with business needs and organization's security policies.\n\nExample: To
disable the tftp
service,\n\nRemove or comment out any tftp lines in /etc/inetd.conf: \n#
tftp stream tcp nowait root
internal",
        "category": "Services",
        "subCategory": "Guidelines/Procedures (Services)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-04-06T09:48:19Z",
        "lastPassDate": "2025-04-06T09:48:19Z",
        "postureModifiedDate": "2025-04-06T09:48:19Z",
        "lastEvaluatedDate": "2025-04-06T09:48:19Z",
        "created": "2025-04-16T12:24:26Z",
        "hostId": 4980343,
        "ip": "34.xxx.xxx.84",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "179.xx.xxx.35.bc.googleusercontent.com",
        "dns": "179.xx.xxx.35.bc.googleusercontent.com",
        "qgHostid": "4bd9e81e-12f8-4d8f-a51d-c475131a55b8",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2025-04-06T09:39:21Z",
        "customerUuid": "93f7ad53-1590-e3ac-83cd-322b91180e13",
        "customerId": "1337821",
        "assetId": 42078290,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
```

```
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2025-04-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n",
           "description": "The following List String value of X indicates
the status of the tftp service
configured within the /etc/xinetd.conf, /etc/xinetd.d/*, /etc/inetd.conf
and /etc/inetd.d/* files on the
host. A value of 0 indicates the service is disabled; and a value of 1
indicates the service is enabled on
the host."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "3.27",
        "totalDataSizeKB": "97.52",
        "currentBatch": 1,
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "2182777093928348127",
            "cloudResourceType": "Instance",
            "cloudAccountId": "175127636344",
            "cloudImageId": null,
            "cloudResourceMetadata": {
                "publicIpAddress": "35.xxx.xx.179",
                "privateIpAddress": "10.xxx.x.27",
                "machineType": "e2-medium",
                "zone": null,
                "projectId": "qlys-devqa-qweb",
                "state": "RUNNING",
                "network": "N/A",
                "macAddress": null
            }
        },
        "CLOUD_RESOURCE_ID": "2182777093928348127"
    }
]
```


V5.0

API URL: <qualys_base_url>/pcrs/5.0/posture/postureInfo?

[POST] [GET]

Note: The V5 API is designed to fetch only PC Asset data. To retrieve both PC and SCA Asset data, continue using API Versions v1 or v2.

This version (/pcrs/5.0/posture/postureInfo) of the API enables you to:

- View cloud metadata in the API response.
- Retrieve the posture information based on the current posture status (passe/failed/error).
- Retrieve the posture information based on the previous status (passed/failed/error) of the posture.
- Retrieve posture information based on the following criticality categories:
  - UNDEFINED (0)
  - MINIMAL (1)
  - MEDIUM (2)
  - SERIOUS (3)
  - CRITICAL (4)
  - URGENT (5)

Input Parameters

Parameter	Description
Authentication Token (Bearer Token)	(Required) Specify the authentication token that is returned by the authentication request.
evidenceRequired	(Optional) Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note:** Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	(Required) Default value is 1, which indicates that the output will be compressed. If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
Request header: Authorization	(Required) JWT encrypted token. **Note:** The token received from the Authorization API and the token used in the second API need to be the input here.
lastEvaluationDate	(Optional) Compliance posture information records when the posture is equal to or greater than the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT).
lastScanDate	(Optional) Compliance posture information on the date on which an asset was last scanned. The formats for date are: lastScanDate=2021-12-17 Or, lastScanDate=2021-12-17T18:48:16Z
lastScanDateFrom, lastScanDateTo	(Optional) Compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.

Parameter	Description
statusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The formats for date and time are: YYYY-MM-DD Or, YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)
excludeInactiveControl	(Optional) Default value is 0, which indicates that inactive controls data is retrieved for the host posture. If you want to exclude inactive control data then, change the value to 1.
cloudMetaDataRequired	(Optional) This parameter allows you to retrieve cloud metadata. Specify "1" to retrieve cloud metadata information in the API response. Specify "0" to not retrieve cloud metadata information in the API response. **Note:** Cloud metadata is returned as null in the response for the postures that do not have cloud metadata.
status	(Optional) This parameter lets you retrieve posture information based on the current posture status. Possible values are Passed, Failed, and Error. You can provide multiple comma-separated values.
previousStatus	(Optional) This parameter lets you retrieve posture information based on the previous posture status. Possible values are Passed, Failed, and Error. You can provide a single value at a time.

Parameter	Description
criticalityValues	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated values. When set to 0, posture information with criticality level UNDEFINED is retrieved. When set to 1, posture information with criticality level MINIMAL is retrieved. When set to 2, posture information with criticality level MEDIUM is retrieved. When set to 3, posture information with criticality level SERIOUS is retrieved. When set to 4, posture information with criticality level CRITICAL is retrieved. When set to 6, posture information with criticality level URGENT is retrieved. **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.
criticalityLabels	(Optional) This parameter lets you retrieve posture information based on the critcality levels. You can provide multiple comma-separated crticality labels. Possible values are: - UNDEFINED - MINIMAL - MEDIUM - SERIOUS - CRITICAL - URGENT **Note:** When executing this API, you can use either the criticalityLabels parameter or criticalityValues parameter, but not both parameters simultaneously.
evidenceRequired={0|1}	(Optional) Set as 1 to retrieve evidence data for posture info or else set 0. By default, the value is set as 0.
extendedEvidenceRequired ={0|1}	(Optional) Set as 1 to retrieve extended evidence data or else set to 0. For using this field, set evidenceRequired=1.
scanSourceRequired={0|1}	(Optional) Specify '1' to display the source of scan and the date on which the scanner was last detected, else specify '0'.

Parameter	Description
qdScoreRequired={0|1}	(Optional) Set as 1 to retrieve QDS in API response or else set 0. By default, the value is set as 0.
Request Body	(Optional) Enter the policy ID, subscription ID, host ID, and the JWT token. OR Enter the Posture ID, subscription ID, and the JWT token. **Note:** Use this parameter to retrieve posture information with Posture ID.

Note: If you are entering multiple comma-separated posture IDs, you can enter a maximum of 400 thousand posture IDs at one time. Otherwise, the size of the entire JSON body (in the curl request) must not exceed 4 megabytes (MB).

Sample - Get Extended Evidence for a Control and Control description

You can retrieve extended evidence and last updated date information for the hosts. The evidence for a control includes the expected and actual values for the control on the host. The extended evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result. You can also view a control description under the evidence section for the particular host posture. To retrieve the extended information in the API response, specify the following input parameters.

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compre
ssionRequired=0"
-H "accept: */*"
-H "Authorization: Bearer Token"
-H "Content-Type: application/json"-d "[{\"policyId\":\"POLICY
ID\",\"subscriptionId\":\"SUBSCRIPTION ID\",\"hostIds\":[\"HOST
ID1\",\"HOST ID2\"]}]"
```

JSON Output

```
  {
        "id": 20245394,
        "instance": "os",
        "policyId": 1455112,
        "policyTitle": "Linux_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
```

```
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN
<required value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\" and also
another PAM module (such as \"pam_cracklib\") during a password change
operation, then the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T10:40:30Z",
        "lastPassDate": "2024-11-15T01:22:58Z",
        "postureModifiedDate": "2024-11-06T10:40:30Z",
        "lastEvaluatedDate": "2024-11-15T01:22:58Z",
        "created": "2025-02-05T06:01:09Z",
        "hostId": 6396397,
        "ip": "10.11.70.111",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:centos:centos:6.6:::",
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T10:42:29Z",
        "customerUuid": "e57ba830-15e4-714c-8243-6d1740d3577e",
        "customerId": "2309240",
        "assetId": 50568616,
        "technology": {
            "id": 43,
            "name": "CentOS 6.x"
        },
        "criticality": {
            "label": "urg_updated",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------ OR ------------\ngreater than or
equal to\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
```

```
            "lastUpdated": "2024-11-06T10:42:29Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN setting as defined within the
/etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.88",
        "totalDataSizeKB": "2.88",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
```


Sample - Exclude Inactive Control Data

You can include/exclude inactive controls (SDC, UDC) from the host compliance posture information in the API response. Inactive controls are the controls removed or deactivated from a policy.

API Request

```
<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compres
sionRequired=0&excludeInactiveControl=1
```

JSON Output


```
"id": xx,
"instance": "oracle19cdb:1:1527:ora19csu",
"policyId": xx,
"policyTitle": "Oracle_DB_UDC",
"netBios": null,
"controlId": 100432,
"controlStatement": "Oracle_DB_UDC_3",
"rationale": "rationle",
"remediation": "Remediation",
"controlReference": null,
"technologyId": 312,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-06-08T09:52:13Z",
"lastFailDate": "2023-08-24T10:00:05Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-06-08T09:52:13Z",
"lastEvaluatedDate": "2023-08-24T10:00:05Z",
"created": "2024-01-30T06:54:04Z",
"hostId": xx,
"ip": "xx.xx.xx.xx",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
```

```
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2024-01-05T10:24:32Z",
"customerUuid": "xx-xx-xx-xx-xx",
"customerId": "xx",
"assetId": xx,
"technology": {
"id": 312,
"name": "Oracle 19c Multitenant"
},
"criticality": {
"label": "SERIOUS",
"value": 3
},
"evidence": {
"expectedValues": "\nSet status to PASS if no data found",
"currentValues": [
"GRANTEE|:|GRANTED_ROLE",
"APPQOSSYS|:|DBA",
"UDC_SENSITIVE_SCAN|:|DBA",
"QUALYS_SCAN|:|DBA"
],
"actualValues": null,
"directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
},
"causeOfFailure": {
"missing": {
"logic": null,
"value": [
"------------ OR ------------",
"Set status to PASS if no data found"
]
},
"unexpected": {
"value": [
"DBA,DBA,DBA",
"APPQOSSYS,UDC_SENSITIVE_SCAN,QUALYS_SCAN"
]
}
},
"currentDataSizeKB": "1.47",
"totalDataSizeKB": "4.59",
"currentBatch": 1,
"totalBatches": 1,
"CLOUD_RESOURCE_ID": null
}
```

Sample - Retrieve Compliance Posture Information along with Control Status

API response now displays the status of the controls on a host as passed when an exception has been created and approved. The controls on which the exception has been approved are displayed as Passed*. Exception is a way to temporarily change the status of a control on a host from Failed to PassedE (passed with an exception). To learn about what is exceptions refer to Exceptions- The Basics.

API Request

<qualys_base_url>/pcrs/5.0/posture/postureInfo?compressionRequired=0' \ --header 'accept: */*' \ --header 'Authorization: Bearer Token' \ --header 'Content-Type: application/json' \ --data '[{ "policyId": "xx", "subscriptionId": "xx", "hostIds": ["xx"] }]'

JSON Response


```
{
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "LinuxAllAssetScan_withAssetTag",
        "netBios": null,
        "controlId": xx,
        "controlStatement": "File_content_check_udc-2",
        "rationale": "rationale",
        "remediation": null,
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 43,
        "status": "Passed*",
        "previousStatus": "Error",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2024-07-10T15:10:32Z",
        "lastEvaluatedDate": "2024-08-25T17:36:31Z",
        "created": "2024-08-29T10:58:49Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": null,
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-06-10T17:08:52Z",
        "customerUuid": "xx-xx-xx-xx-xx",
        "customerId": "xx",
        "assetId": xx,
        "technology":
{           "id": 43,           "name": "CentOS 6.x"         }
```

```
,
        "criticality":
{             "label": "MEDIUM",             "value": 2         }
,
        "evidence": null,
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "1.14",
        "totalDataSizeKB": "1.14",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
```

Sample - Retrieve Compliance Posture Information along with Control Category and Sub-Category

Two new fields in the API response to display control category and sub-category.

- category -Displays control category set on a particular control.
- SubCategory - Displays control Subcategory set on a particular control.

API Request

```
<qualys_base_url>/pcrs/5.0/posture/postureInfo?compressionRequired=0' \ -
-header 'accept: */*' \ --header 'Authorization: Bearer Token' \ --header
'Content-Type: application/json' \ --data '[     {         "policyId":
"5657103",         "subscriptionId": "xx",         "hostIds": [
"xx"         ]     } ]'
```

JSON Response

```
{
  "id": xx,
  "instance": "os",
  "policyId": xx,
  "policyTitle": "LinuxAllAssetScan_withAssetTag",
  "netBios": null,
  "controlId": xx,
  "controlStatement": "File_content_check_udc-2",
  "rationale": "rationale",
  "remediation": null,
  "category": "Access Control Requirements",
  "subCategory": "Authentication/Passwords",
  "controlReference": null,
  "technologyId": 43,
  "status": "Passed*",
  "previousStatus": "Error",
  "firstFailDate": "",
  "lastFailDate": "",
  "firstPassDate": "",
  "lastPassDate": "",
  "postureModifiedDate": "2024-07-10T15:10:32Z",
  "lastEvaluatedDate": "2024-08-25T17:36:31Z",
  "created": "2024-08-29T10:58:49Z",
  "hostId": xx,
```

```
  "ip": "xx.xx.xx.xx",
  "trackingMethod": "IP",
  "os": null,
  "osCpe": null,
  "domainName": null,
  "dns": null,
  "qgHostid": null,
  "networkId": 0,
  "networkName": "Global Default Network",
  "complianceLastScanDate": "2024-06-10T17:08:52Z",
  "customerUuid": "xx-xx-xx-xx-xx",
  "customerId": "xx",
  "assetId": xx,
  "technology": {
    "id": 43,
    "name": "CentOS 6.x"
  },
  "criticality": {
    "label": "MEDIUM",
    "value": 2
  },
  "evidence": null,
  "causeOfFailure": null,
  "userDefinedAttributesList": null,
  "currentDataSizeKB": "1.14",
  "totalDataSizeKB": "1.14",
  "currentBatch": 1,
  "totalBatches": 1,
  "CLOUD_RESOURCE_ID": null
}
```


Sample JSON output response - Get Posture Info (single policy ID)

Get posture Info With lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=0&lastEvaluationDate=2021-12-23"-H "accept: */*"-H
"Authorization: Bearer Token"-H "Content-Type: application/json"-d
"[{\"policyId\":\"POLICY ID\",\"subscriptionId\":\"SUBSCRIPTION
ID\",\"hostIds\":[\"HOST ID1\",\"HOST ID2\"]}]"
```

JSON Output


```
[
{
"id": xxx,
"instance": "os",
"policyId": "<POLICY ID>",
"controlId": "<CONTROL ID>",
"controlStatement": "Status of the 'banner motd' configuration command on
the device",
```

```
"rationale": "The 'Message of the Day (banner motd)' command is used to
provide a warning banner displayed when a
connection to the device is made BEFORE a user successfully authenticates
to the device. The Message of the Day banner can be used to provide an
acceptable use policy or warning prior to login notifying that all user
activity may be monitored and potential legal consequences may result from
unauthorized use. Run this check periodically to ensure content of the
banner displayed is in compliance with the requirements and expectations
driven by internal standards and/or policies.",
"remediation": "Execute following commands to set desired
banner message:\n1. configure terminal\n2. banner motd
'delimiting-character' 'message' 'delimiting-character'\n3.
exit\n\nc",
"controlReference": null,
"technologyId": xxx,
"status": "Error",
"previousStatus": "Error",
"firstFailDate": "",
"lastFailDate": "",
"firstPassDate": "2021-12-21T11:28:21Z",
"lastPassDate": "2021-12-21T11:29:22Z",
"postureModifiedDate": "2021-12-22T12:56:41Z",
"lastEvaluatedDate": "2021-12-23T05:32:40Z",
"created": "2022-02-21T13:10:13Z",
"hostId": "<HOST ID>",
"ip": "xx.xx.xx.xxx",
"trackingMethod": "IP",
"os": null,
"osCpe": "cpe:/o:cisco::7.0%283%29i2%282%29:::",
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2021-12-22T12:49:59Z",
"customerUuid": "<CUSTOMER UUID>",
"customerId": "<CUSTOMER ID>",
"assetId": "<ASSET ID>",
"technology": {
"id": xxx,
"name": "Cisco NX-OS"
},
"criticality": {
"label": "CRITICAL",
"value": 4
},
"evidence": null,
"causeOfFailure": null,
"currentBatch": 1,
"totalBatches": 1
}
```


GET Get Posture Info Without lastEvaluationDate, Without Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=0 and compressionRequired=0

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Response:


```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL ID>,
        "technologyId": xx,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:54:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":  "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "xxx",
        "customerId": "xxx",
        "assetId": "xxx",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": null,
        "causeOfFailure": {
```

```
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xxx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-25T07:21:13Z",
        "lastPassDate": "2021-10-29T07:52:41Z",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:54:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:57:58Z",
        "customerUuid": "xxxx",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "URGENT",
            "value": 5
        },
```

```
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```

Get Posture Info Without lastEvaluationDate, Without Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=0 & compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
]"
```

JSON Output (Compressed)

```
‹        íÝ]sÚHÅñ¯ââ:Îê!ÁÝ¬íŒUœIì8©š©©)
²CÐ2S©|÷•p2Ž_ÖôÁý€ÿ»dŽ~é´8:ýÛçÆ ßè„í(ÈÒfð¬1OËî¸—
7:ÐÚxÖ¸,†ƒÞß‡Õ6Í(ŠÓ${Öè-ãrR
ëÇÂ0Kž5Ê¼÷~\
‹‹ùviõHµ‚6-öñª;æýz?"üã MOî<s>LËÿtÃýnY¿lõÐ°{û'ùFõ‚}(
¢p7
v£äM‚¢° Æ¿~ýÁû¶j×[%Q§Þ:ÿ‚ål'-ýÁù
ïÿß]†ßvyð±;œU[ÝÙôæ~{"¼Þèî--N Ô?¼¯^¸>DY«?ÚÍêh_V?‡Áó0|ž-Ï›QµM9éö>
ÆGyù¾¨÷uøªz´ú,:ãÙpXÿiï²~½Ë¼ó¯¢3ô&Å´8/;Ÿ-ã~ñiúÇ4Ÿ|Ì'?DAu&Q§óW«Ù©öÐ×G½WŒúùÇ
éŸÃêéVõèŸÿ-ÞS}
\í}œ—
ŸŠÉ‡úM6,Æ???ÙÕ¯ùó°8ëwöóóîlXî¼¼z²þÍ‹ÑåpPŸ7/ªÃuÒëŽo©ìMØêÄíN'ÌÔlZ£|r:?Ì_©?g
iž-»ÙYÔÚM³óóÝ,l&»AžeaëÌ¼?¦çßýÔüÝEIPí»z´>Ê«‡Â´Ðiý¾¯OÉFçê ¯OËñÕ¯ñîêHíœÌÔN}¤
vŽ£Æ—ú ?”ƒ^w8(ç?7ìžåÃêöŽß?îýô¢Úq}&TûhV?W't?ŸS¹:v½îlšÿr^Ÿ¸ÕÙuõè—g7€…*°(lE
ÀÜ€Eò´C€ìvrp|øËéÉµ¯x9_±î+Å¾~t_Gû‡§G×¼¢åx5—àõðÿëW»Ÿ×?ÏÜæõ€œû¶°y†ßfx—
?¼àµ'áësc4Ñ«Or¾§âbÐû¶å×ÐÖ¨ßþOe9œÍÊ|g\";çÅl\£8wÏ†ùNYìLòêùüc¾sYý¢Õáîï\'lü^½
‡Ù8ÿë2ïÍO°Ï×û
ª'¿Ü²?ñ_Sæ~ØþÑmŸÿ|ðòÍ5íd¹¡³uƒ×ÑÉÉëõ‹ ·:Õ¹ÖŒãÎü'êß'·ÇW{ûoû»çâf5Þ €Oàü¼ü*ð
èÛAÛ©
\;l-âLêÐ}—@aC>À0óÏ°•Á †0T¶-Æ0„!
Ý&ÃvðOC.¼Âp›.¾úª]?MBÄw¾›d,1^K#†Ì,aC…aìŸa0Â †
Ã¦Ã&
aCÐbÁpÁ—ÿ\àÐ63tˆ×Õo÷mý—éwÙ°.û„÷\öñŸë©h·a¡
ma„5Èõ¤-æ›0„¡ÂÐ ×"'ëÐv0ôtdb ëI‰õ …,Â-Aª'‹PˆB
```

Get Posture Info Without lastEvaluationDate, With Evidence, With Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=1

API Request

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/4.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
1" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"subscriptionId\":\"xxx\",\"hostIds\":[\"xxx\"]}
```

```
]"
```

JSON Output (Compressed)

```
‹        í?sÛFš@ÿ
JµöÎ^ ¼€|"%yâÄr  SvR"ÌNQ$LaC4 ÚÖÌä¿o7HJ¼
ša‹"qR•*YÂµÑ}ú,ßùõß'^ÿ¤mµª¦Ó¬™?=ñü(îú=÷¤}D'?=C¯wÿFlS«VífÝùëI/ðã0ÊßY-
SÿëIìöîü`
'íšâ7âñ$Ç¸îF'Û—ÇÝ/^0%:k?ùä…Qü°ë
/°±<-øÕ°»ú›d#¹ËìWU³j2æiµ~c6ÛU«mÙ?Ÿí¶UKnU¯¶kÖß"{ŠâIè^}ï"çö3iÍyù¥;œ^-Ö6]>n/
tåFë?ÔÚõ†ÜàNœX'ÓhÕ?-š(í±ØØ2+-Uiš•ZUl ‡ÝÞïž?¸rã»@ëÍµø-xm?2?ÊŸÎÇòzc·ý?A{äõÂ
>Åí¯žß¾FÿŒÜð‹?þ³jZÕvXm·¿5jmq„¾/K½Œúî—
èóPü¹!~ûyð?&Y¦G÷Ýøk þ./òÄ<yø÷»îHžóoÃà¶;4.ÜOÝÉ06ÞMÿ(ï<?ž¬7oEquz]?µ¤œ?«Ñ®
‹²p''šDq0rÃ /9S×všnÓ<un«Ó¦óéÓ©cÕê§¦Õ¼u¬Æ§®Õü´°WruÕ°)Ž-
~+ëQ<ý•ÕlÕ?¼îÇ*yÒžVqY-ýémü<-)£"””!KÊx_=ùC>A/özÝ¡'û
»·îPìpÞþÍÍ›ó³·âÀ²&^cÔÄÆ¢B÷Ý¤©üûÄý6v{âÙ?”?-
ý›?áEÝÛ¡Û7^7?óOþ3~|o,þû7ÿÒŸmjånúÞt&·?¸÷†ÄÆ§`â÷óvYÚ8)Ç0týx~-¿ž,^êÉ?D'öâIw8
ÿû´fô½PÜa Þ¿öFú½é¯e'u''ûã'Ù\E›šÿz+-*VªV£
VÀ
```

Get Posture Info Without lastEvaluationDate, With Evidence, Without Compression, Without lastScanDate

User input: evidenceRequired=1, compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xxx\",\"xxx\":\"xxx\",\"hostIds\":[\"xxx\"]}]"
```

JSON Output:

```
[
    {
        "id": xxx,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2021-10-25T07:21:13Z",
        "lastFailDate": "2021-10-29T07:52:41Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2021-10-25T07:21:11Z",
        "lastEvaluatedDate": "2021-10-29T07:52:41Z",
        "created": "2021-10-29T07:55:26Z",
        "hostId": <HOST ID>,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
```

```
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "comdevsql2016",
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-28T16:39:55Z",
        "customerUuid": "0a387e70-8b26-78ff-8145-017b816fa17f",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Windows Server 2012 R2"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\nUnable to retrieve password policy\n------------ OR ----------
--\nequal to\n1",
            "currentValues": [
                "0"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": [
                    "1",
                    "Attribute not found",
                    "Unable to retrieve password policy"
                ]
            },
            "unexpected": {
                "value": [
                    "0"
                ]
            }
        }
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:PCDEV",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
```

```
            "technologyId": "<TECHNOLOGY ID>",
            "status": "Passed",
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-25T07:21:13Z",
            "lastPassDate": "2021-10-29T07:52:41Z",
            "postureModifiedDate": "2021-10-25T07:21:11Z",
            "lastEvaluatedDate": "2021-10-29T07:52:41Z",
            "created": "2021-10-29T07:55:27Z",
            "hostId": <HOST ID>,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:39:55Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "SERIOUS",
                "value": 3
            },
            "evidence": {
                "expectedValues": "\nGrantees not found\n------------ OR ----
--------\nmatches regular expression list\n.*",
                "currentValues": [
                    "Grantees not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            },
            "causeOfFailure": null
        }
    ]
```


Sample JSON output response - Get Posture Info (multiple policy IDs)

Get Posture Info with lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

API Request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0&lastEvaluationDate=2021-12-27T15:35:22Z" -H "accept: /" -H
"Authorization: Bearer Token" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<Policy_ID>\",\"subscriptionId\":\"<Subscription_ID>\",
\"hostIds\":[\"<Host_ID1>\"]},{\"policyId\":\"policyId1\",\"subscriptionI
d\":\"<Subscription_ID\",\"hostIds\":[\"<HOST_ID1>\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL_ID,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": xx,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-12T13:12:26Z",
        "lastPassDate": "2021-12-27T15:35:22Z",
        "postureModifiedDate": "2021-10-12T13:12:26Z",
        "lastEvaluatedDate": "2021-12-27T15:35:22Z",
        "created": "2022-02-24T14:21:06Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "DNS Hostname",
        "os": xx,
        "osCpe": "cpe:/o:microsoft:windows_2003_server::sp2::",
        "domainName": "<DOMAIN NAME>",
        "dns": "client5-25-244.root.vuln.qa.qualys.com",
```

```
        "qgHostid": xx,
        "networkId": xx,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-27T15:31:18Z",
        "customerUuid": "xx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": xx,
            "name": "Windows 2003 Server"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": xx
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n0",
            "currentValues": [
                "1"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "currentBatch": xx,
        "totalBatches": xx
    },
    {
        "id": xx,
        "instance": "os",
        "policyId": <POLICY_ID>,
        "policyTitle": <POLICY TITLE>,
        "netBios": <NETBIOS>,
        "controlId": <CONTROL_ID>,
        "controlStatement": "Status of the
'net.ipv4.conf.all.send_redirects' setting within the '/etc/sysctl.conf'
file",
        "rationale": "The 'net.ipv4.conf.all.send_redirects' network
parameter (/etc/sysctl.conf) allows ICMP routing redirection.  If the
system is not going to be used as a firewall or gateway to pass network
traffic, and this parameter is not disabled, malicious users may attempt
to spoof source addresses or redirect traffic to a host with a network
sniffer, so this value should be set according to the needs of the
business.",
        "remediation": "Set the following parameters in the
/etc/sysctl.conf file:\n\n# net.ipv4.conf.all.send_redirects = 0\n\nOR
\nRun the following commands to set the active kernel parameters:\n#
sysctl -w net.ipv4.conf.all.send_redirects=0\n# sysctl -w
net.ipv4.route.flush=1",
        "controlReference": null,
        "technologyId": 80,
        "status": "Passed",
```

```
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2022-02-11T12:54:23Z",
            "lastPassDate": "2022-02-11T12:54:23Z",
            "postureModifiedDate": "2022-02-11T12:54:23Z",
            "lastEvaluatedDate": "2022-02-11T12:54:23Z",
            "created": "2022-02-24T14:21:06Z",
            "hostId": xx,
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
            "domainName": "<DOMAIN NAME>",
            "dns": null,
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2022-02-11T12:47:29Z",
            "customerUuid": "xx",
            "customerId": "xx",
            "assetId": xx,
            "technology": {
                "id": xx,
                "name": "CentOS 7.x"
            },
            "criticality": {
                "label": "CRITICAL",
                "value": 4
            },
            "evidence": {
                "expectedValues": "\nSetting not found\n------------ OR -----
        -------\nFile not found\n------------ OR ------------\nmatches regular
        expression list\n.*",
                "currentValues": [
                    "Setting not found"
                ],
                "actualValues": null,
                "directoryFimUdc": null
        "description": "The following Integer value X indicates the current value
        of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            },
            "causeOfFailure": null,
            "currentBatch": 1,
            "totalBatches": 1
        }
    ]
```


Get Posture Info without lastEvaluationDate, without evidence, without compression, without lastScanDate

User Input: evidenceRequired=0 & compressionRequired=0

Request:

```
curl -X POST "https://gateway.<assigned
```

```
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:38:14Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": null,
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "os",
```

```
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-25T07:21:13Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-25T07:21:11Z",
    "lastEvaluatedDate": "2021-10-29T08:38:10Z",
    "created": "2021-10-29T08:38:14Z",
    "hostId": "<HOST ID>",
    "ip": "xx.xx.xx.xx",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
    "domainName": "<DOMAIN NAME>",
    "dns": "comdevsql2016",
    "qgHostid": null,
    "networkId": "0",
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2021-10-28T16:53:14Z",
    "customerUuid": "xx-xx-xx-xx-xx",
    "customerId": "<CUSTOMER ID>",
    "assetId": "<ASSET ID>",
    "technology": {
        "id": xx,
        "name": "Windows Server 2012 R2"
    },
    "criticality": {
        "label": "CRITICAL",
        "value": 4
    },
    "evidence": null,
    "causeOfFailure": null
},
{
    "id": 19235413,
    "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
    "policyId": "<POLICY ID>",
    "policyTitle": "<POLICY TITLE>",
    "netBios": "<NETBIOS>",
    "controlId": "<CONTROL ID>",
    "technologyId": "<TECHNOLOGY ID>",
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2021-10-28T16:53:06Z",
    "lastPassDate": "2021-10-29T08:38:10Z",
    "postureModifiedDate": "2021-10-28T16:53:06Z",
```

```
            "lastEvaluatedDate": "2021-10-29T08:38:10Z",
            "created": "2021-10-29T08:38:15Z",
            "hostId": "<HOST ID>",
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:53:14Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": null,
            "causeOfFailure": null
        }
    ]
```


Get Posture Info without lastEvaluationDate, with evidence, without compression, without lastScanDate

User input**:** evidenceRequired=1 & compressionRequired=0

Request**:**

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compressionRequired=
0" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"xx\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]},{\
"policyId\":\"policyId1\",\"subscriptionId\":\"xx\",\"hostIds\":[\"xx\"]}
]"
```

JSON Output:


```
[
    {
        "id": xx,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": "<TECHNOLOGY ID>",
```

```
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-10-14T11:19:31Z",
        "lastPassDate": "2021-10-18T06:17:29Z",
        "postureModifiedDate": "2021-10-14T11:19:30Z",
        "lastEvaluatedDate": "2021-10-18T06:17:29Z",
        "created": "2021-10-29T08:40:38Z",
        "hostId": "<HOST ID>",
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:cisco:asa:9.2%284%29:::",
        "domainName": "<DOMAIN NAME>",
        "dns": null,
        "qgHostid": null,
        "networkId": "0",
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-10-14T09:37:38Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": xx,
            "name": "Cisco ASA 9.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nFilter 2 not found: ^[\\*\\.\\d]\n------
------ OR ------------\nFilter 1 not found: show clock detail\n----------
-- OR ------------\nmatches regular expression list\n.*",
            "currentValues": [
                "show clock detail:08:26:29.074 pdt Thu Oct 14 2021"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null
    },
    {
        "id": xx,
        "instance": "MSSQL 2016:1:1433:MSSQLSERVER:DB",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": "<CONTROL ID>",
        "technologyId": xx,
        "status": "Passed",
```

```
            "previousStatus": "Passed",
            "firstFailDate": "",
            "lastFailDate": "",
            "firstPassDate": "2021-10-28T16:53:06Z",
            "lastPassDate": "2021-10-29T08:39:07Z",
            "postureModifiedDate": "2021-10-28T16:53:06Z",
            "lastEvaluatedDate": "2021-10-29T08:39:07Z",
            "created": "2021-10-29T08:40:46Z",
            "hostId": "<HOST ID>",
            "ip": "xx.xx.xx.xx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_server_2012:r2::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "comdevsql2016",
            "qgHostid": null,
            "networkId": "0",
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-10-28T16:57:58Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": "<ASSET ID>",
            "technology": {
                "id": xx,
                "name": "Microsoft SQL Server 2016"
            },
            "criticality": {
                "label": "MEDIUM",
                "value": 2
            },
            "evidence": {
                "expectedValues": "\nSet status to PASS if no data found\n---
    --------- OR ------------\nmatches regular expression list\n.*",
                "currentValues": [
                    "Error Code 35:Failed to execute database query"
                ],
                "actualValues": null,
                "directoryFimUdc": null
    "description": "The following Integer value X indicates the current value
    of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            },
            "causeOfFailure": null
        }
    ]
```


Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

User input**:** evidenceRequired=0 & compressionRequired=1 & lastScanDate=yyyy-mm-dd:Thh:mm:ssZ

Request**:**

```
Curl-X POST
"<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compre
```

```
ssionRequired=1&lastEvaluationDate=2021-12-
17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z" -H
"accept: */*" -H
"Content-Type: application/json" -d "
[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

JSON output:


```
[
    {
        "id": <HOST INSTANCE ID>,
        "instance": "os",
        "policyId": "<POLICY ID>",
        "policyTitle": "<POLICY TITLE>",
        "netBios": "<NETBIOS>",
        "controlId": <CONTROL ID>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": <TECHNOLOGY ID>,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
```

```
            "osCpe": null,
           "domainName": "<DOMAIN NAME>",
            "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
            "qgHostid": null,
            "networkId": 0,
            "networkName": "Global Default Network",
            "complianceLastScanDate": "2021-12-23T12:59:04Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": <ASSET ID>,
            "technology": {
                "id": 217,
                "name": "Red Hat Enterprise Linux 8.x"
            },
            "criticality": {
                "label": "CRITICAL",
                "value": 4
            },
            "evidence": null,
            "causeOfFailure": null,
            "currentBatch": 8,
            "totalBatches": 12
        },
    ]
```


Get Posture Info without evidence, without compression, with statusChangedSince

Request:

```
curl -X POST
"https://gateway.<assigned
URL>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=
0&statusChangedSince=2021-12-23" -H "accept: */*" -H "Authorization:
Bearer Token" -H "Content-Type: application/json" -d
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONID>\",\"
hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

JSON output:


```
[
    {
        "id": 24705485,
        "instance": "os",
        "policyId": <POLICY ID>,
        "policyTitle": "pcas_win16_redhat7 tech",
        "netBios": "<NETBIOS>",
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
```

```
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
       "remediation": "To establish the recommended configuration via GP,
set the following UI path to 14 or more character(s):\n\n\tComputer
Configuration\\Policies\\Windows Settings\\Security Settings\\Account
Policies\\Password Policy\\Minimum password length",
        "controlReference": null,
        "technologyId": 106,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2022-11-09T12:50:12Z",
        "lastPassDate": "2022-12-06T06:42:21Z",
        "postureModifiedDate": "2022-11-09T12:50:12Z",
        "lastEvaluatedDate": "2022-12-06T06:42:21Z",
        "created": "2022-12-07T07:35:56Z",
        "hostId": <HOST ID>,
        "CLOUD_RESOURCE_ID": null,
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": "cpe:/o:microsoft:windows_server_2016:1607::x64:",
        "domainName": "<DOMAIN NAME>",
        "dns": "<DNS>",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2022-08-23T04:57:05Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": <ASSET ID>,
        "technology": {
            "id": 106,
            "name": "Windows 2016 Server"
        },
        "criticality": {
            "label": "high updated",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nAttribute not found\n------------ OR ---
---------\ngreater than or equal to\n0",
            "currentValues": [
                "6"
            ],
            "actualValues": null,
            "directoryFimUdc": null
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
```

```
        },
        "causeOfFailure": null,
        "currentDataSizeKB": "2.41",
        "totalDataSizeKB": "2.41",
        "currentBatch": 1,
        "totalBatches": 1
    },
]
```

Sample - Retrieve Cloud Metadata

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=0&cloudMetaDataRequired=1" -H "accept: */*" -H
"Authorization: Bearer Token" -H "Content-Type:application/json" -d
"[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST
ID1>\",\"<HOST ID2>\"]}]"
```

JSON Output

```
[    {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xx-xx",
        "controlId": xx,
       "controlStatement": "Status of the 'Trivial File Transfer Protocol
(TFTP)' service",
      "rationale": "The 'TFTP' service is both a command and TCP protocol
that is normally used only for booting diskless workstations, getting or
saving network component configuration files, or as a 'kickstart' type
host configuration from a network-based template.  The connection
initiation and data transfer is all done in clear text without requiring
credentials of any kind.  As a malicious user with a 'sniffer' running on
the network, could easily capture the data and/or reproduce the same
operation, simply by knowing the name of the file(s) and the source
address(es), this process should be disabled/restricted according to the
needs of the business.",
       "remediation": "Review \"/etc/inetd.conf\" file to check whether
tftp service's configuration in line with business needs and
organization's security policies.\n\nExample: To disable the tftp
service,\n\nRemove or comment out any tftp lines in /etc/inetd.conf: \n#
tftp stream tcp nowait root internal",
        "category": "Services",
        "subCategory": "Guidelines/Procedures (Services)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
```

```
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:20:49Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xx-xx-xx-xx-xxx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.98",
        "totalDataSizeKB": "27.09",
        "currentBatch": 1,
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "xx",
            "cloudResourceType": "Instance",
            "cloudAccountId": "xx",
            "cloudImageId": null,
            "cloudResourceMetadata": "{'Public IP
```

```
Address':'xx.xxx.xx.xxx', 'Private IP Address':'xx.xxx.x.xx', 'Machine
Type':'e2-medium', 'Zone':'null', 'ProjectId':'qlys-devqa-qweb',
'State':'RUNNING', 'Network':'N/A', 'MAC Address':'null'}"
        },
        "CLOUD_RESOURCE_ID": "xxx"
    }
]
```


Sample - Retrieve Posture Information Based on Current Posture Status - passed

API Request

curl -X POST "<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&status=Passed" -H "accept: */*" -H "Authorization: `Bearer Token`" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[        {
        "id": xx,
        "instance": "os",
        "policyId": 1438626,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xxxxxx-xxxxx",
        "controlId": xx,
       "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
protocol, most commonly used for accessing remote computers via a command
line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
clear text including any uid/password input, so if a telnet session is
used for privileged communication(s)/host configuration purposes, the
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
      "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xxx,
```

```
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xxxxx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxx",
        "customerId": "xx",
        "assetId": xxx,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"

        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxx"
    }
]
```


Sample - Retrieve Posture Information Based on Previous status-passed

API Request

curl -X POST "<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0&previousStatus=Passed" -H "accept: */*" -H "Authorization: `Bearer Token`" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY

ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "CPS -Test",
        "netBios": "INSTANCE-xx-xx",
        "controlId": xx,
       "controlStatement": "Status of the 'telnet' service (Unix/Linux)",
        "rationale": "'Telnet' is both a user command and a TCP/IP
protocol, most commonly used for accessing remote computers via a command
line interface (CLI) on tcp port 23.  Telnet streams are transmitted in
clear text including any uid/password input, so if a telnet session is
used for privileged communication(s)/host configuration purposes, the
entire session is susceptible to interception by eavesdroppers on the
network.  As this can lead to the session being hijacked or replayed by
malicious users, this process should be disabled/restricted according to
the needs of the business.",
       "remediation": "Edit the file '/etc/inetd.conf' and add or comment
the 'telnet' entry according to the business needs or organization's
security policies.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-10-04T09:47:33Z",
        "lastPassDate": "2024-10-04T09:47:33Z",
        "postureModifiedDate": "2024-10-04T09:47:33Z",
        "lastEvaluatedDate": "2024-10-04T09:47:33Z",
        "created": "2024-11-12T06:32:08Z",
        "hostId": xx,
        "ip": "xx.xxx.xxx.xx",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "dns": "xxx.xx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "xx-xx-xx-xx-xx",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxxxxx",
        "customerId": "xxxx",
        "assetId": 42078290,
        "technology": {
            "id": 346,
```

```
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-10-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.35",
        "totalDataSizeKB": "20.78",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": "xxxxx"
    }
]
```


Sample - Retrieve Posture Information Based on Criticality Value: 2

API Request

```
curl -X POST
"<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequir
ed=0& criticalityValues=2" -H "accept: */*" -H "Authorization: Bearer Token" -H "Content-
Type:application/json" -d "[{\"policyId\":\"<POLICY
ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST
ID2>\"]}]"
```

JSON Output


```
[
        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
based facsimile service that can take system documents and send these out
to a fax-recipient via a hardware modem and analog phone line.  (One
```

```
reported public exploit uses the Windows Picture and Fax Viewer
(SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
can potentially compromise sensitive system documents, by transmitting
information to unauthorized recipients and can be activated remotely, this
capability should be restricted/set according to the needs of the
business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xxx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
"cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T09:12:22Z",
        "customerUuid": "xx-xx-xx-xx-xxxx",
        "customerId": "xx",
        "assetId": xx,
        "technology": {
            "id": 21,
            "name": "Windows 2008 Server"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nAutomatic (2)\n------------ OR ---------
---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
(3)\n------------ OR ------------\nKey not found\n------------ OR -------
-----\nDisabled (4)",
            "currentValues": [
                "Key not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
```

```
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-11-06T09:12:22Z",
            "extendedEvidence": "Row 1:Service Name,Registry Key,Start
Value,Delayed Start\nRow
2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.34",
        "totalDataSizeKB": "7.61",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
]
```


Sample - Retrieve Posture Information Based on Criticality Label: Medium

API Request

curl -X POST "<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=0&compressionRequired=0& criticalityLabels= MEDIUM" -H "accept: */*" -H "Authorization: `Bearer Token`" -H "Content-Type:application/json" -d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBSCRIPTION_ID>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"

JSON Output


```
[
        {
        "id": xx,
        "instance": "os",
        "policyId": xx,
        "policyTitle": "WINDOWS_IP_TRACKED_IPV4_POLICY_AG",
        "netBios": "SYS_xx_xx_xx_xx",
        "controlId": xx,
        "controlStatement": "Status of the 'Fax' service",
        "rationale": "The Microsoft 'Fax' service provides a software-
based facsimile service that can take system documents and send these out
to a fax-recipient via a hardware modem and analog phone line.  (One
reported public exploit uses the Windows Picture and Fax Viewer
(SHIMGVW.DLL) to execute code arbitrarily.)  As this transfer capability
can potentially compromise sensitive system documents, by transmitting
information to unauthorized recipients and can be activated remotely, this
capability should be restricted/set according to the needs of the
business.",
        "remediation": "Remove or disable the Fax (fax) service.",
        "category": "OS Security Settings",
        "subCategory": "Performance Monitoring  (All OSI Layers)",
        "controlReference": null,
        "technologyId": 21,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
```

```
        "firstPassDate": "2024-11-06T09:17:38Z",
        "lastPassDate": "2024-11-06T09:20:57Z",
        "postureModifiedDate": "2024-11-06T09:17:38Z",
        "lastEvaluatedDate": "2024-11-06T09:20:57Z",
        "created": "2024-11-12T07:38:05Z",
        "hostId": xx,
        "ip": "xx.xx.xx.xx",
        "trackingMethod": "IP",
        "os": null,
        "osCpe":
"cpe:/o:microsoft:windows_server_2008:r2::enterprise_x64:",
        "domainName": "xx-xx-xx-xx.bogus.tld",
        "dns": "xx-xx-xx-xx.bogus.tld",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-11-06T09:12:22Z",
        "customerUuid": "xxxxx-xx-xx-xx-xxxxx",
        "customerId": "xxx",
        "assetId": xxx,
        "technology": {
            "id": 21,
            "name": "Windows 2008 Server"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 2
        },
        "evidence": {
            "expectedValues": "\nAutomatic (2)\n------------ OR ---------
---\nAutomatic (Delayed Start) (21)\n------------ OR ------------\nManual
(3)\n------------ OR ------------\nKey not found\n------------ OR -------
-----\nDisabled (4)",
            "currentValues": [
                "Key not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
"description": "The following Integer value X indicates the current value
of the PASS_MIN_LEN setting as defined within the /etc/login.defs file."
            "lastUpdated": "2024-11-06T09:12:22Z",
            "extendedEvidence": "Row 1:Service Name,Registry Key,Start
Value,Delayed Start\nRow
2:Fax,HKLM\\SYSTEM\\CurrentControlSet\\Services\\Fax,,\n"
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.34",
        "totalDataSizeKB": "7.61",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
]
```

Sample - Retrieve compliance posture information

API Request

```
curl --location
'<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compressionRequir
ed=0&clou
 dMetaDataRequired=1' \
--header 'accept: */*' \
--header 'Authorization: Bearer <JWT TOKEN>' \
--header 'Content-Type: application/json' \ --data '[
  {
    "policyId": "1438442",
    "subscriptionId": "822838",
    "hostIds": [
      "4783735",
      "4980343"
    ]
  }
]'
```

JSON Output


```
[
    {
        "id": <id>,
        "instance": "os",
        "policyId": <policy_id>,
        "policyTitle": "GCP policy-Neha",
        "netBios": "NEW-SPIN123",
        "controlId": <control_id>,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file
\"/etc/login.defs\" and add or correct the following lines:
\n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program
consults \"/etc/login.defs\" and also another PAM module (such as
\"pam_cracklib\") during a
password change operation, then the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
```

```
        "controlReference": null,
        "technologyId": 81,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-03-23T07:10:02Z",
        "lastPassDate": "2025-03-23T07:10:02Z",
        "postureModifiedDate": "2025-03-23T07:10:02Z",
        "lastEvaluatedDate": "2025-03-23T07:10:02Z",
        "created": "2025-04-16T12:24:23Z",
        "hostId": 4783735,
        "ip": "10.xxx.x.19",
        "trackingMethod": "AGENT",
        "os": null,
        "osCpe": null,
        "domainName": "121.xxx.xxx.34.bc.googleusercontent.com",
        "dns": "121.xxx.xxx.xx.bc.googleusercontent.com",
        "qgHostid": "c4b0cde6-9017-4340-933e-afbbc71556b4",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-10-04T09:39:21Z",
        "customerUuid": "93f7ad53-1590-e3ac-83cd-322b91180e13",
        "customerId": "1337821",
        "assetId": 41157957,
        "technology": {
            "id": 81,
            "name": "Red Hat Enterprise Linux 7.x"
        },
        "criticality": {
            "label": "URGENT",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nSetting not found\n------------ OR -----
-------\nFile not found\n------------
OR ------------\ngreater than or equal to\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2025-04-20T08:52:58Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN
setting as defined within the /etc/login.defs file."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "3.39",
        "totalDataSizeKB": "3.39",
        "currentBatch": 1,
```

```
        "totalBatches": 1,
        "cloudMetaData": {
            "cloudProvider": "GCP",
            "cloudService": "Compute Engine",
            "cloudResourceId": "3654664005469669138",
            "cloudResourceType": "Instance",
            "cloudAccountId": "175127636344",
            "cloudImageId": null,
            "cloudResourceMetadata": {
                "publicIpAddress": "34.136.202.121",
                "privateIpAddress": "10.128.0.19",
                "machineType": "custom-1-1024",
                "zone": null,
                "projectId": "qlys-devqa-qweb",
                "state": "STOPPED",
                "network": "N/A",
                "macAddress": null
            }
        },
        "CLOUD_RESOURCE_ID": "3654664005469669138"
    },
    .......
    {
        "id": 19029079,
        "instance": "os",
        "policyId": 1438442,
        "policyTitle": "GCP policy-Neha",
        "netBios": "INSTANCE-20250423-173020",
        "controlId": 1131,
       "controlStatement": "Status of the 'Trivial File Transfer Protocol
(TFTP)' service",
      "rationale": "The 'TFTP' service is both a command and TCP protocol
that is normally used only
for booting diskless workstations, getting or saving network component
configuration files, or as a
'kickstart' type host configuration from a network-based template.  The
connection initiation and
data transfer is all done in clear text without requiring credentials of
any kind.  As a malicious user
with a 'sniffer' running on the network, could easily capture the data
and/or reproduce the same
operation, simply by knowing the name of the file(s) and the source
address(es), this process should
be disabled/restricted according to the needs of the business.",
        "remediation": "Review \"/etc/inetd.conf\" file to check whether
tftp service's configuration in line
with business needs and organization's security policies.\n\nExample: To
disable the tftp
service,\n\nRemove or comment out any tftp lines in /etc/inetd.conf: \n#
tftp stream tcp nowait root
internal",
        "category": "Services",
        "subCategory": "Guidelines/Procedures (Services)",
        "controlReference": null,
```

```
        "technologyId": 346,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-04-06T09:48:19Z",
        "lastPassDate": "2025-04-06T09:48:19Z",
        "postureModifiedDate": "2025-04-06T09:48:19Z",
        "lastEvaluatedDate": "2025-04-06T09:48:19Z",
        "created": "2025-04-16T12:24:26Z",
        "hostId": 4980343,
        "ip": "34.xxx.xxx.84",
        "trackingMethod": "AGENT",
        "os": "Debian Linux 11.1",
        "osCpe": null,
        "domainName": "179.xx.xxx.35.bc.googleusercontent.com",
        "dns": "179.xx.xxx.35.bc.googleusercontent.com",
        "qgHostid": "4bd9e81e-12f8-4d8f-a51d-c475131a55b8",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2025-04-06T09:39:21Z",
        "customerUuid": "93f7ad53-1590-e3ac-83cd-322b91180e13",
        "customerId": "1337821",
        "assetId": 42078290,
        "technology": {
            "id": 346,
            "name": "Debian GNU/Linux 11.x"
        },
        "criticality": {
            "label": "SERIOUS",
            "value": 3
        },
        "evidence": {
            "expectedValues": "\nDisabled (0)\n------------ OR ----------
--\nEnabled (1)\n------------ OR ------------\nSetting not found\n-------
----- OR ------------\nFile not found",
            "currentValues": [
                "File not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2025-04-04T09:39:21Z",
            "extendedEvidence": "Row 1:\n",
           "description": "The following List String value of X indicates
the status of the tftp service
configured within the /etc/xinetd.conf, /etc/xinetd.d/*, /etc/inetd.conf
and /etc/inetd.d/* files on the
host. A value of 0 indicates the service is disabled; and a value of 1
indicates the service is enabled on
the host."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "3.27",
```

```
            "totalDataSizeKB": "97.52",
            "currentBatch": 1,
            "totalBatches": 1,
            "cloudMetaData": {
                "cloudProvider": "GCP",
                "cloudService": "Compute Engine",
                "cloudResourceId": "2182777093928348127",
                "cloudResourceType": "Instance",
                "cloudAccountId": "175127636344",
                "cloudImageId": null,
                "cloudResourceMetadata": {
                    "publicIpAddress": "35.xxx.xx.179",
                    "privateIpAddress": "10.xxx.x.27",
                    "machineType": "e2-medium",
                    "zone": null,
                    "projectId": "qlys-devqa-qweb",
                    "state": "RUNNING",
                    "network": "N/A",
                    "macAddress": null
                }
            },
            "CLOUD_RESOURCE_ID": "2182777093928348127"
        }
]
```

Sample - extendedEvidenceRequired field is set to 0

API Request

```
curl location
'<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compre
ssionRequired=0&extendedEvidenceRequired=0%27 \
 header 'Content-Type: application/json' \
 header 'Authorization: Bearer <JWT TOKEN>' \
data '[
    {
        "policyId": "1627436",
        "subscriptionId": "583816",
        "hostIds": [
            "5400713"
        ]
    }
]'
--header 'accept: */*' \
--header 'Authorization: Bearer <JWT TOKEN>' \
--header 'Content-Type: application/json' \ --data '[
    {
        "policyId": "1438442",
        "subscriptionId": "822838",
        "hostIds": [
            "4783735",
            "4980343"
        ]
    }
]'
```

JSON Output


```
{
        "id": 25598740,
        "instance": "os",
        "policyId": 1627436,
        "policyTitle": "OCA Policy",
        "netBios": null,
        "controlId": 4358,
        "controlStatement": "Status of the 'aaa authentication login'
configuration command on the device",
        "rationale": "Requiring an AAA Authentication method(s) to be
employed for local user logins provides a source for managing and
monitoring access into the device. Setting the AAA Authentication for
local user logins enforces a username and password combination be used
when logging into the device locally.  If a named AAA Authentication list
is used in place of the default setting, authentication is required to be
configured for each IOS line for each interface.",
       "remediation": "Before you configure default login authentication
methods, configure RADIUS or TACACS+ server groups as needed\nExecute the
following commands to set the default authentication method\n1. configure
terminal\n2. aaa authentication login default { group 'group-list' [ none
]| local | none }\n3. exit",
        "category": "OS Security Settings",
        "subCategory": "Network Settings (OSI Layers 2-5)",
        "controlReference": null,
        "technologyId": 200,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-08-20T06:54:10Z",
        "lastPassDate": "2025-08-20T06:59:21Z",
        "postureModifiedDate": "2025-08-20T06:54:10Z",
        "lastEvaluatedDate": "2025-08-20T06:59:21Z",
        "created": "2025-10-22T08:19:41Z",
        "hostId": 5400713,
        "ip": "123.231.42.198",
        "trackingMethod": "OCA",
        "os": "Arista EOS 4",
        "osCpe": null,
        "domainName": null,
        "dns": null,
        "qgHostid": "003e160a-7b12-442f-a67c-7c7a08badb5d",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-06-07T00:00:00Z",
        "customerUuid": "bb662c39-f363-d58f-825d-abbcf4f035c2",
        "customerId": "1334625",
        "assetId": 44524164,
        "technology": {
            "id": 200,
            "name": "Arista EOS 4.x"
```

```
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 4
        },
        "evidence": {
            "expectedValues": "\nFilter not found\n OR \nCommand not
found\n OR \nmatches regular expression list\n.*",
            "currentValues": [
                "Filter not found"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "",
            "extendedEvidence": null
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.47",
        "totalDataSizeKB": "2.47",
        "currentBatch": 2,
        "totalBatches": 16,
        "CLOUD_RESOURCE_ID": null
    }
```


Sample - extendedEvidenceRequired field is set to 1 or is not used

API Request

```
curl location
'<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=1&compre
ssionRequired=0&extendedEvidenceRequired=1%27 \
header 'Content-Type: application/json' \
header 'Authorization: Bearer <JWT TOKEN>' \
data '[
    {
        "policyId": "1627436",
        "subscriptionId": "583816",
        "hostIds": [
            "5400713"
        ]
    }
]'
```

JSON Output


```
{
        "id": 25598740,
        "instance": "os",
        "policyId": 1627436,
        "policyTitle": "OCA Policy",
        "netBios": null,
        "controlId": 4358,
        "controlStatement": "Status of the 'aaa authentication login'
configuration command on the device",
```

```
        "rationale": "Requiring an AAA Authentication method(s) to be
employed for local user logins provides a source for managing and
monitoring access into the device. Setting the AAA Authentication for
local user logins enforces a username and password combination be used
when logging into the device locally.  If a named AAA Authentication list
is used in place of the default setting, authentication is required to be
configured for each IOS line for each interface.",
        "remediation": "Before you configure default login authentication
methods, configure RADIUS or TACACS+ server groups as needed\nExecute the
following commands to set the default authentication method\n1. configure
terminal\n2. aaa authentication login default { group 'group-list' [ none
]| local | none }\n3. exit",
        "category": "OS Security Settings",
        "subCategory": "Network Settings (OSI Layers 2-5)",
        "controlReference": null,
        "technologyId": 200,
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2025-08-20T06:54:10Z",
        "lastPassDate": "2025-08-20T06:59:21Z",
        "postureModifiedDate": "2025-08-20T06:54:10Z",
        "lastEvaluatedDate": "2025-08-20T06:59:21Z",
        "created": "2025-10-22T08:19:41Z",
        "hostId": 5400713,
        "ip": "123.231.42.198",
        "trackingMethod": "OCA",
        "os": "Arista EOS 4",
        "osCpe": null,
        "domainName": null,
        "dns": null,
        "qgHostid": "003e160a-7b12-442f-a67c-7c7a08badb5d",
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2024-06-07T00:00:00Z",
        "customerUuid": "bb662c39-f363-d58f-825d-abbcf4f035c2",
        "customerId": "1334625",
        "assetId": 44524164,
        "technology": {
            "id": 200,
            "name": "Arista EOS 4.x"
        },
        "criticality": {
            "label": "MEDIUM",
            "value": 4
        },
        "evidence": {
            "expectedValues": "\nFilter not found\n OR \nCommand not
found\n OR \nmatches regular expression list\n.*",
            "currentValues": [
                "Filter not found"
            ],
            "actualValues": null,
```

```
            "directoryFimUdc": null,
            "lastUpdated": "",
            "extendedEvidence": "Row 1:Command,Filter 1: ^aaa
authentication login\nRow 2:show running-config all,\n",
          "description": "The following List String value(s) X indicates
the status of the aaa authentication login configuration command on the
host."
        },
        "causeOfFailure": null,
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "2.47",
        "totalDataSizeKB": "2.47",
        "currentBatch": 2,
        "totalBatches": 16,
        "CLOUD_RESOURCE_ID": null
    }
```

Sample - Display QDS in API response

API Request

```
curl -X POST
"https://<qualys_base_url>/pcrs/5.0/posture/postureInfo?evidenceRequired=
1&compressionRequired=0?qdScoreRequired=1"
-H "accept: */*"
-H "Authorization: Bearer Token"
-H "Content-Type: application/json"-d "[{\"policyId\":\"POLICY
ID\",\"subscriptionId\":\"SUBSCRIPTION ID\",\"hostIds\":[\"HOST
ID1\",\"HOST ID2\"]}]"
```

JSON Output

```
{
        "id": 33529705,
        "instance": "os",
        "policyId": 5772988,
        "policyTitle": "Centos policy",
        "netBios": null,
        "controlId": 2641,
        "controlStatement": "Current list of 'inactive user
accounts' and their 'last login Information' value(s)",
        "rationale": "Periodic account reviews showing the
'inactive user accounts and their last login information' can be
performed to support security and compliance policies.  This check
can be run against all accounts or only those you specify to
quickly determine if unused accounts need to be disabled.  This
check can also be used in support of incident response activities
and act as evidence to show timeliness associated with when
specific accounts were last used to support legal investigations.
 As inactive accounts can provide access for unauthorized
activities, this check should be run regularly according to the
security and compliance policies of the business.",
```

```
        "remediation": "Review and Verify Periodically the user
accounts and their last login information to determine if inactive
accounts need to be disabled as per business needs and the
organization's security policy.",
        "category": "Access Control Requirements",
        "subCategory": "Account Creation/User Management",
        "controlReference": null,
        "technologyId": 80,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2025-10-20T19:25:43Z",
        "lastFailDate": "2025-12-08T20:37:38Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2025-10-20T19:25:34Z",
        "lastEvaluatedDate": "2025-12-08T20:37:38Z",
        "created": "2025-12-11T10:48:01Z",
        "hostId": 13440667,
        "ip": "10.11.70.161",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": null,
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2025-09-25T08:44:47Z",
        "customerUuid": "8db3e9cd-8e85-494b-817b-098c0cd67934",
        "customerId": "2591847",
        "assetId": 54537016,
        "technology": {
            "id": 80,
            "name": "CentOS 7.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": {
            "expectedValues": "\nLast login info not found\n------
------ OR ------------\n/var/log/lastlog not found\n------------
OR ------------\nmatch all regular expression match\n.*:([0-
9]$|[0-9][0-9]$|100$)",
            "currentValues": [
                "root:0",
```

```
                    "rdlab:1758",
                    "qtestos:1758"
                ],
                "actualValues": null,
                "directoryFimUdc": null,
                "lastUpdated": "2025-09-25T08:44:47Z",
                "extendedEvidence": null,
               "description": "This List String value of X returns the
information of the Inactive User's last login on the host. NOTE :
It returns list of all active user name and the inactive days."
            },
            "causeOfFailure": {
                "missing": {
                    "logic": null,
                    "value": [
                        "------------ OR ------------",
                        "Last login info not found",
                        "------------ OR ------------",
                        "/var/log/lastlog not found"
                    ]
                },
                "unexpected": {
                    "value": [
                        "rdlab:1758",
                        "qtestos:1758"
                    ]
                }
            },
            "userDefinedAttributesList": null,
            "currentDataSizeKB": "2.79",
            "totalDataSizeKB": "233.56",
            "currentBatch": 1,
            "totalBatches": 1,
            "qds": 56,
            "CLOUD_RESOURCE_ID": null
        }
```


Sample - Single Posture ID

API Request

```
curl -X POST
"<qualys_base_url>/5.0/posture/postureInfo?evidenceRequired=1" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json" \
  -d '[
    {
      "subscriptionId": "583816",
```

```
      "postureId": "256743"
    }
  ]'
```

JSON Output

```
[
  {
    "postureId": 256743,
    "hostId": 56433,
    "policyId": 1614425,
    "controlId": "CID-001",
    "status": "passed",
    "currentBatch": 1,
    "totalBatches": 1,
    "evidence": "...",
    ...
  }
]
```

Sample - Multiple Posture IDs

API Request

```
curl -X POST
"<qualys_base_url>/5.0/posture/postureInfo?evidenceRequired=0" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json" \
  -d '[
    {
      "subscriptionId": "583816",
      "postureId": "25678328,25678329,25678330"
    }
  ]'
```

JSON Output

```
[
   {
        "id": 25678328,
        "instance": "os",
        "policyId": 734560,
        "policyTitle": "AllTech_policy- Exception",
        "netBios": null,
        "controlId": 1091,
       "controlStatement": "Status of the number of days before a [Prompt
user] password expiration warning prompt is displayed at login",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting the
'expiration warning date' requirement.  This establishes the number of
days before the host will begin to display 'password expiration warning'
messages upon login.  Without having a pre-expiration warning message, it
is more likely that users will not prepare for this event, which may
```

contribute to the selection of hard-to-remember or easily broken password sequences, which circumvents the intent of having rules for password complexity enforced. This may cause some users to forget or write down their new password, which can lead either to a system compromise or increased calls to Help Desk resources.",

    },
    {
        "id": 25678329,
        "instance": "os",
        "policyId": 725886,
        "policyTitle": "AllTech_policy",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length' setting",
        "rationale": "Among the several characteristics that make 'user identification' via password a secure and workable solution is setting a 'minimum password length' requirement. Each character that is added to the password length squares the difficulty of breaking the password via 'brute force,' which attempts using every combination possible within the password symbol set-space, in order to discover a user's password. While no 'minimum length' can be guaranteed secure, eight (8) is commonly considered to be the minimum for most application access, along with requiring other password security factors, such as increasing the size of the symbol set-space by requiring mixed-cases, along with other forms of password variability creation, increases the difficulty of breaking any password by brute-force attack.",

    },
    {
        "id": 25678330,
        "instance": "os",
        "policyId": 725886,
        "policyTitle": "AllTech_policy",
        "netBios": null,
        "controlId": 1072,
        "controlStatement": "Status of the 'Minimum Password Age' setting",
        "rationale": "Among the characteristics that make 'user identification' via password a workable security solution is setting a 'minimum password age.' Without this minimum age requirement, any user(s) who wish to re-use the same password can merely cycle through a number of previously used passwords until returning to the preferred one (this is determined by the 'Password History' setting). While no specific 'minimum password age' can guarantee password security, one (1) day is generally considered to be the shortest length of time permissible, along with requiring other password security factors, such as increasing the variability of the symbol set-space by requiring mixed-cases, special characters, further increases the difficulty of breaking any password using brute-force methods. Consider implementing this control for all account passwords in conjunction with CID 1318 (Password History) and CID 1071 (Minimum Password Length) and CID 1073 (Maximum Password Age)."
    }

```
]
```

Sample - Posture ID Range

API Request

```
curl -X POST
"https://api.example.com/5.0/posture/postureInfo?evidenceRequired=1&exten
dedEvidenceRequired=1" \
  -H "Authorization: Bearer YOUR_TOKEN" \
  -H "Content-Type: application/json" \
  -d '[
    {
      "subscriptionId": "583816",
      "postureId": "25678328-25678330"
    }
  ]'
```

JSON Output


```
[
   {
        "id": 25678328,
        "instance": "os",
        "policyId": 734560,
        "policyTitle": "AllTech_policy- Exception",
        "netBios": null,
        "controlId": 1091,
       "controlStatement": "Status of the number of days before a [Prompt
user] password expiration warning prompt is displayed at login",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting the
'expiration warning date' requirement.  This establishes the number of
days before the host will begin to display 'password expiration warning'
messages upon login.  Without having a pre-expiration warning message, it
is more likely that users will not prepare for this event, which may
contribute to the selection of hard-to-remember or easily broken password
sequences, which circumvents the intent of having rules for password
complexity enforced.  This may cause some users to forget or write down
their new password, which can lead either to a system compromise or
increased calls to Help Desk resources.",

    },
    {
        "id": 25678329,
        "instance": "os",
        "policyId": 725886,
        "policyTitle": "AllTech_policy",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
```

```
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",

    },
    {
        "id": 25678330,
        "instance": "os",
        "policyId": 725886,
        "policyTitle": "AllTech_policy",
        "netBios": null,
        "controlId": 1072,
        "controlStatement": "Status of the 'Minimum Password Age'
setting",
        "rationale": "Among the characteristics that make 'user
identification' via password a workable security solution is setting a
'minimum password age.'  Without this minimum age requirement, any user(s)
who wish to re-use the same password can merely cycle through a number of
previously used passwords until returning to the preferred one (this is
determined by the 'Password History' setting).  While no specific 'minimum
password age' can guarantee password security, one (1) day is generally
considered to be the shortest length of time permissible, along with
requiring other password security factors, such as increasing the
variability of the symbol set-space by requiring mixed-cases, special
characters, further increases the difficulty of breaking any password
using brute-force methods.  Consider implementing this control for all
account passwords in conjunction with CID 1318 (Password History) and CID
1071 (Minimum Password Length) and CID 1073 (Maximum Password Age).",

    }

]
```


Sample - View scan source and last detection date of the scanner

API Request

```
curl -X POST
"<qualys_base_url>/5.0/posture/postureInfo?scanSourceRequired=1" \
  -H "Authorization: Bearer <AuthToken>" \
  -H "Content-Type: application/json" \
  -d '[
    {
      "subscriptionId": "2062014",
      "postureId": "35796574,35796575,35796576"
    }
  ]'
```

JSON Output


```
[
    {
        "id": 35796574,
        "instance": "os",
        "policyId": 5298742,
        "policyTitle": "Agent PC + IP SCA same IP",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "category": "Access Control Requirements",
        "subCategory": "Authentication/Passwords",
        "controlReference": null,
        "technologyId": 80,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2025-12-12T08:43:48Z",
        "lastFailDate": "2026-02-16T09:52:56Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2025-12-12T08:43:48Z",
        "lastEvaluatedDate": "2026-02-16T09:52:56Z",
        "created": "2026-02-25T09:23:49Z",
        "hostId": 17523783,
        "ip": "10.115.126.187",
        "trackingMethod": "AGENT",
        "os": "CentOS Linux 7.9.2009",
        "osCpe": "cpe:/o:centos:centos_linux:7.9.2009:::",
        "domainName": "qweba.rdlab.in03.qualys.com",
        "dns": "qweba.rdlab.in03.qualys.com",
        "qgHostid": "cxxxxxx1-cxxx-4xxx-9xxx-6xxxxxxxxxa",
        "networkId": 0,
```

```
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2026-02-25T08:57:09Z",
        "customerUuid": "0xxxxxxe-exxx-4xxx-8xxx-3xxxxxxxxxa",
        "customerId": "1xxxxx2",
        "assetId": 82016748,
        "technology": {
            "id": 80,
            "name": "CentOS 7.x"
        },
        "criticality": {
            "label": "URGENT_3",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\nless than\n0",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2026-02-25T08:44:44Z",
            "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n",
            "description": "The following Integer value X indicates the
current value of the PASS_MIN_LEN setting as defined within the
/etc/login.defs file."
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": []
            },
            "unexpected": {
                "value": [
                    "5"
                ]
            }
        },
        "userDefinedAttributesList": null,
        "currentDataSizeKB": "3.07",
        "totalDataSizeKB": "3.07",
        "currentBatch": 1,
        "totalBatches": 1,
        "scannerLastDetectedDate": "2026-02-10T08:33:14Z",
        "agentLastDetectedDate": "2026-02-16T09:50:56Z",
        "scanSource": "Agent + ML Scanner",
        "CLOUD_RESOURCE_ID": null
    },
]
```

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/pcrs/5.0/posture/postureInfo?	Active	Active
/pcrs/4.0/posture/postureInfo?	Active	Active
/pcrs/3.0/posture/postureInfo?	Active	Active
/pcrs/2.0/posture/postureInfo?	Active	Active
/pcrs/1.0/posture/postureInfo?	November 2026	May 2027

New V2 API URL:

<qualys_base_url>/pcrs/2.0/posture/postureInfo?compressionRequired=0&evidenceRequired=1

[POST]

Using this V2 API URL you can retrieve extended evidence and last updated date information for the hosts. The evidence for a control includes the expected and actual values for the control on the host. The extended evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result. To retrieve the extended information in the API response, specify the following input parameters.

Input Parameters

Parameter	Description
Authentication Token (Bearer Token)	(Required) Specify authentication token that is returned by the authentication request.
evidenceRequired	(Optional) Default value is 0, which indicates that evidence data will not be retrieved for the host posture. If you want evidence data to be retrieved, change the value to 1. **Note**: Changing the value to 1 will increase the time required to fetch posture data.
compressionRequired	(Required) Default value is 1, which indicates that the output will be compressed.If you do not want the data to be compressed, change the value to 0. **Note**: Not compressing the data will increase the time required to fetch posture data.
excludeInactiveControl{0|1}	(Optional) Default value is 0, which indicates that inactive controls data is retrieved for the host posture. If you want to exclude inactive control data then, change the value to 1.

Sample-V2 API-

API Request

```
<qualys_base_url>/pcrs/2.0/posture/postureInfo?evidenceRequired=1&compres
sionRequired=0&excludeInactiveControl=1
```

Json Response


```
"id": 26081552,
       "instance": "oracle19cdb:1:1527:ora19csu",
       "policyId": 5561690,
       "policyTitle": "Oracle_DB_UDC",
       "netBios": null,
       "controlId": 100432,
       "controlStatement": "Oracle_DB_UDC_3",
       "rationale": "rationle",
       "remediation": "Remediation",
```

```
"controlReference": null,
"technologyId": 312,
"status": "Failed",
"previousStatus": "Failed",
"firstFailDate": "2023-06-08T09:52:13Z",
"lastFailDate": "2023-08-24T10:00:05Z",
"firstPassDate": "",
"lastPassDate": "",
"postureModifiedDate": "2023-06-08T09:52:13Z",
"lastEvaluatedDate": "2023-08-24T10:00:05Z",
"created": "2024-01-30T06:54:04Z",
"hostId": 11587415,
"ip": "10.14.70.18",
"trackingMethod": "IP",
"os": null,
"osCpe": null,
"domainName": null,
"dns": null,
"qgHostid": null,
"networkId": 0,
"networkName": "Global Default Network",
"complianceLastScanDate": "2024-01-05T10:24:32Z",
"customerUuid": "3b3573f9-dd5e-eb05-8140-8a19a01c5980",
"customerId": "1981058",
"assetId": 37640401,
"technology": {
    "id": 312,
    "name": "Oracle 19c Multitenant"
},
"criticality": {
    "label": "SERIOUS",
    "value": 3
},
"evidence": {
    "expectedValues": "\nSet status to PASS if no data found",
    "currentValues": [
        "GRANTEE|:|GRANTED_ROLE",
        "APPQOSSYS|:|DBA",
        "UDC_SENSITIVE_SCAN|:|DBA",
        "QUALYS_SCAN|:|DBA"
    ],
    "actualValues": null,
    "directoryFimUdc": null
},
"causeOfFailure": {
    "missing": {
        "logic": null,
        "value": [
            "------------ OR ------------",
            "Set status to PASS if no data found"
        ]
    },
    "unexpected": {
        "value": [
```

```
                    "DBA,DBA,DBA",
                    "APPQOSSYS,UDC_SENSITIVE_SCAN,QUALYS_SCAN"
                ]
            }
        },
        "currentDataSizeKB": "1.47",
        "totalDataSizeKB": "4.59",
        "currentBatch": 1,
        "totalBatches": 1,
        "CLOUD_RESOURCE_ID": null
    }
```


Sample-V2 API-Exclude Inactive Control Data

API Request

```
<qualys_base_url>/pcrs/2.0/posture/postureInfo?compressionRequired
=0&evidenceRequired=1
```

Json Response


```
{
        "id": 13603803,
        "instance": "os",
        "policyId": 725886,
        "policyTitle": "AllTech_policy",
        "netBios": null,
        "controlId": 1071,
        "controlStatement": "Status of the 'Minimum Password
Length' setting",
        "rationale": "Among the several characteristics that make
'user identification' via password a secure and workable solution
is setting a 'minimum password length' requirement.  Each
character that is added to the password length squares the
difficulty of breaking the password via 'brute force,' which
attempts using every combination possible within the password
symbol set-space, in order to discover a user's password.  While no
'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along
with requiring other password security factors, such as increasing
the size of the symbol set-space by requiring mixed-cases, along
with other forms of password variability creation, increases the
difficulty of breaking any password by brute-force attack.",
       "remediation": "To specify password length requirements for
new accounts, edit the file \"/etc/login.defs\" and add or correct
the following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD
requirement is \"14\". If a program consults \"/etc/login.defs\"
and also another PAM module (such as \"pam_cracklib\") during a
password change operation, then the most restrictive must be
```

```
satisfied.",
        "controlReference": null,
        "technologyId": 80,
        "status": "Failed",
        "previousStatus": "Failed",
        "firstFailDate": "2023-07-04T13:58:08Z",
        "lastFailDate": "2024-01-23T12:56:18Z",
        "firstPassDate": "",
        "lastPassDate": "",
        "postureModifiedDate": "2023-07-04T13:58:08Z",
        "lastEvaluatedDate": "2024-01-23T12:56:18Z",
        "created": "2024-02-02T13:02:57Z",
        "hostId": 1756436,
        "ip": "10.11.70.116",
        "trackingMethod": "IP",
        "os": null,
        "osCpe": null,
        "domainName": null,
        "dns": null,
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2023-07-04T13:59:25Z",
        "customerUuid": "6009e710-108b-f57b-83d0-1768010d577f",
        "customerId": "1033824",
        "assetId": 9228010,
        "technology": {
            "id": 80,
            "name": "CentOS 7.x"
        },
        "criticality": {
            "label": "URGENT",
            "value": 5
        },
        "evidence": {
            "expectedValues": "\ngreater than or equal to\n9",
            "currentValues": [
                "5"
            ],
            "actualValues": null,
            "directoryFimUdc": null,
            "lastUpdated": "2023-07-04T13:59:25Z",
          "extendedEvidence": "Row 1:File name,Setting,Value\nRow
2:/etc/login.defs,PASS_MIN_LEN,5\n"
        },
```

Control Criticality

Control Criticality is a feature in Policy Compliance that provides ratings for controls, including the ability to customize ratings at the control level and at the policy level. Several APIs include control criticality in the API output.

Control Criticality must be enabled in your account — By default, control criticality will not be enabled while we are updating the default criticality settings in the control library. If you want this feature, please contact Support or your Technical Account Manager.

Exceptions

List, request, update and delete exceptions in your account. Supported method differs per request type, i.e. list, create etc).

The Exception API is only available if you have Policy Compliance (PC) module enabled for your subscription. Non Manager users must be granted this permission in their account settings.

User Permissions

User Role	Permissions
Manager	List, request, update, delete exceptions for all hosts in subscription.
Auditor	List, request, update, delete exceptions for all hosts in subscription.
Unit Manager	List, request, update, delete exceptions for hosts in their assigned business unit.
Scanner, Reader	List, request, update exceptions for hosts in their account. Updates are limited to adding comments.

List exceptions

For API version information, refer to API Version History section.

V2.0|V3.0

V2.0

/api/2.0/fo/compliance/exception//?action=list

[GET] [POST]

By default, all exceptions in the user's account are listed. Use the optional parameters to filter the list output.

Parameter	Description
action=list	(Required)
exception_number={value}	(Optional) Show a specific exception by specifying a valid exception number.
ip={value}	(Optional) Show exceptions associated with a specific host by specifying a host IP address. You may enter individual IP address that belong to the Policy Compliance module.
network_name={value}	(Optional) Show exceptions for a particular network by specifying the network name.
status={value}	(Optional) Show exceptions with specified status value: pending, approved, rejected or expired. Tell me about exception status
control_id={value}	(Optional) Show exceptions for a specific control by specifying valid control ID. If the value is set to 23, the matching control IDs may include 23, 234, 2343, 233.

Parameter	Description
control_statement={value}	(Optional) Show exceptions for certain controls associated with a certain policy by specifying control statement. Partial control statement is also valid.
policy_id={value}	(Optional) Show exceptions for controls associated with a certain policy by specifying a valid policy ID.
technology_name={value}	(Optional) Show exceptions for controls with a certain technology by specifying the technology name.
assignee_id={value}	(Optional) Show exceptions with a certain assignee by specifying an assignee' user ID.
created_by={value}	(Optional) Show exceptions that were created by a particular user by specifying the user ID.
modified_by={value}	(Optional) Show exceptions that were modified by a particular user by specifying the user ID.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each control. A valid value is: None - Only exception numbers. Basic (default) - All details except comments history. All - All details including comments history.
is_active={**0**|1}	(Optional). Show only exceptions that are active or inactive in the output. Specify 1 to show only active exceptions. Specify 0 to show only inactive exceptions. When unspecified, both active and inactive exceptions are shown.
created_after_date={mm/dd/yyyy}	(Optional) Show exceptions created (requested) after the specified date. The valid date format is mm/dd/yyyy.
updated_after_date={mm/dd/yyyy}	(Optional) Show exceptions that were updated after the specified date. The valid date format is mm/dd/yyyy.
expired_before_date={mm/dd/yyyy}	(Optional) Show exceptions that will expire before the specified date. The valid date format is mm/dd/yyyy.
expired_after_date={mm/dd/yyyy}	(Optional) Show exceptions that will expire after the specified date. The valid date format is mm/dd/yyyy.
exception_numbers={value}	(Optional) Show a specific exception by specifying a valid exception number. Multiple entries are comma separated. An exception number range is specified with a hyphen (for example, 289-292).
exception_number_min={value}	(Optional) Show only exceptions that have a exception number greater than or equal to the specified value.
exception_number_max={value}	(Optional) Show only exceptions that have exception number less than or equal to the specified value.
truncation_limit={value}	(Optional) Specify the maximum number of exceptions to be listed per request. When not specified, the truncation limit is set to 1000 records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000).

Tell me about exception status

Pending - An exception is in a Pending state when first requested by a user. Also, if a previously accepted or rejected exception is reopened, then it goes back to Pending.

Approved - An exception is in an Approved state when it is reviewed and accepted by an authorized user. You would accept an exception if it's determined that the host should be exempt from the specified control. As long as the host is exempt for the control, a status of PassedE appears in compliance reports. The status changes back to Failed when the exception expires.

Rejected - An exception is in a Rejected state when it is reviewed and rejected by an authorized user. You would reject an exception if it's determined that the host should not be exempt from the specified control. When an exception is rejected, a status of Failed continues to appear for the host/control in compliance reports.

Expired - An exception is in an Expired state when the exception was previously accepted but the time limit has been reached. When an exception is expired, a status of Failed appears again for the host/control in compliance reports.

Sample - List exceptions with failed status

API request:

```
curl -s -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl demo 2"
-D headers.15
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/?
action=list&policy_id=1174&status=Failed"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/p
osture_info_list_output.dtd">
          ...
           <INFO>
               <ID>1174</ID>
               <HOST_ID>563352</HOST_ID>
               <CONTROL_ID>1072</CONTROL_ID>
               <TECHNOLOGY_ID>2</TECHNOLOGY_ID>
               <INSTANCE></INSTANCE>
               <STATUS>Failed</STATUS>
               <POSTURE_MODIFIED_DATE>2015-09
               -02T08:16:33Z</POSTURE_MODIFIED_DATE>
           </INFO>
          ...
```

Sample - List exception number, show all details

API request:

```
curl -s -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo 2"
```

```
-D headers.15
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/?act
ion=list&exception_number=58&details=All"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/
exception_list_output.dtd">
<EXCEPTION_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-01-15T11:26:34Z</DATETIME>
    <EXCEPTION_LIST>
      <EXCEPTION>
        <EXCEPTION_NUMBER>58</EXCEPTION_NUMBER>
        <HOST>
          <IP_ADDRESS>10.10.30.159</IP_ADDRESS>
        </HOST>
        <TECHNOLOGY>
          <ID>11</ID>
          <NAME><![CDATA[Red Hat Enterprise Linux 5.x]]></NAME>
        </TECHNOLOGY>
        <POLICY>
          <ID>789422824</ID>
          <NAME><![CDATA[RHEL 5.x]]></NAME>
        </POLICY>
        <CONTROL>
          <CID>1073</CID>
          <STATEMENT><![CDATA[Status of the 'Maximum Password Age'
           setting
           (expiration) / Accounts having the 'password never
            expires'
                flag set]]></STATEMENT>
          <CRITICALITY>
            <VALUE>5</VALUE>
            <LABEL><![CDATA[URGENT]]></LABEL>
          </CRITICALITY>
        </CONTROL>
        <ASSIGNEE><![CDATA[Scanner User]]></ASSIGNEE>
        <STATUS>Rejected</STATUS>
        <ACTIVE>1</ACTIVE>
        <REOPEN_ON_EVIDENCE_CHANGE>0</REOPEN_ON_EVIDENCE_CHANGE>
        <EXPIRATION_DATE>N/A</EXPIRATION_DATE>
        <MODIFIED_DATE>2017-01-15T08:53:19Z</MODIFIED_DATE>
        <HISTORY_LIST>
          <HISTORY>
```

```
            <USER><![CDATA[John (mnc_su)]]></USER>
            <COMMENT><![CDATA[test]]></COMMENT>
            <INSERTION_DATE>2017-01-05T06:48:13Z</INSERTION_DATE>
          </HISTORY>
          <HISTORY>
            <USER><![CDATA[Bill (mnc_ru)]]></USER>
            <COMMENT><![CDATA[test]]></COMMENT>
            <INSERTION_DATE>2017-01-15T08:48:38Z</INSERTION_DATE>
          </HISTORY>
          <HISTORY>
            <USER><![CDATA[Mark (mnc_au)]]></USER>
            <COMMENT><![CDATA[test]]></COMMENT>
            <INSERTION_DATE>2017-01-15T08:53:19Z</INSERTION_DATE>
          </HISTORY>
        </HISTORY_LIST>
      </EXCEPTION>
...
```

DTD

<platform API server>/api/2.0/fo/compliance/exception/exception_list_output.dtd

V3.0

/api/3.0/fo/compliance/exception//?action=list

[GET] [POST]

By default, all exceptions in the user's account are listed. Use the optional parameters to filter the list output.

Parameter	Description
action=list	(Required)
exception_number={value}	(Optional) Show a specific exception by specifying a valid exception number.
ip={value}	(Optional) Show exceptions associated with a specific host by specifying a host IP address. You may enter individual IP address that belong to the Policy Compliance module.
network_name={value}	(Optional) Show exceptions for a particular network by specifying the network name.
status={value}	(Optional) Show exceptions with specified status value: pending, approved, rejected or expired. Tell me about exception status
control_id={value}	(Optional) Show exceptions for a specific control by specifying valid control ID. If the value is set to 23, the matching control IDs may include 23, 234, 2343, 233.

Parameter	Description
control_statement={value}	(Optional) Show exceptions for certain controls associated with a certain policy by specifying control statement. Partial control statement is also valid.
policy_id={value}	(Optional) Show exceptions for controls associated with a certain policy by specifying a valid policy ID.
technology_name={value}	(Optional) Show exceptions for controls with a certain technology by specifying the technology name.
assignee_id={value}	(Optional) Show exceptions with a certain assignee by specifying an assignee' user ID.
created_by={value}	(Optional) Show exceptions that were created by a particular user by specifying the user ID.
modified_by={value}	(Optional) Show exceptions that were modified by a particular user by specifying the user ID.
details={**Basic**|All|None}	(Optional) Show the requested amount of information for each control. A valid value is: None - Only exception numbers. Basic (default) - All details except comments history. All - All details including comments history.
is_active={**0**|1}	(Optional). Show only exceptions that are active or inactive in the output. Specify 1 to show only active exceptions. Specify 0 to show only inactive exceptions. When unspecified, both active and inactive exceptions are shown.
created_after_date={mm/dd/yyyy}	(Optional) Show exceptions created (requested) after the specified date. The valid date format is mm/dd/yyyy.
updated_after_date={mm/dd/yyyy}	(Optional) Show exceptions that were updated after the specified date. The valid date format is mm/dd/yyyy.
expired_before_date={mm/dd/yyyy}	(Optional) Show exceptions that will expire before the specified date. The valid date format is mm/dd/yyyy.
expired_after_date={mm/dd/yyyy}	(Optional) Show exceptions that will expire after the specified date. The valid date format is mm/dd/yyyy.
exception_numbers={value}	(Optional) Show a specific exception by specifying a valid exception number. Multiple entries are comma separated. An exception number range is specified with a hyphen (for example, 289-292).
exception_number_min={value}	(Optional) Show only exceptions that have a exception number greater than or equal to the specified value.
exception_number_max={value}	(Optional) Show only exceptions that have exception number less than or equal to the specified value.
truncation_limit={value}	(Optional) Specify the maximum number of exceptions to be listed per request. When not specified, the truncation limit is set to 1000 records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000).

Tell me about exception status

Pending - An exception is in a Pending state when first requested by a user. Also, if a previously accepted or rejected exception is reopened, then it goes back to Pending.

Approved - An exception is in an Approved state when it is reviewed and accepted by an authorized user. You would accept an exception if it's determined that the host should be exempt from the specified control. As long as the host is exempt for the control, a status of PassedE appears in compliance reports. The status changes back to Failed when the exception expires.

Rejected - An exception is in a Rejected state when it is reviewed and rejected by an authorized user. You would reject an exception if it's determined that the host should not be exempt from the specified control. When an exception is rejected, a status of Failed continues to appear for the host/control in compliance reports.

Expired - An exception is in an Expired state when the exception was previously accepted but the time limit has been reached. When an exception is expired, a status of Failed appears again for the host/control in compliance reports.

Sample - List Exception Number, All Details

API request:

```
curl -u "<username>:<password>" -H "X-Requested-With: curl demo 2"
-D headers.15
"<qualys_base_url>/api/3.0/fo/compliance/exception/?action=list&ex
ception_number=761"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE EXCEPTION_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/3.0/fo/compliance/exception/exception_list_
output.dtd%22>
<EXCEPTION_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2025-10-27T06:09:18Z</DATETIME>
        <EXCEPTION_LIST>
            <EXCEPTION>
                <EXCEPTION_NUMBER>761</EXCEPTION_NUMBER>
                <HOST>
                    <IP_ADDRESS>10.115.68.160</IP_ADDRESS>
                    <TRACKING_METHOD>IP</TRACKING_METHOD>
                    <NETWORK>
                        <![CDATA[Global Default Network]]>
                    </NETWORK>
                </HOST>
                <TECHNOLOGY>
                    <ID>45</ID>
                    <NAME>
```

```
                        <![CDATA[Red Hat Enterprise Linux 6.x]]>
                    </NAME>
                </TECHNOLOGY>
                <POLICY>
                    <ID>3342466</ID>
                    <NAME>
                        <![CDATA[Host Purge Policy - AR]]>
                    </NAME>
                </POLICY>
                <CONTROL>
                    <CID>1202</CID>
                    <STATEMENT>
                       <![CDATA[Status of the 'rpcbind' service]]>
                    </STATEMENT>
                    <CRITICALITY>
                        <VALUE>3</VALUE>
                        <LABEL>
                            <![CDATA[SERIOUSS]]>
                        </LABEL>
                    </CRITICALITY>
                </CONTROL>
                <ASSIGNEE>
                    <![CDATA[Samruddhi M]]>
                </ASSIGNEE>
                <STATUS>Pending</STATUS>
                <ACTIVE>1</ACTIVE>

<REOPEN_ON_EVIDENCE_CHANGE>0</REOPEN_ON_EVIDENCE_CHANGE>
                <EXPIRATION_DATE>N/A</EXPIRATION_DATE>
                <MODIFIED_DATE>2025-09-
03T06:27:56Z</MODIFIED_DATE>
            </EXCEPTION>
        </EXCEPTION_LIST>
    </RESPONSE>
</EXCEPTION_LIST_OUTPUT>
```

DTD

<platform API server>/api/3.0/fo/compliance/exception/exception_list_output.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/compliance/exception/?action=list	Active	Active
/api/2.0/fo/compliance/exception/?action=list	December 2025	December 2026

Request exception

For API version information, refer to API Version History section.

V2.0|V3.0

V2.0

/api/2.0/fo/compliance/exception//?action=request

[GET] [POST]

An exception is created with the expiry date matching the creation date. You can update the exception to change it.

Parameter	Description
action=request	(Required) POST method must be used. action=create is also valid.
control_id={value}	(Required) Specify the control ID of the control for which you want to request an exception.
host_id={value}	(Required) Specify the host ID of the host for which you want to request an exception.
policy_id={value}	(Required) Specify the policy ID of the policy that contains the control for which you want to request an exception.
technology_id={value}	(Required) Specify the technology ID of the technology associated with the host for which you want to request an exception.
instance_string={value}	(Optional) Specifies a single instance on the selected host. The instance string may be “os” or a string like “oracle10:1:1521:ora10204u”. This parameter must be specified with: host_id. Note: This parameter is required when you are raising the exception on control that is associated with application based instance technology. For example:-MSSQL 2022:1:1433:MSSQLSERVER:master.

Parameter	Description
assignee_id={value}	(Required) You can assign exception to another user. Specify user ID of the user, who has access to the hosts that the exceptions apply to.
comments={value}	(Required) User defined comments.
reopen_on_evidence_change={**0**|1}	(Optional) This applies only if the exception is approved. Reopen the exception if a future scan returns a value that is different than the current value and the control is still failing.

Sample - Request exception on control that is associated with instance technology

API request:

```
curl -k -H "X-Requested-With: Curl" -u "xxxxxxxxx" -X "POST" -d
"action=request&control_id=16832&host_id=3753479&policy_id=1366063
&technology_id=390&assignee_id=996765&reopen_on_evidence_change=0&
comments=comment&instance_string=MSSQL
2022:1:1433:MSSQLSERVER:master"
"<qualys_base_url>/api/2.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2023-11-28T11:21:31Z</DATETIME>
    <TEXT>Exception created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>EXCEPTION_NUMBER</KEY>
        <VALUE>59</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Request exception

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=request&control_id=1113&host_id=28595192824&
policy_id=801459496&technology_id=45&assignee_id=2449482824
reopen_on_evidence_change=1&comments=new exception"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2015-12-15T10:14:43Z</DATETIME>
    <TEXT>Exception created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>EXCEPTION_NUMBER</KEY>
        <VALUE>15</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD

<platform API server>/api/2.0/fo/compliance/exception/

V3.0

/api/3.0/fo/compliance/exception//?action=request

[GET] [POST]

An exception is created with the expiry date matching the creation date. You can update the exception to change it.

Parameter	Description
action=request	(Required) POST method must be used. action=create is also valid.
control_id={value}	(Required) Specify the control ID of the control for which you want to request an exception.
host_id={value}	(Required) Specify the host ID of the host for which you want to request an exception.
policy_id={value}	(Required) Specify the policy ID of the policy that contains the control for which you want to request an exception.
technology_id={value}	(Required) Specify the technology ID of the technology associated with the host for which you want to request an exception.

Parameter	Description
instance_string={value}	(Optional) Specifies a single instance on the selected host. The instance string may be “os” or a string like “oracle10:1:1521:ora10204u”. This parameter must be specified with: host_id. Note: This parameter is required when you are raising the exception on control that is associated with application based instance technology. For example:-MSSQL 2022:1:1433:MSSQLSERVER:master.
assignee_id={value}	(Required) You can assign exception to another user. Specify user ID of the user, who has access to the hosts that the exceptions apply to.
comments={value}	(Required) User defined comments.
reopen_on_evidence_change={**0**|1}	(Optional) This applies only if the exception is approved. Reopen the exception if a future scan returns a value that is different than the current value and the control is still failing.
tag_set_by = {id|name}	(Optional) Specify ID (the default) to select a tag set by providing tag IDs. Specify name to select a tag set by providing tag names.
ag_include_selector = {all|any}	(Optional) Select any (the default) to include hosts that match at least one of the selected tags. Select all to include hosts that match all of the selected tags.
tag_exclude_selector = {all|any}	(Optional) Select any (the default) to include hosts that match at least one of the selected tags. Select all to include hosts that match all of the selected tags.
tag_set_include = {value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing the tag name or IDs. Multiple entries are comma-separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing the tag name or IDs. Multiple entries are comma-separated.

Note - If you enter the details for the parameters tag_set_by, tag_include_selector, tag_exclude_selector, tag_set_include, and tag_set_exclude, adding the host_id parameter is optional. However, if you do not enter any of the parameters, the host_id parameter must be added.

Sample - Request Multiple Exceptions

API request:

```
curl -s -S -H 'X-Requested-With:curl demo2' -u "username:password"
-d
```

```
"action=request&tag_set_by=id&tag_set_include=50294502&policy_id=1
605419&control_id=1071&technology_id=80&assignee_id=270904&comment
s=exceptionAPI"
"https://<qualys_base_url>/api/3.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-08-12T07:13:47Z</DATETIME>
        <TEXT>Exception created successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>EXCEPTION_NUMBER</KEY>
                <VALUE>101</VALUE>
                <VALUE>102</VALUE>
                <VALUE>103</VALUE>
                <VALUE>104</VALUE>
                <VALUE>105</VALUE>
                <VALUE>106</VALUE>
                <VALUE>107</VALUE>
                <VALUE>108</VALUE>
                <VALUE>109</VALUE>
                <VALUE>110</VALUE>
            </ITEM>
            <ITEM>
                <KEY>EXCEPTION_CREATED_HOSTS</KEY>
                <VALUE>1681371</VALUE>
                <VALUE>1616892</VALUE>
                <VALUE>1692181</VALUE>
                <VALUE>1681549</VALUE>
                <VALUE>8789470</VALUE>
                <VALUE>8789468</VALUE>
                <VALUE>8789469</VALUE>
                <VALUE>8789466</VALUE>
                <VALUE>8789467</VALUE>
                <VALUE>2588281</VALUE>
            </ITEM>
            <ITEM>
                <KEY>EXCEPTION_EXIST_HOSTS</KEY>
                <VALUE></VALUE>
            </ITEM>
            <ITEM>
```

```
                    <KEY>POSTURE_RECORD_NOT_EXIST_HOSTS</KEY>
                    <VALUE>7835619</VALUE>
                    <VALUE>1682339</VALUE>
                    <VALUE>2559258</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

DTD

<platform API server>/api/3.0/fo/compliance/exception/

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/compliance/exception/?action=request	Active	Active
/api/2.0/fo/compliance/exception/?action=request	December 2025	December 2026

Update exceptions

For API version information, refer to API Version History section.

V2.0|V3.0

V2.0

/api/2.0/fo/compliance/exception//?action=update

[GET] [POST]

You can make changes to one or more exceptions on your hosts. All the actions you take are logged in the exception history with your name and a time stamp for when the action took place.

Parameter	Description
action=update	(Required) POST method must be used.
exception_numbers={value}	(Required) Show a specific exception by specifying a valid exception number. Multiple entries are comma separated. An exception number range is specified with a hyphen (for example, 50-55).
comments={value}	(Required) User defined comments. Your comments are saved in the exception history.

Parameter	Description
reassign_to={value}	(Optional) You can reassign exceptions to another user. Specify user ID of the user, who has access to the hosts that the exceptions apply to.
reopen_on_evidence_change={**0**|1}	(Optional) This applies only if the exception is approved. Reopen the exception if a future scan returns a value different than the current value and the control is still failing.
status={Pending|Approved|Rejected}	(Optional) Update the status of the exception request. A valid value is: Pending, Approved, and Rejected. Tell me about exception status.
end_date={mm/dd/yyyy}	(Optional) Set the end date by entering a future date in mm/dd/yyyy format. For a never ending exception, set the expiry date to 0. The end date is only relevant to Approved exceptions.

Sample - Update exception

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&exception_numbers=55&status=Approved&end_date=12/16
/2015&comments=status change"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/exce
ption_batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-07T11:24:42Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <NUMBER_SET>
          <NUMBER>55</NUMBER>
        </NUMBER_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD

<platform API server>/api/2.0/fo/compliance/exception/exception_batch_return.dtd

V3.0

/api/3.0/fo/compliance/exception//?action=update

[GET] [POST]

You can make changes to one or more exceptions on your hosts. All the actions you take are logged in the exception history with your name and a time stamp for when the action took place.

Parameter	Description
action=update	(Required) POST method must be used.
exception_numbers={value}	(Required) Show a specific exception by specifying a valid exception number. Multiple entries are comma separated. An exception number range is specified with a hyphen (for example, 50-55).
comments={value}	(Required) User defined comments. Your comments are saved in the exception history.
reassign_to={value}	(Optional) You can reassign exceptions to another user. Specify user ID of the user, who has access to the hosts that the exceptions apply to.
reopen_on_evidence_change={**0**|1}	(Optional) This applies only if the exception is approved. Reopen the exception if a future scan returns a value different than the current value and the control is still failing.
status={Pending|Approved|Rejected}	(Optional) Update the status of the exception request. A valid value is: Pending, Approved, and Rejected. Tell me about exception status.
end_date={mm/dd/yyyy}	(Optional) Set the end date by entering a future date in mm/dd/yyyy format. For a never ending exception, set the expiry date to 0. The end date is only relevant to Approved exceptions.

Sample - Update exception

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
 "action=update&exception_numbers=55&status=Approved&end_date=12/1
6/2015&comments=status change"
"https://<qualys_base_url>/api/2.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/2.0/fo/compliance/exception/excepti
on_batch_return.dtd">
```

```
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-07T11:24:42Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <NUMBER_SET>
          <NUMBER>55</NUMBER>
        </NUMBER_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD

<platform API server>/api/3.0/fo/compliance/exception/exception_batch_return.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/compliance/exception/?action=update	Active	Active
/api/2.0/fo/compliance/exception/?action=update	December 2025	December 2026

Delete exceptions

For API version information, refer to API Version History section.

V2.0|V3.0

V2.0

/api/2.0/fo/compliance/exception//?action=delete

[GET] [POST]

Parameter	Description
action=delete	(Required) POST method must be used.
exception_numbers={value}	(Required) Specify the exception number. Enter one or more exception numbers and/or ranges. Multiple entries are comma separated.

Sample - Delete exceptions

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&exception_numbers=40-41"
"https://qualyapi.qualys.com/api/2.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/exce
ption_batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-07T11:22:20Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Exception(s) deleted successfully</TEXT>
        <NUMBER_SET>
          <NUMBER_RANGE>40-41</NUMBER_RANGE>
        </NUMBER_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD

<platform API server>/api/2.0/fo/compliance/exception/exception_batch_return.dtd

V3.0

/api/3.0/fo/compliance/exception//?action=delete

[GET] [POST]

Parameter	Description
action=delete	(Required) POST method must be used.
exception_numbers={value}	(Required) Specify the exception number. Enter one or more exception numbers and/or ranges. Multiple entries are comma separated.

Sample - Delete exceptions

API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&exception_numbers=40-41"
"https://<qualys_base_url>/api/3.0/fo/compliance/exception/"
```

XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://<qualys_base_url>/api/3.0/fo/compliance/exception/excepti
on_batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-02-07T11:22:20Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Exception(s) deleted successfully</TEXT>
        <NUMBER_SET>
          <NUMBER_RANGE>40-41</NUMBER_RANGE>
        </NUMBER_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

DTD

<platform API server>/api/3.0/fo/compliance/exception/exception_batch_return.dtd

API Version History

The following table depicts the information about the different versions of this API along with the status:

API Version	EOS	EOL
/api/3.0/fo/compliance/exception/?action=delete	Active	Active
/api/2.0/fo/compliance/exception/?action=detele	December 2025	December 2026

SCAP Cyberscope Report

Under the Federal Information Security Management Act of 2002 (FISMA), government agencies are obliged to report on their information security statuses using a common tool called Cyberscope. Qualys customers with the SCAP module enabled can scan their network and generate Cyberscope compatible XML reports, using new API functions, to meet these requirements.

Qualys provides 3 different API functions for generating Cyberscope compatible XML reports as described below. The Cyberscope reports generated using these API functions return XML output in LASR format.

Cyberscope report specification and the LASR format:

http://scap.nist.gov/use-case/cyberscope

SCAP Scan Results

/api/2.0/fo/asset/host/cyberscope/fdcc/scan/

Create a Cyberscope report using scan results for a particular SCAP scan in the user's account. An SCAP scan ID or scan reference is required as input. The service uses only the data in the raw scan results to generate the report. When the parameters organisation_name1, organisation_name2, and organisation_name3 are specified, the <ai:Organization> elements are included in the XML report.

Permissions: Users have permission to run this API function when the SCAP module is enabled for the user's subscription. Sub-accounts (Unit Managers, Scanners and Readers) must have the "Manage compliance" permission.

Sample 1 - Select SCAP Scan by Scan ID

Use the scan_id parameter to select an SCAP scan by scan ID. (A scan ID or reference number is required.)

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/scan/?scan_id=4244823&organisation_name1=Name1&organisation_name
2=Name2&organisation_name3=Name3"
```

To obtain the SCAP scan ID, log into the Qualys application and go to PC/SCAP > Scans > SCAP Scans to view the SCAP scans in your account. Hover over the SCAP scan that you're interested in and view the scan results (select View from the Quck Actions menu). You'll see the scan results URL in your browser and the scan ID value appears in the "id" parameter, as shown in this sample URL:

```
https://qualyguard.qualys.com/fo/report/fdcc/fdcc_scan_result.php?
id=4297720
```

Sample 2 - Select SCAP Scan by Scan Reference

Use the scan_ref parameter to select an SCAP scan by scan reference number. (A scan reference number or scan ID is required.)

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/scan/?scan_ref=qscap/1337984725.4360&organisation_name1=Name1&or
ganisation_name2=Name2&organisation_name3=Name3"
```

Sample 3 - IPs Filter

Use the optional ips parameter to include only certain IP addresses in the report. You can enter a single IP, multiple IPs and/or IP ranges. Multiple entries are comma separated.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/scan/?scan_id=4268027&ips=10.10.26.183&organisation_name1=Name1&
organisation_name2=Name2&organisation_name3=Name3"
```

SCAP Policy Results

/api/2.0/fo/asset/host/cyberscope/fdcc/policy/

Create a Cyberscope report using scan results data saved for a particular SCAP policy in the user's account. A policy ID is required as input. These parameters allow users to customize the required "OrganisationName" elements in the XML report: organisation_name1, organisation_name2, and organisation_name3.

The service uses automatic SCAP policy data for a selected policy and reports this in the datapoint <sr:DataPoint id:"configuration_management_agency_deviations">. The services uses the evidence data for the special rule "security_patches_up_to_date" and reports this in the datapoint <sr:DataPoint id:"vulnerability_management_product_vulnerabilities">.

Permissions: Users have permission to run this API function when the SCAP module is enabled for the user's subscription and sub-accounts (Unit Managers, Scanners and Readers) have the "Manage compliance" permission.

Sample 1 - Select an SCAP Policy

Use the policy_id parameter to select an SCAP policy. Hosts in the policy will be included in the report unless filters are specified using the parameter ips and/or as_ids.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/policy/?policy_id=30231&organisation_name1=Name1&organisation_na
me2=Name2&organisation_name3=Name3"
```

To obtain the SCAP policy ID, log into the Qualys application and go to PC/SCAP > Policies to view the policies in your account. Hover over the SCAP policy that you're interested in and edit it (select Edit from the Quck Actions menu). You'll see the policy editor URL in your browser and the policy ID value appears in the "id" parameter, as shown in this sample URL:

```
https://qualyguard.qualys.com/fo/fdcc/edit_policy.php?id=12345&re
fresh_parent=1
```

Sample 2 - IPs Filter

Use the ips parameter to include only hosts with the specified IP addresses. Enter a single IP, multiple IPs and/or IP ranges using the ips parameter. Multiple entries are comma separated.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/policy/?policy_id=17012&ips=10.10.24.10&organisation_name1=Name1
&organisation_name2=Name2&organisation_name3=Name3"
```

Sample 3 - Asset Groups Filter

Use the **as_ids** parameter to include only hosts in the specified asset groups. Multiple asset group IDs are comma separated.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/fdc
c/policy/?policy_id=17012&ag_ids=397405&ips=10.10.25.70&organisati
on_name1=Name1&organisation_name2=Name2&organisation_name3=Name3"
```

SCAP Global Results

/api/2.0/fo/asset/host/cyberscope/

Create a Cyberscope report using the SCAP scan data saved for all the SCAP policies in the subscription and also the automatic VM scan data saved in the subscription. You must enter IPs/ranges and/or asset group IDs as input. These parameters allow users to customize the required "OrganisationName" elements in the XML report: organisation_name1, organisation_name2, and organisation_name3.

The service uses SCAP scan data for all the SCAP policies in the subscription and reports this in the datapoint <sr:DataPoint id:"configuration_management_agency_deviations">. This datapoint will include multiple Benchmark Data sections, one for each policy. Also the service uses the automatic VM data for applicable IPs (IPs in SCAP policies) and reports this in the datapoint <sr:DataPoint id:"vulnerability_management_product_vulnerabilities">.

Permissions: Users have permission to run this API function when the SCAP module is enabled for the user's subscription. Sub-accounts (Unit Managers, Scanners, and Readers) will view only data for IP addresses that their accounts have access to.

Sample 1 - Select Hosts by IP

Use the ips parameter to select hosts by IP/range. You can enter a single IP, multiple IPs and/or IP ranges using the ips parameter. Multiple entries are comma separated. (This parameter and/or ag_ids is required.)

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/?ip
s=10.10.24.52&organisation_name1=Name1&organisation_name2=Name2&or
ganisation_name3=Name3"
```

Sample 2 - Select Hosts by Asset Group

Use the as_ids parameter to select hosts by asset group ID. You can enter one or more asset group IDs. Multiple IDs are comma separated. (This parameter and/or ips is required.)

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/?ag
_ids=503424&organisation_name1=Name1&organisation_name2=Name2&orga
nisation_name3=Name3"
```

It's possible to select hosts by entering a combination of IPs/ranges and asset group IDs.

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/cyberscope/?ip
s=10.10.24.52,10.10.25.2-
10.10.25.255&ag_ids=503424,503430&organisation_name1=Name1&organis
ation_name2=Name2&organisation_name3=Name3"
```

SCAP ARF Report

/api/2.0/fo/compliance/scap/arf/

Create a SCAP scan report in Asset Reporting Format (ARF), a requirement in the SCAP 1.2 Specifications from NIST.

Permissions - Users have permission to run this API function when the SCAP module is enabled for the user's subscription. Sub-accounts (Unit Managers, Scanners and Readers) must have the "Manage compliance" permission.

Input parameters:

Parameter	Description
scan_id={value}	(Required) The scan ID for a finished SCAP scan.
ips={value}	(Optional) Use this parameter if you want to include only certain IP addresses in the report. You can enter a single IP, multiple IPs and/or ranges. Multiple entries are comma separated.
ips_network_id={value}	(Optional and valid only when the Network Support feature is enabled and the policy has SCAP 1.2 content) Use this parameter to restrict the report's target to the IPs specified in the "ips" parameter ("ips_network_id" is valid only when "ips" is specified in the same request).

How do I find the scan ID? You'll see the scan ID in the Qualys user interface, when viewing SCAP scan results. In the scan results window's title bar you'll see the report URL with its ID number in the "id" parameter, like this:
https:///qualyguard.qualys.com/fo/report/fdcc/fdcc_scan_result.php?id=3362251

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"scan_id=3362251&ips=10.10.10.1-10.10.10.10"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/scap/arf/"
```

XML Output:

The XML output is compliant with the ARF 1.1 Schema. Show me this schema

SCAP Policy List

/api/2.0/fo/compliance/fdcc_policy/?action=list

[GET] [POST]

View a list of SCAP policies visible to the user. Optional input parameters support filtering the policy list output.

Maximum Policies per API Request

A maximum of 1,000 SCAP policy records can be processed per request. If the requested list identifies more than 1,000 policies, then the XML output includes the <WARNING> element and instructions for making another request for the next batch of policy records.

Permissions

User Role	Permissions
Manager	View all SCAP policies in subscription. View asset group information for all asset groups assigned to policies.
Auditor	View all SCAP policies in subscription. View asset group information for all asset groups assigned to policies.
Unit Manager	View all SCAP policies in subscription, when the “Manage compliance” permission is turned on in the user account settings. View asset group information for asset groups assigned to SCAP policies, when the user has permission to view these asset groups.
Scanner	View all SCAP policies in subscription, when the “Manage compliance” permission is turned on in the user account settings.. View asset group information for asset groups assigned to SCAP policies, when the user has permission to view these asset groups.
Reader	View all SCAP policies in subscription, when the “Manage compliance” permission is turned on in the user account settings.. View asset group information for asset groups assigned to SCAP policies, when the user has permission to view these asset groups.

Input Parameters

Parameter	Description
action=list	(Required)
echo_request={**0**|1}	(Optional) Show (echo) the request’s input parameters (names and values) in the XML output. When unspecified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

Parameter	Description
details={**Basic**|All|None}	(Optional) Show the requested amount of host information for each host. A valid value is: Basic - (default) Includes all SCAP policy details except the asset group list and SCAP file list All - includes all SCAP policy details None - includes SCAP policy ID and title
ids={value}	(Optional) Show only certain SCAP policy IDs/ranges. One or more policy IDs/ranges may be specified. Valid host IDs are required. Multiple entries are comma separated. A policy ID range is specified with a hyphen (for example, 190-400).
id_min={value}	(Optional) Show only SCAP policies which have a minimum SCAP policy ID value. A valid SCAP policy ID is required.
id_max={value}	(Optional) Show only SCAP policies which have a maximum SCAP policy ID value. A valid SCAP policy ID is required.

DTD

<platform API server>/api/2.0/fo/compliance/fdcc_policy/fdcc_policy_list_output.dtd

Sample - SCAP Policy List

Sample SCAP policy list output (fragment) with details=All is below.

```
<!DOCTYPE POLICY_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/fdcc_policy/fd
cc_policy_list_output.dtd">

<FDCC_POLICY_LIST_OUTPUT>
   <RESPONSE>
    <DATETIME>2012-07-19T22:10:16Z</DATETIME>
    <FDCC_POLICY_LIST>
      <FDCC_POLICY>
        <ID>10235</ID>
        <TITLE><![CDATA[XP policy]]></TITLE>
        <DESCRIPTION><![CDATA[This benchmark has been created to
assist IT professionals, in particular Windows XP system
administrators and information security personnel, in effectively
securing Windows XP Professional SP2 systems.]]></DESCRIPTION>
        <BENCHMARK><![CDATA[FDCC-Windows-XP]]></BENCHMARK>
<BENCHMARK_PROFILE><![CDATA[federal_desktop_core_configuration_ver
sion_1.2.1.0]]></BENCHMARK_PROFILE>
        <BENCHMARK_STATUS_DATE>2009-04-
08T00:00:00Z</BENCHMARK_STATUS_DATE>
        <VERSION><![CDATA[v1.2.1.0]]></VERSION>
        <TECHNOLOGY><![CDATA[Windows XP Desktop]]></TECHNOLOGY>
        <NIST_PROVIDED><![CDATA[No]]></NIST_PROVIDED>
```

```
        <CREATED>
          <DATETIME>2012-07-18T23:03:35Z</DATETIME>
          <BY>USERNAME</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2012-07-18T23:03:35Z</DATETIME>
          <BY>USERNAME</BY>
        </LAST_MODIFIED>
        <ASSET_GROUP_LIST>
          <ASSET_GROUP>
            <ID>414242</ID>
            <TITLE><![CDATA[10.10.10.40]]></TITLE>
          </ASSET_GROUP>
          <ASSET_GROUP>
            <ID>414942</ID>
            <TITLE><![CDATA[10 range]]></TITLE>
          </ASSET_GROUP>
          <ASSET_GROUP>
            <ID>419582</ID>
            <TITLE><![CDATA[10.10.10.29]]></TITLE>
          </ASSET_GROUP>
          <ASSET_GROUP>
            <ID>419702</ID>
            <TITLE><![CDATA[10.10.10.28-16-191]]></TITLE>
          </ASSET_GROUP>
        </ASSET_GROUP_LIST>
        <FDCC_FILE_LIST>
          <FDCC_FILE>
           <FILE_NAME><![CDATA[fdcc-winxp-xccdf.xml]]></FILE_NAME>

<FILE_HASH><![CDATA[0c1a49c4ca47187995b543cfdcf35783]]></FILE_HASH
>
          </FDCC_FILE>
          <FDCC_FILE>
            <FILE_NAME><![CDATA[fdcc-winxp-cpe-
oval.xml]]></FILE_NAME>

<FILE_HASH><![CDATA[f397b9068b3881ef2a35c948326e6e4e]]></FILE_HASH
>
          </FDCC_FILE>
          <FDCC_FILE>
            <FILE_NAME><![CDATA[fdcc-winxp-cpe-
dictionary.xml]]></FILE_NAME>

<FILE_HASH><![CDATA[333b9b03961c58e65263bc86b4e0cdef]]></FILE_HASH
>
```

```
            </FDCC_FILE>
            <FDCC_FILE>
              <FILE_NAME><![CDATA[fdcc-winxp-oval.xml]]></FILE_NAME>

<FILE_HASH><![CDATA[d1cf1f195bb58f295ca4b17dea2f99f0]]></FILE_HASH
>
            </FDCC_FILE>
            <FDCC_FILE>
              <FILE_NAME><![CDATA[fdcc-winxp-
patches.xml]]></FILE_NAME>

<FILE_HASH><![CDATA[4ae1b306344ef564c5da479a4a3d7f53]]></FILE_HASH
>
            </FDCC_FILE>
          </FDCC_FILE_LIST>
        </FDCC_POLICY>
        <FDCC_POLICY>
...
    <FDCC_POLICY_LIST>
...
<FDCC_POLICY_LIST_OUTPUT>
```

PCAS Policies

A policy is a collection of controls used to measure and report compliance for a set of hosts. Your compliance reports display the host compliance status (pass or fail) with the policy controls. Use the following policy APIs to manage policy details such as sections, controls, and technologies, and evaluate data. They support functionalities such as retrieval, update, addition, and removal of these policy details.

- Policy
- Lock Policy
- Policy Technology
- Policy Section
- Policy Section Control
- Policy Section Control Technology
- Policy Section Control Technology Evaluate

Note: Policy APIs support only System Defined Controls (SDC). It does not support User Defined Controls (UDC).

Policy

/pcas/v3/policy/

[GET] [PUT] [DELETE]

Using this API, you can export, update, or delete compliance policies.

Note: Ensure to evaluate the policy after making any changes to the policy.

Export Compliance Policies

With this API, you can export compliance policies in JSON format.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy you want to export.
policyTitle={value}	The title of the policy you want to export. Note: When using the GET method with the parameter policyTitle, it is essential to encode the title appropriately for URL compatibility.

Sample - Export policy with policy ID

API request:

```
curl -X 'GET'
\ '<qualys_base_url>/pcas/v3/policy?policyId=<PolicyID>'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer <Auth Token>'
```

XML output:

```
{
  "policyId": 5656121,
  "policyTitle": "Documentation_Policy",
  "exported": "20-06-2024 06:05:25",
  "coverPage": "CoverPage-PC-24431",
  "isActive": true,
  "isLocked": false,
  "technologies": [
    {
      "technologyId": 18,
      "technologyName": "Windows Vista"
    }
  ],
  "sections": [
    {
      "sectionNumber": 1,
      "sectionHeading": "Section-1",
```

```
      "controls": [
        {
          "controlId": 1072,
          "sectionNumber": 1,
          "controlNumber": 1,
          "statement": "Status of the 'Minimum Password Age'
setting",
          "criticality": "CRITICAL",
          "isControlDisable": false,
          "referenceText": "Control 1072",
          "technologies": [
            {
              "technologyId": 18,
              "technologyName": "Windows Vista",
              "evaluate": {
                "dp": {
                  "k": "win.auth.passwords.minage",
                  "v": [
                    "1"
                  ],
                  "description": "The following Integer value
<B>X</B>
indicates the current status of the <B>'Minimum Password Age'
(min_pass_age)</B>  within the <B>Computer Configuration\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password age</B>setting for local accounts.",
                  "fv": [
                    {
                      "value": "161803399999999",
                      "set": "0",
                      "description": "Attribute not found"
                    }
                ],
               "op": "eq"
            }
      },
      "remediation": "To establish the recommended configuration
via GP, set the following UI path to 1 or more day(s): Computer
Configuration\\Policies\\Windows Settings\\Security
Settings\\Account\\Policies\\Password Policy\\Minimum password
age",
      "rational": "Among the characteristics that make 'user
identification' via password a workable security solution is
setting a 'minimum password age.' Without this minimum age
requirement, any user(s) who wish to re-use the same password can
merely cycle through a number of previously used passwords until
```

```
returning to the preferred one (this is determined by the 'Password
History' setting).  While no specific 'minimum password age' can
guarantee password security, one (1) day is generally considered
to be the shortest length of time permissible, along with
requiring other password security factors, such as increasing the
variability of the symbol set-space by requiring mixed-cases,
special characters, further increases the difficulty of breaking
any password using brute-force methods.  Consider implementing
this control for all account passwords in conjunction with CID 1318
(Password History) and CID 1071 (Minimum Password Length) and CID
1073 (Maximum Password Age)."
            }
          ]
        }
      ]
    }
  ]
 }
```

Sample - Export Policy with policy title

API request:

```
curl -X 'GET' \
'<qualys_base_url>/pcas/v3/policy?policyTitle=<PolicyTitle>'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer<Auth Token>'
```

XML output:

```
{
  "policyId": 5656121,
  "policyTitle": "Documentation_Policy",
  "exported": "20-06-2024 06:07:13",
  "coverPage": "CoverPage-PC-24431",
  "isActive": true,
  "isLocked": false,
  "technologies": [
 {
   "technologyId": 18,
   "technologyName": "Windows Vista"
 }
  ],
  "sections": [
 {
   "sectionNumber": 1,
   "sectionHeading": "Section-1",
   "controls": [
```

```
     {
       "controlId": 1072,
       "sectionNumber": 1,
       "controlNumber": 1,
      "statement": "Status of the 'Minimum Password Age' setting",
       "criticality": "CRITICAL",
       "isControlDisable": false,
       "referenceText": "Control 1072",
       "technologies": [
{
  "technologyId": 18,
  "technologyName": "Windows Vista",
  "evaluate": {
"dp": {
 "k": "win.auth.passwords.minage",
 "v": [
   "1"
 ],
 "description": "The following Integer value <B>X</B> indicates
the current status of the
<B>'Minimum Password Age' (min_pass_age)</B>  within the
<B>Computer Configuration\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password age</B>setting for local accounts.",
 "fv": [
   {
     "value": "161803399999999",
     "set": "0",
     "description": "Attribute not found"
   }
 ],
 "op": "eq"
}
     },
     "remediation": "To establish the recommended configuration
via GP, set the following UI path to 1 or more day(s): Computer
Configuration\\Policies\\Windows Settings\\Security
Settings\\Account Policies\\Password Policy\\Minimum password
age", "rational": "Among the characteristics that make 'user
identification' via password a workable security solution is
setting a 'minimum password age.'  Without this minimum age
requirement, any user(s) who wish to re-use the same password can
merely cycle through a number of previously used passwords until
returning to the preferred one (this is determined by the 'Password
History' setting).  While no specific 'minimum password age' can
guarantee password security, one (1) day is generally
considered to be the shortest length of time permissible, along
```

```
with requiring other password security factors, such as increasing
the variability of the symbol set-space by requiring mixed-cases,
special characters, further increases the difficulty of breaking
any password
using brute-force methods.  Consider implementing this control for
all account passwords in conjunction with CID 1318 (Password
History) and CID 1071 (Minimum Password Length) and CID 1073
(Maximum Password Age)."
            }
          ]
        }
      ]
    }
  ]
 }
```

Update Compliance Policies

With this API, you can update compliance policies. The policy fields that can be updated using this API are Policy Title, Cover page, and Status (Active/Inactive).

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy you want to update.
policyTitle={value}	(Optional) Enter a title for the policy.
coverPage={value}	(Optional) Specify the cover page that you want to replace. Replace the existing cover page text from policy and set the specified policy cover page.
isActive={0 or false|1 or true}	(Optional) Specify 0 or false to change policy status to inactive, or else specify 1 or true.

Sample - Update policy

API request:

```
curl -X 'PUT'\'<qualys_base_url>/pcas/v3/policy'
\ -H 'accept: /'
\ -H 'Authorization: Bearer '
\ -H 'Content-Type: application/json'
\ -d '{"policyId":<policyId> , "policyTitle": "<policyTitle>",
"coverPage":"<coverPage>", "isActive":<Boolean True / False> }'
```

XML output:

```
204
```

Delete Policy Details

With this API, you can delete compliance policies and its postures. All details such as its exceptions and its posture are deleted.

Note:

- The delete method can be executed by the Manager and Auditor users only.
- Only one policy can be deleted at a time.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy you want to delete.

Sample - Delete policy

API request:

```
curl --location --request DELETE
'https://<qualys_base_url>/pcas/v3/policy?policyId=<policy_id>' \
--header 'accept: */*' \
--header 'Authorization: Bearer <Bearer Token>'
```

XML output:

```
204
```

Lock Policy

/pcas/v3/policy/lock/

[PUT]

Using this API, you can lock or unlock compliance policies.

Note: Ensure to evaluate the policy after making any changes to the policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy you want to lock or unlock.
isLocked={0 or false|1 or true}	(Required) Use this parameter to lock the policy. Specify 1 or true to lock the policy. Specify 0 or false to unlock the policy.

Sample - Lock policy

API request:

```
curl -X 'PUT' \ '<qualys_base_url>/pcas/v3/policy/lock'
\ -H 'accept: */*'
```

```
\ -H 'Authorization: Bearer <Auth Token>'
\ -H 'Content-Type:application/json'
\ -d '{ "policyId":<policyId> , "isLocked": <Boolean True /
False>}'
```

XML output:

```
204
```

Policy Technology

/pcas/v3/policy/technology/

[GET] [POST] [DELETE]

Using this API, you can list details, add, and remove technologies within a compliance policy. When you add or remove new technologies to the policy, the existing technologies within the policy remain unaffected.

Note: Ensure to evaluate the policy after making any changes to the policy.

List Details of Technologies

With this API, you can get all technologies associated with a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to obtain all associated technologies.

Sample - List all technologies associated to the policy ID

API request:

```
curl -X 'GET'
\'<qualys_base_url>/pcas/v3/policy/technology?policyId=<Policy
ID>'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer <Auth Token>'
```

XML output:

```
{
"policyId": 5656121,
"technologies": [
   {
     "technologyId": 18,
     "technologyName": "Windows Vista"
   }
 ]
```

```
}
```

Add New Technologies

With this API, you can add technologies within a compliance policy. When you add new technologies to the policy, the existing technologies within the policy remain unaffected.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy where the new technology is to be added.
technologyIds={value}	(Required) Specify a valid technology ID in a list format to be added to the policy.

Sample - Add a new technology to a policy

API request:

```
curl -X 'POST' \ '<qualys_base_url>/pcas/v3/policy/technology'
\ -H 'accept: application/json' \ -H 'Authorization: Bearer <Auth
Token>'
\ -H 'Content-Type: application/json' \ -d { "policyId": 5656121,
"technologyIds": [ 331 ]}'
```

XML output:

```
[
 {
  "technologyId": 18,
  "technologyName": "Windows Vista"
 },
 {
  "technologyId": 331,
  "technologyName": "Windows 11"
 }
]
```

Delete Technologies

With this API, you can delete technology from a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy from where the technology is to be deleted.
technologyId={value}	(Required) Specify a valid technology ID to be removed from the policy.

Sample - Remove or Delete a technology from a policy

API request:

```
curl -X 'DELETE'
\'<qualys_base_url>/pcas/v3/policy/technology?policyId=<PolicyID>&
technolo
gyId=<TechnologyID>'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer <Auth Token>'
```

XML output:

```
204
```

Policy Section

/pcas/v3/policy/section/

[GET] [POST] [PUT] [DELETE]

Using this API, you can obtain details, add, update, and remove sections within a compliance policy.

Note: Ensure to evaluate the policy after making any changes to the policy.

List Section for a Policy

With this API, you can list the details of a particular section within a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to list all section details.
sectionNumber={value}	(Required) Enter the section number for which you want to list all details.

Sample - Retrieve details about a particular section in the policy

API request:

```
curl -X 'GET'
\<qualys_base_url>/pcas/v3/policy/section?policyId=5656121&section
```

```
Number=1'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer 'token''
```

XML output:


```
{
  "sectionNumber": 1,
  "sectionHeading": "Section-1",
  "controls": [
    {
      "controlId": 1072,
      "sectionNumber": 1,
      "controlNumber": 1,
      "statement": "Status of the 'Minimum Password Age' setting",
      "criticality": "CRITICAL",
      "isControlDisable": false,
      "referenceText": "Control 1072",
      "technologies": [
        {
          "technologyId": 18,
          "technologyName": "Windows Vista",
          "evaluate": {
            "dp": {
              "k": "win.auth.passwords.minage",
              "v": [
                "1"
              ],
             "description": "The following Integer value <B>X</B>
indicates the current status of the <B>'Minimum Password Age'
(min_pass_age)</B> within the <B>Computer Configuration\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password age</B>setting for local accounts.",
              "fv": [
                {
                  "value": "161803399999999",
                  "set": "0",
                  "description": "Attribute not found"
                }
              ],
              "op": "eq"
            }
          },
         "remediation": "Among the characteristics that make user
identification via 'password' a workable security solution is
setting a minimum password age. Without this minimum age
requirement, any user(s) who wish to re-use the same password can
```

```
merely cycle through a number of previously used passwords until
returning to the preferred one (this is determined by the Password
History setting)."
        }
      ]
    }
  ]
}
```

Add New Sections to a Policy

With this API, you can add sections within a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to add a section.
sectionHeading={value}	(Required) Specify a title for the section to be added for the policy.

Sample - Add a new section to a policy

API request:

```
curl -X 'POST' \
<qualys_base_url>/pcas/v3/policy/section' \
-H 'accept: application/json' \
-H 'Authorization: Bearer 'Auth_Token'\
-H 'Content-Type: application/json' \
-d '{"policyId": 5656121,"sectionHeading": "section 6"
}'
```

XML output:

```
{
 "sectionNumber": 2,
 "sectionHeading": "section 6",
 "controls": []
}
```

Update Existing Sections in a Policy

With this API, you can update sections within a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to update a section.
sectionNumber={value}	(Required) Enter the section number for which you want to update details.
sectionHeading={value}	(Required) Specify the title for the section to be updated for the policy.

Sample - Update an existing section in the policy

API request:

```
curl -X 'PUT' \
'<qualys_base_url>/pcas/v3/policy/section' \
-H 'accept: */*' \
-H 'Authorization: Bearer 'Auth_Token'\
-H 'Content-Type: application/json' \
-d '{"policyId": 5656121,"sectionNumber": 2,"sectionHeading":
"section66"}'
```

XML output:

```
204
```

Delete Sections in a Policy

With this API, you can delete a section within a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to delete a section.
sectionNumber={value}	(Required) Enter the section number for which you want to delete.

Sample - Delete an existing section in the policy

API request:

```
curl -X 'DELETE'
\'<qualys_base_url>/pcas/v3/policy/section?policyId=5656121&sectio
nNumber=2' \
-H 'accept: */*' \
-H 'Authorization: Bearer 'token'
```

XML output:

204

Policy Section Control

/pcas/v3/policy/section/control/

[GET] [POST] [PUT] [DELETE]

Using this API, you can obtain details, add, update, and remove specific controls within a specific section for a compliance policy. Retrieving the details of a specified control within a specified section of a compliance policy.

Note: Ensure to evaluate the policy after making any changes to the policy.

Get Specific Control within a Section for a Policy

With this API, you can get the details of a specified control within a specified section of a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to list all section details.
sectionNumber={value}	(Required) Enter the section number for which you want to list all details.
controlId={value}	(Required) Enter the ID of the control for which you want to retrieve the details.

Sample - List the details of a specified control within a specified section of the policy

API request:

```
curl -X 'GET'
\'<qualys_base_url>/pcas/v3/policy/section/control?policyId=565612
1&sectionNumber=1&controlId=1072'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer 'token'
```

XML output:

```
{
  "controlId": 1071,
  "sectionNumber": 1,
  "controlNumber": 1,
  "statement": "Status of the 'Minimum Password Length' setting",
  "criticality": "URGENT",
  "isControlDisable": false,
  "technologies": [
```

```
    {
      "technologyId": 1,
      "technologyName": "Windows XP desktop",
      "evaluate": {
        "dp": {
          "k": "win.auth.passwords.minlen",
          "v": [
            "0"
          ],
          "l": 0,
          "description": "The following Integer value <B>X</B>
indicates the current status of the <B>Minimum Password Length
(min_pass_len)</B> setting for local accounts.",
          "op": "ge",
          "fv": [
            {
              "value": "161803399999999",
              "set": "0",
              "description": "Attribute not found"
            }
          ]
        }
      },
      "remediation": "To establish the recommended configuration
via GP, set the following UI path to 14 or more
character(s):\n\n\tComputer Configuration\\Policies\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password length",
      "rationale": "Among the several characteristics that make
'user identification' via password a secure and workable solution
is setting a 'minimum password length' requirement. Each character
that is added to the password length squares the difficulty of
breaking the password via 'brute force,' which attempts using
every combination possible within the password symbol set-space,
in order to discover a user's password.  While no 'minimum length'
can be guaranteed secure, eight (8) is commonly considered to be
the minimum for most application access, along with requiring
other password security factors, such as increasing the size of the
symbol set-space by requiring mixed-cases, along with other forms
of password variability creation, increases the difficulty of
breaking any password by brute-force attack."
    }
  ]
}
```

Add New Controls to a Section in the Policy

With this API, you can add controls within a section of a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to add controls within a section.
sectionNumber={value}	(Required) Enter the section number to which you want to add controls.
controls={value}	(Required) Specify the list of controls to be added to a particular section of the policy. Each control should contain the following elements: • controlId={value}: (Required) (Integer) Id of a control to be added to the section. • referenceText={value} : (Optional) (String) Specify a reference text for the control while adding it. If not provided default referenceText of the control will be used. • criticality={value} : (Optional) (String) Specify the control criticality value while adding control. If not provided default criticality of the control will be used. • isControlDisable={value} : (Optional) (Boolean) Specify the value as either 'true' or 'false' to disable/enable the control while adding it. If not provided control will be enabled by default. • controlNumber={value} : (Optional) (Boolean) Specify the position number where you want to add control in a section. If not provided control will be added at the end in the section.

Sample - Sample - Add a new control to a particular section in the policy

API request:

```
curl -X 'POST' \
'https://<qualys_base_url>/pcas/v3/policy/section/control' \
-H 'accept: application/json' \
-H 'Authorization: Bearer 'Auth_Token' ' \
-H 'Content-Type: application/json' \
-d '{
"policyId": 5656121,
"sectionNumber": 1,
"controls": [
{
"controlId": 1048,
"referenceText": "Reference Text",
"isControlDisable": true,
"controlNumber": 2,
"criticality": "CRITICAL"
```

```
}
]
}
```


XML output:


```
[
  {
    "controlId": 1048,
    "sectionNumber": 1,
    "controlNumber": 2,
    "statement": "Status of the 'Shutdown: Clear virtual memory
pagefile'
setting",
    "criticality": "CRITICAL",
    "isControlDisable": false,
    "referenceText": null,
    "technologies": [
      {
        "technologyId": 18,
        "technologyName": "Windows Vista",
        "evaluate": {
          "dp": {
            "k": "secman.system.clearpageonshut",
            "v": [
              "1"
            ],
            "description": "This Integer value <B>X</B> indicates
the current status of the setting <B>Shutdown: Clear virtual
memory pagefile</B> using the registry key path
<B>HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Control\\Session
Manager\\Memory Management\\ClearPageFileAtShutdown</B> if
configured via <B>Group Policy Editor</B> or
<B>Microsoft Intune / MDM</B>. A value of <B>0</B> indicates the
setting is <B>Disabled</B>; a value of <B>1</B> indicates the
setting is <B>Enabled</B>.",
            "fv": [
              {
                "value": "0",
                "set": "1",
                "description": "Disabled"
              },
              {
                "value": "1",
                "set": "1",
                "description": "Enabled"
              },
```

```
                {
                  "value": "314159265358979",
                  "set": "1",
                  "description": "Key not found"
                }
              ],
              "op": "eq"
            }
 },
 "remediation": "To configure the group policy setting go to
Computer Configuration -> Windows Settings -> Security Settings ->
Local Policies -> Security Options -> 'Shutdown: Clear virtual
memory pagefile'.  Set its value as appropriate to the needs of the
business or as per security policy of the organization.",
"rational": "This check provides the current status of the
'Shutdown: Clear virtual memory pagefile' setting.  The Windows
Pagefile contains 'near-time' information stored by system and/or
user processes on the hard disk in 'virtual memory,' so that space
in the RAM can be freed up for real-time processing needs.
Sensitive information, such as logon credentials and other company
proprietary information cached from browser/database downloads may
be stored in the Pagefile.  As this can potentially be read by
using an lternative OS when the Windows OS is shut down,this should
be configured as appropriate to the needs of the business."
      }
    ]
  }
 ]
```


Update Control Within a Section in a Policy

With this API, you can update a control within a section of a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy from which you want to update control within a section.
sectionNumber={value}	(Required) The section number from which you want to update control.
controlId={value}	(Required) The ID of the control which needs to be updated from a particular section of the policy.
criticality={value}	(Optional) Specify the control criticality value as defined in the specific control Default Values: CRITICAL, MEDIUM, UNDEFINE, URGENT, MINIMAL, SERIOUS
referenceText={value}	(Optional) Reference text for the control to be updated within the section of the policy.
isControlDisable={value}	(Optional) The value as either 'true' or 'false' to disable/enable the control status.
controlNumber={value}	(Optional) The new control number if you desired to modify sequence of a control within the section of a policy.

Sample - Update a control within a specified section of the policy

API request:

```
curl -X 'PUT' \
'https://<qualys_base_url>/pcas/v3/policy/section/control' \
-H 'accept: */*' \
-H 'Authorization: Bearer 'token' \
-H 'Content-Type: application/json' \
-d '{
"policyId": 5656121,
"sectionNumber": 1,
"controlId": 1072,
"criticality": "CRITICAL",
"referenceText": "Control 1072",
"isControlDisable": false,
"controlNumber": 1
}'
```

XML output:

```
204
```

Delete Control Within a Section in a Policy

With this API, you can delete a control within a section of a compliance policy.

Input Parameters

Parameter	Description
policyId={value}	(Required) Enter the ID of the policy from which you want to delete a control within a section.
sectionNumber={value}	(Required) Enter the section number for which you want to remove a control.
controlId={value}	(Required) Enter the ID of the control that needs to be removed from a particular section of the policy.

Sample - Delete a control within a specified section of the policy

API request:

```
curl -X 'DELETE'
\'<qualys_base_url>/pcas/v3/policy/section/control?policyId=<Polic
yID>&sectionNumber=<SectionNumber>&controlId=<ControlID>'
\ -H 'accept: */*'
\ -H 'Authorization: Bearer <Auth Token>'
```

XML output:

```
204
```

Policy Section Control Technology

/pcas/v3/policy/section/control/technology/

[GET] [POST] [DELETE]

Using this API, you can list details, add, and remove technology details associated to a specific control within the policy section.

Note: Ensure to evaluate the policy after making any changes to the policy.

List Technologies for Specific Control and Sections

With this API, you can list technologies associated with a specific control within the policy section.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy from which you want to retrieve control technologies within a section.
sectionNumber={value}	(Required) Enter the section number for which you want to retrieve control technologies.
controlId={value}	(Required) Enter the ID of the control within a specific policy section for which you need to retrieve associated technologies.

Sample - List technologies for specified control and section within the Policy

API request:

```
curl -X 'GET'
\'<qualys_base_url>/pcas/v3/policy/section/control/technology?poli
cyId=5656121&sectionNumber=1&controlId=1048'
\ -H 'accept: application/json'
\ -H 'Authorization: Bearer <Auth Token>'
```

XML output:

```
{
    "policyId": 725886,
    "sectionNumber": 1,
    "controlId": 1071,
    "technologies": [
        {
            "technologyId": 1,
            "technologyName": "Windows XP desktop",
            "evaluate": {
                "dp": {
                    "k": "win.auth.passwords.minlen",
                    "v": [
                        "0"
                    ],
                    "l": 0,
                    "description": "The following Integer value
<B>X</B> indicates the current status of the <B>Minimum Password
Length (min_pass_len)</B> setting for local accounts.",
                    "op": "ge",
                    "fv": [
                        {
                            "value": "161803399999999",
                            "set": "0",
                            "description": "Attribute not found"
                        }
```

```
                    ]
                }
            },
            "remediation": "To establish the recommended
configuration via GP, set the following UI path to 14 or more
character(s):\n\n\tComputer Configuration\\Policies\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password length",
            "rationale": "Among the several characteristics that
make 'user identification' via password a secure and workable
solution is setting a 'minimum password length' requirement.  Each
character that is added to the password length squares the
difficulty of breaking the password via 'brute force,' which
attempts using every combination possible within the password
symbol set-space, in order to discover a user's password.  While no
'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along
with requiring other password security factors, such as increasing
the size of the symbol set-space by requiring mixed-cases, along
with other forms of password variability creation, increases the
difficulty of breaking any password by brute-force attack."
        }
    ]
}
```

Add New Technologies to a Control and Section

With this API, you can add new technologies for a specific control within the policy section.

Input Parameters

Parameter	Description
policyId={value}	(Required) Enter the ID of the policy for which you want to add technologies within a section.
sectionNumber={value}	(Required) Enter the section number for which you want to add technologies.
controlId={value}	(Required) Enter the ID of the control within a specific policy section where the technologies needs to be added.
technologyIds={value}	(Required) Enter valid technology IDs in a list format to be added.

Sample - Add technology to a control

API request:

```
curl -X 'POST' \
'http://<Base URL>/pcas/v3/policy/section/control/technology' \
```

```
-H 'accept: */*' \
-H 'Authorization: Bearer <Auth Token>' \
-H 'Content-Type: application/json' \
-d '{
"policyId": 5656121,
"sectionNumber": 1,
"controlId": 1048,
"technologyIds": [
54
]
}'
```

XML output:

```
[
 {
  "technologyId": 18,
  "technologyName": "Windows Vista"
 },
 {
  "technologyId": 54,
  "technologyName": "Windows 8"
 }
]
```

Delete Technology from a Control and Section

With this API, you can delete technology for a specific control within the policy section.

Input Parameters

Parameter	Description
policyId={value}	(Required) Enter the ID of the policy from which you want to remove a technology within a section.
sectionNumber={value}	(Required) Enter the section number for which you want to remove a technology.
controlId={value}	(Required) Enter the ID of the control within a specific policy section where the technology needs to be removed.
technologyId={value}	(Required) Enter a valid technology ID that is to be removed.

Sample - Delete technology from a control and section

API request:

```
curl -X 'DELETE' \
'<qualys_base_url>/pcas/v3/policy/section/control/technology?polic
```

```
yId=5656121&sectionNumber=1&controlId=1048&technologyId=54' \
-H 'accept: */*' \
-H 'Authorization: Bearer <Auth Token>.
```

XML output:

```
204
```

Policy Section Control Technology Evaluate

/pcas/v3/policy/section/control/technology/evaluation/

[GET] [PUT]

Using this API, you can retrieve or modify evaluation fields for technology associated with a specified control within a policy section.

List Detailed Technology Evaluate Data

With this API, you can list evaluation fields for technology associated with a specified control within a policy section.

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy from which you want to retrieve evaluation fields for technology associated with a specified control within a policy section.
sectionNumber={value}	(Required) Enter the section number for which you want to obtain technology evaluation fields.
controlId={value}	(Required) Enter the ID of the control within policy section for which you want to retrieve technology evaluation fields.
technologyId={value}	Enter a valid technology ID for which you want to retrieve technology evaluation fields.

Sample - List detailed technology evaluate data for given technologyId, control and section of the policy

API request:

```
curl -X 'GET' \
'<qualys_base_url>/pcas/v3/policy/section/control/technology/evalu
ation?policyId=5656121&sectionNumber=1&controlId=1048&technologyId
=54' \ -H
'accept: application/json' \ -H 'Authorization: Bearer
```

XML output:

```
{
```

```
  "controlId": 1071,
  "sectionNumber": 1,
  "controlNumber": 1,
  "statement": "Status of the 'Minimum Password Length' setting",
  "criticality": "URGENT",
  "isControlDisable": false,
  "technologies": [
    {
      "technologyId": 1,
      "technologyName": "Windows XP desktop",
      "evaluate": {
        "dp": {
          "k": "win.auth.passwords.minlen",
          "v": [
            "0"
          ],
          "l": 0,
          "description": "The following Integer value <B>X</B>
indicates the current status of the <B>Minimum Password Length
(min_pass_len)</B> setting for local accounts.",
          "op": "ge",
          "fv": [
            {
              "value": "161803399999999",
              "set": "0",
              "description": "Attribute not found"
            }
          ]
        }
      },
      "remediation": "To establish the recommended configuration
via GP, set the following UI path to 14 or more
character(s):\n\n\tComputer Configuration\\Policies\\Windows
Settings\\Security Settings\\Account Policies\\Password
Policy\\Minimum password length",
      "rationale": "Among the several characteristics that make
'user identification' via password a secure and workable solution
is setting a 'minimum password length' requirement.  Each
character that is added to the password length squares the
difficulty of breaking the password via 'brute force,' which
attempts using every combination possible within the password
symbol set-space, in order to discover a user's password.  While no
'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along
with requiring other password security factors, such as increasing
the size of the symbol set-space by requiring mixed-cases, along
with other forms of password variability creation, increases the
```

```
difficulty of breaking any password by brute-force attack."
    }
  ]
}
```

Update Evaluation Condition within a Section of a Policy

With this API, you can update evaluation fields for technology associated with a specified control within a policy section. The following evaluation fields can be updated:

- op (Operator)
- v (Value)
- fv (Fixed Values)
- CD (Cardinalities)
- Remediation

Supporting Operators and Cardinalities are as follows:

- Operators (op)
  - equal (=)
  - less than (<)
  - less than equal (<=)
  - greater than (>)
  - greater than equal (>=)
  - not equal (!=)
  - regular expression
  - XEQ
  - XRE
  - RANGE
  - IN
- Cardinalities - Regular expression, EXQ, and XRE operators can have the following cardinality options:
  - match none
  - match all
  - match any
  - empty

- not empty
- contain
- does not contain
- match
- intersect
- is contained in

Input Parameters

Parameter	Description
policyId={value}	(Required) The ID of the policy for which you want to update technology evaluation fields.
sectionNumber={value}	(Required) The section number for which you want to update technology evaluation fields.
controlId={value}	(Required) The ID of the control within policy section for which you want to update technology evaluation fields.
technologyId={value}	Enter a valid technology ID for which you want to update technology evaluation fields.
evaluate={value}	Enter the evaluate data points to be updated: op (Operator), v (Value), fv (Fixed Values) can be enabled or disabled, CD (Cardinalities), and remediation.
remediation={value}	Enter the Remediation to be updated.

Sample - Update technology evaluate data for control and policy

API request:

```
curl -X 'PUT' \
'<qualys_base_url>/pcas/v3/policy/section/control/technology/evalu
ation'
\
-H 'accept: */*' \
-H 'Authorization: Bearer <Auth Token>' \
-H 'Content-Type: application/json' \
-d '{
"policyId": 5656121,
"sectionNumber": 2,
"controlId": 1114,
"technologyId": 25,
"evaluate": {
"dp": {
"k": "secman.network.www-apache",
"v": [
```

```
"3",
"5"
],
"description": "The following List Integer value <B>X</B>
indicates whether or not this host'\''s <B>Apache webserver</B>
service is operational. When enabled for multiuser operation
(console login only) the RUNLEVEL should be <B>3</B>; when enabled
for multiuser operation
(console + GUI login), the RUNLEVEL should be <B>5</B>.","cd": "is
contained in","op": "xeq",
"fv": [
{
"value": "161803399999999",
"set": "1",
"description": "Service disabled"
},
{
"value": "314159265358979",
"set": "1",
"description": "Service not found"
}
]
}
},
"remediation": "Remediation text to be updated"
} '
```

XML output:

```
204
```

PCAS Library Policy

Using the PCAS Library Policy APIs, you can retrieve and import library policies. They make the process faster and more efficient, helping users save both time and effort.

- Library Label
- Library Label Technology
- Library Policy
- Library Policy Details
- Import Library Policy

Library Label

/pcas/v1/library/label

[GET]

Using this API, you can list all library label details (ID and name) that are currently supported.

Input Parameters

Parameter	Description
Authorization	(Required) Enter the Bearer token.

Sample - List label IDs and their names

API request:

```
curl -X 'GET' '<qualys_base_url>/pcas/v1/library/label' -H 'accept:
application/json' -H 'Authorization: Bearer <AuthToken>
```

JSON output:

```
[
  {
    "labelId": 1000,
    "labelName": "Qualys"
  },
  {
    "labelId": 1051,
    "labelName": "Vendor"
  },
  {
    "labelId": 1017,
    "labelName": "Mandate"
  },
  {
    "labelId": 7325,
    "labelName": "Ransomware"
  },
  {
    "labelId": 2050,
    "labelName": "DISA STIG"
  },
  {
    "labelId": 5019,
    "labelName": "Remote"
  },
  {
    "labelId": 1001,
    "labelName": "CIS"
  },
  {
    "labelId": 4051,
    "labelName": "OCA"
```

```
    },
    {
      "labelId": 4286,
      "labelName": "SCSEM"
    }
  ]
```

Library Label Technology

/pcas/v1/library/technology

[GET]

Using this API, you can list all technology IDs and names associated with the label ID.

Input Parameters

Parameter	Description
Authorization	(Required) Enter the Bearer token.
labelId={value}	(Optional) Label ID for which associated technologies are to be displayed. **Note:** If no label ID is specified, technology details associated with all labels are returned.

Sample - List technology for a label

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/technology?labelId=<labelId> '
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>
```

JSON output:

```
{
  "technologies": [
    {
      "technologyId": 346,
      "technologyName": "Debian GNU/Linux 11.x"
    },
    {
      "technologyId": 391,
      "technologyName": "ISC BIND 9.x"
    },
    {
      "technologyId": 78,
      "technologyName": "MariaDB 10.x"
    }
  ]
}
```

Library Policy

/pcas/v1/library/policy/list

[GET]

Using this API, you can list all policies associated with a specific label ID. The response displays details such as the policy ID, title, version, and date. The results are filtered based on the specified label and technology.

Input Parameters

Parameter	Description
Authorization	(Required) Enter the Bearer token.
labelId={value}	(Optional) List policies associated to the label ID. **Note:** If no label ID is specified, technology details associated with all labels are returned.
technologyId={value}	(Optional) List policies associated with the technology ID. You can enter multiple IDs separated by comma. **Note:** If the technology ID is not provided, display policies from all technologies.
includeDescription={value}	(Optional) Specify 'true' to display the description else specify 'false'.
updatedAfter={value}	(Optional) Filters response based on the given date. Policies updated on and after the provided date are displayed. Date format - dd/mm/yyyy.

Sample 1 - List policy IDs and their names

API request:

```
curl -X 'GET' '<qualys_base_url>/pcas/v1/library/policy/list '
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>
```

JSON output:

```
[
  {
    "policyId": 1464200,
    "policyTitle": "CIS Benchmark for Apple macOS 10.12, v1.1.0[Scored,
Level 1 and Level 2]",
    "version": 1,
    "date": "02/06/2025"
  },
  {
    "policyId": 1464300,
   "policyTitle": "DISA Security Technical Implementation Guide(STIG) for
Windows Server 2008 non-R2 MS, V6R46",
    "version": 1,
    "date": "02/06/2025"
  }
]
```

Sample 2 - List policies for a label ID

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy/list?labelId=<label_id>'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:

```
[
  [
    {
      "policyId": 1465339,
      "policyTitle": "CIS Benchmark for Microsoft Windows Server 2016,
v3.0.0 [Automated and Manual, Level 1 - Domain controller]",
      "version": 1,
      "date": "13/11/2024"
    },
    {
      "policyId": 1465356,
      "policyTitle": "CIS Benchmark for Microsoft Windows Server 2025,
v1.0.0 [Automated and Manual, Level 1 - Domain controller, Level 2 -
Domain controller]",
      "version": 1,
      "date": "09/05/2025"
    }
  ]
]
```

Sample 3 - List policies for a label ID and technology ID

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy/list?labelId=<labelId>&technolo
gyId=<technologyId>'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:

```
[
  [
    {
      "policyId": 1464495,
     "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1 and Level 2]",
      "version": 16,
      "date": "08/08/2025"
    },
    {
```

```
      "policyId": 1441206,
      "policyTitle": "CIS Benchmark for IBM DB2 11.x, v1.1.0 [Automated
and Manual, Level 1 - RDBMS]",
      "version": 3,
      "date": "02/06/2025"
    }
  ]
]
```

Sample 4 - List policies for a label ID, technology ID, and include a description

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy/list?labelId=<label_id>&technol
ogyId=<technologyId>&includeDescription=true'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:

```
[
  [
    {
      "policyId": 1464495,
     "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1 and Level 2]",
      "description": "This CIS certified policy for Red Hat Enterprise
Linux 8 is based on the CIS Benchmark for Red Hat Enterprise Linux 8,
v3.0.0. The policy contains Level 1 and Level 2, Automated, and Manual
types of checks from the benchmark. The controls within the policy are
configured on the basis of values provided by the CIS benchmark.",
      "version": 16,
      "date": "08/08/2025"
    },
    {
      "policyId": 1441206,
      "policyTitle": "CIS Benchmark for IBM DB2 11.x, v1.1.0 [Automated
and Manual, Level 1 - RDBMS]",
     "description": "This CIS certified policy for IBM DB2 11 is based on
the CIS Benchmark for IBM DB2 11, v1.1.0. The policy contains Automated
and Manual types of checks which are of Level 1 - RDBMS profile. The
controls within the policy are configured on the basis of values provided
by CIS benchmark.",
      "version": 3,
      "date": "02/06/2025"
    }
  ]
]
```

Sample 5 - Sample 5 - List policies for a label ID, technology ID, include a description, and the updated date

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy/list?labelId=<labelId>&technolo
gyId=<technologyId>&includeDescription=true&updatedAfter=08-08-2025'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:


```
[
  {
    "policyId": 1464495,
    "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1 and Level 2]",
   "description": "This CIS certified policy for Red Hat Enterprise Linux
8 is based on the CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0.
The policy contains Level 1 and Level 2, Automated, and Manual types of
checks from the benchmark. The controls within the policy are configured
on the basis of values provided by the CIS benchmark.",
    "version": 16,
    "date": "08/08/2025"
  },
  {
    "policyId": 1464494,
    "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1]",
   "description": "This CIS certified policy for Red Hat Enterprise Linux
8 is based on the CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0.
The policy contains Level 1, Automated, and Manual types of checks from
the benchmark. The controls within the policy are configured on the basis
of values provided by the CIS benchmark.",
    "version": 17,
    "date": "08/08/2025"
  }
]
```


Library Policy Details

/pcas/v1/library/policy

[GET]

Using this API, you can get the details about a specific library policy using policy ID or the title of the policy.

Input Parameters

Parameter	Description
Authorization	(Required) Enter the Bearer token.
policyId={value}	(Optional) Specify the policy ID for which details are to be returned.
policyTitle={value}	(Optional) Specify the policy title for which details are to be displayed. **Note:** The policy title must be encoded. For example, Security Configuration in encoded format displays as Security%20Configuration.
details={basic|full}	(Optional) Specify the level of details to be displayed: basic - minimal information full - complete details

Note: For getting the policy details, provide any one of the two parameters - policyID or policyTitle.

Sample 1 - List policy details based on policy ID

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy?policyTitle=<policytitle>&detai
ls=basic'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:


```
{
  "policyId": 1464240,
  "policyTitle": "CIS Benchmark for CentOS Linux 7, v4.0.0 [Automated and
Manual, Level 1 and Level 2]",
  "coverPage": "This CIS certified policy for CentOS Linux 7 is based on
the CIS Benchmark for Oracle Linux 7, v4.0.0. The policy contains Level 1
and Level 2, Automated, and Manual types of checks from the benchmark. The
controls within the policy are configured on the basis of values provided
by the CIS benchmark. As this policy and the controls within the policy
are certified by CIS, the policy is LOCKED to prohibit any changes to the
controls or their configuration values. If the organizational security
policy requires different configuration values or changes to the policy,
please make a copy of this policy and modify the configured values for the
required controls as per the need of the organization's
security/configuration policy.\n\nIn the case of CIS-required Control
duplication (where a Control requirement appears in more than one section
of the benchmark), Policy Editor limits the existence of any Controls
within a single policy to one (1) occurrence of each control.\n\nCIS has
stated that these settings should be considered as minimum allowable
values; if an Organization requires more stringency than the CIS minimum,
these more restrictive and/or stringent values shall all be considered as
a PASS. The settings assigned to any given control by CIS are not
```

guaranteed to be appropriate for any particular environment and all settings should be reviewed and applied according to the needs of the business. Before you apply the recommendations from the policy, check the relevant vendor documentation to avoid discrepancies. Also, it is recommended that these values be tested before applying to the Production Environment.\n\nAdditional Information:\n\n1) The following list of Control(s) in this policy is configured with default configuration value (.*) because the configuration is specific to the needs of an organization. Controls with default configuration values always result in PASS and should be configured as appropriate to the needs of the business and/or as per the need of the organization's security/configuration policy.\n\nCIS Ref #4.2.4:5215 - Status of the 'AllowGroups' setting in the 'sshd_config' file\nCIS Ref #4.2.4:5217 - Status of the 'AllowUsers' setting in the 'sshd_config' file\nCIS Ref #4.2.4:5224 - Status of the 'DenyGroups' setting in the 'sshd_config' file\nCIS Ref #4.2.4:5225 - Status of the 'DenyUsers' setting in the 'sshd_config' file\n\n2) The following list of Manual types of checks from the benchmark is set as INACTIVE in the policy:\n1.2.1, 1.2.3, 1.2.4, 1.2.5, 2.2.22, 3.1.1, 3.4.2.3, 3.4.2.4, 3.4.3.2, 3.4.3.6, 3.4.4.2.2, 3.4.4.3.2, 4.4.2.2.4, 5.1.1.2, 5.1.1.3, 5.1.1.6, 5.1.2.1.1, 5.1.2.1.2, 5.1.2.1.3, 5.1.2.5, 5.1.2.6, 5.1.3, 5.2.3.21, 6.1.13, 6.1.14\n\n3) Being procedural, the following requirement is not part of this policy:\n5.1.1.5\n\n4) The controls for all the requirements are configured as per the CIS recommendation. If you have any alternative methods implemented for the CIS checks through which CIS requirements are met, you can find the controls from the library and replace the controls in this policy by importing the policy and creating your own customized policy or you can take an exception for those CIS checks.\n\nE.g.: For firewalls, the firewalld, nftables and iptables cannot be used at the same time. So if you are using firewalld, you can remove/reconfigure the controls for iptables and nftables or take an exception for those CIS checks.",
  "technologies": [
    {
      "technologyId": 80,
      "technologyName": "CentOS 7.x"
    }
  ],
  "sections": [
    {
      "sectionNumber": 1,
      "sectionHeading": "Initial Setup"
    },
    {
      "sectionNumber": 2,
      "sectionHeading": "Services"
    },
    {
      "sectionNumber": 3,
      "sectionHeading": "Network"
    },
    {
      "sectionNumber": 4,
      "sectionHeading": "Access, Authentication and Authorization"
    },

```
    {
      "sectionNumber": 5,
      "sectionHeading": "Logging and Auditing"
    },
    {
      "sectionNumber": 6,
      "sectionHeading": "System Maintenance"
    }
  ]
}
```


Sample 2 - List policy details based on policy title

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy?policyTitle=<policytitle>'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:


```
{
  "policyId": 1464495,
  "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1 and Level 2]",
  "coverPage": "This CIS certified policy for Red Hat Enterprise Linux 8
is based on the CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0. The
policy contains Level 1 and Level 2, Automated, and Manual types of checks
from the benchmark. The controls within the policy are configured on the
basis of values provided by the CIS benchmark. As this policy and the
controls within the policy are certified by CIS, the policy is LOCKED for
prohibiting any changes to the controls or their configuration values. If
the organizational security policy requires different configuration values
or changes to the policy, please make a copy of this policy and modify the
configured values for the required controls as per the need of the
organization's security/configuration policy.\n\nIn the case of CIS-
required Control duplication (where a Control requirement appears in more
than one section of the benchmark), Policy Editor limits the existence of
any Controls within a single policy to one (1) occurrence of each
control.\n\nCIS has stated that these settings should be considered as
minimum allowable values; if an Organization requires more stringency than
the CIS minimum, these more restrictive and/or stringent values shall all
be considered as a PASS. The settings assigned to any given control by CIS
are not guaranteed to be appropriate for any particular environment and
all settings should be reviewed and applied according to the needs of the
business. Before you apply the recommendations from the policy, check the
relevant vendor documentation to avoid discrepancies. Also, it is
recommended that these values be tested before applying to the Production
Environment.\n\nAdditional Notes:\n\n1. Being procedural, the following
requirements are not part of the policy:\n5.1.1.5\n\n2. The following list
of Manual types of checks from the benchmark is set as INACTIVE in the
policy:\n1.2.1, 1.2.3, 1.2.4, 1.2.5, 2.2.22, 3.1.1, 3.4.2.3, 3.4.2.4,
4.4.3.2.3, 5.1.3, 5.1.1.2, 5.1.1.3, 5.1.1.5, 5.1.1.6, 5.1.2.1.1,
```

5.1.2.1.2, 5.1.2.1.3, 5.1.2.5, 5.1.2.6, 5.2.3.21, 6.1.13, 6.1.14\n\n3. The following requirements in the policy are configured with default values of '.*' or '.+' as the configuration is specific to the needs of an organization. They should be reviewed and configured per the business's needs and the organization's security policies:\n1.2.1, 1.2.5, 1.8.2, 2.2.22, 3.4.2.3, 5.1.1.6, 5.1.2.1.2, 5.1.3, 5.2.2.1, 6.1.13, 6.1.14\n\n4) The controls for all the requirements are configured as per the CIS recommendation. If you have any alternative methods implemented for the CIS checks through which CIS requirements are met, you can find the controls from the library and replace the controls in this policy by importing the policy and creating your own customized policy, or you can take an exception for those CIS checks.\n\n5) For the 4.2.2 requirement, the group name is considered as \"ssh_keys|_?ssh\" as specified by CIS. If you have any other designated group name for SSH, you can include it in this requirement's regex.\n\nExamples:\n - For firewalls, firewalld, nftables, and iptables cannot be used at the same time. If you are using firewalld, you can remove/reconfigure the controls for iptables and nftables or take an exception for those CIS checks.\n - For logging, the requirements in the benchmark may be separated between journald and rsyslog. If you are using journald, you can remove/reconfigure the controls for rsyslog or take an exception for those CIS checks.",
  "technologies": [
    {
      "technologyId": 217,
      "technologyName": "Red Hat Enterprise Linux 8.x"
    }
  ],
  "sections": [
    {
      "sectionNumber": 1,
      "sectionHeading": "Initial Setup"
    },
    {
      "sectionNumber": 2,
      "sectionHeading": "Services"
    },
    {
      "sectionNumber": 3,
      "sectionHeading": "Network"
    },
    {
      "sectionNumber": 4,
      "sectionHeading": "Access, Authentication and Authorization"
    },
    {
      "sectionNumber": 5,
      "sectionHeading": "Logging and Auditing"
    },
    {
      "sectionNumber": 6,
      "sectionHeading": "System Maintenance"
    }
  ]
}

Sample 3 - List policy details based on policy ID and policy details

API request:

```
curl -X 'GET'
'<qualys_base_url>/pcas/v1/library/policy?policyTitle=<policytitle>&detai
ls=basic'
-H 'accept: application/json'
-H 'Authorization: Bearer <AuthToken>'
```

JSON output:


```
{
  "policyId": 1464495,
  "policyTitle": "CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0
[Automated and Manual, Level 1 and Level 2]",
  "exported": "16-09-2025 10:39:48",
  "coverPage": "This CIS certified policy for Red Hat Enterprise Linux 8
is based on the CIS Benchmark for Red Hat Enterprise Linux 8, v3.0.0. The
policy contains Level 1 and Level 2, Automated, and Manual types of checks
from the benchmark. The controls within the policy are configured on the
basis of values provided by the CIS benchmark. As this policy and the
controls within the policy are certified by CIS, the policy is LOCKED for
prohibiting any changes to the controls or their configuration values. If
the organizational security policy requires different configuration values
or changes to the policy, please make a copy of this policy and modify the
configured values for the required controls as per the need of the
organization's security/configuration policy.\n\nIn the case of CIS-
required Control duplication (where a Control requirement appears in more
than one section of the benchmark), Policy Editor limits the existence of
any Controls within a single policy to one (1) occurrence of each
control.\n\nCIS has stated that these settings should be considered as
minimum allowable values; if an Organization requires more stringency than
the CIS minimum, these more restrictive and/or stringent values shall all
be considered as a PASS. The settings assigned to any given control by CIS
are not guaranteed to be appropriate for any particular environment and
all settings should be reviewed and applied according to the needs of the
business. Before you apply the recommendations from the policy, check the
relevant vendor documentation to avoid discrepancies. Also, it is
recommended that these values be tested before applying to the Production
Environment.\n\nAdditional Notes:\n\n1. Being procedural, the following
requirements are not part of the policy:\n5.1.1.5\n\n2. The following list
of Manual types of checks from the benchmark is set as INACTIVE in the
policy.\n1.2.1, 1.2.3, 1.2.4, 1.2.5, 2.2.22, 3.1.1, 3.4.2.3, 3.4.2.4,
4.4.3.2.3, 5.1.3, 5.1.1.2, 5.1.1.3, 5.1.1.5, 5.1.1.6, 5.1.2.1.1,
5.1.2.1.2, 5.1.2.1.3, 5.1.2.5, 5.1.2.6, 5.2.3.21, 6.1.13, 6.1.14\n\n3. The
following requirements in the policy are configured with default values of
'.*' or '.+' as the configuration is specific to the needs of an
organization. They should be reviewed and configured per the business's
needs and the organization's security policies.\n1.2.1, 1.2.5, 1.8.2,
2.2.22, 3.4.2.3, 5.1.1.6, 5.1.2.1.2, 5.1.3, 5.2.2.1, 6.1.13, 6.1.14\n\n4)
The controls for all the requirements are configured as per the CIS
recommendation. If you have any alternative methods implemented for the
```

```
CIS checks through which CIS requirements are met, you can find the
controls from the library and replace the controls in this policy by
importing the policy and create their own customized policy or you can
take an exception for those CIS checks.\n\n5) For the 4.2.2 requirement,
the group name is considered as \"ssh_keys|_?ssh\" as specified by CIS. If
you have any other designated group name for SSH, you can include it in
this requirement's regex.\n\nE.g.\n - For firewalls, the firewalld,
nftables and iptables cannot be used at the same time. So if you are using
firewalld, you can remove/reconfigure the controls for iptables and
nftables or take an exception for those CIS checks.\n - For logging, the
requirements in the benchmark may be separated between journald and
rsyslog. So if you are using journald, you can remove/reconfigure the
controls for rsyslog or take an exception for those CIS checks.",
  "technologies": [
    {
      "technologyId": 217,
      "technologyName": "Red Hat Enterprise Linux 8.x"
    }
  ],
  "sections": [
    {
      "sectionNumber": 1,
      "sectionHeading": "Initial Setup",
      "controls": [
        {
          "controlId": 28951,
          "sectionNumber": 1,
          "controlNumber": 1,
         "statement": "Status of the cramfs kernel module available in any
installed kernel",
          "criticality": "SERIOUS",
          "isControlDisable": false,
          "referenceText": "1.1.1.1.a",
          "technologies": [
            {
              "technologyId": 217,
              "technologyName": "Red Hat Enterprise Linux 8.x",
              "evaluate": {
                "dp": {
                  "k": "oel9.secman.general.kernel_module_cramfs",
                  "v": [".+"],
                  "l": 0,
                  "description": "The List String value of <B>X</B>
indicates the status of the file system <B>cramfs kernel module</B> loaded
in the kernel using <b>lsmod</b> utility.",
                  "op": "xre",
                  "cd": "does not contain",
                  "fv": [
                    {
                      "value": "161803399999999",
                      "set": "1",
                      "description": "Module exists but is not loaded"
                    },
                    {
```

```
                    "value": "3141592653589 79",
                    "set": "1",
                    "description": "Module does not exist"
                  }
                ]
              }
            },
            "remediation": "Configure this setting as per the business
requirements or the organization's security policy.\n\nEdit or create the
file /etc/modprobe.d/CIS.conf and add the following line as
appropriate:\ninstall cramfs /bin/true",
             "rationale": "Cramfs (Compressed ROM File System) is a read-
only file system designed for use in embedded systems and situations where
storage space is limited. Misconfiguration can lead to security risks such
as unauthorized access to sensitive data, data corruption, or exploitation
of vulnerabilities. Configure this setting based on business requirements
or security policy."
          }
        ]
      },
      {
        "controlId": 29271,
        "sectionNumber": 1,
        "controlNumber": 2,
        "statement": "Status of 'install cramfs' setting from
'/lib/modprobe.d/*.conf /etc/modprobe.d/*.conf /run/modprobe.d/*.conf'",
        "criticality": "SERIOUS",
        "isControlDisable": false,
        "referenceText": "1.1.1.1.b",
        "technologies": [
          {
            "technologyId": 217,
            "technologyName": "Red Hat Enterprise Linux 8.x",
            "evaluate": {
              "dp": {
                "k": "oel9.secman.install_module_cramfs",
                "v": [
                  ".+:\\s*install\\s+cramfs\\s+/bin/(true|false)"
                ],
                "l": 0,
                "description": "The List String value of <B>X</B>
indicates the status of the <B>cramfs kernel module</B>.",
                "op": "xre",
                "cd": "matches",
                "fv": [
                  {
                    "value": "161803399999999",
                    "set": "0",
                    "description": "Setting not found"
                  },
                  {
                    "value": "3141592653589 79",
                    "set": "1",
                    "description": "Module does not exist"
```

```
                    }
                  ]
                }
              },
             "remediation": "Configure this setting as per policy.\n\n1.
Add this line to /etc/modprobe.d/cramfs.conf:\ninstall cramfs
/bin/false\n2. Add this line:\nblacklist cramfs\n3. Run:\nsudo rmmod
cramfs",
              "rationale": "The cramfs kernel module is used to mount
compressed read-only filesystems. Misconfiguration may expose the system
to security risks including unauthorized access and denial of service.
Configure this based on business requirements."
            }
          ]
        }
      ]
    }
  ]
}
```


Import Library Policy

/pcas/v1/library/policy/import

[POST]

Using this API, you can import a library policy with configurable options, such as selecting specific technology IDs, importing the policy in an unlocked state, activating it immediately, and optionally assigning a custom policy title.

Input Parameters

Parameter	Description
Authorization	(Required) Enter the Bearer token.
policyId={value}	(Optional) Specify the policy ID generated using the Library Policy Details API for which the details are to be imported.
technologyId={value}	(Optional) Specify the technology ID associated with the policy for which the details are to be imported. Note: If no technology ID is provided, the details of the mapped technologies for the policy are imported.
importAsUnlocked={true|false}	(Optional) Specify 'true' to import policy as unlocked. Specify 'false to import policy as locked.
activatePolicy={true|false}	(Optional) Specify 'true' to import policy as active. Specify 'false to import policy as inactive.
policyTitle={value}	(Optional) Add a title for the policy.

Sample - import a library policy

API request:

```
curl --location '<qualys_base_url>/pcas/v1/library/policy/import'\
--header 'accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer <AuthToken>'
\
--data ' {
"policyId": "<policyId>",
"technologyIds": [
"<technologyId>"
],
"importAsUnlocked": true,
"activatePolicy": true,
"policyTitle": "New policy api"
}'
```

JSON output:

```
{
  "message": "Policy imported successfully",
  "policyId": 1666428,
  "imported": true,
  "active": true
}
```

Users and Activity Log

Add, update, and list users in your subscription and also change password.

User List

Add/Edit User

Change Login Password

Accept Qualys EULA

Activate/Deactivate Users

User Password Change

Export User Activity Log

User List

/msp/user_list.php

[GET] [POST]

View the users in the subscription. XML responses provides details about each user such as the user's login ID, account info, assigned asset groups, permissions. Session based authentication is not supported using this API.

When the API request is made by a Manager or Unit Manager, the last login date for each user is provided in the XML results. This is the most recent date and time the user logged into the service. For a Manager, the last login date appears for all users in the subscription. For a Unit Manager, the last login date appears for all users in the Unit Manager's same business unit.

Permissions - Managers and Administrators can view all users in subscription. See Sub-user Permissions - Reader/ Unit Manager/ Scanner/ Auditor for full details.

Express Lite - This API is available to Express Lite users.

Sub-user Permissions - Reader/ Unit Manager/ Scanner/ Auditor

If the **Restrict view of user information for users outside of business unit** flag is disabled, the sub-users (Reader/ Unit Manager/ Scanner/ Auditor) can view only partial user account details for users outside of their business unit though the list will be populated with all users.

If the **Restrict view of user information for users outside of business unit** flag is enabled, the sub-users (Reader/ Unit Manager/ Scanner/ Auditor) are restricted from accessing user information outside their business unit.

The following table describes the amount of detail visible to sub-users (Unit Manager, Scanner, Reader, Auditor) based on whether the sub-users has a restricted or unrestricted view.

	Amount of Detail Visible	
User Type Being Viewed	**Unrestricted View**	**Restricted View**
Users from the same business unit	Full	Full
Users from different business unit	Partial	None

Full user account details include: user login, general information, assigned asset groups, user role, business unit, the Unit Manager Point of Contact (POC), the Manager POC, extended permissions and email notifications.

With a Partial view, the following details are not visible: user login, user ID, external ID, extended permissions, and email notifications.

Input Parameters

Parameter	Description
external_id_contains={string}	(Optional) Show only user accounts with an external ID value that contains a certain string. The string you specify can have a maximum of 256 characters. The characters can be in uppercase, lowercase or mixed case (the service performs case sensitive matching). HTML or PHP tags cannot be included. Only one of these parameters may be specified for a single API request: external_id_contains or external_id_assigned.
external_id_assigned={0|1}	(Optional) Specify 1 to show only user accounts which have an external ID value assigned. Specify 0 to show only user accounts which do not have an external ID value assigned. Only one of these parameters may be specified for a single API request: external_id_contains or external_id_assigned.
show_access_permissions={integer}	(Optional) Include access permission info (GUI, API, SAML). Specify 1 to include. Specify 0 to exclude. Default is 0.

DTD

<platform API server>/user_list_output.dtd

Add/Edit User

/msp/user.php

[GET] [POST]

Add a user account or edit an existing account. You can add users to the "Unassigned" business unit or an existing, custom business unit. For each new account (except when the user role is Contact) the service automatically generates login credentials, including a login ID and "strong" password.

Permissions -Mangers can add/edit user accounts in any business unit. Unit Managers can add/edit users in their own business unit. Administrators can add/edit user all accounts except Manager and Administrator user.

Express Lite - This API is available to Express Lite users. A total of 3 users can be added per subscription.

Adding user to custom business unit

To add users to a custom business unit, follow these steps:

- With a Manager or user administrator account, log into the Qualys user interface and create the business unit. Note business units may be created using the Qualys user interface only.

- If a Unit Manager is not already assigned to the business unit, you must add one. With a Manager account, make a user.php request to add a Unit Manager who is automatically assigned as the business unit's point of contact (POC).

- With a Manager or Unit Manager account, make a user.php request to add other users to the custom business unit. A Manager and user administrator can add a user to any business unit, while a Unit Manager can add a user to their own business unit.

Delivery of new account credentials to user

When adding a new user (except Contact), the API user has the option to deliver login credentials directly to the user via email or through the application as follows.

Email notification - By default the user.php function sends the new user an email notification with a secure link to their login credentials. When the user clicks the secure link to view the credentials, the service changes the account status automatically from "Pending Activation" to "Active".

XML output - Instead of sending an email notification, the API user has the option to return the new user's login credentials in the XML output document. To do this, make a user.php request with the send_email=0 input parameter. As a result the service returns the user's login ID and password as XML value pairs in the XML output, and the account status is automatically set to "Active".

First login completes account registration

To complete account registration, a new user must log into the Qualys user interface with their assigned login information (platform URL and login credentials). When the user has been created using the user.php function the user can login using the Qualys user interface or using the acceptEULA.php API function. See “Change Login Password” and “Accept Qualys EULA” or more information.

Editing accounts - edit and clear options

For an existing account, you can edit and clear account parameters as follows.

Edit Parameters - An existing user may be edited using user.php to update the user name and general information. Additional parameters can be edited using the Qualys user interface. When editing parameters using user.php, existing parameter values are replaced with newly specified ones. For example, if you edit an existing Scanner with the assigned asset group “New York” and you wish to add the asset group “Hong Kong”, then the edit request would include asset_groups=New+York,Hong+Kong. An edit request can be used to clear (reset) parameters by assigning the empty string ““.

Input Parameters

Parameter	Description
action=add|edit	(Required) A flag indicating an add or edit request. Specify “add” to add a new user, or “edit” to edit an existing user.
login={login}	(Required for Edit, not valid for Add) Specifies the Qualys user login of the user account you wish to edit. This parameter is invalid for an add request.

New User - Login Credentials

Parameter	Description
send_email={0|**1**}	(Optional for Add, not valid for Edit) Specifies whether the new user will receive an email notification with a secure link to their login credentials. This parameter is invalid when the user role is Contact. 1 — (the default) specifies that an email notification will be sent to the new user. The user clicks a secure link in the email to view the login ID and password. 0 — specifies that an email notification will not be sent to the new user, and the XML report returned by the function will include the login ID and password for the user account as XML value pairs.

Permissions

Parameter	Description
user_role={role}	(Required for Add, not valid for Edit, not valid for Express Lite users) Specifies the user role. A valid value is: manager, unit_manager, scanner, reader, contact or administrator. The first user added to a new custom business unit must be unit_manager. This parameter accepts a valid user role. No html tags.
business_unit={title}	(Required for Add, not valid for Edit, not valid for Express Lite user) Specifies the user's business unit. A valid value is "Unassigned", or the title of an existing custom business unit. Note a custom business unit may be added using the Qualys user interface. This parameter accepts a valid business unit. No html tags . should be valid business_unit.
asset_groups={grp1,grp2...}	(Optional) Specifies the asset groups assigned to the user, when the user role is Scanner, Reader or Contact. Multiple asset groups are comma separated. This parameter is invalid when the user role is Manager or Unit Manager.

General Information

Parameter	Description
first_name={name}	(Required for Add, Optional for Edit) Specifies the user's first name. The name may include a maximum of 50 characters. This parameter accepts alphabets,numbers, comma(,) ,dot(.) , dash (-), and space only . No html tags.
last_name={name}	(Required for Add, Optional for Edit) Specifies the user's last name. The name may include a maximum of 50 characters. This parameter accepts alphabets,numbers, comma(,) ,dot(.) , dash (-), and space only. No html tags
title={title}	(Required for Add, Optional for Edit) Specifies the user's job title. The title may include a maximum of 100 characters. This parameter accepts alphabets,numbers, comma(,) ,dot(.) , dash (-), and space only. No html tags .
phone={value}	(Optional for Add and Edit) Specifies the user's phone number. This value may include a maximum of 40 characters. This parameter accepts numbers, and special chars + - ( ) and space only. No html tags .
fax={value}	(Optional) The user's FAX number. This value may include a maximum of 40 characters.

Parameter	Description
email={value}	(Required for Add, Optional for Edit) Specifies the user's email address. The address must be a properly formatted address with a maximum of 100 characters. This parameter accepts valid email address only. No html tags.
address1={value}	(Required for Add, Optional for Edit) Specifies the user's address line 1. This value may include a maximum of 80 characters. This parameter accepts alphabets,numbers,( ), comma(,) ,dot(.) , dash (-), and space only. No html tags .
address2={value}	(Optional) Specifies the user's address line 2. This value may include a maximum of 80 characters. This parameter value accepts alphabets,numbers,( ), comma(,) ,dot(.) , dash (-), and space only. No html tags .
city={value}	(Required for Add, Optional for Edit) Specifies the user's city. This value may include a maximum of 50 characters. This parameter accepts alphabets,numbers,( ), comma(,) ,dot(.) , dash (-), and space only. No html tags .
country={code}	(Required for Add, Optional for Edit) Specifies the user's country code. See "Sample - Add user" to find an appropriate country code. This parameter accepts a valid country code. No html tags .
state={code}	(Required for Add for some country codes, Optional for Edit) Specifies the user's state code. A valid value depends on the country code specified for the country parameter. You must enter a state code using the state parameter when the country code is one of: "United States of America", "Australia", "Canada" or "India". See State Codes for United States For other country codes, a state code does not need to be specified using the state parameter. See State codes. You can enter the state code "none" (optional). This parameter accepts a valid state code. No html tags.
zip_code={zipcode}	(Optional) Specifies the user's zip code. This value may include a maximum of 20 characters. If not specified, this is set to the zip code in the API user's account.
external_id={value}	(Optional) Specify a custom external ID value. The external ID value can have a maximum of 256 characters, and it is case sensitive. The characters can be in uppercase, lowercase or mixed case. HTML or PHP tags cannot be included. Specify external_id= or external_id="" to delete an external ID value from an existing account.

Sample - Add user

Add a new user, Chris Washington, to the Unassigned business unit with the Scanner user role, and automatically send the user an email notification with a secure link to his login credentials.

API request:

```
https://qualysapi.qualys.com/msp/user.php?action=add&user_role=sca
nner&business_unit=Unassigned&first_name=Chris&last_name=Washingto
n&title=Security+Consultant&phone=2126667777&fax=2126667778&email=
chris@mycompany.com&address1=500+Charles_Avenue&address2=Suite+126
0&city=New+York&country=United+States+of+America&state=New+York&zi
p_code=10004
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE USER_OUTPUT SYSTEM
"https://qualysapi.qualys.com/user_output.dtd">
<USER_OUTPUT>
  <API name="user.php" username="sabkl_av1" at="2018-07-
20T22:54:25Z" />
  <RETURN status="SUCCESS">
    <MESSAGE>quays_cw4 user has been successfully
created.</MESSAGE>
  </RETURN>
</USER_OUTPUT>
```

Sample - Edit user to change title

API request:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&login=quays_
ch&title=CIO
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE USER_OUTPUT SYSTEM
"https://qualysapi.qualys.com/user_output.dtd">
<USER_OUTPUT>
  <API name="user.php" username="sabkl_av1" at="2018-07-
20T23:06:35Z" />
  <RETURN status="SUCCESS">
    <MESSAGE>quays_ch user has been successfully
updated.</MESSAGE>
  </RETURN>
</USER_OUTPUT>
```

Sample - External ID

Add the external ID "Qualys123" to the existing user account "qualys_ab5" when that account does not already have an external ID:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=Qualys123
```

Add the external ID "Qualy123" to the existing user account "qualys_ab" when that account already has an external ID:

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=Qualys123
```

Delete the external ID currently defined for the user account "qualys_ab5":

```
https://qualysapi.qualys.com/msp/user.php?action=edit&
login=qualys_ab5&external_id=
```

Sample - Set Timezone

Assign a timezone to a user using the optional parameter "time_zone_code".

Sample - Set specific timezone (i.e. pass timezone code)

```
https://qualysapi.qualys.com/msp/user.php?action=add&user_role=sca
nner&business_unit=Unassigned&asset_groups=New+York,Dallas&first_n
ame=Chris&last_name=Woods&title=Security+Consultant&phone=21266677
77&fax=2126667778&email=chris@mycompany.com&address1=500+Charles_A
venue&address2=Suite+1260&city=New+York&country=United+States+of+A
merica&state=New+York&zip_code=10004&time_zone_code=US-NY
```

Sample - Set user profile to browser's timezone (i.e. pass empty/null)

```
https://qualysapi.qualys.com/msp/user.php?action=edit&login=acme_a
b&time_zone_code="
```

Looking for timezone codes? Use the time zone code list function to request the list:

<platform API server>/msp/time_zone_code_list.php

DTD

<platform API server>/user_output.dtd

Default Parameters - New User

Several user parameters are set automatically when a new user is created. These are identified below. The parameter value *** is the value defined for the user account making the API request.

	Manager	Unit Manager	Adminis-trator	Scanner	Reader	Contact
General and User Role						
Zip code	***	***	***	***	***	***
Company	***	***	***	***	***	***
Language - KnowledgeBase	***	***	***	***	***	***
User Status	Pending activation	Pending activation	Pending activation	Pending activation	Pending activation	Active
Allow access to	GUI and API	GUI and API	GUI and API	GUI and API	GUI and API	n/a
Notification Options						
Latest Vulnerabilities	Weekly	Weekly	n/a	Weekly	Weekly	Weekly
Scan Summary	All	Scans on assigned groups	n/a	Scans on assigned groups	Scans on assigned groups	Scans on assigned groups
Map Summary	All	Maps on assigned groups	n/a	Maps on assigned groups	Maps on assigned groups	Maps on assigned groups
Daily Trouble Ticket Updates	NO	NO		NO	NO	n/a
Extended Permissions						
Add assets	n/a	NO	n/a	n/a	n/a	n/a
Create option profiles	n/a	YES	n/a	YES	n/a	n/a
Purge host information/histo ry	n/a	NO	n/a	NO	n/a	n/a
Create/edit remediation policy	n/a	NO	n/a	n/a	n/a	n/a
Create/edit authentication records	n/a	NO	n/a	n/a	n/a	n/a

Country codes

Afghanistan | Albania | Algeria | Andorra | Angola | Anguilla | Antartica | Antigua and Barbuda | Argentina | Armenia | Aruba | Australia | Austria | Azerbaijan | Bahamas | Bahrain | Bangladesh | Barbados | Belarus | Belgium | Belize | Benin | Bermuda | Bhutan | Bolivia | Bosnia-Herzegovina | Botswana | Bouvet Island | Brazil | British Indian Ocean Territory | Brunei Darussalam | Bulgaria | Burkina Faso | Burundi | Cambodia | Cameroon | Canada | Cape Verde | Cayman Islands | Central African Republic | Chad | Chile | China | Christmas Island | Cocos (Keeling) Islands | Colombia | Comoros | Congo | Cook Islands | Costa Rica | Cote D'Ivoire | Croatia | Cuba | Cyprus | Czech Republic | Denmark | Djibouti | Dominica | Dominican Republic | East Timor | Ecuador | Egypt | El Salvador | Equatorial Guinea | Estonia | Ethiopia | Faeroe Islands | Falkland Islands (Malvinas) | Fiji | Finland | France | French Guiana | French Polynesia | French Southern Territories | Gabon | Gambia | Georgia | Germany | Ghana | Gibraltar | Greece | Greenland | Grenada | Guadeloupe | Guatemala | Guernsey, C.I. | Guinea | Guinea-Bissau | Guyana | Haiti | Heard and McDonald Islands | Honduras | Hong Kong | Hungary | Iceland | India | Indonesia | Iran (Islamic Republic of) | Iraq | Ireland | Isle of Man | Israel | Italy | Jamaica | Japan | Jersey, C.I. | Jordan | Kazakhstan | Kenya | Kiribati | Korea | Kuwait | Kyrgyzstan | Lao Peoples Democratic Republi | Latvia | Lebanon | Lesotho | Liberia | Libyan Arab Jamahiriya | Liechtenstein | Lithuania | Luxembourg | Macau | Macedonia | Madagascar | Malawi | Malaysia | Maldives | Mali | Malta | Marshall Islands | Martinique | Mauritania | Mauritius | Mexico | Micronesia, Fed. States of | Moldova, Republic of | Monaco | Mongolia | Montserrat | Morocco | Mozambique | Myanmar | Namibia | Nauru | Nepal | Netherland Antilles | Netherlands | Neutral Zone (Saudi/Iraq) | New Caledonia | New Zealand | Nicaragua | Niger | Nigeria | Niue | Norfolk Island | Northern Mariana Islands | Norway | Oman | Pakistan | Palau | Panama Canal Zone | Panama | Papua New Guinea | Paraguay | Peru | Philippines | Pitcairn | Poland | Portugal | Puerto Rico | Qatar | Reunion | Romania | Russia | Rwanda | Saint Kitts and Nevis | Saint Lucia | Samoa | San Marino | Sao Tome and Principe | Saudi Arabia | Senegal | Seychelles | Sierra Leone | Singapore | Slovak Republic | Slovenia | Solomon Islands | Somalia | South Africa | Spain | Sri Lanka | St. Helena | St. Pierre and Miquelon | St. Vincent and the Grenadines | Sudan | Suriname | Svalbard and Jan Mayen Islands | Swaziland | Sweden | Switzerland | Syrian Arab Republic | Taiwan | Tajikistan | Tanzania, United Republic of | Thailand | Togo | Tokelau | Tonga | Trinidad and Tobago | Tunisia | Turkey | Turkmenistan | Turks and Caicos Islands | Tuvalu | U.S.Minor Outlying Islands | Uganda | Ukraine | United Arab Emirates | United Kingdom | United States of America | Uruguay | Uzbekistan | Vanuatu | Vatican City State | Venezuela | Vietnam | Virgin Islands (British) | Wallis and Futuna Islands | Western Sahara | Yemen | Yugoslavia | Zaire | Zambia | Zimbabwe

State codes

State Codes for United States

Value state codes when country is “United States of America”:

Alabama | Alaska | Arizona | Arkansas | Armed Forces Asia | Armed Forces Europe | Armed Forces Pacific | California | Colorado | Connecticut | Delaware | District of Columbia | Florida | Georgia | Hawaii | Idaho | Illinois | Indiana | Iowa | Kansas | Kentucky | Louisiana | Maine | Maryland | Massachusetts | Michigan | Minnesota | Mississippi | Missouri | Montana | Nebraska | Nevada | New Hampshire | New Jersey | New Mexico | New York | North Carolina | North Dakota | Ohio | Oklahoma | Oregon | Pennsylvania | Rhode Island | South Carolina | South Dakota | Tennessee | Texas | Utah | Vermont | Virginia | Washington | West Virginia | Wisconsin | Wyoming

State Codes for Australia

Valid state codes when country is “Australia”:

No State | New South Wales | Northern Territory | Queensland | Tasmania | Victoria | Western Australia

State Codes for Canada

Valid state codes when country is “Canada”:

No State | Alberta | British Columbia | Manitoba | New Brunswick | Newfoundland | Northwest Territories | Nova Scotia | Nunavut | Ontario | Prince Edward Island | Quebec | Saskatchewan | Yukon

State Codes for India

Valid state codes when country is “India”:

No State | Andhra Pradesh | Andaman and Nicobar Islands | Arunachal Pradesh | Assam | Bihar | Chandigarh | Chattisgarh | Dadra and Nagar Haveli | Daman and Diu | Delhi | Goa | Gujarat | Haryana | Himachal Pradesh | Jammu and Kashmir | Jharkhand | Karnataka | Kerala | Ladakh | Lakshadweep | Madhya Pradesh | Maharashtra | Manipur | Meghalaya | Mizoram | Nagaland | Orissa | Pondicherry | Punjab | Rajasthan | Sikkim | Tamil Nadu | Telangana | Tripura | Uttar Pradesh | Uttaranchal | West Bengal

Change Login Password

/api/2.0/fo/user/change_password/

[POST]

This API simplifies password management by enabling users to update their existing passwords to a new one of their choice. This enhancement strengthens security practices, and offers a more seamless user experience by integrating password management directly into existing workflows.

When any user logs in to their subscription and changes their login password, the password can be changed only three times in an hour. If there is an attempt to exceed this limit, an error message is returned in the API response.

Note: This API is restricted to JWT token authentication. You must change the password using basic authentication only. Otherwise, it returns the following error in the response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "<qualys_base_url>/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-25T06:54:32Z</DATETIME>
        <CODE>2010</CODE>
        <TEXT>Please use basic authentication, as this endpoint doesn't
support JWT authentication.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Input Parameters

Parameter	Description
newPassword={value}	(Required) The new password for the user (formatted as JSON)

Sample 1- Change Password successfully

API Request

```
curl --location
'<qualys_base_url>/api/2.0/fo/user/change_password/index.php' \
--header 'X-Requested-With: test' \
--header 'Content-Type: application/json' \
--data '{
    "newPassword": "abcd123#"
}'
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd>"

    <SIMPLE_RETURN>
```

```
        <RESPONSE>
            <DATETIME>2024-08-23T05:18:08Z</DATETIME>
            <TEXT>Password changed successfully</TEXT>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample 2 - Rate limit to Change Password

API Request

```
curl --location
'<qualys_base_url>/api/2.0/fo/user/change_password/index.php' \
--header 'X-Requested-With: test' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic Encoded username:passwordstring' \
--data '{
    "newPassword": "xxxxxxx"
}
```

XML Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2026-02-25T05:51:34Z</DATETIME>
        <CODE>1905</CODE>
        <TEXT>You've reached the maximum number of password reset
attempts. Try again in 59 minutes to keep your account secure.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

User Registration Process

When a new user account is created, the service by default sends the user an email titled "Registration - Start Now". This email includes a secure link to the user's login information including platform URL and login credentials. Instead of sending an email notification, the API user has the option to return login credentials using user.php function with the send_email=0 input parameter.

The user must complete the first login to the service in order to complete the account registration and accept the Qualys EULA (End User License Agreement). When the first login is completed, the service sends the user an email titled "Registration - Complete".

A new user has the option to complete the first login by simply logging into the Qualys user interface, as long as the user is granted the GUI access method. (Note a new user created using the user.php function is automatically granted the GUI and API access methods.) Using the Qualys user interface, the user is directed to the First Login form to complete the registration and accept the Qualys EULA.

The acceptEULA.php API function is provided as a programmatic method for completing the registration and accepting the Qualys EULA. To use complete the first login using the acceptEULA.php function, the user must submit an API request using their platform URL and login credentials.

Important: If a new user account is created using the Qualys user interface and the account is granted the API access method only (without the GUI access method), the user must complete the first login using the acceptEULA.php API function. If the acceptEULA.php API request is not made or it is not successful, the new account will not be activated and any API requests submitted using the new account will fail.

Accept Qualys EULA

/msp/acceptEULA.php

[GET] [POST]

Allows Qualys users to complete the registration process and accept the Qualys End User License Agreement (EULA) on behalf of their customers. This function provides programmatic acceptance of the Qualys EULA.

Note: Qualys End User Licence Agreement (EULA) must be accepted with basic authentication. Once accepted, msp and VM, PA APIs from V2.0 onwards work with JWT token authentication. Otherwise, it returns an ACCESS DENIED error.

A new user can complete the registration process and accept the Qualys EULA through the Qualys user interface as long as their account is granted the GUI access method. (Note a new user created using the user.php function is automatically granted the GUI and API access methods.) Optionally, a new user can complete the registration and accept the Qualys EULA using the acceptEULA.php function. See Change Login Password

A Web application that allows Qualys EULA acceptance can be setup as follows. Inside the third party web application, a developer can setup a Web form that displays the Qualys EULA and has an "I Accept" button. A new Qualys user opens the Web form in a browser, reads the EULA description and clicks "I Accept" in the Web form. The third party's program submits an HTTP request to the Qualys API server using the acceptEULA.php. Along with the acceptEULA.php URL, the application must send Qualys user account credentials (login and password) as part of the HTTP request.

Permissions - Any user with permission to log in to Qualys can complete the registration and accept the EULA.

Sample - Accept the Qualys EULA on behalf of a user

API request:

```
https://qualysapi.qualys.com/msp/acceptEULA.php
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC_RETURN SYSTEM
"https://qualysapi.qualys.com/generic_return.dtd">
<GENERIC_RETURN>
<API name="acceptEULA.php" username="rob" at="2018-05-
10T13:44:23" />
<RETURN status="SUCCESS">
      TNC accepted within MSP
 </RETURN>
</GENERIC_RETURN>
```

DTD

<platform API server>/generic-return.dtd

Activate/Deactivate Users

/msp/user.php

[GET] [POST]

Activate and deactivate user accounts. A user with inactivate status can be activated. A user with active status can be deactivated. Session based authentication is not supported using this API.

These actions correspond to the activate/deactivate options in the Qualys UI. Note new accounts are activated by default after the user completes the account activation process (registration) by logging into the service for the first time.

Permissions -Mangers can activate/deactivate all users in subscription. Unit Managers can activate/deactivate users in their own business unit. Administrators can activate/deactivate all users except Manager and Administrator user.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
action=activate|deactivate	(Required) A flag indicating the desired action. Specify "activate" to activate a user account that has an "Inactive" status, or specify "deactivate" to deactivate a user account that has an "Active" status. When an account is deactivated, the user's account settings will not be deleted. A user account cannot be activated or deactivated if the account status is "Pending Activation".
login={login}	(Required) Specifies the Qualys user login for the user account you wish to activate or deactivate.

Samples

Deactivate the user account "qualys_ab3" (and this account has an "Active status):

```
https://qualysapi.qualys.com/msp/user.php?action=deactivate&
login=qualys_ab3
```

Activate the user account "qualys_ab3" (and this account has an "Inactive" status):

```
https://qualysapi.qualys.com/msp/user.php?action=activate&
login=qualys_ab3
```

DTD

<platform API server>/user_output.dtd

User Password Change

/msp/password_change.php

[GET] [POST]

Change passwords for all or some users in the same subscription. Many Qualys customers have an internal security policy requirement to change passwords for users at a particular time interval. Changing password for multiple users at once as batch process is supported. New passwords are automatically generated by the service.

Note: When a user changes the password of a sub-user, the password can be changed only three times within an hour. If this limit is exceeded, the API returns an error message in the response.

It's possible to change passwords for user accounts with a status of "active", "inactive" or "pending activation". It's not possible to change passwords for deleted accounts. Since Contact users do not have login access to Qualys, it's not possible to change passwords for Contacts.

A password change API request returns a password change XML report indicating the user accounts affected and whether password changes were made for each account. A success message is included when passwords were changed on all target accounts. A warning message is included if passwords for any of the target accounts could not be changed. Upon error, an error message is included.

By default the password changes made by the password_change.php API causes the service to automatically send each affected user an email which notifies them of the password change. If you do not wish users to receive this email notification, you have the option to return the user login ID and password for affected users as XML value pairs in the password change report. To do this, make a password_change.php request and specify the email=0 parameter. If you make such a request on an account with the status "pending activation", the function automatically assigns the "active" status since the login credentials are available in the XML report.

Note: This API is restricted to JWT token authentication. You must change the password using basic authentication only. Otherwise, it returns the following error in the response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "<qualys_base_url>/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2025-09-25T06:54:32Z</DATETIME>
        <CODE>2010</CODE>
        <TEXT>Please use basic authentication, as this endpoint doesn't
support JWT authentication.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Permissions - Managers can change passwords for all users in subscription, except the user making the request. Unit Managers can change passwords for all users in same business unit, except the user making the request. Administrators can change passwords for all users in subscription, except Manager, Administrator, and the user making the request.

Express Lite - This API is available to Express Lite users.

Input Parameters

Parameter	Description
user_logins={value}	(Required) Specifies one or more QualysGuard user login IDs of target user accounts. Multiple user login IDs are comma separated. Specify user_logins=all to change the password for all users in the user's account, except the requesting user. See Permissions
email={0|1}	(Optional) Specifies whether users will receive an email notification alerting them to the password change. 1 — (the default) specifies that an email notification will be sent to affected users. Each user clicks a secure link in the email to view the new password. 0 — specifies that email notifications will not be sent to affected users, and the XML report returned by the function will include the login ID and password for each user account as XML value pairs.

Sample 1 - Change Password Request, Send Email

Make a password change request for two accounts and send affected users an email notification including a secure link to their new password:

API Request

```
curl -s -S -H 'Requested-With:curl demo2' -u "username:passwordstring"
 "https://<qualys_base_url>/msp/password_change.php?user_logins=username1
,username2"
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PASSWORD_CHANGE_OUTPUT SYSTEM "https://
<qualys_base_url>/password_change_output.dtd">
    <PASSWORD_CHANGE_OUTPUT>
        <API name="password_change.php" username="username" at="2026-03-
06T07:36:55Z" />
        <RETURN status="SUCCESS">
            <MESSAGE>The operation was successfully completed</MESSAGE>
            <CHANGES count="2">
                <USER_LIST>
                    <USER>
                        <USER_LOGIN>username1</USER_LOGIN>
                    </USER>
```

```
                    <USER>
                        <USER_LOGIN>username2</USER_LOGIN>
                    </USER>
                </USER_LIST>
            </CHANGES>
        </RETURN>
    </PASSWORD_CHANGE_OUTPUT>
```

Sample 2 - Rate limit to Change Password of a sub-user

API Request

```
curl -s -S -H 'Requested-With:curl demo2' -u "<username>:<password>"
 "<qualys_base_url>/msp/password_change.php?user_logins=uername&email=0"
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PASSWORD_CHANGE_OUTPUT SYSTEM "
<qualys_base_url>/password_change_output.dtd">
    <PASSWORD_CHANGE_OUTPUT>
        <API name="password_change.php" username="xxx" at="2026-02-
24T09:30:55Z" />
        <RETURN status="FAILED" number="1905">
            <MESSAGE>
              <![CDATA[Invalid value for 'user_logins' : username. You've
reached the maximum number of password reset attempts. Try again in 59
minutes to keep your account secure.]]>
            </MESSAGE>
        </RETURN>
    </PASSWORD_CHANGE_OUTPUT>
```

DTD

<platform API server>/password_change_output.dtd

Export User Activity Log

/api/2.0/fo/activity_log/

[GET] [POST]

Export the user activity log for a subscription to CSV format.

Input Parameters

Parameter	Description
action=list	(Required)
user_action={value}	(Optional) You can filter the output based on the actions. For example, login (for user login), launch (for scan launched), finished (for scan finished), etc. Refer to the other user actions available and their descriptions in User actions to filter the output. The actions which are included in the output depend on the user who runs the API. Managers see all actions taken by all users. Unit Managers see actions taken by users in their business unit. Scanners and Readers see their own actions only.
action_details={value}	(Optional) Filter on further information about the user actions. For example, for the action “error”, you can filter by the error details “No connection from scanner appliance”.
username={value}	(Optional) The name of the user who performed the action. Usernames are included in the output only if the user running the API is a Manager or a Unit Manager. A Unit Manager can see usernames only for users in the Unit Manager’s hierarchy.
since_datetime={value}	(Optional) Specify the date to include the activity log starting from that point in time. Date must be in the YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z” and must be less than or equal to today’s date.
until_datetime={value}	(Optional) Specify the date to include the activity log until a specific point in time. Date must be in the YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”, must be more than or equal to since_datetime, and less than or equal to today’s date.

Parameter	Description
user_role={value}	(Optional) A Manager or Unit Manager can choose to export logs for certain user roles instead of all user roles. Specify this parameter to export logs for users with certain user roles. Multiple roles are comma separated. User roles you can specify: - Manager - Unit Manager - Auditor - Scanner - Reader - KnowledgeBase Only - Remediation User - Contact What logs are exported by default? For a Manager logs are exported for all users (all user roles) by default. For a Unit Manager logs are exported only for users (all user roles) in the Unit Manager's hierarchy (i.e. business unit).
output_format=CSV	(Optional) CSV (default)
truncation_limit={value}	(Optional) Limit the number of log records to include in the CSV output.

User actions to filter the output

Action	Description
options	Select an option for example, load balancer detection off, HTTP process to run in parallel and so on.
set	Set configuration for example, to set title, password, user configuration and so on.
cancel	Cancel process such as cancel a scan or run a cancel report case.
add_fqdn	Activity related to adding the FQDN.
send	Send configuration like sending any information and so on.
crashed	Process crashed such as report process on the platform is crashed and so on.
disable	Disable any existing encryption for example, disabling an PDF encryption.
migrate	Status of migration for example AGMS migration status.
reboot	Reboot process like scanner rebooting.
purge	Purge process such as purging an asset.

Action	Description
logout	Action for logout of any process.
replace	Replace action for example, replacing one scanner appliance with the other.
restore	Restore process for example when you want to ignore or restore the specified vulnerabilities and so on.
cleanup	Set the cleanup process, for example, when you set up asset tracking and data merging to clean up.
update	Update action, such as updating account settings, updating default ranges, and so on.
delay	Delay in any action for example, delay in the report launch or any schedule scan.
launch	Launch any process such as scan launch, scheduled report, and so on.
request	Request action for example make any API request and so on.
log	Store the status in the log for example, storing the template setting in the log when you generate report.
del_fqdn	Deleting the FQDN.
enable	Enable the encryption for example, enablingan PDF encryption.
change	Change in the configuration such as change password and so on.
created	Create anything new for example, create new account, create new partner, and so on.
transfer	Transfer process for example when you want to transfer the subscription from one partner to another. and so on.
bind	Binding process such as binding of scanners.
success	Process completion for example when account is activated or password is reset and so on.
kill	Kill the process.
redirect	For any redirection such as redirecting to the portal.
deleted	Deleting action such as deleting user or any process.
upload	Upload any file or data.
s-count	When you execute extra asset tool.
delete	Any delete action such as delete asset group, unix/windows/oracle authetication ip address deleted and so on.
provision	Configuration of any device for example any virtual scanner appliance with a name, id and code.

Action	Description
paused	Pause in any process for example pause scan, and so on.
tnc	Accept any terms and conditions.
errors	Any error for example, error in the report or failed to encrypt
remove	Remove any information, records or data such as any assets, asset group and so on.
entity	Related to AGMS
updated	Update action for example update the partner or administrator.
scandata	Request to get any data such as request for scan data tool to collect the scan XML.
add	Perform any add action for example, add IPs to asset groups, authentication records, and so on.
create	Perform any create action such as create an authentication records, new search list and so on.
try	Try to perform some action such as retry the skipped network targets.
download	Download any information such as download report, virtual scanner image and so on.
resume	Resume any process such as to restart the scan post pause.
activate	Activate any device for example when you activate the scanner appliance.
declined	Decline any process.
search	Any search action such as searching additional asset.
error	Any type of error for example, error when executing scan, report and so on.
save	Save any actions such as policy rule and so on.
edit	Any edit action such as edit any subscriptions, tickets and so on.
pause	Pause any process for example when you pause the scan.
reset	Change in configuration such as reset scan, password.
loading	Wait for any action to load for example, execute any scan and the scan is loading.
ignore	Ignore the information, data for example ignoring the vulnerabilities when the report is generated.
decline	Decline any action.

Action	Description
accept	Accept any configuration.
enabled	Enable any setting.

Sample - Export activity log to csv format

API request:

```
curl -u "username:password" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/activity_log/?action=list
"
```

Sample CSV output:

```
"Date","Action","Module","Details","User Name","User Role","User
IP"
"2017-02-03T04:35:38Z","login","auth","user_logged
in","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:58:16Z","login","auth","user_logged
in","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:48:07Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T13:31:19Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T13:28:38Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T13:28:17Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T13:27:27Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T13:26:41Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.1
95.136"
"2017-02-02T12:52:43Z","set","host_attribute","comment=[vvv] for
11.11.11.4","saand_rn","Manager","10.113.14.208"
"2017-02-02T12:52:43Z","add","option","11.11.11.4 added to both
VM-PC license","saand_rn","Manager","10.113.14.208"
"2017-02-02T12:50:32Z","create","network","New Network:
'abc'","saand_rn","Manager","10.113.14.208"
```

Appendix A - API Documentation

Looking for details on XML output and DTDs? Download this reference

Qualys API (VM/PC) XML/DTD Reference

You can find all our latest API Documentation at the Qualys Community at Qualys Documentation

HTML documentation is available through the product for your convenience. Just log into your account, choose Help > Resources from the top menu.

Appendix B - Ports used for scanning

Here's a list of ports used by Qualys Vulnerability Management to scan your host assets.

TCP Standard Scan (about 2800 ports)

TCP Light Scan (about 160 ports)

UDP Standard Scan (about 180 ports)

UDP Light Scan (about 30 ports)

TCP Standard Scan (about 2800 ports)

1-3, 5, 7, 9, 11, 13, 15, 17-25, 27, 29, 31, 33, 35, 37-39, 41-223, 242-246, 256-265, 280-282, 309, 311, 318, 322-325, 344-351, 363, 369-581, 587, 592-593, 598, 600, 606-620, 624, 627, 631, 633-637, 666-674, 700, 704-705, 707, 709-711, 729-731, 740-742, 744, 747-754, 758-765, 767, 769-777, 780-783, 786, 799-801, 860, 873, 886-888, 900-901, 911, 950, 954-955, 990-993, 995-1001, 1008, 1010-1011, 1015, 1023-1100, 1109-1112, 1114, 1123, 1155, 1167, 1170, 1207, 1212, 1214, 1220-1222, 1234-1236, 1241, 1243, 1245, 1248, 1269, 1313-1314, 1337, 1344-1625, 1636-1774, 1776-1815, 1818-1824, 1900-1909, 1911-1920, 1944-1951, 1973, 1981, 1985-2028, 2030, 2032-2036, 2038, 2040-2049, 2053, 2065, 2067, 2080, 2097, 2100, 2102-2107, 2109, 2111, 2115, 2120, 2140, 2160-2161, 2201-2202, 2213, 2221-2223, 2232-2239, 2241, 2260, 2279-2288, 2297, 2301, 2307, 2334, 2339, 2345, 2381, 2389, 2391, 2393-2394, 2399, 2401, 2433, 2447, 2500-2501, 2532, 2544, 2564-2565, 2583, 2592, 2600-2605, 2626-2627, 2638-2639, 2690, 2700-2702, 2716, 2766, 2784-2789, 2801, 2908-2912, 2953-2954, 2967, 2998, 3000-3002, 3006-3007, 3010-3011, 3020, 3047-3049, 3080, 3127-3128, 3141-3145, 3180-3181, 3205, 3232, 3260, 3264, 3267-3269, 3279, 3306, 3322-3325, 3333, 3340, 3351-3352, 3355, 3372, 3389, 3421, 3454-3457, 3689-3690, 3700, 3791, 3900, 3984-3986, 4000-4002, 4008-4009, 4080, 4092, 4100, 4103, 4105, 4107, 4132-4134, 4144, 4242, 4321, 4333, 4343, 4443-4454, 4500-4501, 4567, 4590, 4626, 4651, 4660-4663, 4672, 4899, 4903, 4950, 5000-5005, 5009-5011, 5020-5021, 5031, 5050, 5053, 5080, 5100-5101, 5145, 5150, 5190-5193, 5222, 5236, 5300-5305, 5321, 5400-5402, 5432, 5510, 5520-5521, 5530, 5540, 5550, 5554-5558, 5569, 5599-5601, 5631-5632, 5634, 5650, 5678-5679, 5713-5717, 5729, 5742, 5745, 5755, 5757, 5766-5767, 5800-5802, 5900-5902, 5977-5979, 5997-6053, 6080, 6103, 6110-6112, 6123, 6129, 6141-6149, 6253, 6346, 6387, 6389, 6400, 6455-6456, 6499-6500, 6515, 6543, 6558, 6588, 6660-6670, 6672-6673, 6699, 6767, 6771, 6776, 6789, 6831, 6883, 6912, 6939, 6969-6970, 7000-7021, 7070, 7080, 7099-7100, 7121, 7161, 7174, 7200-7201, 7300-7301, 7306-7308, 7395, 7426-7431, 7491, 7511, 7777-7778, 7781, 7789, 7895, 7938, 7999-8020, 8023, 8032, 8039, 8080-8082, 8090, 8100, 8181, 8192, 8200, 8383, 8403, 8443, 8450, 8484, 8500, 8732, 8765, 8886-8894, 8910, 9000-9002, 9005, 9043, 9080, 9090, 9098-9100, 9400, 9443, 9495, 9535, 9570, 9872-9876, 9878, 9889, 9989-10002, 10005, 10007, 10080-10082, 10101, 10202, 10204, 10520, 10607, 10666, 11000-11002, 11004, 11223, 12000-12002, 12076, 12223, 12287, 12345-12346, 12361-12362, 12456, 12468-12469, 12631, 12701, 12753, 13000, 13333, 14237-14238, 15858, 16384, 16660, 16959, 16969, 17000, 17007, 17300, 18000, 18181-18186, 18190-18192, 18194, 18209-18210, 18231-18232, 18264, 19541, 20000-20001, 20011, 20034, 20200, 20203, 20331, 21544, 21554, 21845-21849, 22222, 22273, 22289, 22305, 22321, 22555, 22800, 22951, 23456, 23476-23477, 25000-25009, 25252, 25793, 25867, 26000, 26208, 26274, 26409, 27000-27009, 27374, 27665, 29369, 29891, 30029, 30100-30102, 30129, 30303, 30999, 31336-31337, 31339, 31554, 31666, 31785, 31787-31788, 32000, 32768-32790, 33333, 33567-33568, 33911,

34324, 37651, 40412, 40421-40423, 42424, 44337, 47557, 47806, 47808, 49400, 50000-50001, 50505, 50766, 51102, 51107, 51112, 53001, 54320-54321, 57341, 60008, 61439, 61466, 62078, 65000, 65301, 65512

TCP Light Scan (about 160 ports)

11, 13, 15, 17, 19-23, 25, 37, 42, 53, 66, 69-70, 79-81, 88, 98, 109-111, 113, 118-119, 123, 135, 139, 143, 220, 256-259, 264, 371, 389, 411, 443, 445, 464-465, 512-515, 523-524, 540, 548, 554, 563, 580, 593, 636, 749-751, 873, 900-901, 990, 992-993, 995, 1080, 1114, 1214, 1234, 1352, 1433, 1494, 1508, 1521, 1720, 1723, 1755, 1801, 2000-2001, 2003, 2049, 2301, 2401, 2447, 2690, 2766, 3128, 3268-3269, 3306, 3372, 3389, 4100, 4443-4444, 4661-4662, 5000, 5432, 5555-5556, 5631-5632, 5634, 5800-5802, 5900-5901, 6000, 6112, 6346, 6387, 6666-6667, 6699, 7007, 7100, 7161, 7777-7778, 8000-8001, 8010, 8080-8081, 8100, 8888, 8910, 9100, 10000, 12345-12346, 20034, 21554, 32000, 32768-32790

UDP Standard Scan (about 180 ports)

7, 9, 13, 17, 19, 21, 37, 53, 67-69, 80, 98, 111, 121, 123, 135, 137-138, 161, 177, 371, 389, 407, 443, 445, 456, 464, 500, 512, 514, 517-518, 520, 555, 635, 666, 858, 1001, 1010-1011, 1015, 1024-1049, 1051-1055, 1170, 1194, 1243, 1245, 1434, 1492, 1600, 1604, 1645, 1701, 1807, 1812, 1900, 1978, 1981, 1999, 2001-2002, 2023, 2049, 2115, 2140, 2801, 2967, 3024, 3129, 3150, 3283, 3527, 3700, 3801, 4000, 4092, 4156, 4569, 4590, 4781, 5000-5001, 5036, 5060, 5321, 5400-5402, 5503, 5569, 5632, 5742, 6051, 6073, 6502, 6670, 6771, 6912, 6969, 7000, 7111, 7222, 7300-7301, 7306-7308, 7778, 7789, 7938, 9872-9875, 9989, 10067, 10167, 11000, 11223, 12223, 12345-12346, 12361-12362, 15253, 15345, 16969, 17185, 20001, 20034, 21544, 21862, 22222, 23456, 26274, 26409, 27444, 30029, 31335, 31337-31339, 31666, 31785, 31789, 31791-31792, 32771, 33333, 34324, 40412, 40421-40423, 40426, 47262, 50505, 50766, 51100-51101, 51109, 53001, 54321, 61466

UDP Light Scan (about 30 ports)

7, 13, 17, 19, 37, 53, 67-69, 111, 123, 135, 137, 161, 177, 407, 464, 500, 517-518, 520, 1434, 1645, 1701, 1812, 2049, 3527, 4569, 4665, 5036, 5060, 5632, 6502, 7778, 15345

Appendix C - Scan Results JSON

This section describes all the possible keys involved when a Scan API "fetch" request is made in JSON format (/api/2.0/fo/scan/?action-fetch&output_format=json). Click here for sample JSON output

A list of keys for various scan scenarios is provided

Scan Finished with Vulnerabilities

Scan Cancelled

Scan Error

Scan Finished (Host Not Alive)

Scan Paused

Scan Interrupted

Scan Finished with Vulnerabilities

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile
```

Per Host

```
ip, dns, netbios, os, ip_status, qid, title, type, severity, port, protocol,
fqdn, ssl, cve_id, vendor_reference, bugtraq_id, cvss_base, cvss_temporal,
cvss3_base, cvss3_temporal, threat, impact, solution, exploitability,
associated_malware, results, pci_vuln, instance, os_cpe, category, instance
```

If PCI is Enabled

```
pci_vuln
```

Host Stats

```
target_distribution_across_scanner_appliances
hosts_not_scanned_excluded_host_ip
hosts_not_scanned_host_not_alive_ip
hosts_not_scanned_host_not_alive_dns
hosts_not_scanned_host_not_alive_netbios
hosts_not_scanned_hostname_not_found_ip
hosts_not_scanned_scan_discontinued_ip
hosts_not_scanned_scan_discontinued_netbios_instace_ids
hosts_not_scanned_scan_discontinued_netbios_dns
hosts_not_scanned_scan_discontinued_netbios
hosts_not_scanned_dns_hostname_could_not_be_resolved
hosts_not_scanned_netbios_could_not_be_resolved
no_vulnerabilities_match_your_filters_for_these_hosts

hosts_not_scanned_dns_could_not_be_resolved
hosts_not_scanned_ip_could_not_be_resolved
```

```
hosts_not_scanned_hostname_not_found_netbios
hosts_not_scanned_hostname_not_found_dns
```

Scan Cancelled

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile
```

Host Stats

```
no_vulnerabilities_match_your_filters_for_these_hosts

host_not_scanned,_scan_canceled_by_user_ip_
host_not_scanned,_scan_canceled_by_administrator_ip_
host_not_scanned,_scan_canceled_by_service_ip_
host_not_scanned,_scan_canceled_by_unknown_ip_

host_not_scanned,_scan_canceled_by_user, (#No of IP) hosts
host_not_scanned,_scan_canceled_by_administrator, (#No of IP) hosts
host_not_scanned,_scan_canceled_by_service, (#No of IP) hosts
host_not_scanned,_scan_canceled_by_unknown, (#No of IP) hosts

host_not_scanned,_scan_canceled_by_user_dns_
host_not_scanned,_scan_canceled_by_administrator_dns_
host_not_scanned,_scan_canceled_by_service_dns_
host_not_scanned,_scan_canceled_by_unknown_dns_

host_not_scanned,_scan_canceled_by_user_instance_ids_
host_not_scanned,_scan_canceled_by_administrator_instance_ids_
host_not_scanned,_scan_canceled_by_service_instance_ids_
host_not_scanned,_scan_canceled_by_unknown_instance_ids_

host_not_scanned,_scan_canceled_by_user, dns,(#No of DNS) hosts
host_not_scanned,_scan_canceled_by_administrator,  dns,(#No of DNS) hosts
host_not_scanned,_scan_canceled_by_service, dns,(#No of DNS) hosts
host_not_scanned,_scan_canceled_by_unknown, dns,(#No of DNS) hosts

host_not_scanned,_scan_canceled_by_user, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_canceled_by_administrator,  instance_ids,(#No of DNS)
hosts
host_not_scanned,_scan_canceled_by_service, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_canceled_by_unknown, instance_ids,(#No of DNS) hosts

host_not_scanned,_scan_canceled_by_user_netbios_
host_not_scanned,_scan_canceled_by_administrator_netbios_
host_not_scanned,_scan_canceled_by_service_netbios_
host_not_scanned,_scan_canceled_by_unknown_netbios_

host_not_scanned,_scan_canceled_by_user, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_canceled_by_administrator, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_canceled_by_service, netbios,(#No of Netbios) hosts
```

```
host_not_scanned,_scan_canceled_by_unknown, netbios,(#No of Netbios) hosts
```

Scan Error

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile
```

Host Stats

```
no_vulnerabilities_match_your_filters_for_these_hosts
```

Scan Finished (Host Not Alive)

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile
```

Host Stats

```
target_distribution_across_scanner_appliances
hosts_not_scanned_host_not_alive_ip
```

Scan Paused

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile, network
```

Per Host

```
ip, dns, netbios, os, ip_status, qid, title, type, severity, port, protocol,
fqdn, ssl, cve_id, vendor_reference, bugtraq_id, cvss_base, cvss_temporal,
cvss3_base, cvss3_temporal, threat, impact, solution, exploitability,
associated_malware, results, pci_vuln, instance, os_cpe, category
```

Host Stats

```
target_distribution_across_scanner_appliances
hosts_not_scanned_host_not_alive_ip
host_not_scanned,_scan_paused_by_service_ip_
no_vulnerabilities_match_your_filters_for_these_hosts

host_not_scanned,_scan_paused_by_user_ip_
host_not_scanned,_scan_paused_by_administrator_ip_
host_not_scanned,_scan_paused_by_service_ip_
host_not_scanned,_scan_paused_by_unknown_ip_

host_not_scanned,_scan_paused_by_user, (#No of IP) hosts
host_not_scanned,_scan_paused_by_administrator, (#No of IP) hosts
```

```
host_not_scanned,_scan_paused_by_service, (#No of IP) hosts
host_not_scanned,_scan_paused_by_unknown, (#No of IP) hosts

host_not_scanned,_scan_paused_by_user_dns_
host_not_scanned,_scan_paused_by_administrator_dns_
host_not_scanned,_scan_paused_by_service_dns_
host_not_scanned,_scan_paused_by_unknown_dns_

host_not_scanned,_scan_paused_by_user_instance_ids_
host_not_scanned,_scan_paused_by_administrator_instance_ids_
host_not_scanned,_scan_paused_by_service_instance_ids_
host_not_scanned,_scan_paused_by_unknown_instance_ids_

host_not_scanned,_scan_paused_by_user, dns,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_administrator, dns,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_service, dns,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_unknown, dns,(#No of DNS) hosts

host_not_scanned,_scan_paused_by_user, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_administrator, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_service, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_paused_by_unknown, instance_ids,(#No of DNS) hosts

host_not_scanned,_scan_paused_by_user, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_paused_by_administrator, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_paused_by_service, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_paused_by_unknown, netbios,(#No of Netbios) hosts

host_not_scanned,_scan_paused_by_user_netbios_
host_not_scanned,_scan_paused_by_administrator_netbios_
host_not_scanned,_scan_paused_by_service_netbios_
host_not_scanned,_scan_paused_by_unknown_netbios_
```

Scan Interrupted

Scan Job

```
launch_date, active_hosts, total_hosts, type, status, reference,
scanner_appliance, duration, scan_title, asset_groups, ips, excluded_ips,
option_profile, network
```

Host Stats

```
no_vulnerabilities_match_your_filters_for_these_hosts

host_not_scanned,_scan_unknown_by_user_ip_
host_not_scanned,_scan_unknown_by_administrator_ip_
host_not_scanned,_scan_unknown_by_service_ip_
host_not_scanned,_scan_unknown_by_unknown_ip_

host_not_scanned,_scan_unknown_by_user_dns_
host_not_scanned,_scan_unknown_by_administrator_dns_
host_not_scanned,_scan_unknown_by_service_dns_
host_not_scanned,_scan_unknown_by_unknown_dns_
```

```
host_not_scanned,_scan_unknown_by_user_instance_ids_
host_not_scanned,_scan_unknown_by_administrator_instance_ids_
host_not_scanned,_scan_unknown_by_service_instance_ids_
host_not_scanned,_scan_unknown_by_unknown_instance_ids_

host_not_scanned,_scan_unknown_by_user, (#No of IP) hosts
host_not_scanned,_scan_unknown_by_administrator, (#No of IP) hosts
host_not_scanned,_scan_unknown_by_service, (#No of IP) hosts
host_not_scanned,_scan_unknown_by_unknown, (#No of IP) hosts

host_not_scanned,_scan_unknown_by_user, dns,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_administrator, dns,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_service, dns,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_unknown, dns,(#No of DNS) hosts

host_not_scanned,_scan_unknown_by_user, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_administrator, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_service, instance_ids,(#No of DNS) hosts
host_not_scanned,_scan_unknown_by_unknown, instance_ids,(#No of DNS) hosts

host_not_scanned,_scan_unknown_by_user_netbios_
host_not_scanned,_scan_unknown_by_administrator_netbios_
host_not_scanned,_scan_unknown_by_service_netbios_
host_not_scanned,_scan_unknown_by_unknown_netbios_

host_not_scanned,_scan_unknown_by_user, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_unknown_by_administrator, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_unknown_by_service, netbios,(#No of Netbios) hosts
host_not_scanned,_scan_unknown_by_unknown, netbios,(#No of Netbios) hosts

hosts not scanned, hostname not found, (#NumberOfNoTrackerIP) hosts
hosts not scanned, hostname not found, netbios,(#NumberOfNoTrackerNETBIOS) hosts
hosts not scanned, hostname not found, dns, (#NumberOfNoTrackerDNS) hosts
hosts not scanned, hostname not found, instance ids, (#NumberOfNoTrackerDNS)
hosts

hosts_not_scanned_excluded_host_dns
hosts_not_scanned_excluded_host_instance_ids

hosts_not_scanned_excluded_host_netbios

hosts_not_scanned_host_not_alive_dns
hosts_not_scanned_host_not_alive_instance_ids
```

Sample JSON output

```
[
    {
        "scan_report_template_title": "Scan Results",
        "result_date": "06/29/2018 06:19:26",
        "company": "Qualys, Inc",
        "add1": "919 E Hillsdale Blvd,4th Floor",
        "add2": null,
```

```
        "city": "Foster City",
        "state": "California",
        "country": "United States of America",
        "zip": "94404",
        "name": "<name>",
        "username": "<username>",
        "role": "Manager"
    },
    {
        "scan_date": "09/29/2018 21:20:35",
        "active_hosts": null,
        "total_hosts": "457660",
        "type": "On Demand",
        "status": "Canceled",
        "reference": "scan/1527628838.16797",
        "scanner_appliance": "",
        "duration": "00:00:24",
        "scan_title": "My Scan",
        "asset_groups": "4.5LIPs",
        "ips": "10.10.0.0, 10.10.0.2, 10.10.0.4, 10.10.0.6",
        "excluded_ips": "",
        "option_profile": "Initial Options"
    },
    {
        "host_not_scanned,_scan_canceled_by_user_ip_": "10.10.0.0,
10.10.0.2,  10.10.0.4,  10.10.0.6"
    }
]
```

Appendix D - Error Codes / Descriptions

Here's a list of Qualys API error codes along with a description of what each code means. For an API request that had an error, you'll find the error code and text in the XML response.

HTTP Status	Error Code	Error Text	Meaning
HTTP/1.1 400 Bad Request	1901	Unrecognized parameter(s):...	The API request contained one or more parameters which are not supported, or are not available to the browsing user.
HTTP/1.1 400 Bad Request	1903	Missing required parameter(s):...	The API request did not contain one or more parameters which are required.
HTTP/1.1 400 Bad Request	1904	Please specify only one of these parameters:...	The API request contained 2 or more parameters from a group from which at most one may be specified.
HTTP/1.1 400 Bad Request	1905	parameter ... has invalid value ...	The API request contained a valid parameter specified with an invalid value.
HTTP/1.1 400 Bad Request	1907	The following combination of key=value pairs is not supported:...	The API request contained an invalid or unsupported combination of parameters.
HTTP/1.1 400 Bad Request	1908	Request method (GET or POST) is incompatible with specified parameter(s):...	The API request was made with an unsupported HTTP request method (GET or POST or PUT or DELETE or HEAD).
HTTP/1.1 409 Conflict	1920	The requested operation is blocked by one or more existing Business Objects	The API request was blocked by other API requests. In practice this should be replaced by one of error code 1960 or 1965 (see below).
HTTP/1.1 409 Conflict	1960	The requested operation is blocked by one or more existing Business Objects	Too many other API requests currently running (i.e. concurrency limit).
HTTP/1.1 409 Conflict	1965	The requested operation is blocked by one or more existing Business Objects	Too many other API requests have run recently (i.e. rate limit).
HTTP/1.1 400 Bad Request	1922	Please specify at least one of the following parameters:...	The API request was missing some required information (but not necessarily a single specific parameter).
HTTP/1.1 202 Accepted	1981	Your request is being processed. Please try this same request again later.	The API request is for a business operation which is already underway.

HTTP Status	Error Code	Error Text	Meaning
HTTP/1.1 400 Bad Request	999	Internal Error	The API request failed for some reason having to do with the (client) request. In practice this should always be expressed as some other error type, giving more information about what was actually wrong with the request.
HTTP/1.1 501 Internal Error	999	Internal Error	The API request failed due to a problem with QWEB.
HTTP/1.1 503 Maintenance	1999	We are performing scheduled maintenance on our System. We apologize for any inconvenience.	The API request failed because the Qualys Cloud Platform is in maintenance mode.
HTTP/1.1 401 Unauthorized	2000	Bad Login/Password	The API request failed because of an authentication failure.
HTTP/1.1 403 Forbidden	2002	User account is inactive.	The API request failed because of an authorization failure.
HTTP/1.1 409 Conflict	2003	Registration must be completed before API requests will be served for this account	The API request failed because nobody has yet accepted the EULA on behalf of the user's subscription.
HTTP/1.1 409 Conflict	2011	SecureID authentication is required for this account, so API access is blocked	The API request failed because SecureID authentication won't work with API calls.
HTTP/1.1 403 Forbidden	2012	User license is not authorized to run this API.	The API request failed because the user's subscription does not have API access enabled.

Note: For msp Users API requests, the server returns HTTP 200 status code in the response irrespective of whether it is successful or an error.

PCRS Error Codes

This section includes information on the PCRS error codes that you may encounter and their descriptions.

Error Code	Description	Action Required

Error Code: 401	Incorrect credentials provided by the user.
	{
	"authentication_exceptions" : [
	["Authentication Failure: 1 errors, 0 successes:authenticationFailure.InvalidCredentialsException"]
	]
	}
		Enter correct credentials and run the API again.

Error code: 401	Expired authentication token entered by user.
	{
	"status": 401,
	"error": "Unauthorized",
	"message": "JWT expired"
	}
		Enter correct valid token from /auth API and call the API again.

Error code: 401	Invalid token provided.
	{
	"status": 401,
	"error": "Unauthorized",
	"message": "Not authenticated"
	}
		Enter correct valid token from /auth API and call the APIs again.

200 ok	Compliance Policy does not exist
	[
	{
	"policyId": "94473",
	"subscriptionId": "1981983",
	"hostIds": [],
	"error": "Error: Compliance Policy does not exist."
	}
	]
		Enter correct policy ID and run the API again.

Error Code	Description	Action Required
400	Policy ID entered contains non-numeric characters. [{"response":{"datetime":"2021-10-28T13:29:06Z","code":1905,"text":"parameter policy_ids has invalid value: 4199751a (Invalid value: 4199751a)"}}]	Enter only numeric value for policy IDs.

404	Invalid parameter for “evidenceRequired".
	
	{
	"message": "Invalid input Parameter."
	}
		Enter integer value - 0 or 1 for the evidenceRequired request parameter.

404	Invalid input parameter for “compressionRequired”
	
	{
	"message": "Invalid input Parameter."
	}
		Enter integer value - 0 or 1 for the compressionRequired request parameter.

Connection broken (client error)	Output stream has no data in stream. “Connection broken: InvalidChunkLength(got length b'', 0 bytes read)", InvalidChunkLength(got length b'', 0 bytes read)	Run the API again with all valid inputs and options.
Server side error	Client and server connection is broken due to connectivity loss then below error will get on server logs.	Run the API again with all valid inputs and options.
403	This error occurs in case of an SCA-only account. 403 Forbidden: [{"response":{"datetime":"2021-10-28T07:24:26Z","code":2012,"text":"User license is not authorized to run this API."}}]	Use a valid PC license.

You can find all our latest API Documentation at the Qualys Community at Qualys Documentation.

Appendix E - Streaming Posture API Client Sample Code (Python)

The following table contains output parameters and their descriptions:

Following is a sample code to demonstrate how to use Qualys Policy Compliance Streaming Posture API to download host posture by using Python script.

Output Parameter Name	Description
id	Posture record ID
instance	Instance type/name
policyId	Policy ID
controlId	Control ID
technologyId	Technology ID
status	Posture Status
previousStatus	Previous Posture Status
firstFailDate	Posture first fail date
lastFailDate	Posture last fail date
firstPassDate	Posture pass date
lastPassDate	Posture last date
postureModifiedDate	Posture last modified date
lastEvaluatedDate	Posture last evaluated date
created	Posture creation date
hostId	Host ID
ip	Asset instance IP address
trackingMethod	Asset tracking method
os	Asset instance operating system
osCpe	OS Platform Enumeration
dns	Host ID
qgHostid	QualysGuard Host ID
networkId	Network ID
networkName	Network name
complianceLastScanDate	Policy Compliance last scan date
customerUuid	Customer UUID
customerId	Customer ID
assetId	Asset ID
technology : id	Technology ID
technology : name	Technology name
criticality : label	Control criticality label

Output Parameter Name	Description
criticality : value	Control criticality value
evidence : expectedValues	Posture evidence expected values
evidence : currentValues	Posture evidence current values
causeOfFailure : missing	Failed Posture cause of failure missing values
causeOfFailure : unexpected	Failed Posture unexpected value for failure result

Following is the sample code to demonstrate how to use Qualys Policy Compliance Streaming Posture API to download host posture by using Python script.

You need to install requests library such as PIP Install Requests.

```
import requests
from requests.exceptions import Timeout
import json
import datetime
import time
import sys
import zlib

# Function to handle various errors
def handlerError(size, error):
   print('Total size downloaded %.2fm'%size/1048576)
#Print total data downloaded in MBs
    print(type(error))
    print(error.args)
    print(error)

# First authenticate the user to get the token needed for
subsequent API calls
headers = {'Content-Type': 'application/x-www-form-urlencoded'}
authUrl='https://gateway.<assigned URL>/auth'                #
data = {'username':'username',
'password':'password','token':true}   # Replace username and
password with actual userid and password. For token, the value
can be 'true' or 'True'.
authResp=requests.post(authUrl, data=data, headers=headers,
verify=False)
token=authResp.content.decode('utf-8')

# Use the token returned by the authentication call
# Retrieve the host IDs associated with the particular policy
headers={
    'accept':'application/json',
    'Authorization': 'Bearer '+token}
```

```
params={'policyId':'policyid'}
#Replace with the actual policy ID, pass multiple policy IDs as
comma-separated list

url='https://gateway.<assigned URL>/pcrs/1.0/posture/hostids'
response=requests.get(url, params=params, headers=headers,
verify=False)

# check the response of host IDs API
if (response.status_code!=200):
    print("Unexpected response from hostids API: ")
    print(response.status_code)
    exit()

# Pass the host IDs retrieved in the previous APIs to posture
info API
headers={
    'accept':'application/json',
    'Authorization': 'Bearer '+token,
    'Content-Type':'application/json'}

postureUrl = 'https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressio
nRequired=1'
# If compression is used and you want to decompress the data on
the fly
d = zlib.decompressobj(16+zlib.MAX_WBITS)

#with open("output.json", 'wb') as f: #If compression is used
the zip file is to be stored
with open("output.json", 'w') as f: #If compression is used and
decompressing on the fly or no compression used
    print('API Invoked at:')
    print(datetime.datetime.now())
    size=0.0
    try:
        with requests.post(url=postureUrl, headers=headers,
data=response.content, stream=True, timeout=3600, verify=False)
as postureStream:
            if (postureStream.status_code!=200):
                print("Unexpected response from posture API: ")
                print(postureStream.status_code)
                exit()
            print('First response received at: ')
            start = time.time()
```

```
            print(datetime.datetime.now())
            for chunk in
postureStream.iter_content(chunk_size=1048576):
                if chunk:
                    chunk_size=len(chunk)
                    end=time.time()+1
                  outstr = d.decompress(chunk) # If compression
is not used or storing zip file, please comment this line
                    size += len(outstr)
                    print('Download speed: [%.2fkbps], Chunk
size: [%.2fk], total size: [%.2fm] at time %s'%((size/(end-
start))/1024,

chunk_size/1024,size/1048576,datetime.datetime.now().strftime("
%H:%M:%S")),end="\r")
                    f.write(outstr.decode())
                    f.flush()
            postureStream.close
        f.flush()
        print('\nAPI finished at')
        print(datetime.datetime.now())
    except Exception as e:
        handlerError(size. e)
    except ProtocolError as pe:
        handlerError(size, pe)
f.close()
```

Following is a sample code to demonstrate how to use Qualys Policy Compliance Streaming Posture API for concurrent processing of host posture by using Python script.

You need to install requests library such as PIP install requests, PIP install json_stream, and PIP install dicttoxml.

```
import requests
from requests.exceptions import Timeout
import json
import datetime
import time
import sys
import zlib
import threading
import json_stream

def worker():
    with open("output.json", 'r') as f:
        data = json_stream.load(f)
        count=0
```

```
        for posture in data.persistent():
          print('Count [%d] Control Id [%s] IP[%s] Criticality
[%s] Status[%s]'%(count,
                                      posture['controlId'],
posture['ip'],
posture['criticality']['label'],posture['status']),end="\r")
            count += 1

    f.close()

# Function to handle various errors
def handlerError(size, error):
    print(type(error))
    print(error.args)
    print(error)

# First authenticate the user to get the token needed for
subsequent API calls
headers = {'Content-Type': 'application/x-www-form-urlencoded'}
authUrl='https://gateway.<assigned URL>/auth'                #
data = {'username': <USER NAME>,
'password':<PASSWORD>,'token':true}   # Replace username and
password with actual user ID and password. For token, the value
can be 'true' or 'True'.
authResp=requests.post(authUrl, data=data, headers=headers,
verify=False)
token=authResp.content.decode('utf-8')

# Use the token returned by the authentication call
# Retrieve the host ids associated with the particular policy
headers={
    'accept':'application/json',
    'Authorization': 'Bearer '+token}

params={'policyId':'xxx'}
#Replace with the policyid, pass multiple policyids as comma
separated list

url='https://gateway.<assigned URL>/pcrs/1.0/posture/hostids'
response=requests.get(url, params=params, headers=headers,
verify=False)

# check the response of host ids API
if (response.status_code!=200):
    print("Unexpected response from hostids API: ")
    print(response.status_code)
```

```
    exit()

# Pass the host ids retrieved in the previous APIs to posture
info API
headers={
    'accept':'application/json',
    'Authorization': 'Bearer '+token,
    'Content-Type':'application/json'}

postureUrl = 'https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressio
nRequired=1'
# If compression is used and you want to decompress the data on
the fly
d = zlib.decompressobj(16+zlib.MAX_WBITS)

apiTime = datetime.datetime.now()
with open("output.json", 'w') as f: #If compression is used and
decompressing on the fly or no compression used
    print('API Invoked at:')
    print(datetime.datetime.now())
    t1 = threading.Thread(target=worker, daemon=True)
    try:
        with requests.post(url=postureUrl, headers=headers,
data=response.content, stream=True, timeout=3600, verify=False)
as postureStream:
            if (postureStream.status_code!=200):
                print("Unexpected response from posture API: ")
                print(postureStream.status_code)
                exit()
            print('First response received at: ')
            start = time.time()
            print(datetime.datetime.now())

            count=0
            for chunk in
postureStream.iter_content(chunk_size=1048576):
                if chunk:
                  outstr = d.decompress(chunk) # If compression
is not used or storing zip file, please comment this line
                    f.write(outstr.decode())
                    f.flush()
                    if count == 0:
                        # turn-on the worker thread
                        t1.start()
                        count += 1
```

```
            postureStream.close
        apiTime = datetime.datetime.now()
    except Exception as e:
        handlerError(size. e)
    except ProtocolError as pe:
        handlerError(size, pe)
f.close()
t1.join()
print('\nAPI Finished at [%s] All the procesing completed at
[%s]'%(apiTime,datetime.datetime.now()))
```

Index

A

add IP addresses 987
API limits 14
Application Server authentication 631
asset search report 1433
authentication 11, 605
authentication to your account 25

B

basic HTTP authentication 25

C

cancel report 1414, 1415
characters in URLs 13
compliance control list 1579, 1604, 1625
compliance policy export 1649, 1668, 1671
compliance policy import 1676, 1678, 1679
compliance policy list 1631, 1635, 1641
compliance policy, manage asset groups 1691
compliance scan list 60
control criticality 1930
country codes 2010
Cyberscope report 1950

D

date format 13
delete report 1431
discovery scans 173
Docker authentication 654, 680
download report 1417, 1422

E

Expires header 29

G

GET method 13

H

header parameter 25
host detection list 1119, 1150, 1183, 1221, 1265
host list 995, 1009, 1029, 1055, 1082
HTTP authentication 657
HTTP Expires header 29

I

IBM DB2 authentication 660
invalid tickets 1560
IP list 984, 1728, 1730
IPv6 asset mapping record list 1354

L

launch compliance scan 66
launch compliance scan on EC2 assets 67
launch report 1370, 1376
launch scorecard report 1407
launch VM scan 51
launch VM scan on EC2 assets 53

M

manage compliance scans 69
manage VM scans 56
maps 173
MariaDB authentication 683, 714
MongoDB authentication 704
MS SQL authentication 719
MySQL authentication 729, 735

N

network
    assign appliance to 1361
    create 1358
    update 1360
network list 1357
network maps 173
network support 1357

O

option profiles
  export 219
  for compliance 387, 398, 411, 424
  for PCI 379
  for VM 297
  import 262
Oracle authentication 757
Oracle Listener authentication 765
Oracle WebLogic authentication 767
overdue tickets 1559

P

Palo Alto Firewall authentication 770
POST method 13
PostgreSQL authentication 781

Q

Qualys
  user account 11
Qualys End User Agreement (EULA) 2015
Qualys EULA 2015
Qualys Support 10
Qualys user account 11

R

report
  asset search 1433
  cancel 1414, 1415
  Cyberscope report 1950
  delete 1431
  download 1417, 1422
  SCAP ARF report 1954
  scorecard report 1407
report DTDs, most recent 14
report, launch 1370, 1376
reports
  date format 13
  decoding reports 14

S

scan authentication
  Application Server 631
  Docker 654, 680
  HTTP 657
  IBM DB2 660
  MariaDB 683, 714
  MongoDB 704
  MS SQL 719
  MySQL 729, 735
  Oracle 757
  Oracle Listener 765
  Oracle WebLogic 767
  Palo Alto Firewall 770
  PostgreSQL 781
  SNMP 798
  Sybase 803, 809
  Unix 829, 844, 868
  VMware 909
  Windows 931, 939
scan list parameters 124
scan schedules 85
scanner appliances
  list 199
  manage virtual 203
  replace 212
  update physical 208
SCAP ARF report 1954
SCAP Cyberscope Report 1950
SCAP policy list 1955
SCAP scan list 64
scheduled report, launch 1433
scheduled reports list 1432
session based authentication 26
session login 29
session logout 31
session timeout 29
share PCI scan 169
SNMP authentication 798
special characters in URLs 13

state codes
    Australia 2010
    Canada 2010
    India 2011
    United States of America 2010
Sybase authentication 803, 809

T

ticket state/status 1559

U

Unix authentication 829, 844, 868
updated IP addresses 990
URL elements 14
URL encoded variables 13
user account
    login credentials 11
user management functions
    `acceptEULA.php` 2015
`user.php` function
    country codes 2010
    state codes 2010, 2011
UTF-8 encoding 13

V

VM scan list 38, 41
VM scan statistics 149
VM scan summary (hosts not scanned) 164
VM scans 38
VMware authentication 909

W

Windows authentication 931, 939