



# **Qualys API V2**

User Guide

Version 8.12

February 13, 2018

Copyright 2007-2018 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

# CONTENTS

---

## **Preface**

## **Chapter 1 Welcome**

Get Started .....	9
Get API Notifications .....	9
API Conventions.....	10
Qualys User Account .....	10
URL to the Qualys API Server.....	10
Making API Calls.....	12
API Limits.....	14
Tracking API usage by user .....	14
HTTP Response Headers.....	15
Activity Log.....	18

## **Chapter 2 Using the API V2 Architecture**

Authentication Using the V2 APIs.....	20
Using the API V2 Session Resource .....	22
Session Login.....	26
Session Logout .....	28

## **Chapter 3 Scan API**

VM Scans .....	31
VM Scan List .....	31
Launch a VM Scan.....	35
Launch a VM Scan on EC2 Hosts.....	37
Take Actions on VM Scans.....	39
PC and SCAP Scans.....	41
PC Scan List.....	42
SCAP Scan List.....	43
Launch a PC Scan .....	45
Launch a PC Scan on EC2 hosts .....	46
Take Actions on PC Scans .....	48
Scan Schedules .....	51
Scan List Parameters .....	58
Scan Parameters.....	61
Scan Schedule Parameters.....	66
VM Scan Statistics.....	70
Share PCI Scan .....	73
Scanner Appliances .....	77
Scanner Appliance List.....	77
Manage VLANs and Static Routes.....	82

Virtual Scanner Appliances .....	87
Physical Scanner Appliances.....	92
KnowledgeBase .....	95
Editing Vulnerabilities .....	100
Static Search List.....	104
Dynamic Search List .....	110
Vendor IDs and References .....	122

## Chapter 4 Report API

About Report Share .....	127
Report List.....	128
Launch Report .....	131
Launch Scorecard .....	147
Cancel Running Report .....	155
Download Saved Report .....	157
Delete Saved Report .....	162
Schedule Report .....	164

## Chapter 5 Asset API

IP List .....	167
Host List .....	170
Host List Detection .....	178
Excluded Hosts List .....	206
Excluded Hosts Change History.....	210
Manage Excluded Hosts .....	214
Purge Hosts.....	218
Virtual Host List .....	222
Take Actions on Virtual Hosts .....	223
Restricted IPs List.....	225
Add IPs .....	231
Update IPs .....	233
Manage Asset Groups .....	237
Asset Search Report .....	245

## Chapter 6 IPv6 Asset API

API Support for IPv6 Asset Management and Scanning .....	255
View IPv6 Mapping Records.....	264
Add IPv6 Mapping Records .....	266
Remove IPv6 Mapping Records .....	268

## Chapter 7 Compliance API

Compliance Control List .....	271
Compliance Policy List.....	277
Compliance Policy - Export .....	282
Compliance Policy - Import.....	287

Compliance Policy - Merge .....	289
Compliance Policy - Manage Asset Groups .....	295
Compliance Posture Information .....	298
Control Criticality .....	305
Exceptions.....	306
SCAP Cyberscope Report.....	315
SCAP ARF Report.....	319
SCAP Policy List .....	320

## Chapter 8 Scan Authentication API

User Permissions Summary .....	326
List Authentication Records.....	327
List Authentication Records by Type .....	329
Application Server Records .....	332
Docker Record (PC, SCA).....	336
HTTP Record.....	341
IBM DB2 Record .....	345
MongoDB Record .....	350
MS SQL Record (PC, SCA).....	356
MySQL Record.....	367
Oracle Record.....	372
Oracle Listener Record.....	380
Oracle WebLogic Server Record (PC, SCA).....	384
Palo Alto Firewall Record .....	387
PostgreSQL Record (PC, SCA).....	391
SNMP Record.....	397
Sybase Record (PC, SCA) .....	404
Unix Record .....	410
VMware Record .....	435
Windows Record .....	439

## Chapter 9 Vault Support API

Vault Support matrix .....	446
Vault Definition .....	449
List Vaults.....	453
Manage Vaults .....	456

## Chapter 10 Option Profile API

Option Profile - Export .....	465
Option Profile - Import .....	474

## Chapter 11 Report Template API

API Support for Report Templates .....	481
Scan Template .....	482
PCI Scan Template.....	494

Patch Template .....	496
Map Template.....	501

## Chapter 12 Activity Log API

Export user activity log for subscription .....	516
---	-----

## Chapter 13 Network API

Network List .....	520
Create Network .....	521
Update Network .....	522
Assign Scanner Appliance to Network.....	523

## Appendix A Scan XML

Simple Return .....	526
Batch Return .....	528
Scan List Output.....	530
SCAP Scan List Output .....	534
Scheduled Scan List Output .....	537
Vulnerability Scan Results.....	547
Compliance Scan Results .....	548
VM Recrypt Results (Scan Statistics).....	555
PCI Scan Share Status Output.....	558
Map Report Output .....	560
Network List.....	564
KnowledgeBase Output .....	566
Customized Vulnerability List Output.....	579

## Appendix B Asset XML

IP List Output .....	583
Host List Output .....	585
Host List VM Detection Output.....	592
Excluded Hosts List Output.....	601
Excluded Hosts Change History Output.....	603
Virtual Host List Output.....	606
IPv6 Mapping Records List Output .....	608
Restricted IPs List Output.....	610
Duplicate Hosts Error Output.....	612
Asset Group List Output.....	615
Asset Search Report .....	621

## Appendix C Compliance Data XML

Compliancea Control List Output .....	629
Compliance Policy List Output.....	641
Compliance Policy Export Output .....	648
Compliance Posture Information Output .....	664

Compliance Policy Report.....	678
Compliance Authentication Report.....	693
Compliance Scorecard Report .....	700
Exception List Output.....	708
Exception Batch Return Output .....	713
SCAP Policy List Output .....	715

## **Appendix D Scan Authentication XML**

Authentication Record List Output .....	721
Authentication Record List by Type Output.....	726
Authentication Record Return.....	748
Authentication Vault List Output .....	750
Authentication Vault View Output .....	753

## **Appendix E Scorecard Report XML**

Asset Group Vulnerability Report.....	758
Ignored Vulnerabilities Report.....	763
Most Prevalent Vulnerabilities Report.....	767
Most Vulnerable Hosts Report .....	771
Patch Report .....	775

## **Appendix F Scan Configuration XML**

Scanner Appliance List Output.....	781
Scanner Appliance Create Output .....	796
Static Search List Output .....	798
Dynamic Search List Output.....	802

## **Appendix G Option Profile XML**

Option Profile Output.....	810
----------------------------	-----

## **Appendix H Report XML**

Report List .....	827
Schedule Report List .....	830
Scan Report Template Output .....	835
PCI Scan Template Output.....	837
Patch Template Output.....	839
Map Template Output .....	841

## **Appendix I Error Codes / Descriptions**

### **Index**

---

# 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 API functions described in this guide are available to customers with Qualys Vulnerability Management (VM) and Policy Compliance (PC).

## About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations 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, Fujitsu, HCL Comnet, HPE, 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](http://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/](http://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. The API functions described in this guide are available to customers with Qualys Vulnerability Management (VM) and Policy Compliance (PC).

### Get Started

This chapter gives you an introduction to the Qualys API v2 and how to make requests using this API. We'll discuss API conventions and best practices to get you up and running quickly.

Some Qualys users will want to use both the API V1 and V2 functions. Refer to the Qualys API v1 User Guide for documentation on the V1 APIs.

### Get API Notifications

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

#### From our Community

[Join our Community](#)

[API Notifications RSS Feeds](#)

# API Conventions

The Qualys API V2 is based on a newer API architecture that provides many features and benefits to Qualys API customers. The API V2 architecture is optimized for performance and security, and will be the basis for future Qualys API functionality.

## 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.

When calling the V2 API functions, users have the option to choose session based authentication using login and logout operations, or basic HTTP authentication. See “Authentication Using the V2 APIs” in Chapter 2 for information.

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.

## URL to the Qualys API Server

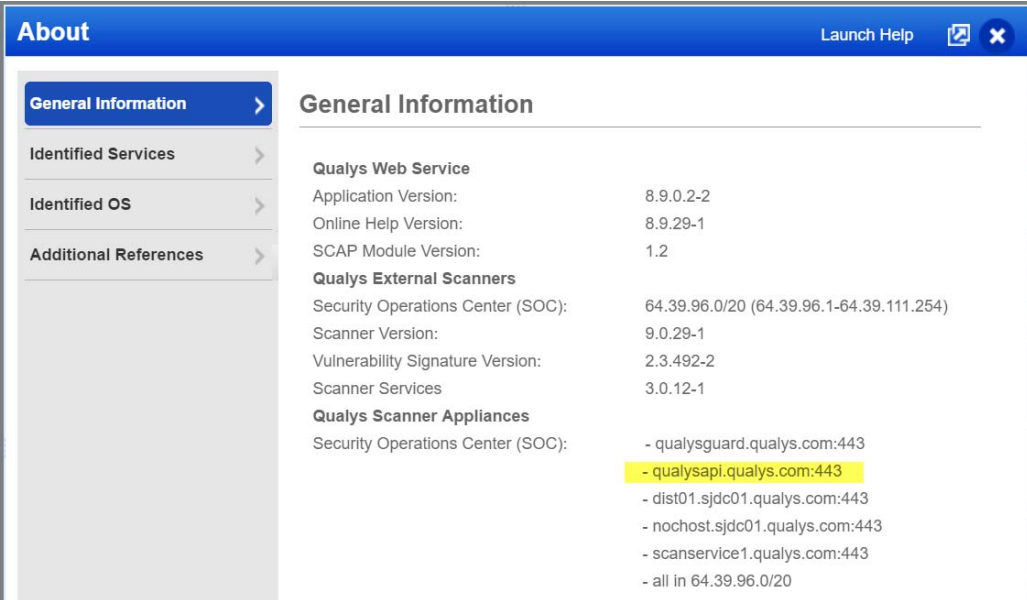
Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysapi.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysapi.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysapi.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located 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).



The screenshot shows the 'About' page of the Qualys interface. It has a blue header with the title 'About' and a 'Launch Help' button. A left sidebar contains a menu with 'General Information' (selected), 'Identified Services', 'Identified OS', and 'Additional References'. The main content area is titled 'General Information' and lists various system details.

General Information	
<b>Qualys Web Service</b>	
Application Version:	8.9.0.2-2
Online Help Version:	8.9.29-1
SCAP Module Version:	1.2
<b>Qualys External Scanners</b>	
Security Operations Center (SOC):	64.39.96.0/20 (64.39.96.1-64.39.111.254)
Scanner Version:	9.0.29-1
Vulnerability Signature Version:	2.3.492-2
Scanner Services	3.0.12-1
<b>Qualys Scanner Appliances</b>	
Security Operations Center (SOC):	- qualysguard.qualys.com:443
	- <b>qualysapi.qualys.com:443</b>
	- dist01.sjdc01.qualys.com:443
	- nochohost.sjdc01.qualys.com:443
	- scanservice1.qualys.com:443
	- all in 64.39.96.0/20

# Making API Calls

## GET and POST Methods

Qualys API V2 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.

## 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-ddThh-mm-ssZ`

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 URL to the scan report can be found at the URL shown below:

```
https://qualysapi.qualys.com/scan-1.dtd
```

The URLs to current report DTDs are included with the function descriptions in this document. There is a generic report returned by a few functions.

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 appendices at the end of this document. For each XML report a recent report DTD and the report's XML elements and attributes (XPaths) are described in detail.

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” V2 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” V2 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.
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. <a href="#">Click here</a> 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 2011 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 2011 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 V2 Call Blocked (Concurrency Limit exceeded)**

Returned from API V2 call using API V2 session authentication.

```
HTTP/1.1 409 Conflict
Date: Fri, 22 Apr 2011 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 2011 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" V2 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.

## Using the API V2 Architecture

The latest Qualys API Suites are based on a new API architecture that provides new features and benefits to Qualys API customers. The new API architecture is optimized for performance and security, and will be the basis for future Qualys APIs.

When using APIs based on the V2 API architecture, you'll notice these features:

**API Versioning** - An API version number is incorporated in V2 API URLs. This will allow us to introduce significant API updates from one release to the next in the future, while allowing customers to choose when to migrate to the latest version.

**API Login/Logout Sequence** - Authentication with valid Qualys user account credentials is required for making Qualys API requests to the Qualys API servers. When calling the V2 API functions, users have the option to choose between session based authentication (using login and logout operations) and basic HTTP authentication (identical method used for the V1 API functions).

This chapter provides important information about the API V2 architecture and the session login/logout functions. These topics are covered:

- Authentication Using the V2 APIs
- Using the API V2 Session Resource
- Session Login
- Session Logout

## Authentication Using the V2 APIs

Authentication with valid Qualys account credentials is required for making Qualys API requests to the Qualys API servers. When calling the V2 APIs, users have the option to choose between session based authentication (using login and logout operations) and basic HTTP authentication (identical method used for the V1 API functions). Specifying the “X-Requested-With” parameter is required for all V2 API requests regardless of the authentication method used.

The code examples that follow assume that the user’s account is located on US Platform 1 with the base URL `https://qualysapi.qualys.com`. As a reminder, if your account is located on another platform please replace this with the base URL for your platform.

### Required Header Parameter

The following header parameter must be included in all API v2 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.

See sample API requests below for examples using Curl.

### 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.

### Sample API Request (Curl)

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 V2 requests as follows:

### 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=passwd"  
"https://qualysapi.qualys.com/api/2.0/fo/session/"
```

### Step 2: Make resource requests

Use the V2 API resources to make V2 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 V2 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	Qualys API resource name. In the sample session login URL above, the resource “session” is specified for the session login request. For a reporting request, the resource “report” is used.
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_abl2&password=passwd"
"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_abl2&password=passwd"
"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.

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 is shown below:

```
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, is shown below:

```
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” later in this chapter 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

The `/api/2.0/fo/session` resource is used to make a request for session login. Parameters are described below.

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.
password	(Required) The password of a Qualys user account.
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 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. Thus, a session login request is required before making API calls to the Scan API or the Report Share API.

The POST access method must be used to make a session login request.

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_abl2&password=passwd"
"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

The `/api/2.0/fo/session` resource is used to make a request for session logout. Parameters are described below.

Parameter	Description
<code>action=logout</code>	(Required) A flag used to make a session logout request.
<code>echo_request={0 1}</code>	(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.

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.

The POST access method must be used to make a 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" 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
"http://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

## Scan API

The Scan API V2 provides a suite of API functions for managing vulnerability scans and compliance scans across the enterprise.

This chapter describes how to use Scan API functions. These topics are covered:

- VM Scans
- PC and SCAP Scans
- Scan Schedules
- Scan List Parameters
- Scan Parameters
- Scan Schedule Parameters
- VM Scan Statistics
- Share PCI Scan
- Scanner Appliances
- Virtual Scanner Appliances
- Physical Scanner Appliances
- KnowledgeBase
- Editing Vulnerabilities
- Static Search List API
- Dynamic Search List API

# VM Scans

The VM Scan API v2 (**/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. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

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	View scans with targets containing IPs in the user’s business unit. Download scan results when the target includes at least one IP in the user’s business unit.
Scanner	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.
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 permission to manage a scan.

# VM Scan List

The VM Scan List API v2 (**/api/2.0/fo/scan/?action=list**) lists vulnerability scans in the user’s account. By default the XML output lists scans launched in the past 30 days. The GET or POST access method may be used to make a scan list request. Authentication is required to make a request. See Chapter 2, “Authentication Using the V2 APIs.”

## Benefits

Using the V2 API **scan** function for listing scans in your account provides these benefits over using the V1 API **scan\_report\_list.php** function:

- Ability to make a single API request to view all scans in your scan history list, including running and completed scans, paused and resumed scans.
- More efficient performance especially when downloading a large amount of scan data from your Qualys account.

- Supports the most scalable and efficient method for integration of host detection data and vulnerability data in the KnowledgeBase when used in conjunction with the scan fetch API (/scan/?action=fetch) and the knowledgebase API (/api/2.0/fo/knowledge\_base/vuln/?action=list).
- More input parameters to filter out scans from the scan list output, so you don't have to retrieve and view the entire scan history list as it appears in your account.
- Numerous ways to precisely filter scans based on the when scans were launched. By default, a scan list request selects scans launched within the past 30 days. You may choose a longer window (for example within the past 60 days) or a custom window with specific start and end times (for example starting 2010-02-25T22:42:00Z and ending 2010-02-27T08:00:00Z).

### Parameters

The input parameters for requesting a VM scan list are shown below. Please 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
Show/Hide Information	show_aggs, show_op, show_status, show_last, ignore_target

### Sample Requests

Sample 1. The sample scan list API call (GET method) below returns all scans in the user account.

```
curl -H "X-Requested-With: Curl Sample"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/
?action=list&echo_request=1&show_aggs=1&show_op=1"

<?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>
  <REQUEST>
    <DATETIME>2007-09-25T12:28:29Z</DATETIME>
    <USER_LOGIN>acme_ab</USER_LOGIN>
    <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/scan/
  </RESOURCE>
```



```

<PARAM_LIST>
  <PARAM>
    <KEY>action</KEY>
    <VALUE>list</VALUE>
  </PARAM>
  <PARAM>
    <KEY>echo_request</KEY>
    <VALUE>1</VALUE>
  </PARAM>
  <PARAM>
    <KEY>show_agrs</KEY>
    <VALUE>1</VALUE>
  </PARAM>
  <PARAM>
    <KEY>show_op</KEY>
    <VALUE>1</VALUE>
  </PARAM>
</PARAM_LIST>
</REQUEST>
<RESPONSE>
  <DATETIME>2007-09-25T12:28:29Z</DATETIME>
  <SCAN_LIST>
    <SCAN>
      <REF>scan/1187117392.587</REF>
      <TYPE>On-Demand</TYPE>
      <TITLE><![CDATA[Web Servers 09/25]]></TITLE>
      <USER_LOGIN>acme_ab</USER_LOGIN>
      <LAUNCH_DATETIME>2014-09-25T08:10:43Z</LAUNCH_DATETIME>
      <DURATION>00:05:16</DURATION>
      <PROCESSED>1</PROCESSED>
      <STATUS>
        <STATE>Finished</STATE>
      </STATUS>
      <TARGET><![CDATA[10.10.10.10-10.10.10.113]]></TARGET>
      <OPTION_PROFILE>
        <TITLE><![CDATA[Initial Options]]></TITLE>
        <DEFAULT_FLAG>1</DEFAULT_FLAG>
      </OPTION_PROFILE>
    </SCAN>
    <SCAN>
      <REF>scan/1169604974.6553</REF>
      <TYPE>Scheduled</TYPE>
      <TITLE><![CDATA[Web Servers]]></TITLE>
      <USER_LOGIN>acme_sb3</USER_LOGIN>
      <LAUNCH_DATETIME>2014-09-24T15:40:02Z</LAUNCH_DATETIME>
      <DURATION>00:05:16</DURATION>
      <PROCESSED>0</PROCESSED>
    </SCAN>
  </SCAN_LIST>
</RESPONSE>

```

```
<STATUS>
  <STATE>Finished</STATE>
</STATUS>
<TARGET><![CDATA[10.10.10.10-10.10.10.113]]></TARGET>
<OPTION_PROFILE>
  <TITLE><![CDATA[Initial Options]]></TITLE>
  <DEFAULT_FLAG>1</DEFAULT_FLAG>
</OPTION_PROFILE>
</SCAN>
</SCAN_LIST>
</RESPONSE>
</SCAN_LIST_OUTPUT>
...
```

Sample 2. The sample scan list API call (GET method) below returns 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"
```

Sample 3. The sample scan list API call (GET method) below returns all scheduled scans that were launched after September 3, 2007.

```
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=2007-09-03"
```

## XML Output

The scan list output uses the scan list output DTD (scan\_list\_output.dtd). This DTD can be found at the following URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/scan/scan\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd)

## Launch a VM Scan

The VM Scan API v2 (`/api/2.0/fo/scan/?action=launch`) is used to launch vulnerability scans in the user's account.

A major benefit of using the new Launch Scan API v2 is that it 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. We recommend using this new Launch Scan API v2 instead of the Launch Scan API v1 (`/msp/scan.php`) for this reason.

Using networks? Choose the Global Default Network to scan IPs on your network perimeter. Search the Qualys help center using the keyword “networks” to learn more.

### Parameters

The input parameters for launching a VM scan are shown below. Please see “Scan Parameters” for complete details.

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
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, 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)

## Sample Requests

### Launch Vulnerability Scan API v2 Request (IP Address):

This request launches a vulnerability scan on the IP address 10.10.10.10 using the scanner appliance “scanner1”.

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

### XML Output:

```
cat outputfile.txt
```

```
<?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>
```

### Launch Vulnerability Scan API v2 Request (Asset Tags):

This request launches a vulnerability scan on hosts with the asset tag Windows using the scanner appliance “scanner1”.

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

### Launch Vulnerability Scan API v2 Request (All Scanners in Network):

This request launches a vulnerability scan using all the scanner appliances in your network.

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

## Launch a VM Scan on EC2 Hosts

The VM Scan API v2 (`/api/2.0/fo/scan/?action=launch`) is also used to launch vulnerability scans on your Amazon EC2 hosts (in your Amazon Web Services account).

The Amazon *EC2 Scan* workflow using Qualys is pre-authorized by AWS. Want to learn more? Check out our [Help Center for Amazon Web Services](#) at the Qualys Community.

A few things to consider...

- EC2 Scanning must be enabled for your Qualys account.
- Only a Manager user can launch EC2 scans.
- Before scanning you'll need to complete some set up steps. See [Getting Started with Amazon EC2 Pre-Authorized Scanning](#) at the Qualys Community.

### 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
Processing Priority	priority
Target Hosts	<div>target_from=tags (required) Use tags to select the EC2 hosts you want to scan.</div> <div>use_ip_nt_range_tags=0 The default setting is “0”. Important - This cannot be set to “1” for EC2 scanning.</div> <div>These tag parameters are used to select tags: tag_set_include={tag1,tag2,...} (required) tag_set_exclude={tag1,tag2,...} (optional) tag_include_selector={<b>any</b>   all} (default in bold) tag_exclude_selector={<b>any</b>   all} (default in bold) tag_set_by={<b>id</b>   name} (default in bold)</div>

## Sample Requests

### Launch EC2 Vulnerability Scan API v2 Request:

This request launches an EC2 vulnerability scan using the connector “EC2\_Connector” on assets that match tags with IDs 1558997 and 1559222.

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -X "POST" -d
"action=launch&scan_title=My+EC2+Scan&connector_name=EC2_Connector&ec2_en
dpoint=us-east-1&target_from=tags&use_ip_nt_range_tags=0
&tag_include_selector=any&tag_set_by=id&tag_set_include=1558997,1559222&o
ption_id=43165&iscanner_name=EC2-1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/" > outputfile.txt
```

### XML Output:

```
cat outputfile.txt
```

```
<?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>2014-02-25T21:32:40Z</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>
```

## Take Actions on VM Scans

The VM Scan API v2 (`/api/2.0/fo/scan/?action={action}`) allows users to 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

## Parameters

The parameters used to manage VM scans are described below.

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.

Parameter	Description
mode={ <b>brief</b>   extended}	(Optional for a 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={ <b>csv</b>   json   csv_extended   json_extended}	(Optional for a 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. See Appendix A for details.

## Sample Requests

Sample 1: A sample API call to 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/"
```

Sample 2: A sample API call to 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/"
```

Sample 3: A sample API call to 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/"
```

## XML Output

A request to cancel, pause or resume a scan returns XML output using the DTD "simple\_return.dtd", which can be found at the following URL (where <qualysapi.qualys.com> identifies the Qualys API server URL where your account is located):

```
https://qualysapi.qualys.com/api/2.0/simple_return.dtd
```

The DTD for the simple return XML output is provided in Appendix A.



# PC and SCAP Scans

The PC Scan API v2 (/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 v2 (/api/2.0/fo/scan/scap/) is used to get a list of SCAP scans in your account.

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

## Permissions

To use this API, these options must be enabled in the user’s subscription: Policy Compliance (PC) module and New Scanner Services. 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.

## PC Scan List

The PC Scan List API v2 (`/api/2.0/fo/scan/compliance/` with `action=list`) gives you a 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. Please 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
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>2012-09-12T07:28:46Z</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>2012-08-13T07:30:09Z</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:

The scan list output DTD can be found at the following URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/scan/scan\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd)

**SCAP Scan List**

The SCAP Scan List API v2 (/api/2.0/fo/scan/scap/ with **action=list**) gives you a list of 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. Please 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_aggs, 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>2014-06-13T22:56:19Z</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>2014-06-13T21:24:42Z</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:

The SCAP scan list output DTD can be found at the following URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/scan/qscap\\_scan\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/qscap_scan_list_output.dtd)

## Launch a PC Scan

The PC Scan API v2 (`/api/2.0/fo/scan/compliance/?action=launch`) is used to launch compliance scans. The POST method is required.

Using networks? Choose the Global Default Network to scan IPs on your network perimeter. Search the Qualys help center using the keyword “networks” to learn more.

### Parameters

The input parameters for launching a PC scan are shown below. Please see “Scan Parameters” for complete details.

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, 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)

### Sample API Request to Launch a PC Scan

A sample API request to launch a compliance scan is below. You’ll notice the XML output uses the simple return DTD (`simple_return.dtd`).

#### 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=Initia
l+PC+Options&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/" >
apiOutputScan.txt
```

#### API Request to launch a PC scan using all scanners in network:

```
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=128079
13&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/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2016-09-15T21:55:36Z</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 a PC Scan on EC2 hosts**

The PC Scan API v2 (**/api/2.0/fo/scan/compliance/?action=launch**) is also used to launch PC scans on your Amazon EC2 hosts (in your Amazon Web Services account).

The Amazon *EC2 Scan* workflow using Qualys is pre-authorized by AWS. Want to learn more? Check out our [Help Center for Amazon Web Services](#) at the Qualys Community.

A few things to consider...

- EC2 Scanning must be enabled for your Qualys account.
- Only a Manager user can launch EC2 scans.
- Before scanning you'll need to complete some set up steps. See [Getting Started with Amazon EC2 Pre-Authorized Scanning](#) at the Qualys Community.

**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

Type	Parameter List
EC2 environment	connector_name (required), ec2_endpoint (required)
Option Profile	option_id or option_title
Scanner Appliance	iscanner_id or iscanner_name
Target Hosts	<p>target_from=tags (required) Use tags to select the EC2 hosts you want to scan.</p> <hr/> <p>use_ip_nt_range_tags=0 The default setting is “0”. Important - This cannot be set to “1” for EC2 scanning.</p> <hr/> <p>These tag parameters are used to select tags: tag_set_include={tag1,tag2,...} (required) tag_set_exclude={tag1,tag2,...} (optional) tag_include_selector={<b>any</b>   all} (default in bold) tag_exclude_selector={<b>any</b>   all} (default in bold) tag_set_by={<b>id</b>   name} (default in bold)</p>

### Sample Requests

#### 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>2014-06-24T10:10:51Z</DATETIME>
    <USER_LOGIN>USERNAME</USER_LOGIN>
  <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/</RESOU
RCE>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2014-06-24T10:10:57Z</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>
```

## Take Actions on PC Scans

The PC Scan API v2 (`/api/2.0/fo/scan/compliance/?action={action}`) allows users to 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 API Request to Fetch PC Scan Results

A sample API request to fetch (download) PC scan results is below. The PC scan must have the status Finished in order to download the scan results. You’ll notice the XML output uses the compliance scan result output DTD.

### 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/compliance_scan_
result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2012-09-17T10:23:53Z</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">2012-09-15T11:49:08Z</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>
      </HEADER>
    </COMPLIANCE_SCAN>
  </RESPONSE>
</COMPLIANCE_SCAN_RESULT_OUTPUT>
```

```
<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>
```

# Scan Schedules

The Scan Schedule API v2 (**/api/2.0/fo/schedule/scan/**) supports defining schedules for vulnerability scans. This API delivers improvements to the API v1 (**/msp/scheduled\_scans.php**) and supports scanning targets in multiple network zones.

## 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

Use these parameters:

Parameter	Description
action=list	(Required) Supported method: GET
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.
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.

Parameter	Description
fqdn={value}	(Optional) The target FQDN for a CertView type VM scan. For a CertView type scan you must specify at least one target i.e. IPs, asset groups or FQDNs. Multiple values are comma separated. This option will be supported when CertView GA is released and enabled for your account.
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.

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=list&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_scan_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" />
      </SCHEDULE>
    </SCAN>
  </SCHEDULE_SCAN_LIST>
</RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

```
<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>
```

**DTD:**

The output DTD is found at this URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule\\_scan\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule_scan_list_output.dtd)

**Create a scan schedule**

The input parameters for creating a scan schedule are below. For complete details see “Scan Parameters” and “Scan Schedule Parameters”.

Type	Parameter List
Request	action=create (required), echo_request
Scan	scan_title (required), active=0   1 (required)
Option Profile	option_id or option_profile (one is required)
Scanner Appliance	iscanner_id or iscanner_name
Processing Priority	priority

Type	Parameter List
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
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=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
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

#### 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=tags&tag
_set_include=tag1,tag2,tag3&scanner_name=scanner1&occurrence=daily&frequ
ency_days=5&time_zone_code=US-CA&observe_dst=yes&start_hour=14&start_minu
te=0"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=create"
```

API request to create scan schedule using all scanners in network:

```
curl -u 'username:password' -H 'X-Requested-With:curl demo 2' -d
"action=create&scan_title=API+Schedule+scan&option_title=Initial+Options&
ip_network_id=12807913&scanners_in_network=1&ip=10.10.10.10,10.10.10.11&o
ccurrence=monthly&frequency_months=12&day_of_month=20&start_minute=00&sta
rt_hour=22&time_zone_code=IN&observe_dst=no&pause_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>2015-01-20T21:32:40Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

**Update a scan schedule**

The input parameters for updating a scan schedule are below. For complete details see “Scan Parameters” and “Scan Schedule 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

Type	Parameter List
Asset Tags	target_from=tags, 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
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

#### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=146754&pause_after_hours=5&pause_after_mins=5&resume_in
_days=5&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>2017-09-14T11:57:42Z</DATETIME>
    <TEXT>Edit scheduled Scan Completed successfully</TEXT>
    <ITEM_LIST>
```



```
<ITEM>
  <KEY>ID</KEY>
  <VALUE>146754</VALUE>
</ITEM>
</ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

## Delete a scan schedule

Use these parameters:

Parameter	Description
action=delete	(Required) Supported method: POST
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.

### 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=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>2015-01-30T21:32:40Z</DATETIME>
    <TEXT>Schedule scan deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>123456</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

# Scan List Parameters

Request type - The scan list type parameters are described below.

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.

Parameter	Description
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.
launched_after_datetime={date}	<p>(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".</p> <p>When <b>launched_after_datetime</b> and <b>launched_before_datetime</b> are unspecified, the service selects scans launched within the past 30 days.</p> <p>A date/time in the future returns an empty scans list.</p>
launched_before_datetime={date}	<p>(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".</p> <p>When <b>launched_after_datetime</b> and <b>launched_before_datetime</b> are unspecified, the service selects scans launched within the past 30 days.</p> <p>A date/time in the future returns a list of all scans (not limited to scans launched within the past 30 days).</p>
scan_type=certview	(Optional) List CertView VM scans only. This option will be supported when CertView GA is released and enabled for your account.

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.
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 <b>pci_only=1</b> 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 described 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={ <b>assets</b>   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.
ip={value}	<p>(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.</p> <p>ip is valid only when target_from=assets is specified.</p>
asset_groups={value}	<p>(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.</p> <p>asset_groups is valid only when target_from=assets is specified.</p> <p>These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.</p>
asset_group_ids={value}	<p>(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.</p> <p>asset_group_ids is valid only when target_from=assets is specified.</p> <p>These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.</p>
exclude_ip_per_scan={value}	<p>(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.</p> <p>exclude_ip_per_scan is valid only when target_from=assets is specified.</p>

Parameter	Description
tag_include_selector= {all   <b>any</b> }	(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   <b>any</b> }	(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={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.  use_ip_nt_range_tags is valid only when target_from=tags is specified.

Parameter	Description
iscanner_id={value}	<p>(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.</p> <hr/> <p>One of these parameters must be specified in a request: isscanner_name, isscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used.</p> <hr/> <p>These parameters are mutually exclusive and cannot be specified in the same request: isscanner_id and isscanner_name.</p>
iscanner_name={value}	<p>(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.</p> <hr/> <p>One of these parameters must be specified in a request for an internal scan: isscanner_name, isscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used.</p> <hr/> <p>These parameters are mutually exclusive and cannot be specified in the same request: isscanner_id and isscanner_name.</p>
default_scanner={0   1}	<p>(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.</p> <hr/> <p>One of these parameters must be specified in a request for an internal scan: isscanner_name, isscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used.</p> <hr/> <p>default_scanner is valid when the scan target is specified using one of these parameters: asset_groups, asset_group_ids.</p>

Parameter	Description
scanners_in_ag={0   1}	<p>(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.</p> <p>One of these parameters must be specified in a request for an internal scan: <code>iscanner_name</code>, <code>iscanner_id</code>, <code>default_scanner</code>, <code>scanners_in_ag</code>, <code>scanners_in_tagset</code>. When none of these are specified, External scanners are used.</p> <p><code>scanners_in_ag</code> is valid when the scan target is specified using one of these parameters: <code>asset_groups</code>, <code>asset_group_ids</code>.</p>
scanners_in_tagset={0   1}	<p>(Optional) Specify 1 to distribute the scan to scanner appliances that match the asset tags specified for the scan target.</p> <p>One of these parameters must be specified in a request for an internal scan: <code>iscanner_name</code>, <code>iscanner_id</code>, <code>default_scanner</code>, <code>scanners_in_ag</code>, <code>scanners_in_tagset</code>. When none of these are specified, External scanners are used.</p> <p><code>scanners_in_tagset</code> is valid when the <code>target_from=tags</code> is specified.</p>
scanners_in_network={value}	<p>(Optional) Specify 1 to distribute the scan to all scanner appliances in the network.</p>
option_title={value}	<p>(Optional) The title of the compliance option profile to be used.</p> <p>One of these parameters must be specified in a request: <code>option_title</code> or <code>option_id</code>. These are mutually exclusive and cannot be specified in the same request.</p>
option_id={value}	<p>(Optional) The ID of the compliance option profile to be used.</p> <p>One of these parameters must be specified in a request: <code>option_title</code> or <code>option_id</code>. These are mutually exclusive and cannot be specified in the same request.</p>



Parameter	Description
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
connector_name={value}	(Required for an EC2 scan) 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: <a href="http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions-availability-zones">http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions-availability-zones</a>
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}	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) 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 CertView type VM scan. For a this scan you must specify at least one target i.e. IPs, asset groups or FQDNs. Multiple values are comma separated. This option will be supported when CertView GA is released and enabled for your account.

# Scan Schedule Parameters

## Scan Schedule - Occurrence

Parameter	Description
<b>occurrence=daily</b>	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.
<b>occurrence=weekly</b>	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.
<b>occurrence=monthly</b>	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 an 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.

Parameter	Description
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   <b>no</b> }	(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 1 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.
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 1 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.
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}	<p>(Optional) Resume a paused scan in some number of hours. A valid value is an integer from 0-23.</p> <hr/> <p>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.</p> <hr/> <p>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.</p>
set_start_time={0   1}	<p>(Optional for Update only) Specify set_start_time=1 to update any of the start time parameters.</p> <hr/> <p>Must be specified with all start time parameters together: start_date, start_hour, start_minute, time_zone_code, observe_dst</p>

## Scan Schedule - Notifications

Parameter	Description
before_notify={0   1}	<p>(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.</p>
before_notify_unit={value}	<p>(Optional) Specify the time unit for when to send the before scan notification. Possible values are: days, hours, minutes.</p> <hr/> <p>This parameter is required when before_notify=1. Not valid when before_notify=0.</p>
before_notify_time={value}	<p>(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.</p> <hr/> <p>This parameter is required when before_notify=1. Not valid when before_notify=0.</p>

Parameter	Description
before_notify_message={value}	<p>(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.</p> <p>For update requests:</p> <ul style="list-style-type: none"> <li>- When not specified we keep the previous setting.</li> <li>- Specify an empty string to delete the last saved message.</li> </ul> <p>This parameter is only valid when before_notify=1.</p>
after_notify={0   1}	<p>(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.</p>
after_notify_message={value}	<p>(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.</p> <p>For update requests:</p> <ul style="list-style-type: none"> <li>- When not specified we keep the previous setting.</li> <li>- Specify an empty string to delete the last saved message.</li> <li>- If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the after notify message.</li> </ul> <p>This parameter is only valid when after_notify=1.</p>
recipient_group_ids={value}	<p>(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.</p> <p>For update requests:</p> <ul style="list-style-type: none"> <li>- When not specified we keep the previous setting.</li> <li>- Specify an empty string to delete the list of IDs.</li> <li>- If both notifications are disabled (before_notify=0 and after_notify=0) we will delete the list of IDs.</li> </ul> <p>This parameter is only valid when before_notify=1 or after_notify=1 is specified in the same request.</p>

## VM Scan Statistics

The VM Scan Statistics API (`/api/2.0/fo/scan/stats/`) is used to get details about vulnerability scans and assets that are waiting to be processed.

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 API Request and Output

#### API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/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_results.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:

The VM Recrypt Results DTD can be found at the following URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/scan/stats/vm\\_recrypt\\_results.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/stats/vm_recrypt_results.dtd)



# Share PCI Scan

The Share PCI Scan API v2 (`/api/2.0/fo/scan/pci/`) provides 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

The share PCI scan API (`/api/2.0/fo/scan/pci/`) with `action=share` is used to 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. For a share request, the allowed method is: POST.

The input parameters used to make a request to share a PCI scan are below.

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 Request

This sample request works on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Please be sure to replace the FQDN with the proper API server URL for your platform. For a partner platform, use the URL for your @customer platform API server. The header parameter “X-Requested-With” is also provided as an example.

### Sample:

```
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/1281646610.
5720'
'https://qualysapi.qualys.com/api/2.0/fo/scan/pci/'
```

## Sample Share Output

### Successful Share

When the request to share a PCI scan is successful, 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>2012-01-17T00:50:39Z</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>
```

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
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2012-01-04T14:54:01Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>This scan has already been shared with the Merchant
account.</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Get Share Status

The share PCI scan API (/api/2.0/fo/scan/pci/) with **action=status** is used to get the share status of a PCI scan that has already been shared. For a status request, the allowed methods are: POST and GET.

The input parameters used to make a request to get the PCI scan share status are below.

Parameter	Description
action=status	(Required) Specify “status” to return the status of a PCI scan export for a given scan report reference and PCI Merchant account.
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 exported to.

Sample Status Request

This sample request works on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Be sure to replace the FQDN with the proper API server URL for your platform. For a partner platform, use the URL for your @customer platform API server. The header parameter “X-Requested-With” is also provided as an example.

### Sample:

```
curl -s -H 'X-Requested-With: curl demo 2' -D headers.15 -b  
'QualysSession=38255848108d68a2feaf9ee664ca78a7; path=/api; secure' -d  
'action=status&merchant_username=manager1@qualys&scan_ref=scan/1281646610  
.5720' 'https://qualysapi.qualys.com/api/2.0/fo/scan/pci/'
```

### Sample Status Output

The PCI scan share status XML output uses the PCI scan share status DTD.

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_status.d  
td">  
<PCI_SCAN_SHARE_STATUS>  
  <RESPONSE>  
    <SCAN>  
      <MERCHANT_USERNAME>manager1@qualys</MERCHANT_USERNAME>  
      <SCAN_REF>scan/1281646610.5720</SCAN_REF>  
      <STATUS>Finished</STATUS>  
      <LAST_SHARED>1970-01-01T00:33:32Z</LAST_SHARED>  
    </SCAN>  
  </RESPONSE>  
</PCI_SCAN_SHARE_STATUS>
```

### PCI Scan Share Status DTD

An API request to get the share status of a PCI scan that has been shared returns XML output using the “pci\_scan\_share\_status.dtd” which can be found at the following URL (where <qualysapi.qualys.com> identifies the Qualys API server URL where your account is located):

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

The DTD for “pci\_scan\_share\_status.dtd” is provided in Appendix A.

# Scanner Appliances

The Scanner Appliance API v2 (**/api/2.0/fo/appliance/**) is used to get a list of the scanner appliances in your account - both physical and virtual - and to manage VLANs and static routes for appliances in your account. See Chapter 2, “Authentication Using the V2 APIs.”

Express Lite: This API is available to Express Lite users when Internal Scanning is enabled in the user’s account.

Permissions for using the Scanner Appliance API v2:

User Role	Permissions
Manager	View all scanner appliances in the subscription. Manage (add, remove) VLANs and static routes for all appliances.
Unit Manager	View scanner appliances in user’s business unit. Manage (add, remove) VLANs and static routes for appliances in their assigned business unit.
Scanner	View scanner appliances in user’s account.
Reader	View scanner appliances in user’s account.

## Scanner Appliance List

The Scanner Appliance List API v2 (**/api/2.0/fo/appliance/** with **action=list**) is used to 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).

The parameters used to request a scanner appliance list are described below.

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.

Parameter	Description
output_mode={ <b>brief</b>   full}	<p>(Optional) The amount of detail provided for each scanner appliance in the output: brief (default) or full.</p> <p>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).</p> <p>The “full” output includes the full appliance information, including the same details available in the Qualys user interface.</p>
scan_detail={0   1}	<p>(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.</p>
include_cloud_info={0   1}	<p>(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.</p>
busy={0   1}	<p>(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.</p>
scan_ref={value}	<p>(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.</p> <p>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.</p>
name={string}	<p>(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.</p>
ids={id1,id2,...}	<p>(Optional) List only scanner appliances (physical and virtual) that have certain IDs. Multiple IDs are comma separated.</p>

Parameter	Description
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   offline}	(Optional) Type of scanner appliances: physical, virtual, offline. Appears when output_mode=full is specified in API request.

### 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&include_cloud_info=1&output_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>
</CLOUD_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 type of scanner appliance.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.p04.eng.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>
```

DTD:

An API request to view a list of scanner appliances returns XML output using the “appliance\_list\_output.dtd” which can be found at the following URL (where <qualysapi.qualys.com> identifies the Qualys API server URL where your account is located):

```
https://<qualysapi.qualys.com>/api/2.0/fo/appliance/  
appliance_list_output.dtd
```

The DTD for “appliance\_list\_output.dtd” is provided in Appendix A.

**Manage VLANs and Static Routes**

Manage your VLANs and static routes for virtual and physical scanner appliances using the Virtual Scanner Appliance API (api/2.0/fo/appliance/?action=update) 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.

**Set VLANs on Scanner Appliance**

Use the “set\_vlans” parameter to specify one or more VLANs.

The format for a single VLAN is ID|IP\_ADDRESS|NETMASK|NAME, with pipe (|) used as a delimiter. All attributes are required (ID, IP\_ADDRESS, etc). 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.
IP_ADDRESS	A valid IPv4 IP address (dotted quad), such as 10.10.10.1
NETMASK	A valid network mask (dotted quad), such as 255.255.255.0
NAME	A valid name (can be empty). The name can be a maximum of 256 ASCII characters. The charater : (colon) is permitted. These characters are not permitted: , (comma), < (less than), > (greater than), " (double quote), & (ampersand),   (pipe), = (equals).

### API request (1 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 (multiple VLANs):

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"id=43463&set_vlans=1|10.10.10.1|255.255.255.0|vlan1,2|10.10.10.2|255.255.
.255.0|vlan2"
"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 IP\_ADDRESS|NETMASK|GATEWAY|NAME, with pipe (|) used as the delimiter. All attributes are required (IP\_ADDRESS, NETMASK, etc). 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
IP_ADDRESS	A valid IPv4 IP address (dotted quad), such as 10.10.26.0
NETMASK	A valid network mask (dotted quad), such as 255.255.255.0
GATEWAY	A valid IPv4 address (dotted quad), such as 10.10.25.255

Attribute	Description
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).

API request (1 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|SRoute1"  
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=update"
```

API request (multiple static routes):

```
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|Route1,10.10.2  
6.0|255.255.255.0|10.10.26.255|Route2"  
"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:  
"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>
  </RESPONSE>
</SIMPLE_RETURN>
...

```

## 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>
  ...
```

# Virtual Scanner Appliances

Use the Scanner Appliance API v2 (/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

Use these parameters:

Parameter	Description
action=create	(Required) The POST method must be used.
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 for XML output:

The DTD for the XML output can be found here (where qualysapi.qualys.com is the base URL for your Qualys platform:

[https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance\\_create\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_create_output.dtd)

## Update a Virtual Scanner

During update, you can add tags, remove and reset tags for your scanner appliances. Use these parameters:

Parameter	Description
action=update	(Required) The POST method must be used.
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.

### Sample 1

#### 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:

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>2014-04-03T12:12:45Z</DATETIME>
    <TEXT>Virtual scanner updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>17110</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### Sample 2

The request will add tags for windows agent and 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 3**

This request will assign the tags local\_host and local\_IP to the 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 a Virtual Scanner

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.

Use these parameters:

Parameter	Description
action=delete	(Required) The POST method must be used.
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>
```

# Physical Scanner Appliances

Using the Physical Scanner Appliance API v2 (/api/2.0/fo/appliance/physical/), Managers and Unit Managers can update physical scanner appliances.

## Update Physical Scanner

Use these parameters:

Parameter	Description
action=update	(Required) The POST method must be used.
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 <a href="#">Manage VLANs and Static Routes</a> .
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.

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.
set_routes={value}	Use this parameter to specify one or more routes for scanner. See <a href="#">Manage VLANs and Static Routes</a> .
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:

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>2016-10-01T00:12:29Z</DATETIME>  
    <TEXT>Physical scanner updated successfully</TEXT>  
    <ITEM_LIST>  
      <ITEM>  
        <KEY>ID</KEY>  
        <VALUE>5115</VALUE>  
      </ITEM>  
    </ITEM_LIST>  
  </RESPONSE>  
</SIMPLE_RETURN>
```

# KnowledgeBase

Qualys’ Software-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.

The KnowledgeBase API V2 (`api/2.0/fo/knowledge_base/vuln/?action=list`) allows API users to download a list of vulnerabilities from Qualys’ KnowledgeBase. This V2 API offers numerous benefits over the `knowledgebase_download.php` V1 function. 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. The GET or POST access method may be used to make an API request.

Authorized Qualys users have the ability to download vulnerability data using the KnowledgeBase API V2. Please contact Qualys Support or your sales representative if you would like to obtain authorization for your subscription.

## Permissions

User permissions for the KnowledgeBase API V2 are described below. Note: Your subscription must be granted permission to run this function. Please contact Qualys Support or your sales representative to receive this authorization.

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.
Auditor	No permission to download vulnerability data from the KnowledgeBase.

## Parameters

The input parameters for the KnowledgeBase API V2 are described below. 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
<code>action=list</code>	(Required) A flag used to request the download of vulnerability data from the KnowledgeBase.

Parameter	Description
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={ <b>Basic</b>   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.
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).
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).



Parameter	Description
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}	<p>(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.</p> <p>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.</p>
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, 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.

## Sample API Requests

These sample requests work on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Please be sure to replace the FQDN with the proper API server URL for your platform. For a partner platform, use the URL for your @customer platform API server.

**Sample 1.** Request all vulnerabilities in the KnowledgeBase showing basic details:

```
curl -u "user:password" -H "X-Requested-With: Curl" -X "POST"
-d "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/" >
output.txt
```

**Sample 2.** Request patchable vulnerabilities that have QIDs 1-200 showing all details:

```
curl -u "user:password" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&ids=1-200&is_patchable=1&details=All"
"https://qualysapi.qualys.com/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 "user:password" -H "X-Requested-With: Curl" -X "POST"
-d "action=list&last_modified_by_service_after=2011-07-20
&discovery_method=RemoteAndAuthenticated"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/" >
output.txt
```

## XML Output

A KnowledgeBase API request returns XML output using the `knowledge_base_vuln_list_output.dtd`, which can be found at the following URL:

```
https://<basurl>/api/2.0/fo/knowledge_base/vuln/  
knowledge_base_vuln_list_output.dtd
```

The DTD for the KnowledgeBase output is provided in Appendix A.

# Editing Vulnerabilities

The Edit Vulnerability API v2 (`/api/2.0/fo/knowledge_base/vuln/`) allows users to edit, reset and then 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) The action required for the API request: edit. The POST method must be used.
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"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

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>2017-03-02T08:51:59Z</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) The action required for the API request: reset. The POST method must be used.
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"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

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>2017-03-02T08:55:11Z</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) The action required for the API request: custom. The GET or POST method should be used.

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST  
"action=custom"  
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE KB_CUSTOM_VULN_LIST_OUTPUT SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/kb_custom_vu  
ln_list_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>
```

```
</RESPONSE>  
</KB_CUSTOM_VULN_LIST_OUTPUT>
```

## **XML Output**

DTD:

[https://<basurl>/api/2.0/fo/knowledge\\_base/vuln/kb\\_custom\\_vuln\\_list\\_output.dtd](https://<basurl>/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_list_output.dtd)

Refer to Appendix A, Customized Vulnerability List Output

# Static Search List

The Static Search List API (`/api/2.0/fo/qid/search_list/static/`) lets you create static search lists and get information about them.

User permissions for the Static Search API are 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 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

#### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/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
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/static/static_list_output.dtd">
<STATIC_SEARCH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2015-01-06T06:20:03Z</DATETIME>
    <STATIC_LISTS>
      <STATIC_LIST>
        <ID>381</ID>
        <TITLE><![CDATA[static search list]]></TITLE>
```



```

<GLOBAL>Yes</GLOBAL>
<OWNER>acme_tb</OWNER>
<CREATED><![CDATA[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>
<!-- 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

Refer to Appendix F, Static Search List Output

## Create static 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).
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

#### 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"  
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/static/"
```

#### 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>2015-09-01T21:32:40Z</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...)	<p>(Optional) QIDs/ranges to include in the search list. Multiple entries are comma separated.</p> <p>***QIDs specified will replace all existing ones defined for the search list, if any.</p> <p>qids cannot be specified with add_qids or remove_qids in the same request.</p>
add_qids=(num1, num2...)	<p>(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.</p> <p>add_qids cannot be specified with qids in the same request.</p>
remove_qids=(num1, num2...)	<p>(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.</p> <p>remove_qids cannot be specified with qids in the same request.</p>
comments={value}	(Optional) User defined comments.

## Sample

### 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"  
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/static/"
```

### 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>2015-09-01T21:32:40Z</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

### API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d  
"action=delete&id=136992"  
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/static/"
```

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>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>search list deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

# Dynamic Search List

The Dynamic Search List API (`/api/2.0/fo/qid/search_list/dynamic/`) lets you create dynamic search lists and get information about them.

User permissions for the Dynamic Search API are 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

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/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
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/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>
    <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

Refer to Appendix F, Dynamic Search List Output

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; 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

Parameter	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={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

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
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

Parameter	Value
cvss_base_operand={value}	Set the value to <b>1</b> to use the greater than equal to operand. Set the value to <b>2</b> 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 <b>1</b> to use the greater than equal to operand. Set the value to <b>2</b> 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 <b>1</b> to use the greater than equal to operand. Set the value to <b>2</b> 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 <b>1</b> to use the greater than equal to operand. Set the value to <b>2</b> 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
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

Parameter	Value
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

## Samples

### API request 1:

```
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"
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/"
```

### 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>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>New search list created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>136992</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### API request 2:

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"
"https://qualysapi.qualys.com/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

### API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d  
"action=update&id=136992"  
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/"
```

### 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>2015-09-01T21:32:40Z</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

#### API request:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&id=123456"
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/"
```

#### 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>2015-09-01T21:32:40Z</DATETIME>
    <TEXT>search list deleted successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>123456</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

# Vendor IDs and References

The Vendor API (`/api/2.0/fo/vendor/`) lists vendor IDs and names. This vendor information may be defined as part of dynamic search list query criteria. All users except Auditors have permission to run this APIs.

## Request 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.

## List vendor IDs and names

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/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
"https://qualysapi.qualys.com/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 -->

```

### **List vendor references for qids**

#### API request:

```

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/vendor/?action=list_vendor_refer
ences"

```

#### XML response:

```

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VENDOR_REFERENCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/vendor/vendor_reference_list_out
put.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:

```
<!-- QUALYS VENDOR_REFERENCE_LIST_OUTPUT DTD -->
<!ELEMENT VENDOR_REFERENCE_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, VENDOR_REFERENCES?)>
<!ELEMENT VENDOR_REFERENCES (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (QID?, REFERENCE_INFO+)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT REFERENCE_INFO (REFERENCE?, URL?)>
<!ELEMENT REFERENCE (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!-- EOF -->
```

## Report API

Report Share is a subscription level feature. When enabled, completed reports can be posted to Report Share where they can be shared with other users. This promotes collaboration on vulnerability issues within the IT infrastructure. Report Share is available through both the Qualys user interface and Qualys API.

Report Share is available to users with Enterprise accounts; it is not available to users with Express accounts. Please contact Qualys Support if you would like information on how to upgrade your account to use Report Share.

This chapter describes how to use the Report Share API, which is built on the API V2 Architecture.

These topics are covered:

- About Report Share
- Report List
- Launch Report
- Launch Scorecard
- Cancel Running Report
- Download Saved Report
- Delete Saved Report
- Schedule Report

# About Report Share

Report Share provides these enhanced reporting features:

- Allows for generation, storage and distribution of reports for large enterprise networks
- Enables API users to automate report generation, retrieval and management
- Report email notification (optional) allows users to review reports upon completion

The Report Share capabilities available in the Report Share API mirror the same capabilities available in the Qualys user interface. Users may opt in to receive report email notifications by editing their account in the Qualys user interface.

The Report Share APIs enable users to programmatically launch reports based on existing report templates in the user's account, as well as to list, manage and download saved reports in the user's account. When making an API request to launch a report, the user must specify the output format (each report type has a list of available output formats). While a report is running, the user can make API requests for a report list to check the percentage complete and when report generation has completed. Once the report is generated and saved to Report Share, the user can make an API request to fetch (download) the report. Like API requests for scans, the user has the option make API requests to cancel a running report and to delete a saved report.

Qualys manages report storage. Reports are available in Report Share storage until they expire 7 days after the report creation date. Each user is allocated an amount of disk space for reports. See the Qualys online help for more information.

The Report Share API allows users to perform the following actions.

Action	Supported Access Method	Description
Launch	POST	Launch a report for a selected report template and format.
List	GET POST	List reports in the user's Report Share storage space. Both in progress and saved reports are included.
Cancel	POST	Cancel a running report in the user's Report Share.
Delete	POST	Delete a report in the user's Report Share.
Fetch	GET POST	Download a report in the user's Report Share.

# Report List

The `/api/2.0/fo/report` resource with the parameter `action=list` is used to view a list of reports in the user's Report Share. The report list output includes all report types, including scorecard reports. Authentication is required for each API request. See "Authentication Using the V2 APIs."

The XML output identifies reports in progress and saved reports. This information is provided for each report: report ID, title, name of user who launched the report, the date launched, report format, report size (in megabytes), report status (finished or percentage complete), and number of days before the report will expire.

The GET or POST access method may be used to make a report list request.

User permissions for viewing reports are described below.

User Role	Permissions
Manager	View all reports in subscription.
Auditor	View all policy reports in subscription.
Unit Manager	View reports in user's business unit, including reports launched by the user and reports launched by other users in the same business unit.
Scanner	View reports launched by the user.
Reader	View reports launched by the user.

## Parameters

The parameters used to request a report list are described below.

Parameter	Description
<code>action=list</code>	(Required) A flag used to make a request for a report list.
<code>echo_request={0   1}</code>	(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.
<code>id={value}</code>	(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.
<code>state={value}</code>	(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.



Parameter	Description
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}	<p>(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.</p> <p>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".</p>

## Example

A sample report list API call (GET method) is shown below.

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

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/report_list_out
put.dtd">

<REPORT_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2009-10-30T22:32:15Z</DATETIME>
    <REPORT_LIST>
      <REPORT>
        <ID>42703</ID>
        <TITLE><![CDATA[Test now]]></TITLE>
        <TYPE>Scan</TYPE>
        <USER_LOGIN>acme_aa</USER_LOGIN>
        <LAUNCH_DATETIME>2009-10-30T17:59:22Z</LAUNCH_DATETIME>
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
        <SIZE>129.1 MB</SIZE>
        <STATUS>
          <STATE>Finished</STATE>
        </STATUS>
        <EXPIRATION_DATETIME>2009-11-
06T17:59:24Z</EXPIRATION_DATETIME>
```

```
</REPORT>
<REPORT>
  <ID>42700</ID>
  <TYPE>Scorecard</TYPE>
  <USER_LOGIN>acme_ts2</USER_LOGIN>
  <LAUNCH_DATETIME>2009-10-29T22:12:42Z</LAUNCH_DATETIME>
  <OUTPUT_FORMAT>SECURE_PDF</OUTPUT_FORMAT>
  <SIZE>18.1 KB</SIZE>
  <STATUS>
    <STATE>Finished</STATE>
  </STATUS>
  <EXPIRATION_DATETIME>2009-11-
05T22:12:44Z</EXPIRATION_DATETIME>
</REPORT>
<REPORT>
  <ID>42699</ID>
  <TYPE>Scorecard</TYPE>
  <USER_LOGIN>quays_ts2</USER_LOGIN>
  <LAUNCH_DATETIME>2009-10-29T21:52:19Z</LAUNCH_DATETIME>
  <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>
  <SIZE>19.87 KB</SIZE>
  <STATUS>
    <STATE>Finished</STATE>
  </STATUS>
  <EXPIRATION_DATETIME>2009-11-
05T21:52:21Z</EXPIRATION_DATETIME>
</REPORT>
</REPORT_LIST>
</RESPONSE>
</REPORT_LIST_OUTPUT>
```

## XML Output

A report list request (parameter **action=list**) returns XML output using the DTD “report\_list\_output.dtd” which can be found at the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/report/
report_list_output.dtd
```

The DTD for the report list XML output is provided in Appendix A.

# Launch Report

The `/api/2.0/fo/report` resource with the parameter **action=launch** is used to launch a report in the user's Report Share. Authentication is required for each API request. See Chapter 2, "Authentication Using the V2 APIs."

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.

The POST access method must be used to make a request to launch a report.

User permissions for launching reports are described below.

User Role	Permissions
Manager	Launch report for all assets (IPs, domains) in subscription.
Auditor	Launch policy report for all IPs in subscription.
Unit Manager	Launch report for assets in user's business unit.
Scanner	Launch report for assets in user's account.
Reader	Launch report for assets in user's account.

## Report Source

When launching a manual scan report, you specify a scan reference to include. Optionally you may specify IPs/ranges to restrict the report to certain IPs.

When launching other reports, you can specify asset groups and IPs/ranges to include. Hosts may be specified as follows:

Host Entry	Example
Single IP	123.123.123.1
Multiple IPs	123.123.123.1,123.123.123.4,123.123.123.5
IP Ranges	
IP Range	123.123.123.1-123.123.123.8
IP Range and Single IPs	10.10.10.1-10.10.10.100,64.41.134.60,64.41.134.66

When specifying hosts, these syntax elements may be used:

- Multiple IPs/ranges are separated by a comma (,).
- For an IP range, use a dash (-) to separate the first and last IP.

# All Report Requests

Input parameter for all API reporting requests are described below. See the following sections for input parameters per report type.

Parameter	Description
action=launch	(Required) A flag used to make a request to launch a report.
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.
template_id={value}	(Required) The template ID of the report you want to launch.  Use the <b>report_template_list.php</b> function to find the appropriate template ID.
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. When <b>output_format=pdf</b> is specified, the Secure PDF Distribution may be used. See "Launch Report Sample."  For a map report, a valid value is: pdf, html (a zip file), mht, xml, or csv  For a scan report, a valid value is: pdf, html (a zip file), mht, xml, csv, or docx  For a remediation report, a valid value is: pdf, html (a zip file), mht, or csv  For a compliance report (not PCI), a valid value is: pdf, html (a zip file), or mht  For a PCI compliance report, a valid value is: pdf or html (a zip file)  For a compliance policy report, a valid value is: pdf, html (a zip file), mht, xml, or csv  For a Qualys patch report, a valid value is: pdf, online, or csv
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.

## Launch Report Sample

A sample launch report API call (POST method) is shown below.

```
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>2013-06-20T21:45:23Z</DATETIME>
    <TEXT>New report launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1665</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

# Secure PDF Distribution

Once this feature is enabled for the subscription, Managers and Unit Managers can create encrypted PDF reports and securely distribute them to users via email. Want to learn more? See “Securely Distribute PDF Reports” in the Qualys online help.

Use these parameters when you launch a PDF report (**output\_format=pdf**).

Parameter	Description
pdf_password={value}	(Optional; Required for secure PDF distribution) The password to be used for encryption. Requirements: <ul style="list-style-type: none"><li>- the password must have a minimum of 8 characters (ascii), and a maximum of 32 characters</li><li>- the password must contain alpha and numeric characters</li><li>- the password cannot match the password for the user’s Qualys account.</li><li>- the password must follow the password security guidelines defined for your subscription (log in and go to Subscription Setup &gt; Security Options).</li></ul>
recipient_group={value}	(Optional; Optional for secure PDF distribution) 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 <b>recipient_group</b> parameter can only be specified when the <b>pdf_password</b> parameter is also specified.  The <b>recipient_group</b> parameter cannot be specified in the same request as <b>recipient_group_id</b>
recipient_group_id={value}	(Optional; Optional for secure PDF distribution) 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 <b>recipient_group_id</b> parameter can only be specified when the <b>pdf_password</b> parameter is also specified.  The <b>recipient_group_id</b> parameter cannot be specified in the same request as <b>recipient_group</b>

## Map Report

Input parameters for an API request that launches a map report are described below. Only valid parameters for this type of request are listed.

Parameter	Description
report_type=Map	(Optional) Specifies the template type of the report. For a map report, specify Map.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a map report, a valid value is: pdf, html (a zip file), mht, xml, or csv.
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
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 <b>ip_restriction</b> 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 <b>domain</b> 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 (manual)

Input parameters for an API request that launches a scan report including scan based findings are described below. Only valid parameters for this type of request are listed.

Parameter	Description
report_type=Scan	(Optional) Specifies the template type of the report. For a scan report, specify Scan.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a scan report, a valid value is: pdf, html (a zip file), mht, xml, or csv.

Parameter	Description
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
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.

## Scan Report: Host Based Findings (automatic)

Input parameters for an API request that launches an scan report including host based findings are below. Only valid parameters for this type of request are listed.

Parameter	Description
report_type=Scan	(Optional) Specifies the template type of the report. For a scan report, specify Scan.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a scan report, a valid value is: pdf, html (a zip file), mht, xml, or csv.
hide_header={0   1}	(Valid for CSV format only) Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
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. See also "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. Looking for asset group IDs? Use the <b>asset_group_list.php</b> function (in the API v1 User Guide).
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

Input parameters for an API request that launches a Qualys Patch Report are described below. Only valid parameters for this type of request are listed. By default, an API request to launch a patch report uses the report source defined in the report template.

Parameter	Description
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a patch, a valid value is: pdf, online, or csv.
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
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. See also “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. Looking for asset group IDs? Use the <b>asset_group_list.php</b> function (see the API v1 User Guide).

## Remediation Report

Input parameters for an API request that launches a remediation report are described below. Only valid parameters for this type of request are listed.

The parameters **ips** and/or **asset\_group\_ids** are used to specify hosts to include in the report. One or both parameters must be specified. When both parameters are specified, all hosts specified by the parameter values are combined (ANDed) and included in the report.

By default, tickets assigned to the current user are included in the report. Using the optional **assignee\_type** parameter, you can include all tickets in the user account.

Parameter	Description
report_type=Remediation	(Optional) Specifies the template type of the report. For a remediation report, specify Remediation.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a remediation report, a valid value is: pdf, html (a zip file), mht, or csv.

Parameter	Description
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
ips={value}	(Optional for remediation report) Specify IPs/ranges you want to include in the report. Multiple IPs and/or ranges are comma separated.
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. Looking for asset group IDs? Use the <b>asset_group_list.php</b> function (in the API v1 User Guide).
assignee_type={User   All}	(Optional for remediation report) Specifies whether the report will include tickets assigned to the current user, or all tickets in the user account. By default tickets assigned to the current user are included. Valid values are: User (default) or All.

## Compliance Report

Input parameters are described below for an API request that launches a compliance report based on vulnerability management data. Only valid parameters for this type of request are listed. Compliance reports are: Qualys Top 20 Report, SANS Top 20 Report, Qualys PCI Executive Report, and Qualys PCI Technical Report.

The parameters **ips** and/or **asset\_group\_ids** are used to specify hosts to include in the Qualys Top 10 Report and SANS Top 20 Report. One or both parameters must be specified. When both parameters are specified, all hosts specified by the parameter values are combined (ANDed) and included in the report.

Parameter	Description
report_type=Compliance	(Optional) Specifies the template type of the report. For a compliance report, specify Compliance.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a compliance report other than a PCI report, a valid value is: pdf, html (a zip file), or mht. For a PCI report, a valid value is: pdf or html (a zip file).

Parameter	Description
ips={value}	<p>(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.</p> <p>This parameter or the <b>asset_group_ids</b> parameter must be specified for these reports: Qualys Top 20 Report, 2008 SANS Top 20 Report.</p> <p>Optional: Qualys Top 20 Report, SANS Top 20 Report</p> <p>Invalid: PCI Executive Report, PCI Technical Report</p>
asset_group_ids={value}	<p>(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. Looking for asset group IDs? Use the <b>asset_group_list.php</b> function (in the API v1 User Guide).</p> <p>This parameter or the <b>ips</b> parameter must be specified for these reports: Qualys Top 20 Report, SANS Top 20 Report.</p> <p>Optional: Qualys Top 20 Report, SANS Top 20 Report</p> <p>Invalid: PCI Executive Report, PCI Technical Report</p>
report_refs={value}	<p>(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.</p> <p>Required: PCI Executive Report, PCI Technical Report</p> <p>Invalid: Qualys Top 20 Report, SANS Top 20 Report</p>

## Compliance Policy Report

Input parameters for an API request that launches a compliance policy report are described below. Only valid parameters for this type of request are listed.

Parameter	Description
report_type=Policy	(Optional) Specifies the template type of the report. For a compliance policy report, specify Policy.
output_format={value}	(Required) Specifies the output format of the report. One output format may be specified. For a compliance report other than a PCI report, a valid value is: pdf, html (a zip file), mht, xml, or csv.

Parameter	Description
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.
policy_id={value}	(Required) Specifies the policy to run the report on. A valid policy ID must be entered.
asset_group_ids={value}	<p>(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. Looking for asset group IDs? Use the <b>asset_group_list.php</b> function (in the API v1 User Guide).</p> <p>Want to limit your report to certain IP addresses? You can select asset group IDs (<b>asset_group_ids</b>), IP addresses/ranges (<b>ips</b>) or asset tags. See "Using Asset Tags."</p>
ips={value}	<p>(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.</p> <p>Want to limit your report to certain IP addresses? You can select asset group IDs (<b>asset_group_ids</b>), IP addresses/ranges (<b>ips</b>) or asset tags. See "Using Asset Tags."</p>
host_id={value}	<p>(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.</p> <p>This parameter must be specified with: <b>instance_string</b>.</p>
instance_string={value}	<p>(Optional) Specifies a single instance on the selected host. The instance string may be "os" or a string like "oracle10:1:1521:ora10204u".</p> <p>Use the "Compliance Posture Information" API v2 (with the endpoint /api/2.0/fo/compliance/posture/info) to find the appropriate instance string.</p> <p>This parameter must be specified with: <b>host_id</b>.</p>

## 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
<code>use_tags={0   1}</code>	(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, <code>use_tags=0</code> is used.
<code>tag_include_selector={all   <b>any</b>}</code>	(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.  <code>tag_include_selector</code> is valid only when <code>use_tags=1</code> is specified.
<code>tag_exclude_selector={all   <b>any</b>}</code>	(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.  <code>tag_exclude_selector</code> is valid only when <code>use_tags=1</code> is specified.
<code>tag_set_by={id   name}</code>	(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.  <code>tag_set_by</code> is valid only when <code>use_tags=1</code> is specified.
<code>tag_set_include={value}</code>	(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.  <code>tag_set_include</code> is valid only when <code>use_tags=1</code> is specified.
<code>tag_set_exclude={value}</code>	(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.  <code>tag_set_exclude</code> is valid only when <code>use_tags=1</code> 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
"http://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>
```

## Report Template List

The **report\_template\_list.php** function provides a list of available report templates, including template titles and IDs, in the user account. The report list includes templates for all report types.

To retrieve a list of report templates, use this URL:

[https://qualysapi.qualys.com/msp/report\\_template\\_list.php](https://qualysapi.qualys.com/msp/report_template_list.php)

The DTD for the XML document returned from **report\_template\_list.php** can be found at the following URL:

[https://qualysapi.qualys.com/report\\_template\\_list.dtd](https://qualysapi.qualys.com/report_template_list.dtd)

Sample report template list output is shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORT_TEMPLATE_LIST SYSTEM
"http://qualysapi.qualys.com/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>2014-02-12T18:09:10Z</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>2013-12-09T22:47:58Z</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>2013-11-11T17:11:55Z</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.

Sample report template list output is shown below:

```
<!DOCTYPE REPORT_TEMPLATE_LIST SYSTEM
"https://qualysapi.qualys.com/report_template_list.dtd">

<REPORT_TEMPLATE_LIST>
  <REPORT_TEMPLATE>
    <ID>12399</ID>
    <TYPE>Auto</TYPE>
    <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
    <TITLE><![CDATA[Executive Report]]></TITLE>
    <USER>
      <LOGIN><![CDATA[acme_ab12]]></LOGIN>
      <FIRSTNAME><![CDATA[Alice]]></FIRSTNAME>
      <LASTNAME><![CDATA[Bucher]]></LASTNAME>
    </USER>
    <LAST_UPDATE>2006-12-20T03:21:54Z</LAST_UPDATE>
```



```

    <GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>
<REPORT_TEMPLATE>
  <ID>12400</ID>
  <TYPE>Auto</TYPE>
  <TEMPLATE_TYPE>Scan</TEMPLATE_TYPE>
  <TITLE><![CDATA[Technical Report]]></TITLE>
  <USER>
    <LOGIN><![CDATA[acme_ab12]]></LOGIN>
    <FIRSTNAME><![CDATA[Alice]]></FIRSTNAME>
    <LASTNAME><![CDATA[Bucher]]></LASTNAME>
  </USER>
  <LAST_UPDATE>2006-12-22T23:11:24Z</LAST_UPDATE>
<GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>
<REPORT_TEMPLATE>
  <ID>12403</ID>
  <TYPE>Auto</TYPE>
  <TEMPLATE_TYPE>Compliance</TEMPLATE_TYPE>
  <TITLE><![CDATA[SANS Top 20 Report]]></TITLE>
  <USER>
    <LOGIN><![CDATA[System]]></LOGIN>
    <FIRSTNAME><![CDATA[System]]></FIRSTNAME>
    <LASTNAME><![CDATA[System]]></LASTNAME>
  </USER>
  <LAST_UPDATE>2004-08-09T18:07:17Z</LAST_UPDATE>
<GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>
<REPORT_TEMPLATE>
  <ID>12404</ID>
  <TYPE>Auto</TYPE>
  <TEMPLATE_TYPE>Compliance</TEMPLATE_TYPE>
  <TITLE><![CDATA[Qualys Top 20 Report]]></TITLE>
  <USER>
    <LOGIN><![CDATA[System]]></LOGIN>
    <FIRSTNAME><![CDATA[System]]></FIRSTNAME>
    <LASTNAME><![CDATA[System]]></LASTNAME>
  </USER>
  <LAST_UPDATE>2004-08-09T18:07:17Z</LAST_UPDATE>
<GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>

```

```
<REPORT_TEMPLATE>
  <ID>44154</ID>
  <TYPE>N/A</TYPE>
  <TEMPLATE_TYPE>Remediation</TEMPLATE_TYPE>
  <TITLE><![CDATA[Executive Remediation Report]]></TITLE>
  <USER>
    <LOGIN><![CDATA[System]]></LOGIN>
    <FIRSTNAME><![CDATA[System]]></FIRSTNAME>
    <LASTNAME><![CDATA[System]]></LASTNAME>
  </USER>
  <LAST_UPDATE>2006-11-04T02:37:00Z</LAST_UPDATE>
  <GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>
<REPORT_TEMPLATE>
  <ID>44155</ID>
  <TYPE>N/A</TYPE>
  <TEMPLATE_TYPE>Remediation</TEMPLATE_TYPE>
  <TITLE><![CDATA[Tickets per Vulnerability]]></TITLE>
  <USER>
    <LOGIN><![CDATA[System]]></LOGIN>
    <FIRSTNAME><![CDATA[System]]></FIRSTNAME>
    <LASTNAME><![CDATA[System]]></LASTNAME>
  </USER>
  <LAST_UPDATE>2006-11-04T02:37:00Z</LAST_UPDATE>
  <GLOBAL>1</GLOBAL>
</REPORT_TEMPLATE>
...
</REPORT_TEMPLATE>
</REPORT_TEMPLATE_LIST>
```

## XML Output

A launch report request returns XML output using the DTD “simple\_return.dtd”, which can be found at the following URL:

[https://qualysapi.qualys.com/api/2.0/simple\\_return.dtd](https://qualysapi.qualys.com/api/2.0/simple_return.dtd)

The DTD for the simple return XML output is provided in Appendix A.

# Launch Scorecard

The `/api/2.0/fo/report/scorecard` resource with the parameter **action=launch** is used to 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. Authentication is required for each API request. See Chapter 2, "Authentication Using the V2 APIs."

Service-provided scorecards and user-defined scorecards may be launched. The service-provided scorecards are:

- Asset Group Vulnerability Report. Identifies vulnerabilities with severity levels 3-5
- Ignored Vulnerabilities Report. Identifies vulnerabilities that are currently ignored
- Most Prevalent Vulnerabilities Report. Identifies vulnerabilities with the highest number of detected instances
- Most Vulnerable Hosts Report. Identifies hosts with the highest number of critical vulnerabilities
- Patch Report. Identifies hosts with missing patches and software

When a scorecard 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.

The POST access method must be used to make a request to launch a scorecard report.

User permissions for launching scorecard reports are described below.

User Role	Permissions
Manager	Launch scorecard report including all IP addresses in subscription.
Auditor	No permissions to launch scorecard reports.
Unit Manager	Launch scorecard report including IP addresses in user's business unit.
Scanner	Launch scorecard report including IP addresses in user's account.
Reader	Launch scorecard report including IP addresses in user's account.

# Parameters

The parameters used to launch a scorecard report are below. Parameters are classified as Required, Optional or Conditional (meaning they may be required depending on other parameters specified for the request and user account settings).

Parameter	Description
action=launch	(Required) A flag used to make a request to launch a scorecard report.
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 with Report Share. 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), mht, xml, or csv.  When <b>output_format=pdf</b> is specified, the Secure PDF Distribution may be used. See "Launch Report Sample."
hide_header={0   1}	(Valid for CSV format report only). Specify <b>hide_header=1</b> to omit the header information from the report. By default this information is included.

Parameter	Description
pdf_password={value}	<p>(Conditional for Manager or Unit Manager; not valid for other users)</p> <p>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.</p> <p>Conditions:</p> <p>a) The <b>pdf_password</b> parameter can only be specified by a Manager or Unit Manager.</p> <p>b) The <b>pdf_password</b> parameter can only be specified when Report Share is enabled for your subscription and the option "Enable Secure PDF Distribution" is selected (Setup &gt; Report Share).</p>
recipient_group={value}	<p>(Conditional for Manager or Unit Manager; not valid for other users)</p> <p>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.</p> <p>Conditions:</p> <p>a) The <b>recipient_group</b> parameter can only be specified when the <b>pdf_password</b> parameter is also specified.</p> <p>b) The <b>recipient_group</b> parameter can only be specified by a Manager or Unit Manager.</p> <p>c) The <b>recipient_group</b> parameter can only be specified when Report Share is enabled for your subscription and the option "Enable Secure PDF Distribution" is selected (Setup—&gt;Report Share).</p> <p>d) The <b>recipient_group</b> parameter cannot be specified in the same request as <b>recipient_group_id</b></p>

Parameter	Description
recipient_group_id={value}	<p>(Optional) 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 &gt; Distribution Groups and select Info for a group in the list.</p> <p>Conditions:</p> <p>a) The <b>recipient_group_id</b> parameter can only be specified when the <b>pdf_password</b> parameter is also specified.</p> <p>b) The <b>recipient_group_id</b> parameter can only be specified by a Manager or Unit Manager.</p> <p>c) The <b>recipient_group_id</b> parameter can only be specified when Report Share is enabled for your subscription and the option “Enable Secure PDF Distribution” is selected (Setup—&gt;Report Share).</p> <p>d) The <b>recipient_group_id</b> parameter cannot be specified in the same request as <b>recipient_group</b></p>
source={value}	<p>(Conditional) The source asset groups for the report. Specify <b>asset_groups</b> to select asset groups. Specify <b>business_unit</b> to select all the asset groups in a business unit.</p> <p>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.</p> <p>Conditions:</p> <p>a) The <b>source</b> parameter is required for a service-provided scorecard.</p> <p>b) For a user scorecard, the source selection specified in the <b>source</b> parameter replaces an existing source selection set in the scorecard attributes (as defined in your Qualys account). If you set this parameter to <b>asset_groups</b>, you must specify one of these parameters: <b>asset_groups</b> or <b>all_asset_groups</b>. If you set this parameter to <b>business_unit</b> then you must specify one or more of these parameters: <b>business_unit</b>, <b>division</b>, <b>function</b> and/or <b>location</b>.</p>

Parameter	Description
asset_groups={value}	<p>(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.</p> <p>Conditions:</p> <p>a) The <b>asset_groups</b> parameter can only be specified when <b>source=asset_groups</b>.</p> <p>b) These parameters cannot be specified for the same API request: <b>asset_groups</b> and <b>all_asset_groups</b>.</p>
all_asset_groups={1}	<p>(Conditional) Set to 1 to select all asset groups available in your account as the source asset groups for the scorecard report.</p> <p>Conditions:</p> <p>a) The <b>asset_groups</b> parameter can only be specified when <b>source=asset_groups</b>.</p> <p>b) These parameters cannot be specified for the same API request: <b>asset_groups</b> and <b>all_asset_groups</b>.</p>
business_unit={value}	<p>(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.</p> <p>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 (<b>business_unit=</b>), the existing business unit in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) When <b>source=business_unit</b>, one or more of these parameters must be specified: <b>business_unit</b>, <b>division</b>, <b>function</b> and/or <b>location</b>.</p> <p>b) The <b>business_unit</b> parameter can only be specified by a Manager.</p>

Parameter	Description
division={value}	<p>(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.</p> <p>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 (<b>division=</b>), the existing division tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) When <b>source=business_unit</b>, one or more of these parameters must be specified: <b>business_unit</b>, <b>division</b>, <b>function</b> and/or <b>location</b>.</p> <p>b) The <b>division</b> parameter can only be specified when <b>source=business_unit</b>.</p>
function={value}	<p>(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.</p> <p>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 (<b>function=</b>), the existing function tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) When <b>source=business_unit</b>, one or more of these parameters must be specified: <b>business_unit</b>, <b>division</b>, <b>function</b> and/or <b>location</b>.</p> <p>b) The <b>function</b> parameter can only be specified when <b>source=business_unit</b>.</p>



Parameter	Description
location={value}	<p>(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.</p> <p>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 (<b>location=</b>), the existing location tag in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) When <b>source=business_unit</b>, one or more of these parameters must be specified: <b>business_unit</b>, <b>division</b>, <b>function</b> and/or <b>location</b>.</p> <p>b) The <b>location</b> parameter can only be specified when <b>source=business_unit</b>.</p>
patch_qids={value}	<p>(Conditional for Patch Report scorecard; not valid for other scorecards)</p> <p>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.</p> <p>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 (<b>patch_qids=</b>), the existing patches QIDs list in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) The <b>patch_qids</b> parameter may be specified only for a Patch Report.</p> <p>b) For a Patch Report, <b>patch_qids</b> or <b>missing_qids</b> must be specified. Both parameters may be specified together.</p>

Parameter	Description
missing_qids={value}	<p>(Conditional for Patch Report scorecard; not valid for other scorecards)</p> <p>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.</p> <p>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 (<b>missing_qids=</b>), the existing missing QIDs list in the scorecard attributes is not included in the scorecard parameters submitted with the API request.</p> <p>Conditions:</p> <p>a) The <b>missing_qids</b> parameter may be specified only for a Patch Report.</p> <p>b) For a Patch Report, <b>patch_qids</b> or <b>missing_qids</b> must be specified. Both parameters may be specified together.</p>

## XML Output

A launch report request returns XML output using the DTD “simple\_return.dtd”, which can be found at the following URL:

`https://qualysapi.qualys.com/api/2.0/simple\_return.dtd`

The DTD for the simple return XML output is provided in Appendix A.

# Cancel Running Report

The `/api/2.0/fo/report` resource with the parameter `action=cancel` is used to cancel a running report in the user's Report Share. This function may be used to cancel a running scorecard report. Authentication is required for each API request. See Chapter 2, "Authentication Using the V2 APIs."

The POST access method must be used to make a request to cancel a running report.

User permissions for canceling running reports are described below.

User Role	Permissions
Manager	Cancel all running reports in subscription.
Unit Manager	Cancel running reports in user's business unit, including reports launched by the user and reports launched by other users in the same business unit.
Scanner	Cancel running reports launched by the user.
Reader	Cancel running reports launched by the user.

## Parameters

The parameters used to cancel a running report are described below.

Parameter	Description
action=cancel	(Required) A flag used to make a request to cancel a running report.
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.

## Example

A sample API call to cancel a running report in Report Share (POST method) is shown below.

```
curl -H "X-Requested-With: Curl Sample"
-d "action=cancel&id=1462"
-b "QualysSession=71e6cda2a35d2cd404cddaf305ea0208; path=/api;
secure" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

## XML Output

A cancel report request (parameter **action=cancel**) returns XML output using the DTD “simple\_return.dtd”, which can be found at the following URL:

`https://qualysapi.qualys.com/api/2.0/simple\_return.dtd`

The DTD for the simple return XML output is provided in Appendix A.

# Download Saved Report

The `/api/2.0/fo/report` resource with `action=fetch` is used to download a saved report in the user’s account. You can download all report types (map, scan, patch, authentication, scorecard, remediation, compliance). Just tell us the ID of the report you want to download. The GET or POST access method may be used to make a request.

Statistics information for UDCs is reported using <STATS> under <STATISTICS>. We use this format for Unix directory search, Windows directory search, and Windows group membership check.

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

User permissions are below.

User Role	Permissions
Manager	Download all saved reports in subscription.
Unit Manager	Download saved reports in user’s business unit, including reports launched by the user and reports launched by other users in the same business unit.
Scanner	Download saved reports launched by the user.
Reader	Download saved reports launched by the user.

## Parameters

Use these parameters:

Parameter	Description
<code>action=fetch</code>	(Required) A flag used to make a request to download (fetch) a saved report.
<code>id={value}</code>	(Required) Specifies the report ID of a saved report that you want to download. The status of the report must be “finished”.
<code>echo_request={0   1}</code>	(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  
cXV---= -F action=list  
https://qualysapi.qualys.com/api/2.0/fo/report/
```

**Response:**

```
<?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>2014-07-02T15:29:52Z</DATETIME>  
    <REPORT_LIST>  
      <REPORT>  
        <ID>7592049</ID>  
        <TITLE><![CDATA[Fixed Vuln Report]]></TITLE>  
        <TYPE>Scan</TYPE>  
        <USER_LOGIN>acme_ur15</USER_LOGIN>  
        <LAUNCH_DATETIME>2014-07-02T14:52:45Z</LAUNCH_DATETIME>  
        <OUTPUT_FORMAT>HTML</OUTPUT_FORMAT>  
        <SIZE>-</SIZE>  
        <STATUS>  
          <STATE>Running</STATE>  
          <MESSAGE><![CDATA[Rendering...]]></MESSAGE>  
          <PERCENT>80</PERCENT>  
        </STATUS>  
        <EXPIRATION_DATETIME>2014-07-30T14:52:48Z</EXPIRATION_DATETIME>  
      </REPORT>  
      ...  
      <REPORT>  
        <ID>7589800</ID>  
        <TITLE><![CDATA[My Authentication Report]]></TITLE>  
        <TYPE>Authentication</TYPE>  
        <USER_LOGIN>acme_ee17</USER_LOGIN>  
        <LAUNCH_DATETIME>2014-07-02T07:00:21Z</LAUNCH_DATETIME>  
        <OUTPUT_FORMAT>PDF</OUTPUT_FORMAT>  
        <SIZE>15 KB</SIZE>  
        <STATUS>  
          <STATE>Finished</STATE>  
        </STATUS>  
        <EXPIRATION_DATETIME>2014-07-
```

```
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
```

API request

Sample API request:

```
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"
```

XML output

The XML output uses a DTD for the report you've downloaded. For example, if you download a scan report with host based findings (automatic data) then the report uses this DTD (where qualysapi.qualys.com is your Qualys API platform):

```
https://qualysapi.qualys.com/asset_data_report.dtd
```

**Learn more** Check out descriptions of various report DTDs in our user guides.

Report	DTD (description)
Scan Results	scan-1.dtd (API v1 User Guide, Appendix A)
Scan Report Host with Based Findings (automatic)	asset_data_report.dtd (API v1 User Guide, Appendix D)
Map Results	map.dtd (API v1 User Guide, Appendix B)
Scorecard Report	multiple DTDs (Appendix E)

Report	DTD (description)
Authentication Report	compliance_authentication_report.dtd (Appendix C)
Compliance Policy Report	compliance_policy_report.dtd (Appendix C)

## Sample Report API

### API request (Fetch report):

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -d  
"action=fetch&id=8188" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM  
"https://qualysapi.qualys.com/compliance_policy_report.dtd">  
<COMPLIANCE_POLICY_REPORT>  
  ...  
<FILTERS>  
  <POLICY><![CDATA[UDCs - policy]]></POLICY>  
  <POLICY_LOCKING><![CDATA[Unlocked]]></POLICY_LOCKING>  
  <POLICY_LAST_EVALUATED><![CDATA[09/01/2016 at 08:08:37  
(GMT)]]></POLICY_LAST_EVALUATED>  
</FILTERS>  
</HEADER>  
<SUMMARY>  
  <TOTAL_ASSETS>1</TOTAL_ASSETS>  
  <TOTAL_CONTROLS>39</TOTAL_CONTROLS>  
  <CONTROL_INSTANCES>  
    <TOTAL>22</TOTAL>  
    <TOTAL_PASSED>12</TOTAL_PASSED>  
    <TOTAL_FAILED>2</TOTAL_FAILED>  
    <TOTAL_ERROR>8</TOTAL_ERROR>  
    <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>  
  </CONTROL_INSTANCES>  
<HOST_STATISTICS>  
  <HOST_INFO>  
    <IP><![CDATA[10.10.10.10]]></IP>  
    <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>  
    <DNS><![CDATA[win7-10-10]]></DNS>  
    <NETBIOS><![CDATA[WIN7-10-10]]></NETBIOS>  
    <OPERATING_SYSTEM><![CDATA[Windows 7 Ultimate 64 bit Edition  
Service Pack 1]]></OPERATING_SYSTEM>  
    <LAST_SCAN_DATE><![CDATA[2016-08-04T05:20:49Z]]></LAST_SCAN_DATE>  
  ...  
</HOST_INFO>  
</HOST_STATISTICS>  
</SUMMARY>  
</COMPLIANCE_POLICY_REPORT>  
</HEADER>  
<NAME>  
  <![CDATA[ Policy Report Template ]]>
```



```

</NAME>
<GENERATION_DATETIME>2016-09-06T04:58:09Z</GENERATION_DATETIME>
<COMPANY_INFO>
  <NAME>
    ...
  <CHECK>
    <NAME>CHECK1</NAME>
    <DP_NAME>custom.win_group_membership.1001037</DP_NAME>
    <EXPECTED logic="OR">
      <CRITERIA>
        <EVALUATION><![CDATA[contains regular expression
list]]></EVALUATION>
        <V><![CDATA[. *]]></V>
      </CRITERIA>
    </EXPECTED>
    <ACTUAL lastUpdated="2016-08-04T05:20:49Z">
      <V><![CDATA[WIN7-10-10\Administrator]]></V>
      <V><![CDATA[S-1-5-21-2714588763-2906973749-3247541722-
1394]]></V>
      <V><![CDATA[S-1-5-21-2714588763-2906973749-3247541722-
1109]]></V>
    </ACTUAL>
    <STATISTICS>
      <STATS><![CDATA[Group members total: 3]]></STATS>
      <STATS><![CDATA[Group members reported: 3]]></STATS>
      <STATS><![CDATA[Limit reached: no
]]></STATS>
    </STATISTICS>
  </CHECK>
  ...

```

# Delete Saved Report

The `/api/2.0/fo/report` resource with the parameter **action=delete** is used to delete a saved report in the user's Report Share. This function may be used to delete a saved scorecard report in the user's Report Share. Authentication is required for each API request. See "Authentication Using the V2 APIs."

The POST access method must be used to make a request to delete a saved report.

User permissions for deleting saved reports are described below.

User Role	Permissions
Manager	Delete all saved reports in the subscription.
Unit Manager	Delete saved reports in user's business unit, including reports launched by the user and reports launched by other users in the same business unit.
Scanner	Delete saved reports launched by the user.
Reader	Delete saved reports launched by the user.

## Parameters

The parameters used to delete a saved report are described below.

Parameter	Description
action=delete	(Required) A flag used to make a request to delete a saved report.
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.

## Example

A sample API call to download a saved report in Report Share (POST method) is shown below.

```
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/scan/"
```

## XML Output

A delete report request (parameter **action=delete**) returns XML output using the DTD “simple\_return.dtd”, which can be found at the following URL:

`https://qualysapi.qualys.com/api/2.0/simple\_return.dtd`

The DTD for the simple return XML output is provided in Appendix A.

# Schedule Report

The Schedule Report API v2 (/api/2.0/fo/schedule/report/) allows you to list scheduled reports in your account and launch new scheduled reports.

## List Scheduled Reports

Use these parameters:

Parameter	Description
action=list	(Required)
id={value}	(Optional) Show only 1 scheduled report that has the report ID you specify.
is_active={true   false}	(Optional) Active and inactive scheduled reports are listed by default. Set to “true” to list active scheduled reports only, or set to “false” to list inactive scheduled reports only.

## Example

A sample API call to list all scheduled reports is shown below.

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

## XML Output

A request to list scheduled reports returns XML output using the DTD “schedule\_report\_list\_output.dtd”, which can be found at the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/schedule/report/schedule_report_list_output.dtd
```

The DTD for the schedule report list XML output is provided in Appendix A.

## Launch Scheduled Report

Use these parameters:

Parameter	Description
action=launch_now	(Required)
id={value}	(Required) A valid scheduled report ID.

## Example

A sample API call to launch a scheduled report with ID 12345 is shown below.

```
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/"
```

## XML Output

A launch scheduled report request returns XML output using the DTD “simple\_return.dtd”, which can be found at the following URL:

```
https://qualysapi.qualys.com/api/2.0/simple_return.dtd
```

The DTD for the simple return XML output is provided in Appendix A.

## Asset API

The Asset API provides information about the hosts in the user account. The host list API function is used to list information about scanned hosts in the user account, including hosts assigned to the VM application and/or PC application.

This chapter describes how to use the Asset API, which is built on the API V2 Architecture. These APIs are covered:

- IP List
- Host List
- Host List Detection
- Excluded Hosts List
- Excluded Hosts Change History
- Manage Excluded Hosts
- Purge Hosts
- Virtual Host List
- Take Actions on Virtual Hosts
- Restricted IPs List
- Add IPs
- Update IPs
- Manage Asset Groups
- Asset Search Report

# IP List

The IP List API v2 (**/api/2.0/fo/asset/ip/?action=list**) is used to view a list of 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. The GET or POST access method may be used to make an API request.

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

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

## Permissions

User permissions are described below.

User Role	Permissions
Manager	View IP addresses for all hosts in subscription.
Auditor	View IP addresses for all compliance hosts in subscription.
Unit Manager	View IP addresses in user’s business unit. To view IP addresses for compliance hosts, the “Manage compliance” permission must be granted in the user’s account.
Scanner	View IP addresses in user’s account. To view IP addresses for compliance hosts, the “Manage compliance” permission must be granted in the user’s account.
Reader	View IP addresses in user’s account. To view IP addresses for compliance hosts, the “Manage compliance” permission must be granted in the user’s account.

## Parameters

The parameters used to make an IP list request are described below.

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).

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 ID.
tracking_method={value}	(Optional) Show only IP addresses/ranges which have a certain tracking method. A valid value is: IP, DNS, or NETBIOS.
compliance_enabled={0   1}	<p>(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.</p> <p>Use this parameter to filter the IP list to show either: 1) a list of compliance IP addresses, or 2) a list of vulnerability management IP addresses.</p> <p>Specify 1 to list compliance IP addresses in the user's account. These hosts are assigned to the policy compliance module.</p> <p>Specify 0 to list hosts which are not assigned to the policy compliance module.</p> <p>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.</p> <p>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.</p> <p>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.</p>

## XML Output

DTD: [https://qualysapi.qualys.com/api/2.0/fo/asset/ip/ip\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/asset/ip/ip_list_output.dtd)

The DTD described in Appendix B, IP List Output.

## Sample IP List

Sample IP list output is below.

```
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/asset/ip/
ip_list_output.dtd">
```



```
<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2008-05-21T13:32:17Z</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>
```

# Host List

The Host List API v2 (resource `/api/2.0/fo/asset/host/` with parameter **action=list**) is used to view a list of scanned hosts in the user 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. Optional input parameters support filtering the list. The GET or POST access method may be used to make an API request.

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.

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

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

## User Permissions

User permissions are described below.

User Role	Permissions
Manager	View all scanned hosts in subscription.
Auditor	View all scanned compliance hosts in subscription.
Unit Manager	View scanned hosts in user’s business unit. To view compliance hosts, the “Manage compliance” permission must be granted in the user’s account.
Scanner	View scanned hosts in user’s account. To view compliance hosts, the “Manage compliance” permission must be granted in the user’s account.
Reader	View scanned hosts in user’s account. To view compliance hosts, the “Manage compliance” permission must be granted in the user’s account.

## Parameters

The parameters used to make a host list request are described below.

Parameter	Description
action=list	(Required) A flag used to make a host 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.
truncation_limit={value}	<p>(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).</p> <p>If the requested list identifies more host records than the truncation limit, then the XML output includes the &lt;WARNING&gt; element and the URL for making another request for the next batch of host records. See "Sample Record Limit Exceeded Warning".</p> <p>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.</p>
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).
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.

Parameter	Description
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.
details={ <b>Basic</b>   Basic/AGs   All   All/AGs   None}	<p>(Optional) Show the requested amount of host information for each host. A valid value is: Basic, Basic/AGs, All, All/AGs, or None.</p> <p>Basic (default) Show basic host information. Basic host information includes the host ID, IP address, tracking method, DNS and NetBIOS hostnames, and operating system.</p> <p>Basic/AGs Show basic host information plus asset group information. Asset group information includes the asset group ID and title.</p> <p>All. Show all host information. All host information includes the basic host information plus the last vulnerability and compliance scan dates.</p> <p>All/AGs. Show all host information plus asset group information. Asset group information includes the asset group ID and title.</p> <p>None. Show only the host ID.</p>
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}	<p>(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".</p> <p>Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user is granted permissions to manage compliance information.</p>

Parameter	Description
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.
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".
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
compliance_enabled={0   1}	<p>(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.</p> <p>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.</p> <p>Specify 1 to list scanned compliance hosts in the user’s account. These hosts are assigned to the policy compliance module.</p> <p>Specify 0 to list scanned hosts which are not assigned to the policy compliance module.</p> <p>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).</p>
os_pattern={expression}	<p>(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.</p> <p><b>Important Note:</b> The regular expression string you enter must follow the PCRE standard and it must be URL encoded.</p> <p>Sample regular expression strings for matching operating system names: <a href="#">Sample OS Pattern Filters</a></p> <p>For information about the Perl Compatible Regular Expressions (PCRE) standard visit: <a href="http://php.net/manual/en/book.pcre.php">http://php.net/manual/en/book.pcre.php</a></p> <p>For the PCRE syntax, see: <a href="http://php.net/manual/en/reference.pcre.pattern.syntax.php">http://php.net/manual/en/reference.pcre.pattern.syntax.php</a></p> <p><a href="http://www.php.net/manual/en/reference.pcre.pattern.posix.php">http://www.php.net/manual/en/reference.pcre.pattern.posix.php</a></p>

## Report on hosts using asset tags

The input parameters below allow you to report on hosts using 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.
show_tags={0   1}	(Optional) Specify 1 to display asset tags associated with each host in the XML output.

## EC2 metadata

These parameters allow you to manage assets using EC2 metadata.

Parameter	Description
host_metadata={value}	(Optional) Specify the name of the cloud provider to show the assets managed by that cloud provider, i.e. EC2. Note: Only supports fetching EC2 assets for now.
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify the EC2 instance fields to fetch the data for.  Data can be fetched for the following fields: accountId, region, availabilityZone, instanceId, instanceType, imageId, kernelId.

## XML Output

DTD: `https://<base_url>/api/2.0/fo/asset/host/host_list_output.dtd`

The DTD described in Appendix B, Host List Output.

## Samples

### Fetch region, accountId, and instanceId info for EC2 assets

#### 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>2016-11-15T09:50:46Z</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/instanceId]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[i-0bb87c3281243cdfd]]></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

A truncated response is returned when the API request returns more host records than the truncation limit. 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>1000 record limit exceeded. Use URL to get next batch
of results.</TEXT>

        <URL><![CDATA[https://qualysapi.qualys.com/api/2.0/fo/asset/host/?
action=list&id_min=2400356]]></URL>
    </WARNING>
</RESPONSE>
...

```

## Host List Detection

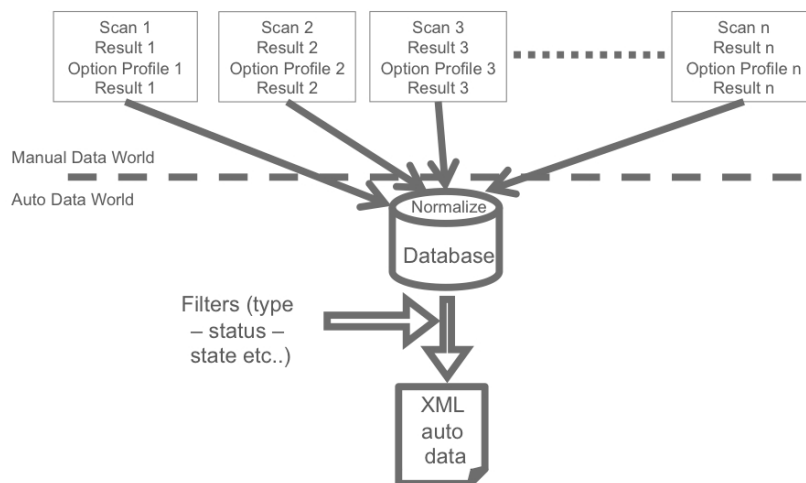
The Host List Detection API v2 (resource `/api/2.0/fo/asset/host/vm/detection/` with parameter `action=list`) gives API users the ability to obtain “automatic” vulnerability detection data that can be easily imported into a third party solution. Using the host detection API users can request a list of hosts with the hosts latest vulnerability data, based on the “automatic” data available in the user’s account. The GET or POST access method may be used to make an API request.

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

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

The new host list detection API is recommended as a replacement for other Qualys APIs when the API user wants to manage “automatic” data and integrate this with third party applications. For many third party applications this API is a replacement for the following existing Qualys APIs: `asset_range_info.php`, `asset_data_report.php`, `asset_search.php` and `get_host_info.php`.

Qualys normalizes the vulnerability scan results into the database using a complex and sophisticated process. This mechanism generates what is called the vulnerability “automatic data”. Automatic 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. Automatic 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).

## Use Cases

The detection API is most likely 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 “automatic” vulnerability data for hosts in your account, as described in this section.

**Step 2.** Use the KnowledgeBase 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:

```
https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/?action=list&ids=90082
```

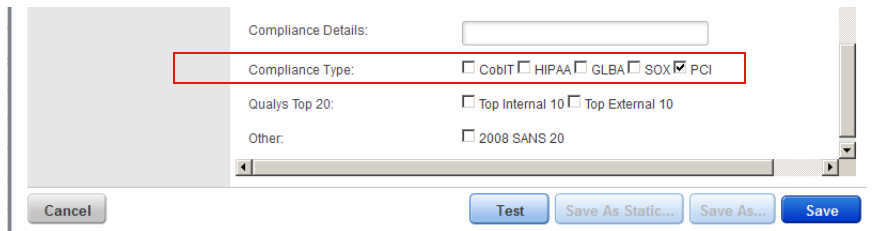
where “qualysapi.qualys.com” is the name of the API server where your account is located (in this case US Platform 1). If your account is located on another platform please insert the appropriate platform URL. For example “qualysapi.qualys.eu” if your account is located on the EU platform.

**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”:

```
https://qualysapi.qualys.com/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). If your account is located on another platform please insert the appropriate platform URL. For example “qualysapi.qualys.eu” if your account is located on the EU platform.

## Asset Search Portal Capability

The new host detection API endpoint allows users to do the same kind of searches as the Asset Search Portal user interface (under Assets > Asset Search) using these search parameters: Asset Groups, IPs/Ranges, Operating Systems, QID and more.

The host detection API offers users more search parameters and capability than the Asset Search user interface. Using the API users can get the details of vulnerability detections. Also, the API allows users to do more advanced searches on QIDs using all the power of search lists.

## User Permissions

User permissions are described below.

User Role	Permissions
Manager	View all VM scanned hosts in subscription.
Auditor	No permissions to view VM scanned hosts.
Unit Manager	View VM scanned hosts in user's business unit.
Scanner	View VM scanned hosts in user's account.
Reader	View VM scanned hosts in user's account.

## 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.

### API Request and Detection Filters.

Parameter	Description
action=list	(Required) Specify <b>action=list</b> to view a list of detection records for VM scanned hosts.
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 <b>show_results=0</b> to exclude the results. If you exclude the results, CSV will have an empty <b>Results</b> column, and XML will not contain the <b>Results</b> tag.
show_reopened_info={0   1}	(Optional) When not specified, reopened info for reopened vulnerabilities is not included in the output. Specify <b>show_reopened_info=1</b> to include reopened info i.e. first/last reopened date, times reopened.

Parameter	Description
arf_kernel_filter= {0 1 2 3 4}	<p>(Optional) Identify vulnerabilities found on running or non-running Linux kernels.</p> <p>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.</p> <p>When unspecified, vulnerabilities are not filtered based on kernel activity. &lt;AFFECT_RUNNING_KERNEL&gt; does not appear in the output.</p> <p>When set to 0, vulnerabilities are not filtered based on kernel activity. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output for kernel related vulnerabilities.</p> <p>When set to 1, exclude kernel related vulnerabilities that are not exploitable (found on non-running kernels). &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output for kernel related vulnerabilities.</p> <p>When set to 2, only include kernel related vulnerabilities that are not exploitable (found on non-running kernels). &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output with a value of 0 for each detection.</p> <p>When set to 3, only include kernel related vulnerabilities that are exploitable (found on running kernels). &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output with a value of 1 for each detection.</p> <p>When set to 4, only include kernel related vulnerabilities. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output with a value of 0 or 1 for each detection.</p> <hr/> <p>Note that <b>active_kernels_only</b> is deprecated and will be removed in a future release. Please use <b>arf_kernel_filter</b> instead.</p> <hr/>

Parameter	Description
arf_service_filter= {0 1 2 3 4}	<p>(Optional) Identify vulnerabilities found on running or non-running ports/services.</p> <p>When unspecified, vulnerabilities are not filtered based on running ports/services. &lt;AFFECT_RUNNING_SERVICE&gt; does not appear in the output.</p> <p>When set to 0, vulnerabilities are not filtered based on running ports/services. &lt;AFFECT_RUNNING_SERVICE&gt; appears in the output for service related vulnerabilities.</p> <p>When set to 1, exclude service related vulnerabilities that are not exploitable (found on non-running ports/services). &lt;AFFECT_RUNNING_SERVICE&gt; appears in the output for service related vulnerabilities.</p> <p>When set to 2, only include service related vulnerabilities that are not exploitable (found on non-running ports/services). &lt;AFFECT_RUNNING_SERVICE&gt; appears in the output with a value of 0 for each detection.</p> <p>When set to 3, only include exploitable service related vulnerabilities (found on running ports/services). &lt;AFFECT_RUNNING_SERVICE&gt; appears in the output with a value of 1 for each detection.</p> <p>When set to 4, only include service related vulnerabilities. &lt;AFFECT_RUNNING_SERVICE&gt; appears in the output with a value of 0 or 1 for each detection.</p>
arf_config_filter= {0 1 2 3 4}	<p>(Optional) Identify vulnerabilities that may or may not be exploitable due to the current host configuration.</p> <p>When unspecified, vulnerabilities are not filtered based on host configuration. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; does not appear in the output.</p> <p>When set to 0, vulnerabilities are not filtered based on host configuration. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; appears in the output for config related vulnerabilities.</p> <p>When set to 1, exclude vulnerabilities not exploitable due to host configuration. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; appears in the output for config related detections.</p> <p>When set to 2, only include config related vulnerabilities that are not exploitable. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; appears in the output with a value of 0 for each detection.</p> <p>When set to 3, only include config related vulnerabilities that are exploitable. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; appears in the output with a value of 1 for each detection.</p> <p>When set to 4, only include config related vulnerabilities. &lt;AFFECT_EXPLOITABLE_CONFIG&gt; appears in the output with a value of 0 or 1 for each detection.</p>

Parameter	Description
active_kernels_only= {0 1 2 3}	<p>Optional) Identify vulnerabilities related to running and non-running kernels in the output in the tag &lt;AFFECT_RUNNING_KERNEL&gt;.</p> <p>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.</p> <p>When unspecified, vulnerabilities are not filtered based on kernel activity. &lt;AFFECT_RUNNING_KERNEL&gt; does not appear in the output for kernel related vulnerabilities.</p> <p>When set to 0, vulnerabilities are not filtered based on kernel activity. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output for kernel related vulnerabilities.</p> <p>When set to 1, exclude vulnerabilities found on non-running Linux kernels. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output for kernel related vulnerabilities.</p> <p>When set to 2, only include vulnerabilities found on non-running Linux kernels. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output with a value of 0 for all vulnerabilities.</p> <p>When set to 3, only include vulnerabilities found on running Linux kernels. &lt;AFFECT_RUNNING_KERNEL&gt; appears in the output with a value of 1 for all vulnerabilities.</p> <hr/> <p>Note that <b>active_kernels_only</b> is deprecated and will be removed in a future release. Please use <b>arf_kernel_filter</b> instead.</p>
output_format={ <del>XML</del>   CSV   CSV_NO_METADATA}	<p>(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. A valid value is XML, CSV, or CSV_NO_METADATA.</p> <p>XML (default). Specifies XML format for the output.</p> <p>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 <b>echo_request=1</b> is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable).</p> <p>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.</p>



Parameter	Description
<code>suppress_duplicated_data_from_csv={0   1}</code>	<p>(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.</p> <p>This parameter must be specified with: <b>output_format=CSV</b> or <b>output_format=CSV_NO_METADATA</b>.</p>
<code>truncation_limit={value}</code>	<p>(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.</p> <p>If the requested list identifies more host records than the truncation limit and <b>output_format=XML</b>, then the XML output includes the &lt;WARNING&gt; element and the URL for making another request for the next batch of host records.</p> <p>If the requested list identifies more host records than the truncation limit and <b>output_format=CSV</b>, 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.</p> <p>See these sections for further information:  “Sample 2: Host List Detection XML Output - With Truncation”  “Sample 4: Host List Detection CSV Output - With Truncation”  “Sample Script for Pagination Logic”</p>
<code>max_days_since_detection_updated={value}</code>	<p>(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.</p> <p>One of these parameters may be specified in the same request: <code>detection_updated_since</code>, <code>max_days_since_detection_updated</code></p>

Parameter	Description
detection_updated_since={value}	<p>(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”.</p> <p>Tip: You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections shown to a specific date range.</p> <p>One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated</p>
detection_updated_before={value}	<p>(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”.</p> <p>Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range.</p> <p>One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated</p>
detection_processed_before={date}	<p>(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”.</p>
detection_processed_after={date}	<p>(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”.</p>

**Host Filters.** These input parameters are used to filter hosts. All of these parameters are optional.

Parameter	Description
ids={value}	<p>(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.</p>

Parameter	Description
id_min={value}	(Optional) Show only hosts which have a minimum host ID value.
id_max={value}	(Optional) Show only hosts which have a maximum host ID value. A valid host ID is required.
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).
ag_ids={value}	<p>(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.</p> <p>The <b>ag_ids</b> and <b>ag_titles</b> parameters are mutually exclusive and cannot be specified together in the same request.</p>
ag_titles={value}	<p>(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).</p> <p>The <b>ag_ids</b> and <b>ag_titles</b> parameters are mutually exclusive and cannot be specified together in the same request.</p>
network_ids={value}	<p>(Optional, and valid only when the Network Support feature is enabled for the user's account)</p> <p>Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.</p>
vm_scan_since={date}	<p>(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".</p> <p>This parameter cannot be specified with <b>max_days_since_vm_scan</b> in the same request.</p>
no_vm_scan_since={date}	<p>(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".</p> <p>This parameter cannot be specified with <b>max_days_since_vm_scan</b> in the same request.</p>
max_days_since_last_vm_scan={value}	<p>(Optional) Show only hosts scanned and processed in the past number of days, where the value is a number of days.</p>

Parameter	Description
	This parameter cannot be specified with any of these parameters in the same request: <b>vm_scan_since</b> and <b>no_vm_scan_since</b> .
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".
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.
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.

Parameter	Description
os_pattern={expression}	<p>(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.</p> <p><b>Important Note:</b> The regular expression string you enter must follow the PCRE standard and it must be URL encoded.</p> <p>See page 203 for sample regular expression strings for matching operating system names.</p> <p>For information about the Perl Compatible Regular Expressions (PCRE) standard visit:  <a href="http://php.net/manual/en/book.pcre.php">http://php.net/manual/en/book.pcre.php</a></p> <p>For the PCRE syntax, see:  <a href="http://php.net/manual/en/reference.pcre.pattern.syntax.php">http://php.net/manual/en/reference.pcre.pattern.syntax.php</a></p> <p><a href="http://www.php.net/manual/en/reference.pcre.pattern.posix.php">http://www.php.net/manual/en/reference.pcre.pattern.posix.php</a></p>

**QID Filters.** These input parameters are used to filter QIDs. All of these parameters are optional.

Parameter	Description
qids={value}	<p>(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.</p>
severities={value}	<p>(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.</p>
show_igs={0   1}	<p>(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.</p> <p>The <b>show_igs</b> parameter is required in one use case. The parameter <b>show_igs=1</b> must be specified if both these conditions are met: 1) search lists are included using the parameter <b>include_search_list_titles</b> or <b>include_search_list_ids</b>, and 2) if the included search lists contain only information gathered.</p>

Parameter	Description
include_search_list_titles={value}	<p>(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.</p> <p>This parameter cannot be specified with any of these parameters in the same request: <b>qids</b>, <b>severities</b> or <b>include_search_list_ids</b>.</p>
exclude_search_list_titles={value}	<p>(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.</p> <p>This parameter cannot be specified with any of these parameters in the same request: <b>qids</b>, <b>severities</b> or <b>exclude_search_list_ids</b>.</p>
include_search_list_ids={value,value...}	<p>(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.</p> <p>This parameter cannot be specified with any of these parameters in the same request: <b>qids</b>, <b>severities</b> or <b>include_search_list_titles</b>.</p>
exclude_search_list_ids={value,value...}	<p>(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.</p> <p>This parameter cannot be specified with any of these parameters in the same request: <b>qids</b>, <b>severities</b> or <b>exclude_search_list_titles</b>.</p>

**Asset tags.** The input parameters below allow you to report on hosts using 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.

Parameter	Description
tag_include_selector= { <b>any</b>   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= { <b>any</b>   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.

**EC2 metadata.** These parameters allow you to manage assets using EC2 metadata.

Parameter	Description
host_metadata={value}	(Optional) Specify the name of the cloud provider to show the assets managed by that cloud provider, i.e. EC2. Note: Only supports fetching EC2 assets for now.
host_metadata_fields= {value1,value2}	(Optional when host_metadata is specified) Specify the EC2 instance fields to fetch the data for.  Data can be fetched for the following fields: accountId, region, availabilityZone, instanceId, instanceType, imageId, kernelId.

## Detection Related Timestamp Values

Using the host detection API users can view various timestamp values in the output. Few of them are listed here. For a complete list of all the elements in the host detection API, you can refer to Appendix section

Parameter	Description
LAST_SCAN_DATETIME= {date}	The date and time of the most recent vulnerability scan of the asset.
LAST_VM_SCANNED_DATE= {date}	The scan end date/time for the most recent unauthenticated vulnerability scan of the asset.

Parameter	Description
LAST_VM_SCANNED_DURATION={date}	The scan duration (in seconds) for the most recent unauthenticated vulnerability scan of the asset.
LAST_VM_AUTH_SCANNED_DATE={date}	The scan end date/time for the last successful authenticated vulnerability scan of the asset.
LAST_VM_AUTH_SCANNED_DURATION={date}	The scan duration (in seconds) for the last successful authenticated vulnerability scan of the asset.
LAST_PC_SCANNED_DATE={date}	The scan end date/time for the most recent compliance scan on the asset.
FIRST_FOUND_DATETIME={date}	The date/time when the vulnerability was first found.
LAST_FOUND_DATETIME={date}	The most recent date/time when the vulnerability was found.
LAST_TEST_DATETIME={date}	The most recent date/time when the vulnerability was tested.
LAST_UPDATE_DATETIME={date}	The most recent date/time when the detection record was updated.
LAST_FIXED_DATETIME={date}	The date/time when the vulnerability was verified fixed by a scan.

## 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 API Requests

These sample requests work on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Please be sure to replace the FQDN with the proper API server URL for your platform. For a partner platform, use the URL for your @customer platform API server.



The header parameter “X-Requested-With” is also provided as an example. Please change this parameter according to your need. This parameter is exposed in the activity log (only displayed when used with session cookie authentication - does not apply for basic authentication as used in the following examples) and it is useful for monitoring API activity.

## XML Output

DTD:

```
https://<base_url>/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd
```

The DTD is described in Appendix B, Host List VM Detection Output.

## Samples

### Sample 1: Host List Detection XML Output

Request a list of VM scanned hosts:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list"
```

Sample XML output:

```
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2016-12-21T08:34:30Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>5641287</ID>
        <IP>10.10.10.28</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[Windows XP]]></OS>
        <DNS><![CDATA[xpsp3-10-28]]></DNS>
        <NETBIOS><![CDATA[XPSP3-10-28]]></NETBIOS>
        <LAST_SCAN_DATETIME>2016-12-20T20:59:05Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2016-12-
20T20:59:05Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>260</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2016-12-
20T20:46:17Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
          <DETECTION>
            <QID>38094</QID>
            <TYPE>Potential</TYPE>
            <SEVERITY>2</SEVERITY>
```

```
<PORT>3389</PORT>
<PROTOCOL>tcp</PROTOCOL>
<SSL>0</SSL>
<RESULTS><![CDATA[Detected service win_remote_desktop and
os WINDOWS XP SERVICE PACK 2-3]]></RESULTS>
<STATUS>Active</STATUS>
<FIRST_FOUND_DATETIME>2016-09-
27T09:13:49Z</FIRST_FOUND_DATETIME>
<LAST_FOUND_DATETIME>2016-12-
20T20:59:05Z</LAST_FOUND_DATETIME>
<LAST_TEST_DATETIME>2016-12-
20T20:59:05Z</LAST_TEST_DATETIME>
<LAST_UPDATE_DATETIME>2016-12-
20T20:52:34Z</LAST_UPDATE_DATETIME>
<IS_IGNORED>0</IS_IGNORED>
<IS_DISABLED>0</IS_DISABLED>
<TIMES_FOUND>48</TIMES_FOUND>
</DETECTION>
<DETECTION>
  <QID>38104</QID>
  <TYPE>Info</TYPE>
  <SEVERITY>1</SEVERITY>
  <RESULTS>
    <![CDATA[IP addressHost name
      10.10.10.410-10-10-4.bogus.tld]]>
  </RESULTS>
  <FIRST_FOUND_DATETIME>2016-09-
27T07:30:31Z</FIRST_FOUND_DATETIME>
  <LAST_FOUND_DATETIME>2016-12-
20T09:40:25Z</LAST_FOUND_DATETIME>
  <TIMES_FOUND>8</TIMES_FOUND>
  <IS_DISABLED>0</IS_DISABLED>
</DETECTION>
<DETECTION>
  <QID>38252</QID>
  <TYPE>Confirmed</TYPE>
  <SEVERITY>2</SEVERITY>
  <SSL>0</SSL>
  <RESULTS><![CDATA[Detected on TCP port 23.]]></RESULTS>
  <STATUS>Active</STATUS>
  <FIRST_FOUND_DATETIME>2016-09-
27T09:13:49Z</FIRST_FOUND_DATETIME>
  <LAST_FOUND_DATETIME>2016-12-
20T20:59:05Z</LAST_FOUND_DATETIME>
  <LAST_TEST_DATETIME>2016-12-
20T20:59:05Z</LAST_TEST_DATETIME>
  <LAST_UPDATE_DATETIME>2016-12-
```

```

20T20:52:34Z</LAST_UPDATE_DATETIME>
    <IS_IGNORED>0</IS_IGNORED>
    <IS_DISABLED>0</IS_DISABLED>
    <TIMES_FOUND>48</TIMES_FOUND>
  </DETECTION>
</DETECTION_LIST>
</HOST>
<HOST>
  <ID>5641289</ID>
  <IP>10.10.32.17</IP>
  <TRACKING_METHOD>IP</TRACKING_METHOD>
  <OS><![CDATA[Windows 2008 R2 Enterprise Service Pack 1]]></OS>
  <DNS><![CDATA[com-mssql2012]]></DNS>
  <NETBIOS><![CDATA[COM-MSSQL2012]]></NETBIOS>
  <LAST_SCAN_DATETIME>2016-12-20T09:29:19Z</LAST_SCAN_DATETIME>
  <LAST_VM_SCANNED_DATE>2016-12-
20T09:29:19Z</LAST_VM_SCANNED_DATE>
    <LAST_VM_SCANNED_DURATION>495</LAST_VM_SCANNED_DURATION>
    <LAST_VM_AUTH_SCANNED_DATE>2016-09-
27T10:22:10Z</LAST_VM_AUTH_SCANNED_DATE>

<LAST_VM_AUTH_SCANNED_DURATION>341</LAST_VM_AUTH_SCANNED_DURATION>
  <LAST_PC_SCANNED_DATE>2016-10-
04T09:03:44Z</LAST_PC_SCANNED_DATE>
  <DETECTION_LIST>
    <DETECTION>
      <QID>19824</QID>
      <TYPE>Potential</TYPE>
      <SEVERITY>3</SEVERITY>
      <PORT>1433</PORT>
      <PROTOCOL>tcp</PROTOCOL>
      <SSL>0</SSL>
      <RESULTS><![CDATA[QID 19824 detected on port 1433 -
Microsoft SQL Server 11.00.2100 (MS SQL 2012)]]></RESULTS>
      <STATUS>Active</STATUS>
      <FIRST_FOUND_DATETIME>2016-09-
27T09:13:49Z</FIRST_FOUND_DATETIME>
      <LAST_FOUND_DATETIME>2016-12-
20T09:29:19Z</LAST_FOUND_DATETIME>
      <LAST_TEST_DATETIME>2016-12-
20T09:29:19Z</LAST_TEST_DATETIME>
      <LAST_UPDATE_DATETIME>2016-12-
20T09:29:49Z</LAST_UPDATE_DATETIME>
      <LAST_FIXED_DATETIME>2016-12-
06T20:41:22Z</LAST_FIXED_DATETIME>
      <IS_IGNORED>0</IS_IGNORED>
      <IS_DISABLED>0</IS_DISABLED>

```

```
        <TIMES_FOUND>38</TIMES_FOUND>
      </DETECTION>
    </DETECTION_LIST>
  </HOST>
</HOST_LIST>
</RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

### Sample 2: Host List 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.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act
ion=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.

```
...
      </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[https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/d
etection/?action=list&truncation_limit=100&id_min=5641289]]></URL>
  </WARNING>
</RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

### Sample 3: Host List Detection CSV Output

By default, the output of the detection API is returned in XML, but when the parameter “output\_format=CSV” is provided, then the output is returned in a comma separated value (csv) format. This format is convenient because it can be opened as a spreadsheet.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act
ion=list&output_format=CSV"
```

Sample CSV output:

```

----BEGIN_RESPONSE_HEADER_CSV
----END_RESPONSE_HEADER_CSV
----BEGIN_RESPONSE_BODY_CSV
"Host ID","IP Address","Tracking Method","Operating System","DNS
Name","Netbios Name","Last Scan Datetime","OS CPE","Last VM Scanned
Date","Last VM Scanned Duration","Last VM Auth Scanned Date","Last VM
Auth Scanned Duration","Last PC Scanned
Date","QID","Type","Port","Protocol","FQDN","SSL","Instance","Status"
,"Severity","First Found Datetime","Last Found Datetime","Last Test
Datetime","Last Update Datetime","Last Fixed
Datetime","Results","Ignored","Disabled","Times Found","Service"
"5641287","10.10.10.28","IP","Windows XP","xpsp3-10-28","XPSP3-10-
28","2016-12-20T20:59:05Z","2016-12-20T20:59:05Z","260","","2016-12-
20T20:46:17Z","38094","Potential","3389","tcp","","0","Active","2","20
16-09-27T09:13:49Z","2016-12-20T20:59:05Z","2016-12-
20T20:59:05Z","2016-12-20T20:52:34Z","Detected service
win_remote_desktop and os WINDOWS XP SERVICE PACK 2-3","0","0","48",
"5641287","10.10.10.28","IP","Windows XP","xpsp3-10-28","XPSP3-10-
28","2016-12-20T20:59:05Z","2016-12-20T20:59:05Z","260","","2016-12-
20T20:46:17Z","38252","Confirmed","","0","Active","2","2016-09-
27T09:13:49Z","2016-12-20T20:59:05Z","2016-12-20T20:59:05Z","2016-12-
20T20:52:34Z","Detected on TCP port 23.","0","0","48",
"5641288","10.10.30.159","IP","Linux 2.4-2.6 / Embedded Device / F5
Networks Big-IP / Linux 2.6","","2016-12-20T21:06:59Z","2016-12-
20T21:06:59Z","734","2016-09-
27T10:20:52Z","272","","15034","Confirmed","53","udp","","0","Active","2
","2016-09-27T09:29:21Z","2016-12-20T21:06:59Z","2016-12-
20T21:06:59Z","2016-12-20T21:01:55Z","Server supports recursive name
resolution to IPv4 addresses.
Server supports recursive name resolution to IPv6
addresses.","0","0","43",
"5641290","10.11.72.21","IP","Windows 10 Enterprise","qwbw10es-72-
21","QWBW10ES-72-21","2016-12-19T20:52:07Z","2016-12-
19T20:51:11Z","284","","2016-12-
20T20:46:17Z","38628","Confirmed","3389","tcp","","1","Active","3","20
16-09-27T09:29:21Z","2016-12-19T20:51:11Z","2016-12-
19T20:51:11Z","2016-12-19T20:53:25Z","TLSv1.0 is
supported","0","0","29",
----END_RESPONSE_BODY_CSV
----BEGIN_RESPONSE_FOOTER_CSV
"Status Message"
"Finished"
----END_RESPONSE_FOOTER_CSV

```

### Sample 4: Host List Detection CSV Output - With Truncation

A truncated response is returned when the API request returns more host records than the truncation limit - in this case the limit is set to 2.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&output_format=CSV&truncation_limit=2"
```

The FOOTER\_CSV section in the output (shown below) indicates the URL you need to use to request the next 2 host records.

```
...
----BEGIN_RESPONSE_FOOTER_CSV
"Status Message", "Next ID", "Next URL"
"Truncated", "5641289", "https://qualysapi.qualys.com/api/2.0/fo/asset/
host/vm/detection/?action=list&output_format=CSV&truncation_limit=2&i
d_min=5641289"
----END_RESPONSE_FOOTER_CSV
```

### Sample 5: Include Redundant Information in CSV Output

When “suppress\_duplicated\_data\_from\_csv=0” is provided, host details will be repeated in each detection line in the CSV output. This CSV format with all the redundant information included is convenient for quick ad-hoc text manipulation with tools such as “grep”, “cut”, “sed”, “awk” etc.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&output_format=CSV&suppress_duplicated_data_from_csv=0"
```

Sample output with redundant information for each line:

```
----BEGIN_RESPONSE_HEADER_CSV
----END_RESPONSE_HEADER_CSV
----BEGIN_RESPONSE_BODY_CSV
"Host ID", "IP Address", "Tracking Method", "Operating System", "DNS
Name", "Netbios Name", "Last Scan Datetime", "OS CPE", "Last VM Scanned
Date", "Last VM Scanned Duration", "Last VM Auth Scanned Date", "Last VM
Auth Scanned Duration", "Last PC Scanned
Date", "QID", "Type", "Port", "Protocol", "FQDN", "SSL", "Instance", "Status"
, "Severity", "First Found Datetime", "Last Found Datetime", "Last Test
Datetime", "Last Update Datetime", "Last Fixed
Datetime", "Results", "Ignored", "Disabled", "Times Found", "Service"
"5641287", "10.10.10.28", "IP", "Windows XP", "xpsp3-10-28", "XPSP3-10-
28", "2016-12-20T20:59:05Z", "2016-12-20T20:59:05Z", "260", "2016-12-
20T20:46:17Z", "38094", "Potential", "3389", "tcp", "0", "Active", "2", "20
16-09-27T09:13:49Z", "2016-12-20T20:59:05Z", "2016-12-
20T20:59:05Z", "2016-12-20T20:52:34Z", "Detected service
```

```
win_remote_desktop and os WINDOWS XP SERVICE PACK 2-3","0","0","48",
"5641287","10.10.10.28","IP","Windows XP","xpsp3-10-28","XPSP3-10-
28","2016-12-20T20:59:05Z",,"2016-12-20T20:59:05Z","260",,"2016-12-
20T20:46:17Z","38252","Confirmed",,"0",,"Active","2","2016-09-
27T09:13:49Z","2016-12-20T20:59:05Z","2016-12-20T20:59:05Z","2016-12-
20T20:52:34Z",,"Detected on TCP port 23.",,"0","0","48",
...
```

### Sample 6: Remove Redundant Information from CSV Output

When “suppress\_duplicated\_data\_from\_csv=1” is provided, host details will not be repeated in each detection line. In other words, the duplicated data is suppressed. The output is trimmed down to remove the redundant information.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act
ion=list&output_format=CSV&suppress_duplicated_data_from_csv=1"
```

Sample output with redundant information removed:

```
----BEGIN_RESPONSE_HEADER_CSV
----END_RESPONSE_HEADER_CSV
----BEGIN_RESPONSE_BODY_CSV
"Host ID","IP Address","Tracking Method","Operating System","DNS
Name","Netbios Name","Last Scan Datetime","OS CPE","Last VM Scanned
Date","Last VM Scanned Duration","Last VM Auth Scanned Date","Last VM
Auth Scanned Duration","Last PC Scanned
Date","QID","Type","Port","Protocol","FQDN","SSL","Instance","Status"
,"Severity","First Found Datetime","Last Found Datetime","Last Test
Datetime","Last Update Datetime","Last Fixed
Datetime","Results","Ignored","Disabled","Times Found","Service"
"5641287","10.10.10.28","IP","Windows XP","xpsp3-10-28","XPSP3-10-
28","2016-12-20T20:59:05Z",,"2016-12-20T20:59:05Z","260",,"2016-12-
20T20:46:17Z",,,,,,,,,,,,,,
,,,,,,,,,,,,,"38094","Potential",,"3389","tcp",,"0",,"Active","2","201
6-09-27T09:13:49Z","2016-12-20T20:59:05Z","2016-12-
20T20:59:05Z","2016-12-20T20:52:34Z",,"Detected service
win_remote_desktop and os WINDOWS XP SERVICE PACK 2-3","0","0","48",
,,,,,,,,,,,,,"38252","Confirmed",,"0",,"Active","2","2016-09-
27T09:13:49Z","2016-12-20T20:59:05Z","2016-12-20T20:59:05Z","2016-12-
20T20:52:34Z",,"Detected on TCP port 23.",,"0","0","48",
...
```

## Sample 7: Fetch region info for EC2 assets

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=  
list&host_metadata=ec2&host_metadata_fields=region"
```

### XML output:

```
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/host_lis  
t_vm_detection_output.dtd">  
<HOST_LIST_VM_DETECTION_OUTPUT>  
  <RESPONSE>  
    <DATETIME>2016-11-14T11:21:02Z</DATETIME>  
    <HOST_LIST>  
      <HOST>  
        <ID>135151</ID>  
        <IP>10.97.5.247</IP>  
        <TRACKING_METHOD>EC2</TRACKING_METHOD>  
        <OS><![CDATA[Amazon Linux 2016.09]]></OS>  
        <DNS><![CDATA[i-0bb87c3281243cdfd]]></DNS>  
        <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdfd]]></EC2_INSTANCE_ID>  
        <LAST_SCAN_DATETIME>2017-03-21T13:41:20Z</LAST_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_PC_SCANNED_DATE>2017-03-21T13:21:51Z</LAST_PC_SCANNED_DATE>  
        <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>  
          </EC2>  
        </METADATA>  
      </HOST>  
    </HOST_LIST>  
  </RESPONSE>  
</HOST_LIST_VM_DETECTION_OUTPUT>
```



## More Sample API Requests

Here are more samples you may want to try.

### Scanned Hosts in IP Range

Request a list of VM scanned hosts with IP addresses in the range 10.10.10.10-10.10.10.80:

```
curl -u "username:password" -H "X-Requested-With: curl"  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act  
ion=list&ips=10.10.10.10-10.10.10.80"
```

### Scanned Hosts with Certain QIDs

Request a list of VM scanned hosts with detected QIDs included in the search list titled “High Severity”:

```
curl -u "username:password" -H "X-Requested-With: curl"  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act  
ion=list&include_search_list_titles=High+Severity"
```

### Scanned Hosts in IP Range with Certain QIDs

Request a list of VM scanned hosts that have IP addresses in the range 10.10.10.10-10.10.10.80 and also QIDs included in the search list titled “High Severity”:

```
curl -u "username:password" -H "X-Requested-With: curl"  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act  
ion=list&include_search_list_titles=High+Severity&ips=10.10.10.10-  
10.10.10.80"
```

Only hosts that match both filters will be included in the host list output. If a host has an IP in the range 10.10.10.10-10.10.10.80 and the host does not have detected QIDs in “High Severity” then the host will not be listed in the output.

### Return Fixed Detections

By default, when no specific parameters are passed to this API, the output contains detections with New, Active or Re-Opened <STATUS> only. The reason for this is because the primary goal of the detection API is to return the most updated vulnerability status for the hosts. By using the parameter “status=Fixed” like in the example below, it is possible to get the Fixed vulnerabilities in the output:

```
curl -u "username:password" -H "X-Requested-With: curl"  
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act  
ion=list&status=Fixed"
```

The “status” parameter can also be used to filter the output to only include certain status levels. For example:

status=Fixed only returns Fixed detections

status=New,Fixed only returns New and Fixed detections

status=New,Fixed,Active,Re-Opened returns All detections

## Filter by Scan Processed Date

Request a list of hosts with vulnerability scan results processed before or after a certain date/time. Use the “vm\_processed\_before” and “vm\_processed\_after” parameters.

Return hosts with vulnerability scans processed after November 5th:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&vm_processed_after=2016-11-05"
```

Return hosts with vulnerability scans processed before December 31st:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&vm_processed_before=2016-12-31"
```

You can also use these date filters together:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&vm_processed_after=2016-11-05&vm_processed_before=2016-12-31"
```

## Filter by Scan End Date

Request a list of hosts with vulnerability scans that ended before or after a certain date/time. Use the “vm\_scan\_date\_before” and “vm\_scan\_date\_after” parameters.

Starting with version 8.9, host scan time is based on when a scan finished, not when the scan started. We get this information from QID 45038 “Host Scan Time”. If this QID was not included in the vulnerability scan then we’ll use the scan start date/time. In the following example, I want to return hosts with vulnerability scans that ended after December 19th and before December 21st.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&vm_scan_date_after=2016-12-19&vm_scan_date_before=2016-12-21"
```

## Filter by Authenticated Scan End Date

Interested in authenticated scans? Use the “vm\_auth\_scan\_date\_before” and “vm\_auth\_scan\_date\_after” parameters to request a list of hosts with successful authenticated vulnerability scans that ended before or after a certain date/time. In this example, I want to return hosts with a successful authenticated scan that ended after October 31st and before December 31st.

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act
ion=list&vm_auth_scan_date_after=2016-10-
31&vm_auth_scan_date_before=2016-12-31"
```

## Exclude Results

For any request you can choose to exclude results in the vulnerability detection data:

```
curl -u "username:password" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?act
ion=list&show_results=0"
```

## Sample OS Pattern Filters

**Important Note:** The regular expression string you provide in the “os\_pattern” parameter must follow the PCRE standard and it must be URL encoded to make sure that special characters are correctly passed to the filter.

### OS Name “Beginning With”

To list hosts in the range 10.10.10.1-10.10.10.100 which have an operating system beginning with “Windows”, you can use the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?acti
on=list&ips=10.10.10.1-10.10.10.100&os_pattern=%5EWindows
```

where “%5EWindows” is the URL encoded version of the PCRE regular expression “^Windows”. Any host which was scanned for vulnerabilities and which has an operating system starting with “Windows” will be included in the host list output.

### OS Name “Ending With”

To list hosts in the range 10.10.10.1-10.10.10.100 which have the operating system name “FreeBSD”, you can use the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?acti
on=list&ips=10.10.10.1-10.10.10.100&os_pattern=BSD%24
```

where “BSD%24” is the URL encoded version of the PCRE regular expression “BSD\$”. For the above sample, hosts which are in the range 10.10.10.1-10.10.10.100 and which have an operating system ending in BSD, such as FreeBSD, will be included in the host list output.

## OS Name with Simple Pattern

To list hosts which have an operating system name containing “2003” you can use the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&os_pattern=2003
```

Any host which was scanned for vulnerabilities and which has an operating system including the string “2003” will be included in the host list output.

## OS Name with More Complex Pattern

To list hosts in the range 10.10.10.1-10.10.10.100 which have an operating system name containing a more complex string like “Windows 64 bit” you could use the OS pattern shown in the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&ips=10.10.10.1-10.10.10.100&os_pattern=%5EWin.*64%20bit.*Service%20Pack%201%24
```

where “%5EWin.\*64%20bit.\*Service%20Pack%201%24” is the URL encoded version of the PCRE regular expression “^Win.\*64+bit.\*Service+Pack+1”. The above regular expression matches OS string starting with “Win”, containing “64 bit” and ending with “Service Pack 1”. Possible matches include hosts in the range 10.10.10.1-10.10.10.100 which have some flavors of Windows 64 Bit Service Pack 1 such as these:

Windows XP 64 bit Edition Service Pack 1

Windows 2008 Core 64 bit Edition Service Pack 1

Windows 2003 Server 64 bit Edition AD Service Pack 1

## Hosts with No OS

To list hosts with no operating system defined, you can use the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&ips=10.10.10.1-10.10.10.100&os_pattern=%5E%24
```

where “%5E%24” is the URL encoded version of the PCRE regular expression “^\$”. The above request will list all hosts in the user account that do not have an operating system defined.

## Sample Script for Pagination Logic

The following script illustrates how it's possible for a third party application to retrieve paginated results using the host list detection API.

```
#!/bin/sh

BASE_URL='https://qualysapi.qualys.com'
OUTPUT_FILENAME='detection'
USERNAME='username'
PASS='password'
N='01'

# Specify filtering parameters here (Remember to URL encode
os_pattern, if specified):

#PARAMETER="&show_igs=1&include_search_list_titles=QID+45038&os_patte
rn=%5Cd%2B"

echo
"${BASE_URL}/api/2.0/fo/asset/host/vm/detection/?action=list${PARAMET
ER}"
curl -H 'X-Requested-With: curl example QWEB 6.17' -k -u
"${USERNAME}:${PASS}"
"${BASE_URL}/api/2.0/fo/asset/host/vm/detection/?action=list${PARAMET
ER}" > "${OUTPUT_FILENAME}-${N}.xml"

while grep '<URL><![CDATA\[https:\\\\.qualys\\.com'
"${OUTPUT_FILENAME}-${N}.xml"
do
    NEXT_URL=`grep "<URL>" "${OUTPUT_FILENAME}-${N}.xml" | sed
s/'^.*<URL><![CDATA\[ '//g | sed s/'\\]\\\]><\/URL>'//g`

    N=`expr ${N} + 1`
    if [[ ${N} -lt 10 ]] ; then N=`echo "0${N}"` ; fi
    if [[ ${N} -gt 99 ]] ; then echo "bailing out after fetching the
first 99 batches of data"; exit 0; fi

    echo "next url = ${NEXT_URL}"
    curl -H 'X-Requested-With: curl example QWEB 6.17' -k -u
"${USERNAME}:${PASS}" "${NEXT_URL}" > "${OUTPUT_FILENAME}-${N}.xml"
done
```

# Excluded Hosts List

The Excluded Hosts List API v2 (`api/2.0/fo/asset/excluded_ip/?action=list`) allows API users to request a list of excluded hosts. The GET or POST access method may be used to make an API request.

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

## User Permissions

User permissions are described below.

User Role	Permissions
Manager	View all excluded hosts in subscription.
Auditor	View excluded compliance hosts in subscription.
Unit Manager	View excluded hosts in user’s business unit.
Scanner	View excluded hosts in user’s account.
Reader	View excluded hosts in user’s account.

## Input Parameters

The input parameters for the excluded hosts API are described below.

Parameter	Description
action=list	(Required) A flag used to make an excluded hosts 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 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. Please see “ <a href="#">User Scenarios</a> ” to know more about the behavior of this parameter.
Asset Groups	

Parameter	Description
ag_ids={value}	<p>(Optional) Show excluded 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.</p> <p>These parameters are mutually exclusive and cannot be specified together: ag_ids and ag_titles.</p>
ag_titles={value}	<p>(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).</p> <p>These parameters are mutually exclusive and cannot be specified together: ag_ids and ag_titles.</p>
Asset Tags	
use_tags={0   1}	<p>(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.</p>
tag_include_selector={any   all}	<p>(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.</p>
tag_exclude_selector={any   all}	<p>(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.</p>
tag_set_by = {id   name}	<p>(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.</p>
tag_set_include={value}	<p>(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.</p>
tag_set_exclude={value}	<p>(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.</p>

User Scenarios

Let us consider different user scenarios to know more about the behavior of `network_id` parameter:

User	Networks with access	Is net-work_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 API Requests

These sample requests work on Qualys US Platform 1 where the FQDN in the API server URL is `qualysapi.qualys.com`. Please be sure to replace the FQDN with the proper API server URL for your platform. For the EU platform, use `qualysapi.qualys.eu`. For a partner platform, use the URL for your @customer platform API server.

The header parameter “X-Requested-With” is also provided as an example. Please change this parameter according to your need. This parameter is exposed in the activity log (only displayed when used with session cookie authentication - does not apply for basic authentication as used in the following examples) and it is useful for monitoring API activity.

**Sample 1.** Request an excluded hosts list that includes all excluded hosts in your account:

```
curl -s -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'
```

**Sample 2.** Request an excluded hosts list that includes only IP addresses in the range 10.10.24.1-10.10.24.255:

```
curl -s -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'
```

## XML Output

DTD: [https://<base\\_url>/api/2.0/fo/asset/excluded\\_ip/ip\\_list\\_output.dtd](https://<base_url>/api/2.0/fo/asset/excluded_ip/ip_list_output.dtd)

The DTD is described in Appendix B, Excluded Hosts List Output.

## Sample Excluded Hosts List

Sample excluded hosts list XML output is shown below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/ip_list_ou
tput.dtd">
<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2015-04-23T00:33:24Z</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 network_id="0">100.100.100.100</IP>
    </IP_SET>
  </RESPONSE>
</IP_LIST_OUTPUT>
```

# Excluded Hosts Change History

The excluded hosts change history V2 API (`api/2.0/fo/asset/excluded_ip/history/?action=list`) allows API users to request the change history for excluded hosts in the user’s subscription. History record IDs in the XML output are listed in decreasing order. The GET or POST access method may be used to make an API request.

Unlike other V2 APIs, the excluded hosts change history 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.

A maximum of 1,000 history records will be returned. If the maximum is reached, a warning message appears in the XML output with the URL to be used to obtain the next batch of records. The truncation warning is issued using the “id\_max” parameter. See below for sample output showing this warning.

## User Permissions

Users with these roles have permission to view all excluded hosts in the subscription: Manager, Auditor, Unit Manager, Scanner and Reader.

## Input Parameters

The input parameters for the excluded hosts API are described below.

Parameter	Description
action=list	(Required) A flag used to show all changes made to excluded hosts within your subscription.
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 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) Restrict the request to a certain custom network ID.
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.

Parameter	Description
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 API Requests

These sample requests work on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Please be sure to replace the FQDN with the proper API server URL for your platform. For the EU platform, use qualysapi.qualys.eu. For a partner platform, use the URL for your @customer platform API server.

The header parameter “X-Requested-With” is also provided as an example. Please change this parameter according to your need. This parameter is exposed in the activity log (only displayed when used with session cookie authentication - does not apply for basic authentication as used in the following examples) and it is useful for monitoring API activity.

**Sample 1.** Request excluded hosts change history that includes all excluded hosts in your subscription:

```
curl -s -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/?a
ction=list'
```

**Sample 2.** Request excluded hosts change history that includes only IP addresses in the range 10.10.24.1-10.10.24.255:

```
curl -s -u user:password
-H 'X-Requested-With: curl demo 2' -D headers.16
'https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/history/?a
ction=list&ips=10.10.24.1-10.10.24.255'
```

## XML Output

DTD:

`https://<base_url>/api/2.0/fo/asset/excluded_ip/history/history_list_output.dtd`

The DTD is described in Appendix B, Excluded Hosts Change History Output.

## Sample Excluded Hosts Change History

Sample excluded hosts change history XML output is shown below:

```
<!DOCTYPE HISTORY_LIST_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/history/history_list_output.dtd">

<HISTORY_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2011-03-18T01:48:42Z</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>2009-07-02T05:19:06Z</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>2009-06-01T23:51:26Z</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>2009-04-29T06:56:13Z</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[https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_
ip/history/?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>
```

# Manage Excluded Hosts

Manage your excluded IPs list using the Excluded IP API v2 (/api/2.0/fo/asset/excluded\_ip/). The IPs in your excluded IPs list will not be scanned.

## Add IPs

Use the parameter “action=add” to add IPs to your excluded IPs list.

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
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.

### API request 1 - add IPs:

```
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>2015-04-23T00:33:21Z</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>
```

### API request 2 - IPs already in excluded IPs list:

```
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>2014-09-14T13:09:03Z</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 IPs

Use the parameter “action=remove” to remove IPs from your excluded IPs list.

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

Parameter	Description
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.

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>2014-09-15T04:05:04Z</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 IPs

Use the parameter “action=remove\_all” to remove all IPs from your excluded IPs list.

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.



API request:

```
curl -H "X-Requested-With: curl" -u "USERNAME:PASSWD" -d  
"action=remove_all&comment=remove all 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>2015-04-24T00:08:19Z</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>
```

# Purge Hosts

The Purge Hosts API (`/api/2.0/fo/asset/host/?action=purge`) is used to purge hosts. Purging hosts will remove automatic host data in the user’s account (scan results will not be removed). Purged host information will not appear in new reports generated by users. The POST access method must be used to make an API request.

One or both types of host data is removed, based on the user’s API request: vulnerability data and compliance data.

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

## User Permissions

User permissions are described below.

User Role	Permissions
Manager	Purge automatic host data for all hosts in the subscription, including vulnerability data and compliance data.
Auditor	Purge automatic host data for all compliance hosts in the subscription. Only compliance data will be removed (not vulnerability data).
Unit Manager	Sub-accounts must be granted permissions.
Scanner	
Reader	Purge vulnerability data: User must be granted the permission “Purge host information/history”. When granted this permission, the users can purge vulnerability data for hosts in their account.  Purge compliance data: User must be granted the permission “Purge host information/history” and the permission “Manage compliance”. When granted these permissions, the user can purge compliance data for compliance hosts in their account.

## Parameters

The parameters used to make a purge hosts request are described below.

Parameter	Description
action=purge	(Required) A flag used to make a purge hosts 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.

Parameter	Description
ids={value}	<p>(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.</p> <p>One of these host selection parameters must be specified in an API request: <b>ids</b>, <b>ips</b>, <b>ag_ids</b> or <b>ag_titles</b>. Multiple host selection parameters may be specified together in the same request.</p>
ips={value}	<p>(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).</p> <p>One of these host selection parameters must be specified in an API request: <b>ids</b>, <b>ips</b>, <b>ag_ids</b> or <b>ag_titles</b>. Multiple host selection parameters may be specified together in the same request.</p>
ag_ids={value}	<p>(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.</p> <p>One of these host selection parameters must be specified in an API request: <b>ids</b>, <b>ips</b>, <b>ag_ids</b> or <b>ag_titles</b>. Multiple host selection parameters may be specified together in the same request. These parameters are mutually exclusive and cannot be specified together: <b>ag_ids</b> and <b>ag_titles</b>.</p>
ag_titles={value}	<p>(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).</p> <p>One of these parameters must be specified in an API request: <b>ids</b>, <b>ips</b>, <b>ag_ids</b> or <b>ag_titles</b>. Multiple host selection parameters may be specified together in the same request. These parameters are mutually exclusive and cannot be specified together: <b>ag_ids</b> and <b>ag_titles</b>.</p>
network_ids={value}	<p>(Optional, and valid only when the Network Support feature is enabled for the user's account)</p> <p>Restrict the request to certain custom network IDs. Multiple network IDs are comma separated.</p>

Parameter	Description
no_vm_scan_since={date}	<p>(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".</p> <p>User Permissions: An Auditor cannot be specify this parameter.</p>
no_compliance_scan_since={date}	<p>(Optional) Purge compliance hosts not scanned since a certain date and time (optional). This parameter is invalid for an Express Lite user.</p> <p>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".</p> <p>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 "User Permissions".</p>

Parameter	Description
compliance_enabled={0   1}	<p>(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.</p> <p>Specify 1 to purge compliance hosts in the user's account. These hosts are assigned to the policy compliance module. When selected, the service will remove vulnerability information and compliance information associated with the selected hosts.</p> <p>Specify 0 to purge hosts which are not assigned to the policy compliance module. When selected, the service will remove vulnerability information associated with the selected hosts.</p> <p>User Permissions: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user account is granted permissions to purge compliance information. See "User Permissions". An Auditor does not have permission to set <b>compliance_enabled=0</b>.</p>
os_pattern={expression}	<p>(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.</p> <p><b>Important Note:</b> The regular expression string you enter must follow the PCRE standard and it must be URL encoded. See page 203 for sample regular expression strings for matching operating system names.</p> <p>For information about the Perl Compatible Regular Expressions (PCRE) standard visit: <a href="http://php.net/manual/en/book.pcre.php">http://php.net/manual/en/book.pcre.php</a></p> <p>For the PCRE syntax, see: <a href="http://php.net/manual/en/reference.pcre.pattern.syntax.php">http://php.net/manual/en/reference.pcre.pattern.syntax.php</a></p> <p><a href="http://www.php.net/manual/en/reference.pcre.pattern.posix.php">http://www.php.net/manual/en/reference.pcre.pattern.posix.php</a></p>

## XML Output

DTD: [https://<base\\_url>/api/2.0/fo/batch\\_return.dtd](https://<base_url>/api/2.0/fo/batch_return.dtd)

# Virtual Host List

The virtual host list API (**/api/2.0/fo/asset/vhost/?action=list**) is used to view a list of virtual hosts in the user account. By default, all virtual hosts in the user account are included. Optional input parameters support filtering the list by port and IP address. The GET or POST access method may be used to make an API request.

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

User permissions are described below.

User Role	Permissions
Manager	View virtual hosts in subscription.
Auditor	No permission to view virtual hosts.
Unit Manager	View virtual hosts for IP addresses in user’s business unit.
Scanner	View virtual hosts for IP addresses in user’s account.
Reader	View virtual hosts for IP addresses in user’s account.

## Parameters

The parameters used to make a virtual host list request are described below.

Parameter	Description
action=list	(Required) A flag used to make a virtual host 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.
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.

## XML Output

DTD: `https://<base_url>/api/2.0/fo/asset/vhost/vhost_list_output.dtd`

The DTD is described in Appendix B, Virtual Host List Output.

## Take Actions on Virtual Hosts

The virtual host API (`/api/2.0/fo/asset/vhost/?action=<value>`) is used to create, edit and delete virtual hosts in the user account. One subscription can have a maximum of 1024 virtual hosts. The POST access method may be used to make an API request.

Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

User permissions are described below.

User Role	Permissions
Manager	Create, edit and delete virtual hosts in subscription.
Auditor	No permissions to create, edit and delete virtual hosts.
Unit Manager	Create, edit and delete virtual hosts for IP addresses in user’s business unit. The “Create/edit virtual hosts” permission must be granted in the user’s account.
Scanner	Create, edit and delete virtual hosts for IP addresses in user’s account. The “Create/edit virtual hosts” permission must be granted in the user’s account.
Reader	No permissions to create, edit and delete virtual hosts.

## Parameters

The parameters used to make a request to create, edit or delete a virtual host request.

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) 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.
ip={value}	(Required) An IP address for the virtual host configuration.

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.*

\* Note: A virtual host must have at least one FQDN. If you make a request using the parameter **action=delete\_FQDN** it’s not possible to remove all of the FQDNs defined for the virtual host.

### XML Output

DTD: https://<base\_url>/api/2.0/simple\_return.dtd

The “simple return” DTD is provided in Appendix A.



# Restricted IPs List

The Restricted IPs API v2 ([/api/2.0/fo/setup/restricted\\_ips/](#)) gives Managers (users assigned the Manager role) the ability to manage and update the list of restricted IPs within their subscription so this list stays in sync with their organization’s security policy. Once the feature is activated and a restricted IPs list is enabled, only users logging in from restricted IPs will be allowed to connect to your Qualys subscription.

## Parameters

Restricted IPs input parameters are described below.

Parameter	Description
action={value}	<p>(Required) The action for the request. One of:</p> <ul style="list-style-type: none"> <li>activate - enable or disable the restricted IPs feature</li> <li>add - add restricted IPs</li> <li>delete - delete restricted IPs</li> <li>replace - replace restricted IPs</li> <li>list - download list of all restricted IPs</li> <li>clear - clear all restricted IPs and de-active this feature</li> </ul> <p>Allowed methods: For the actions activate, list and clear: GET or POST may be used. For the actions add, replace and delete: the POST method must be used when the “ips” parameter is specified, and the GET or POST method may be used when uploading CSV raw data.</p>
echo_request={0   1}	(Optional) Set to 1 if you want to include the input parameters in the XML output.
enable={0   1}	(Optional; 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}	<p>(Optional; valid when action is add, replace or delete)</p> <p>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 &lt;data&gt;.</p> <p>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.</p>
output_format={CSV   <b>XML</b> }	<p>(Optional; valid when action is list)</p> <p>The list output will be in XML format by default. For CSV format, set output_format=CSV.</p>

## XML Output

DTD: `https://<base_url>/api/2.0/fo/setup/restricted_ips/restricted_ips_output.dtd`

The DTD is described in Appendix B, Restricted IPs List Output.

## Sample API Requests

### Add Restricted IPs ("ips" parameter)

#### API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d  
"action=add&ips=10.10.10.1-10.10.10.255"  
"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>2013-03-22T11:04:52Z</DATETIME>  
    <TEXT>Successfully added restricted ips</TEXT>  
    <ITEM_LIST>  
      <ITEM>  
        <KEY>STATUS</KEY>  
        <VALUE>disabled</VALUE>  
      </ITEM>  
    </ITEM_LIST>  
  </RESPONSE>  
</SIMPLE_RETURN>
```

### Download Restricted IPs List

#### 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.

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

```
<!DOCTYPE RESTRICTED_IPS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/setup/restricted_ips/restricted_ips_output.dtd">
<RESTRICTED_IPS_OUTPUT>
  <RESPONSE>
    <DATETIME>2013-03-22T11:12:56Z</DATETIME>
    <IP_SET>
      <IP_RANGE>10.10.10.1-10.10.10.255</IP_RANGE>
    </IP_SET>
    <STATUS>disabled</STATUS>
  </RESPONSE>
</RESTRICTED_IPS_OUTPUT>
```

## Replace Restricted IPs (IPs in CIDR notation)

### 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>2013-03-22T11:45:00Z</DATETIME>
    <TEXT>Successfully replaced restricted ips</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
        <VALUE>disabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### **Delete Restricted IPs (upload CSV raw data)**

#### CSV raw data file (file1.csv):

```
$ 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/?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>2013-03-22T11:45:34Z</DATETIME>
    <TEXT>Successfully deleted restricted ips</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>STATUS</KEY>
        <VALUE>disabled</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### **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>2013-03-22T11:46:45Z</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>
```

## 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
```

## 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>2013-03-22T12:04:34Z</DATETIME>
    <TEXT>Successfully cleared restricted ips</TEXT>
```

```
<ITEM_LIST>
  <ITEM>
    <KEY>STATUS</KEY>
    <VALUE>disabled</VALUE>
  </ITEM>
</ITEM_LIST>
</RESPONSE>
</SIMPLE_RETURN>
```

# Add IPs

The Add Asset IP API v2 (`/api/2.0/fo/asset/ip/?action=add`) gives you the ability to add IP addresses to the subscription. Once added they are available for scanning. You can choose to add IP addresses to VM and/or PC, depending on your license.

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 user roles (Scanner, Reader, Auditor) do not have permissions to add IP addresses.

## Parameters

These input parameters are used to add IP addresses.

Parameter	Description
action=add	(Required) A flag used to make a request to add IP addresses to the subscription.
echo_request={0   1}	(Optional) Specify 1 to show (echo) the request’s input parameters (names and values) in the XML output. When unspecified, input parameters are not included in the XML output.
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.
enable_vm={0   1} enable_pc={0   1}	(Required) You must enable the hosts for the VM application (enable_vm=1) or the PC application (enable_pc=1) or both VM and PC.
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).

Parameter	Description
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.

## XML Output

The DTD is described in Appendix A, Simple Return.

## Sample API Request

API request (POSTED raw data in CSV format):

```
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&enable_
vm=1&enable_pc=1&tracking_method=IP&owner=quays_es1"
```

API request ("ips" parameter):

```
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/"
```

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>2013-08-07T01:21:03Z</DATETIME>
    <TEXT>IPs successfully added to Vulnerability
Management/Compliance Management</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```



# Update IPs

The Update Asset IP API v2 (**/api/2.0/fo/asset/ip/?action=update**) gives you the ability to update IP addresses within the subscription.

Permissions: A Manager has permissions to update IP addresses. A Unit Manager can update IP addresses in asset groups assigned to the user's business unit. Users with other user roles (Scanner, Reader, Auditor) do not have permissions to update IP addresses.

## Parameters

These input parameters are used to update IP addresses.

Parameter	Description
action=update	(Required) A flag used to make a request to update IP addresses within the subscription.
echo_request={0   1}	(Optional) Specify 1 to show (echo) the request's input parameters (names and values) in the XML output. When unspecified, input parameters are not included in the XML output.
ips={value} -or- {POSTed CSV raw data}	<p>(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 &lt;data&gt;.</p> <p>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.</p>
tracking_method={value}	(Optional) To change to another tracking method specify IP for IP address, DNS or NETBIOS.
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.

Parameter	Description
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 API Requests

### Update IPs - Add new IPs

#### API request:

For the request below we're adding new IPs 10.10.10.200,10.10.23.40 (not already in the subscription) and assigning them the DNS tracking method.

```
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>2013-08-07T17:27:36Z</DATETIME>
    <TEXT>IPs successfully updated</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

### Update IPs - update IP with matching NetBIOS name

#### API request:

IP 10.10.26.167 has multiple entries so we're specifying the NetBIOS hostname in the request to identify which entry to update.

```
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/"
```

#### XML output:

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

```
"qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-01-02T05:23:15Z</DATETIME>
    <TEXT>IPs successfully updated</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

## Update IPs - duplicate host error

### API request:

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.

```
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.d
td">
<DUPLICATE_HOSTS_ERROR_OUTPUT>
  <RESPONSE>
    <CODE>1982</CODE>
    <DATETIME>2017-03-16T04:54:15Z</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.php]]></U
RL>
```

```
</WARNING>  
</RESPONSE>  
</DUPLICATE_HOSTS_ERROR_OUTPUT>
```

## XML Output

Duplicate hosts error is returned with instructions in cases where you try to update hosts with multiple scan data entries. This can happen when scans identified multiple hostnames for the same IP address.

The DTD is described in Appendix B, Duplicate Hosts Error Output.

# Manage Asset Groups

The Asset Group API v2 (</api/2.0/fo/asset/group/>) lets you manage asset groups with more granularity. These operations are supported: list, add, edit and delete.

Permissions are below:

User Role	Permissions
Manager	<ul style="list-style-type: none"> <li>- List all asset groups in the subscription.</li> <li>- Add, edit, delete asset groups in subscription.</li> </ul>
Unit Manager	<ul style="list-style-type: none"> <li>- List 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).</li> <li>- Add, edit, delete asset groups owned by any user in the business unit.</li> </ul>
Scanner	<ul style="list-style-type: none"> <li>- List asset groups in the user's account (those assigned to the user, and those owned by the user).</li> <li>- Add, edit, delete asset groups owned by the user.</li> </ul>
Reader	<ul style="list-style-type: none"> <li>- List asset groups in the user's account (those assigned to the user).</li> <li>- No permission to add, edit, delete asset groups.</li> </ul>

## List all your asset groups

Use these parameters:

Parameter	Description
action=list	(Required) The GET or POST method may be used.
output_format={csv   xml}	(Required) The requested output format: CSV or XML.
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.

Parameter	Description
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.
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.
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. Your options are: None, All or a comma-separated list of attribute names. Attribute names: TITLE, OWNER, NETWORK_IDS, LAST_UPDATE, IP_SET, APPLIANCE_LIST, DOMAIN_LIST, DNS_LIST, NETBIOS_LIST, EC2_ID_LIST, HOST_IDS, USER_IDS, UNIT_IDS, BUSINESS_IMPACT, CVSS, COMMENTS.

API request 1:

```
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 1:

```
<?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_list
_output.dtd">
<ASSET_GROUP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-06-17T08:48:41Z</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>
```

### API request 2 - show all attributes:

```
curl -u "USERNAME:PASSWD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=634851&show_attributes=ALL"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/"
```

### XML output 2:

```
<?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_list
_output.dtd">
<ASSET_GROUP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-06-17T09:08:01Z</DATETIME>
    <ASSET_GROUP_LIST>
      <ASSET_GROUP>
        <ID>634851</ID>
        <TITLE><![CDATA[mp1]]></TITLE>
        <OWNER_ID>70953</OWNER_ID>
        <UNIT_ID>0</UNIT_ID>
        <LAST_UPDATE>2014-06-13T11:44:04Z</LAST_UPDATE>
        <BUSINESS_IMPACT>High</BUSINESS_IMPACT>
        <CVSS_ENVIRO_CDP>Not Defined</CVSS_ENVIRO_CDP>
        <CVSS_ENVIRO_TD>Not Defined</CVSS_ENVIRO_TD>
        <CVSS_ENVIRO_CR>Not Defined</CVSS_ENVIRO_CR>
        <CVSS_ENVIRO_IR>Not Defined</CVSS_ENVIRO_IR>
        <CVSS_ENVIRO_AR>Not Defined</CVSS_ENVIRO_AR>
        <COMMENTS>
          <![CDATA[comment]]>
```

```
</COMMENTS>
<DEFAULT_APPLIANCE_ID>43575</DEFAULT_APPLIANCE_ID>
<APPLIANCE_IDS>43576, 43575</APPLIANCE_IDS>
<DOMAIN_LIST>
  <DOMAIN netblock="10.10.10.0, 10.10.25.50">ad.lan</DOMAIN>
</DOMAIN_LIST>
<NETBIOS_LIST>
  <NETBIOS>WIN2003-SRV-O</NETBIOS>
</NETBIOS_LIST>
</ASSET_GROUP>
</ASSET_GROUP_LIST>
</RESPONSE>
</ASSET_GROUP_LIST_OUTPUT>
```

DTD:

DTD: [https://<base\\_url>/api/2.0/fo/asset/group/asset\\_group\\_list\\_output.dtd](https://<base_url>/api/2.0/fo/asset/group/asset_group_list_output.dtd)

The DTD is described in Appendix B, Asset Group List Output.

### Add a new asset group

Use these parameters:

Parameter	Description
action=add	(Required) The POST method must be used.
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.
See "Asset Group Parameters"	

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=low&
cvss_enviro_cr=medium&cvss_enviro_ir=high&cvss_enviro_ar=medium&ips=1
0.1.1.1/31"
"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
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-05-28T22:57:50Z</DATETIME>
    <TEXT>Asset Group successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>395752377</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

## Edit an asset group

Use these parameters:

Parameter	Description
action=edit	(Required) The POST method must be used.
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.
See "Asset Group Parameters"	

### 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
"http://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 an asset group

By deleting an asset group any scheduled scans using the asset group will be deactivated. Use these parameters:

Parameter	Description
action=delete	(Required) The POST method must be used.
echo_request={0   1}	(Optional) Specify 1 to show (echo) the request's input parameters (names, values) in the XML output.
id={value}	(Required) The ID of the asset group you want to delete.

#### 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=delete"
```

#### 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>2014-05-29T15:49:35Z</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

These 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 <a href="#">Scanner Appliances</a> in Chapter 3 for details.	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

Parameter	Parameter Name action=add	Parameter Name action=edit
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
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

# Asset Search Report

The Asset Search API v2 (/api/2.0/fo/report/asset) helps you easily create reports on assets you're interested in. The new DTD for the asset search report is available here: [https://<base\\_url>/api/2.0/fo/report/asset/asset\\_search\\_report\\_v2.dtd](https://<base_url>/api/2.0/fo/report/asset/asset_search_report_v2.dtd) (see Appendix B for details).

## API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/?action=search&
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>2016-06-03T20:21:13Z</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>2016-06-03T20:21:13Z</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>2016-06-03T09:11:21Z</LAST_SCAN_DATE>
    <FIRST_FOUND_DATE>2016-06-03T07:11:46Z</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>2016-06-03T07:12:47Z</LAST_SCAN_DATE>
    <LAST_COMPLIANCE_SCAN_DATE>2016-05-
13T21:15:01Z</LAST_COMPLIANCE_SCAN_DATE>
    <FIRST_FOUND_DATE>2016-05-12T15:16:54Z</FIRST_FOUND_DATE>
  </HOST>

</HOST_LIST>
</ASSET_SEARCH_REPORT>
```

**DTD:**

DTD: [https://<base\\_url>/asset\\_search\\_report\\_v2.dtd](https://<base_url>/asset_search_report_v2.dtd)

The DTD is described in Appendix B, Asset Search Report.

### CSV output:

```

----BEGIN_RESPONSE_HEADER_CSV
"Launch Datetime","User Login","Resource","Parameter Name","Parameter
Value"
"2016-06-
07T22:51:23Z","john_sm","https://qualysapi.qualys.com/api/2.0/fo/repo
rt/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","DNSHos
tname","NetBIOSHostname","TargetTrackingMethod","TargetOperatingSyste
m","TargetService","TargetPort","TargetQID","QIDTitle","TargetLastSca
nDate","TargetFirstFoundDate","OSCP","Tags","TargetComplianceLastSca
nDate","Total"
"Corsa","John Smith","2016-06-07T22:51:23Z","", "10.10.10.10-
10.10.10.20",,,,,,,,,,,,,, "2"
"IP","DNSHostname","NetBIOSHostname","OperatingSystem","OSCP","Port/
Service/Default
Service","TrackingMethod","LastScanDate","LastComplianceScanDate","Fi
rst Found","Tags"
"10.10.10.10",,, "Linux 2.4-2.6 / Embedded Device / F5 Networks Big-
IP",,, "IP address","2016-06-03T09:11:21Z",, "2016-06-03T07:11:46Z",
"10.10.10.11",, "SYS_10_10_10_11",,, "IP address","2016-06-
03T07:12:47Z","2016-05-13T21:15:01Z","2016-05-12T15:16:54Z",

```

### Input parameters

Parameter	Description
action=search	(Required) GET or POST method may be used.
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. A valid value is: IP, DNS, NETBIOS, EC2, or AGENT.

Parameter	Description
ips={value}	<p>(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).</p> <p>One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.</p>
ips_network_id={value}	<p>(Optional) The network ID applied on IPs. The default value is ALL.</p>
asset_group_ids={value}	<p>(Optional) The IDs of asset groups containing the hosts to be included in the asset search report. Multiple IDs are comma separated.</p> <p>One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.</p>
asset_groups={value}	<p>(Optional) The titles of asset groups containing the hosts to be included in the asset search report. Multiple titles are comma separated.</p> <p>One of these parameters must be specified in a request: ips, asset_groups, asset_group_ids, or use_tags.</p>
assets_in_my_network_only={0   1}	<p>(Optional) Specify 1 to include the specified asset groups and/or IP ranges. Valid for 'All' Asset Group and/or specified IP ranges.</p>
ec2_instance_status={value}	<p>(Optional) Specify the EC2 instance status to be searched. Possible values: RUNNING,TERMINATED, PENDING, STOPPING, SHUTTING_DOWN, STOPPED. Values are case-sensitive. See “EC2 search samples”</p>
ec2_instance_id={value}	<p>(Optional) Specify the EC2 instance ID to be searched. See “EC2 search samples”</p> <p>ec2_instance_id is valid only when ec2_instance_id_modifier is specified</p>
ec2_instance_id_modifier={value}	<p>(Optional) Show only hosts with ec2_instance_id that is either: beginning with, containing, matching, ending with, not empty. See “EC2 search samples”</p> <p>ec2_instance_id_modifier is valid only when ec2_instance_id is specified</p>
display_ag_titles={0   1}	<p>(Optional) Specify 1 to display AssetGroup Titles for each Host in the output. Otherwise the AssetGroup Titles are not displayed in the output.</p>



Parameter	Description
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.
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.

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.
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.
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.
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.

Parameter	Description
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.

## EC2 search samples

### Sample 1 - Search EC2 asset with certain EC2 instance ID

Search EC2 asset with EC2 instance ID i-0fb7086f985856fa4.

#### API request:

```
curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl" -d
"action=search&output_format=xml&tracking_method=EC2&use_tags=1&tag_set_b
y=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>2017-04-11T10:17:32Z</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 2 - 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" -k -H "X-Requested-With: Curl" -d
"action=search&output_format=xml&tracking_method=EC2&use_tags=1&tag_set_by=name&tag_set_include=useasttag&ec2_instance_status=TERMINATED&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
"http://qualysapi.qualys.com/asset_search_report_v2.dtd">

<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[qualys-test]]></COMPANY>
  <USERNAME>sada-customer customer</USERNAME>
  <GENERATION_DATETIME>2017-04-11T10:49:05Z</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, Vrginia, 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>
```

## IPv6 Asset API

The IPv6 Asset 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.

This chapter describes how to use the IPv6 Asset API, built on the API V2 Architecture.

These topics are covered:

- API Support for IPv6 Asset Management and Scanning
- View IPv6 Mapping Records
- Add IPv6 Mapping Records
- Remove 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 and remove 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

##### Input:

```
$ curl -u username:password -H "X-Requested-With: curl"  
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/?act  
ion=list&output_format=csv"
```

##### 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. <b>Important:</b> 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://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

#### Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysguard.api.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

#### Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/?action=list&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_list_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. <b>Important:</b> 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)

#### Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
-d @file2.xml
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

#### Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysguard.api.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: Remove IPv6 Mapping Records (optional)

Manager users can remove IPv6 mapping records for the subscription by submitting the records to be removed in CSV or XML format. A maximum of 10,000 records can be removed per API request.

It's not necessary to specify both the IPv4 address and the IPv6 address for each record to be deleted in the data file (CSV or XML). If you specify only the IPv4 address, any associated record will be deleted. If you specify only the IPv6 address, any associated record will be deleted. If you specify both the IPv4 and IPv6 addresses, any record containing either address will be deleted. If no IP addresses specified in a mapping record to be deleted match any IP addresses already defined in mapping records in the subscription, the mapping record listed in the data file will be silently ignored.

Important: When an IPv6 mapping record is removed, any scan data associated with your IPv6 host is removed from your subscription and this data is not recoverable.

## How to Remove IPv6 Records in CSV

Review the steps below to learn how to remove 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

Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/?action=list&output_format=csv"
```

### 2) Prepare file3.csv with records to be removed

The CSV file contents identify one or more IPv6 mapping records to be removed.

Sample file3.csv used to remove IPv6 mapping records:

```
$ cat file3.csv
action=remove&csv_data=
"0.0.0.4", "2001:470:8418:a18::a0a:1849"
"0.0.0.5", "2001:470:8418:a18::a0a:189c"
```

### 3) POST data from file3.csv (Success)

Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
-d @file3.csv
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

Output:

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

```
"https://qualysguard.api.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2011-11-03T19:31:27Z</DATETIME>
    <TEXT>Removed 2 records (any associated scanned host data is
now queued for purging)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

## How to Remove IPv6 Records in XML

Review the steps below to learn how to remove 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

#### Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/?act
ion=list&output_format=xml"
```

### 2) Prepare file4.xml with records to be removed

The XML file contents identify one or more IPv6 mapping records to be removed.

Sample file4.XML used to remove IPv6 mapping records:

```
$ cat file4.xml
action=remove&xml_data=
<IP_MAP_LIST>
  <IP_MAP>
    <V4>0.0.0.4</V4>
    <V6>2001:470:8418:a18::a0a:1849</V6>
  </IP_MAP>
  <IP_MAP>
    <V4>0.0.0.5</V4>
    <V6>2001:470:8418:a18::a0a:189c</V6>
  </IP_MAP>
</IP_MAP_LIST>
```

### 3) POST data from file4.xml (Success)

#### Input:

```
$ curl -u username:password -H "X-Requested-With: curl"
-d @file4.xml
"https://qualysguard.api.qualys.com/api/2.0/fo/asset/ip/v4_v6/"
```

#### Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysguard.api.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2011-11-03T20:59:07Z</DATETIME>
    <TEXT>Removed 2 records (any associated scanned host data is
now queued for purging)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

## Step 4: 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 5: Launch Scan

Using the Qualys API you can launch scans on the IPv4 addresses which are mapped to IPv6 addresses.

## Step 6: 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/detectio  
n/?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.ad.vuln.qa.qualys.com]]></DNS>  
  <LAST_SCAN_DATETIME>2010-11-  
17T19:06:31Z</LAST_SCAN_DATETIME>  
  <DETECTION_LIST>  
  ...
```

# View IPv6 Mapping Records

The `/api/2.0/fo/asset/ip/v4_6` resource with the **action=list** parameter is used to view a list of IPv6 mapping records. 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. The GET method may be used to make an API request. Authentication is required; see Chapter 2, “Authentication Using the V2 APIs.”

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

User permissions are described below.

User Role	Permissions
Manager	View all IPv6 mapping records, when the IPv6 Support feature is enabled for the user’s subscription.
Auditor, Unit Manager, Scanner, Reader	No permission to view all IPv6 mapping records.

## Parameters

The input parameters used to request a list of IPv6 mapping records are described below.

Parameter	Description
action=list	(Required) The action type for requesting a list of IPv6 mapping records.
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.



Parameter	Description
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.

## XML Output

### DTD for IPv6 Mapping Records List

An API request for a mapping record list returns XML output using the DTD which can be found at the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/  
asset/ip/v4_v6/ip_map_list_output.dtd
```

The DTD for the IPv6 mapping records list XML is provided in Appendix B.

### Sample IPv6 Mapping Records List Output

For sample mapping records list output in CSV format, see “How to Add IPv6 Records in CSV.”

For sample mapping records list output in XML format, see “How to Add IPv6 Records in XML.”

# Add IPv6 Mapping Records

The `/api/2.0/fo/asset/ip/v4_6` resource with the **action=add** parameter is used to 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. The POST method may be used to make an API request. Authentication is required; see Chapter 2, “Authentication Using the V2 APIs.”

A maximum of 10,000 mapping records can be added per API request.

## Permissions

User Role	Permissions
Manager	Add IPv6 mapping records, when the IPv6 Support feature is enabled for the user’s subscription.
Auditor, Unit Manager, Scanner, Reader	No permission to add IPv6 mapping records.

## Parameters

The input parameters used to add IPv6 mapping records are described below.

Parameter	Description
action=add	(Required) The action type to add IPv6 mapping records.
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 <b>xml_data</b> must be specified. See “How to Add IPv6 Records in CSV.”  The parameters <b>csv_data</b> and <b>xml_data</b> cannot be specified in the same request.

Parameter	Description
xml_data={value}	<p>The CSV data file containing the IPv6 mapping records that you want to add. This parameter or <b>csv_data</b> must be specified. See “How to Add IPv6 Records in XML.”</p> <hr/> <p>The parameters <b>csv_data</b> and <b>xml_data</b> cannot be specified in the same request.</p>
all_or_nothing={0   1}	<p>(Optional) This parameter controls how the service processes the IPv6 mapping records in the upload data. When unspecified or set to <b>1</b>, 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 <b>0</b> the service does not cancel the request if an IP conflict is found.</p>

## XML Output

### DTD for Simple Return

An API request to add IPv6 mapping records returns XML output using the simple return DTD which can be found at the following URL:

`https://qualysapi.qualys.com/api/2.0/simple\_return.dtd`

A description of the simple return DTD is provided in Appendix A.

### Sample XML Output

For simple return output in CSV format, see “How to Add IPv6 Records in CSV.”

For simple return output in XML format, see “How to Add IPv6 Records in XML.”

# Remove IPv6 Mapping Records

The `/api/2.0/fo/asset/ip/v4_6` resource with the **action=remove** parameter is used to remove IPv6 mapping records from the subscription. The POST method may be used to make an API request. Authentication is required; see Chapter 2, “Authentication Using the V2 APIs.”

A maximum of 10,000 mapping records can be removed per API request.

It's not necessary to specify both the IPv4 address and the IPv6 address for each record to be deleted in the data file (CSV or XML). If you specify only the IPv4 address, any associated record will be deleted. If you specify only the IPv6 address, any associated record will be deleted. If you specify both the IPv4 and IPv6 addresses, any record containing either address will be deleted. If no IP addresses specified in a mapping record to be deleted match any IP addresses already defined in mapping records in the subscription, the mapping record listed in the data file will be silently ignored.

Important: When an IPv6 mapping record is removed, any scan data associated with your IPv6 host is removed from your subscription and this data is not recoverable.

## Permissions

User Role	Permissions
Manager	Remove all IPv6 mapping records, when the IPv6 Support feature is enabled for the user's subscription.
Auditor, Unit Manager, Scanner, Reader	No permission to remove IPv6 mapping records.

## Parameters

The input parameters used to remove IPv6 mapping records are described below.

Parameter	Description
action=remove	(Required) The action type to remove IPv6 mapping records.
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.

Parameter	Description
csv_data={value}	The CSV data file containing the IPv6 mapping records that you want to remove from your subscription. This parameter or <b>xml_data</b> must be specified. See “How to Remove IPv6 Records in CSV.”
xml_data={value}	The CSV data file containing the IPv6 mapping records that you want to remove from your subscription. This parameter or <b>csv_data</b> must be specified. See “How to Remove IPv6 Records in XML.”

## XML Output

### DTD for Simple Return

An API request to remove IPv4 to IPv6 mapping records returns XML output using the simple return DTD which can be found at the following URL:

[https://qualysapi.qualys.com/api/2.0/simple\\_return.dtd](https://qualysapi.qualys.com/api/2.0/simple_return.dtd)

A description of the simple return DTD is provided in Appendix A.

### Sample XML Output

For simple return output in CSV format, see “How to Remove IPv6 Records in CSV.”

For simple return output in XML format, see “How to Remove IPv6 Records in XML.”

## Compliance API

Qualys Policy Compliance allows customers to audit host configurations and measure their level of compliance with internal and external policies. The Compliance API allows API users to report on policy compliance data in their user account. This chapter describes how to use the Compliance API, built on the API V2 Architecture.

These topics are covered:

- Compliance Control List
- Compliance Policy List
- Compliance Policy - Export
- Compliance Policy - Import
- Compliance Policy - Merge
- Compliance Policy - Manage Asset Groups
- Compliance Posture Information
- Control Criticality
- Exceptions
- SCAP Cyberscope Report
- SCAP ARF Report
- SCAP Policy List

# Compliance Control List

The “Compliance Control List” API v2 (the resource `/api/2.0/fo/compliance/control/` with the parameter **action=list**) is used to view a list of compliance controls which are visible to the user. The compliance control ID for each control is listed in the output. Controls in the XML output are sorted by control ID in ascending order. Optional input parameters support filtering the list. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

The user has the ability to select the amount of additional information to include for each control in the output. By default, this basic control information is included: the control ID, the control category, the control sub-category, the control statement, and a list of technologies.

Use the **details** input parameter to select another level of detail to be included in the control list output. Two parameter settings are available. Specify **details=All** to show the basic compliance control information and a list of framework mappings for each control. Specify **details=None** to list the compliance control ID only for each control.

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.

## 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.

## User Permissions

User permissions are described below.

User Role	Permissions
Manager	View all compliance controls.
Auditor	View all compliance controls.
Unit Manager	View all compliance controls.
Scanner	View all compliance controls.
Reader	View all compliance controls.

## Request

**URL.** Use this URL to request a compliance control list, where `<qualysapi.qualys.com>` is the API server URL where your account is located. Replace the API server URL if your account is located on another platform.

```
https://<qualysapi.qualys.com>/api/2.0/fo/
compliance/control/
```

**Method.** The GET or POST access method may be used.

**Authentication.** Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

## Parameters

The parameters used to make a control list request are described below.

Parameter	Description
action=list	(Required) Specifies the action type used to request a control list.
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={ <b>Basic</b>   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.



Parameter	Description
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}	<p>(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).</p> <p>If the requested list identifies more records than the truncation limit, then the XML output includes the &lt;WARNING&gt; element and the URL for making another request for the next batch of records.</p> <p>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.</p>

## 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).

## XML Output

### DTD for Control List

An API request for a technical control list returns XML output using the DTD which can be found at the following URL:

```
https://<qualysapi.qualys.com>/api/2.0/fo/
compliance/control/control_list_output.dtd
```

where `<qualysapi.qualys.com>` is the API server URL where your account is located.

The DTD for the compliance control list XML is provided in Appendix C.

## 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/control_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 '07_DICTIONARY_ACCESSIBILITY'
setting in init.ora (ORACLE Data Dictionary)]]></STATEMENT>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>7</ID>
            <NAME>Oracle 9i</NAME>
            <RATIONALE><![CDATA[The "07_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 "07_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>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_LIST>

```

```
<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>
```

# Compliance Policy List

The “Compliance Policy List” API v2 (the resource `/api/2.0/fo/compliance/policy/` with the parameter `action=list`) is used to view a list of compliance policies visible to the user. The compliance policy ID for each policy is listed in the policy list output. Policies in the XML output are sorted by compliance policy ID in ascending order. Optional input parameters support filtering the policy list output. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

By default, the compliance policy list output shows all compliance policies in the subscription. Optional input parameters allow you to set filters to restrict the policy list output to policies with certain compliance policy IDs.

## 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.

## User Permissions

User permissions are described below.

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.

User Role	Permissions
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.

# Request

**URL.** Use this URL to request a compliance policy list, where `<qualysapi.qualys.com>` is the API server URL where your account is located. Replace the API server URL if your account is located on another platform.

```
https://<qualysapi.qualys.com>/api/2.0/fo/  
compliance/policy/
```

**Method.** The GET or POST access method may be used.

**Authentication.** Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

# Parameters

The parameters used to make a compliance policy list request are described below.

Parameter	Description
action=list	(Required) Specifies the action type to request a policy list.
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={ <b>Basic</b>   All   None}	<p>(Optional) Show requested amount of information for each policy. A valid value is:</p> <p>None — show policy ID only</p> <p>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.</p> <p>All — show the basic policy information, plus a technology list for each control, IP list for each asset group, and a user list</p>
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.

## XML Output

### DTD for Compliance Policy List

An API request for a compliance policy list returns XML output using the DTD which can be found at the following URL:

```
https://<qualysapi.qualys.com>/api/2.0/fo/  
compliance/policy/policy_list_output.dtd
```

where `<qualysapi.qualys.com>` is the API server URL where your account is located.

The DTD for the compliance policy list XML output is provided in Appendix C.

### Sample Compliance Policy List

Sample compliance policy list output is below:

#### 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>2016-11-03T21:15:29Z</DATETIME>  
    <POLICY_LIST>  
      <POLICY>  
        <ID>18948</ID>  
        <TITLE><![CDATA[XP policy]]></TITLE>  
        <CREATED>  
          <DATETIME>2016-10-19T18:37:15Z</DATETIME>  
          <BY>quays_as</BY>  
        </CREATED>  
        <LAST_MODIFIED>  
          <DATETIME>2016-10-26T23:31:57Z</DATETIME>  
          <BY>quays_as</BY>  
        </LAST_MODIFIED>  
        <LAST_EVALUATED>  
          <DATETIME>2016-11-03T08:40:44Z</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 'Clipboard' 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>

```

# Compliance Policy - Export

The Export Compliance Policy API v2 (the resource `/api/2.0/fo/compliance/policy/` with the parameter `action=export`) gives you the ability to export compliance policies.

Your account must have the Policy Compliance application enabled in order to export policies using this API.

## Exporting a policy

You can export a compliance policy, that exists in your account, to an XML file. We'll include all service-provided controls in the policy. You can choose to also include 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 this permission must be turned on in your account: Manage PC module.

## Input Parameters

Parameter	Description
action=export	(Required) Specifies the action type for exporting the policy. GET and POST methods may be used.
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. When not specified, UDCs are not included.
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.
show_user_controls={0   1}	(Optional) Set to 1 to show 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, the appendix section is not included in the output.  Interested in Qualys Custom Controls? Log in to Qualys, go to Help > Online Help and search for "custom controls".

## Sample Requests

### 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_export_ou
tput.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="74378d12a39f82721a3cb156dee58c663a650a9ce422bd311b5e5443c2a20f1
4">&lt;CTRL&gt;&lt;NOT&gt;&lt;DP&gt;&lt;K&gt;auth.general.logintext&lt;/K
&gt;&lt;OP&gt;re&lt;/OP&gt;&lt;V&gt;&lt;![CDATA[^(\s*|314159265358979|161
8033999999999)$]]&gt;&lt;/V&gt;&lt;/DP&gt;&lt;/NOT&gt;&lt;/CTRL&gt;</EVALU
ATE>
              </TECHNOLOGY>
            </TECHNOLOGIES>
          </CONTROL>
        </SECTION>
      </SECTIONS>
    </POLICY>
```

## 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/">showApp.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>2016-09-09T09:07:13Z</DATETIME>  
    <POLICY>  
      <TITLE><![CDATA[Solaris]]></TITLE>  
      <EXPORTED><![CDATA[ 2016-09-09T09:07:12Z]]></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="1618033999999999"><![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="1618033999999999"><![CDATA[Setting not found]]></FV>
            <FV id="314159265358979"><![CDATA[File not found]]></FV>
        </DP>
        ...
    </DATA_POINT_ACRONYMS>
</APPENDIX>
</POLICY>
</RESPONSE>
</POLICY_EXPORT_OUTPUT>

```

## 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>
        <CATEGORY>
          <ID>3</ID>
          <NAME><![CDATA[Access Control Requirements]]></NAME>
        </CATEGORY>
        <SUB_CATEGORY>
          <ID>1007</ID>
          <NAME><![CDATA[Authentication/Passwords]]></NAME>
        </SUB_CATEGORY>
      </USER_DEFINED_CONTROL>
    </CONTROLS>
  </SECTION>
  ...

```

## Policy Export Output DTD

An API request returns output using the policy export output DTD which can be found at the following URL (where qualysapi.qualys.com is the API server where your account is located):

```
https://qualysapi.qualys.com/api/2/fo/compliance/policy/policy_export_output.dtd
```

This DTD is described in Appendix C.

# Compliance Policy - Import

The Import Compliance Policy API v2 (the resource `/api/2.0/fo/compliance/policy/` with the parameter `action=import`) gives you the ability to import compliance policies.

Your account must have the Policy Compliance application enabled in order to import policies using this API.

## Importing a policy

You can 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 this permission must be turned on in your account: Manage PC module.

## Input Parameters

Parameter	Description
action=import	(Required) Specifies the action type for importing the policy. POST method must be used.
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 Request

### 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>2016-09-15T21:32:40Z</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>
```



# Compliance Policy - Merge

The “Compliance Policy Merge” API v2 (the resource `/api/2.0/fo/compliance/policy/` with the parameter `action=merge`) allows you to merge (combine) 2 or more compliance policies using Qualys Policy Compliance (PC). You can choose to merge some or all parts of a new policy into an existing one. Also you can preview merge changes before saving them. This API is available to Managers and Auditors.

For example, say you imported a policy from our library (Policy A) and configured it to add asset groups, controls and sections. Later we might release an updated version of this policy (Policy B) with new controls and technologies. 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.

## Parameters

The policy merge input parameters give you flexibility with merging different parts of a new policy (Policy B) into an existing one (Policy A). For example you can choose to update controls with newer definitions, replace asset groups, and add new technologies and controls. By default no changes are applied to your existing policy unless parameters are specified (see below).

Parameter	Description
<code>action=merge</code>	(Required)
<code>id={value}</code>	(Required) The ID of the policy that will be updated with merged content (let’s call this Policy A).
<code>merge_policy_id={value}</code> -or- policy XML data	(Required) Tell us the 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: <code>--data-binary @path_to_xml_file.xml</code>  These options are mutually exclusive: policy XML data and replace_asset_groups.
<code>replace_cover_page={0   1}</code>	(Optional) Set <code>replace_cover_page=1</code> to replace the cover page in Policy A with the cover page in Policy B.
<code>replace_asset_groups={0   1}</code>	(Optional) Set <code>replace_asset_groups=1</code> to replace asset groups in Policy A with asset groups in Policy B.  These options are mutually exclusive: add_asset_groups and replace_asset_groups.
<code>add_asset_groups={0   1}</code>	(Optional) Set <code>add_asset_groups=1</code> 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, i.e. add technologies from Policy B if they are not already in Policy A.
add_new_controls={0   1}	(Optional) Set add_new_controls=1 to add new controls, i.e. add controls 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: <b>add_new_controls</b> or <b>update_existing_controls</b> .
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).
preview_merge={0   1}	(Optional) Set preview_merge= 1 to view the changes merged into Policy A without saving them.

## XML Output

### DTD for Policy Merge Results Output

The DTD for policy merge results output XML can be found at this URL:

[https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy\\_merge\\_result\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_merge_result_output.dtd)

If your account is not located on Qualys Platform 1, please replace “qualysapi.qualys.com” with your platform URL.

### 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&add_new_
asset_groups=1&add_new_technologies=1&update_section_heading=1&add_new_co
ntrols=1&update_existing_controls=1&preview_merge=1"
```

#### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_MERGE_RESULT_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_merge_r
esult_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2013-12-24T05:28:04Z</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&add_new_
asset_groups=1&add_new_technologies=1&update_section_heading=1&add_new_co
ntrols=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_r
esult_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2013-12-24T05:31:26Z</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_existi
ng_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_r
esult_output.dtd">
<POLICY_MERGE_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2013-12-24T05:38:26Z</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 Groups

Manage asset groups for your compliance policies using the “Compliance Policy” API v2 (/api/2.0/fo/compliance/policy). Parameters allow you to add, remove and set asset groups for a policy. You must have permission to modify the policy you want to update.

## action=add\_asset\_group\_ids

Use this action to add asset groups to a specified policy. Parameters:

Parameter	Description
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/?action=add_a
sset_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>
```

**action=remove\_asset\_group\_ids**

Use this action to remove asset groups from a specified policy. Parameters:

Parameter	Description
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/?action=remov
e_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>
```



## action=set\_asset\_group\_ids

Use this action to reset the asset groups for a specified policy. Any assigned asset groups not specified in this request will be removed. Parameters:

Parameter	Description
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 Posture Information

The “Compliance Posture Info” API v2 (the resource `/api/2.0/fo/compliance/posture/info/` with the parameter `action=list`) is used to view current compliance posture data (info records) for hosts within the user’s account. Each compliance posture info record includes a compliance posture ID and other attributes. Optional input parameters support filtering the posture info record output. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

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).
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 your account has permission to see. Optional input parameters 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 <b>details=All</b> 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 <b>details=All</b> 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 <b>details=All</b> 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.

## User Permissions

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 permissions are described below.

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.
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.

### Request

**URL.** Use this URL to request a compliance posture information, where `<qualysapi.qualys.com>` is the API server URL where your account is located. Replace the API server URL if your account is located on another platform.

```
https://<qualysapi.qualys.com>/api/2.0/fo/  
compliance/posture/info/
```

**Method.** The GET or POST access method may be used.

**Authentication.** Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

## Parameters

The parameters used to make a compliance info records request are described below.

Parameter	Description
action=list	(Required) Specifies the action type used to request compliance policy info records.
policy_id={value}	<p>(<b>policy_id</b> or <b>policy_ids</b> is required) Show compliance posture info records for a specified policy. A valid policy ID is required.</p> <p>The parameters <b>policy_id</b> and <b>policy_ids</b> cannot be specified in the same request.</p>
policy_ids={value}	<p>(<b>policy_id</b> or <b>policy_ids</b> 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).</p> <p>The parameters <b>policy_id</b> and <b>policy_ids</b> cannot be specified in the same request. When <b>policy_ids</b> is specified, <b>truncation_limit</b> is invalid. For CSV output, <b>policy_id</b> must be specified (and <b>policy_ids</b> is invalid).</p>
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 <b>policy_id</b> is required.
details={ <b>Basic</b>   All   None   Light}	<p>(Optional) Show a certain amount of information for each compliance posture info record. A valid value is:</p> <p>None — show posture info and minimum exception information (assignee and status) if appropriate</p> <p>Basic (default) — show posture info, full exception information if appropriate, and a minimum glossary (basic info for hosts and controls)</p> <p>Light — show posture info, exception info if appropriate, and a limited glossary (host info and last scan date/time, control ID, and evidence info)</p> <p>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</p>

Parameter	Description
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.
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}	<p>(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.</p> <p>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”.</p>
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}	<p>(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.</p> <p>The parameters <b>criticality_labels</b> and <b>criticality_values</b> cannot be specified in the same request.</p>
criticality_values={value}	<p>(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.</p> <p>The parameters <b>criticality_labels</b> and <b>criticality_values</b> cannot be specified in the same request.</p>
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.
truncation_limit={value}	<p>(Optional) The parameter is valid only when the API request is for a single policy and the <b>policy_id</b> parameter is specified.</p> <p>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.</p> <p>If the requested list identifies more records than the truncation limit, then the XML output includes the &lt;WARNING&gt; element and the URL for making another request for the next batch of records.</p> <p>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.</p>

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.
tag_include_selector={all   <b>any</b> }	(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   <b>any</b> }	(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.

## XML Output

### DTD for Compliance Posture Information

An API request for compliance posture information returns XML output using the DTD which can be found at the following URL (where `<base_url>` is the API server URL where your account is located):

```
https://<base_url>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd
```

The DTD for the compliance posture information XML output is provided in Appendix C.

### Sample Compliance Posture Information API

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>

...

```

## 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

The Exception API (/api/2.0/fo/compliance/exception/) lets you list, request, update and delete exceptions.

## User Permissions

To use the Exception API the user must have compliance management privileges. Unit Managers, Scanners and Readers must be granted this permission in their account settings.

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	List, request, update exceptions for hosts in their account. Updates are limited to adding comments.
Reader	List, request, update exceptions for hosts in their account. Updates are limited to adding comments.

**Good to Know:** The Exception API is only available if you have Policy Compliance (PC) module enabled for your subscription.

To request an exception or to filter exceptions in API, you may need to specify parameter IDs (like host ID, control ID or policy ID). To quickly know the ID of a parameter, simply use the “Compliance Posture Information” API v2 (the endpoint/api/2.0/fo/compliance/posture/info) with failed status.

## Sample API request:

```
curl -s -k -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"
```

## Sample XML response:

```
<?xml version="1.0" encoding="UTF-8" ?>
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_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>
...
```

## List exceptions

### Input parameters

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) GET or POST method may be used.
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. <a href="#">Tell me about exception status</a>
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.
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.

Parameter	Description
modified_by={value}	(Optional) Show exceptions that were modified by a particular user by specifying the user ID.
details={ <b>Basic</b>   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

### API request:

```
curl -s -k -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo 2" -D
headers.15
"https://qualysapi.qualys.com/api/2.0/fo/compliance/exception/?action=lis
t&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>2016-01-15T11:26:34Z</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>2016-01-15T08:53:19Z</MODIFIED_DATE>
<HISTORY_LIST>
    <HISTORY>
        <USER><![CDATA[John (mnc_su)]]></USER>
        <COMMENT><![CDATA[test]]></COMMENT>
        <INSERTION_DATE>2016-01-05T06:48:13Z</INSERTION_DATE>
    </HISTORY>
    <HISTORY>
        <USER><![CDATA[Bill (mnc_ru)]]></USER>
        <COMMENT><![CDATA[test]]></COMMENT>
        <INSERTION_DATE>2016-01-15T08:48:38Z</INSERTION_DATE>
    </HISTORY>
    <HISTORY>
        <USER><![CDATA[Mark (mnc_au)]]></USER>
        <COMMENT><![CDATA[test]]></COMMENT>
        <INSERTION_DATE>2016-01-15T08:53:19Z</INSERTION_DATE>
    </HISTORY>
</HISTORY_LIST>
</EXCEPTION>

...

```

## XML DTD

The DTD for the exception list XML output is provided in Appendix C.

## Request exception

An exception is created with the expiry date matching the creation date. You can update the exception to change it.

## Input parameters

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.
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

### API request:

```
curl -k -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>
```

**XML DTD**

The DTD for the simple return XML output is provided in Appendix A.

**Update exceptions**

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.

**Input parameters**

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.



Parameter	Description
status={Pending   Approved   Rejected}	(Optional) Update the status of the exception request. A valid value is: Pending, Approved, and Rejected. <a href="#">Tell me about exception status.</a>
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

#### 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&c  
omments=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/exception_b  
atch_return.dtd">  
<BATCH_RETURN>  
  <RESPONSE>  
    <DATETIME>2016-01-07T11:24:42Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Updated</TEXT>  
        <NUMBER_SET>  
          <NUMBER>55</NUMBER>  
        </NUMBER_SET>  
      </BATCH>  
    </BATCH_LIST>  
  </RESPONSE>  
</BATCH_RETURN>
```

### XML DTD

The DTD for the exception batch return XML output is provided in Appendix C.

# Delete exceptions

## Input parameters

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

### API request:

```
curl -k -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/exception_b  
atch_return.dtd">  
<BATCH_RETURN>  
  <RESPONSE>  
    <DATETIME>2016-01-07T11:22:20Z</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>
```

## XML DTD

The DTD for the exception batch return XML output is provided in Appendix C.

# 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. For information on the Cyberscope report specification and the LASR format please see:

<http://scap.nist.gov/use-case/cyberscope>

## SCAP Scan Results API

The “SCAP Scan Results” API v2 (the resource `/api/2.0/fo/asset/host/cyberscope/fdcc/scan/`) creates 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/fdcc/scan/
?scan_id=4244823&organisation_name1=Name1&organisation_name2=Name2&organi
sation_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 Quick 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=4297
720
```

## 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/fdcc/scan/
?scan_ref=qscap/1337984725.4360&organisation_name1=Name1&organisation_nam
e2=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/fdcc/scan/
?scan_id=4268027&ips=10.10.26.183&organisation_name1=Name1&organisation_n
ame2=Name2&organisation_name3=Name3"
```

## SCAP Policy Results API

The “SCAP Policy Results” API v2 (the resource **/api/2.0/fo/asset/host/cyberscope/fdcc/policy/**) creates 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/fdcc/polic
y/?policy_id=30231&organisation_name1=Name1&organisation_name2=Name2&orga
nisation_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 Quick 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&refresh_pa
rent=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/fdcc/polic
y/?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/fdcc/polic
y/?policy_id=17012&ag_ids=397405&ips=10.10.25.70&organisation_name1=Name1
&organisation_name2=Name2&organisation_name3=Name3"
```

## SCAP Global Results API

The "SCAP Global Results" API v2 (the resource `/api/2.0/fo/asset/host/cyberscope/`) creates 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/?ips=10.10
.24.52&organisation_name1=Name1&organisation_name2=Name2&organisation_nam
e3=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=50
3424&organisation_name1=Name1&organisation_name2=Name2&organisation_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/?ips=10.10
.24.52,10.10.25.2-
10.10.25.255&ag_ids=503424,503430&organisation_name1=Name1&organisation_n
ame2=Name2&organisation_name3=Name3"
```

# SCAP ARF Report

The “SCAP ARF Report” API v2 (the resource `/api/2.0/fo/compliance/scap/arf/`) allows users to 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

The “SCAP Policy List” API v2 (the resource `/api/2.0/fo/compliance/fdcc_policy/` with the parameter `action=list`) is used to 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.

## User Permissions

User permissions are described below.

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.



# Request

**URL.** Use this URL to request an SCAP policy list, where `<qualysapi.qualys.com>` is the API server URL where your account is located. Replace the API server URL if your account is located on another platform.

```
https://qualysapi.qualys.com/api/2.0/fo/  
compliance/fdcc_policy/
```

**Method.** The GET or POST access method may be used.

**Authentication.** Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

# Parameters

The parameters used to make an SCAP policy list request are below.

Parameter	Description
action=list	(Required) The action type required to request a list of SCAP policies.
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 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.

## XML Output

### DTD for SCAP Policy List

An API request for an SCAP policy list returns XML output using the DTD which can be found at the following URL:

```
https://qualysapi.qualys.com/api/2.0/fo/
compliance/fdcc_policy/fdcc_policy_list_output.dtd
```

where `<qualysapi.qualys.com>` is the API server URL where your account is located.

The DTD for the SCAP policy list XML output is provided in Appendix C.

### 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/fdcc_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_version_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>
```

## Scan Authentication API

The Authentication API is used to manage authentication records used to support authenticated scanning (e.g. trusted scanning).

<b>Authentication summary</b>	
<a href="#">User Permissions Summary</a>	
<b>List Records</b>	
<a href="#">List Authentication Records</a>	
<a href="#">List Authentication Records by Type</a>	
<b>Record types</b>	
<a href="#">Application Server Records</a>	<a href="#">Palo Alto Firewall Record</a>
<a href="#">Docker Record (PC, SCA)</a>	<a href="#">PostgreSQL Record (PC, SCA)</a>
<a href="#">HTTP Record</a>	<a href="#">SNMP Record</a>
<a href="#">IBM DB2 Record</a>	<a href="#">Sybase Record (PC, SCA)</a>
<a href="#">MongoDB Record</a>	<a href="#">Unix Record</a>
<a href="#">MS SQL Record (PC, SCA)</a>	<a href="#">VMware Record</a>
<a href="#">MySQL Record</a>	<a href="#">Windows Record</a>
<a href="#">Oracle Record</a>	
<a href="#">Oracle Listener Record</a>	
<a href="#">Oracle WebLogic Server Record (PC, SCA)</a>	

## 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

The API `/api/2.0/fo/auth/?action=list` resource with the parameter **action=list** is used to view a list of all authentication records visible to the user. The record ID for each authentication record is listed in the authentication record list output. The output shows the authentication record ID only. To see authentication record attributes for a particular record, use the type-specific record list function (see “List Authentication Records by Type”).

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.

## Record List: Parameters

The parameters below may be specified for an authentication record list request.

Parameter	Description
action=list	(Required) GET or POST method may be used.
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.

## Record List: XML Output

DTD: `https://<baseurl>/api/2.0/fo/auth/auth_records.dtd`

For details, see Appendix D.

## Sample Authentication Record List: All Types

```
<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>
```



# List Authentication Records by Type

The API `/api/2.0/fo/auth/<type>` resource with the parameter `action=list` is used to view a list of authentication records visible to the user for a specific authentication type (Unix, Windows etc).

Types include: docker, http, ibm\_db2, mongodb, ms\_sql, mysql, oracle, oracle\_listener, oracle\_weblogic, palo\_alto\_firwall, postgresql, snmp, sybase, unix (for Unix, Cisco, Checkpoint Firewall), 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.

## Record List by Type: Parameters

The parameters below may be specified for an authentication record list request.

Parameter	Description
action=list	(Required) GET or POST method may be used.
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.
details={ <b>Basic</b>   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.

Parameter	Description
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.

Record List by Type: XML Output

DTD: https://<baseurl>/api/2.0/fo/auth/<type>/

where <type> is the authentication record type, such as unix, windows, oracle, etc.

Sample authentication record list output listing 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>https://qualysapi.qualys.com/api/2.0/fo/auth/?action=list&id_min=
3457</URL>
  </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>
```

# Application Server Records

Policy Compliance includes content in the control Knowledgebase to provide support of Application Server Technologies. You can create and manage these authentication records using the “Authentication” API v2 (resource `/api/2.0/fo/auth/`):

Application Server Technology Record	Authentication API v2 endpoint
Apache 2.2 - IBM HTTP Server 7.x (on Red Hat Linux 5/6) - VMware vFabric Web Server 5.2 (on Red Hat Linux 5/6)	<code>/api/2.0/fo/auth/apache/</code>
Microsoft Internet Information Services (IIS) 6.0, 7.x	<code>/api/2.0/fo/auth/ms_iis/</code>
IBM WebSphere Application Server 7.0	<code>/api/2.0/fo/auth/ibm_websphere/</code>
Tomcat Server - Apache Tomcat 6.x and 7.x - VMware vFabric tc Server 2.9.x - Pivotal tc Server 3.x	<code>/api/2.0/fo/auth/tomcat/</code>

See [User Permissions Summary](#)

Using the Authentication Server API you can submit API requests to view Server authentication records, add new records, update records and delete records. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

Apache server authentication - support for multiple instances per host. Want to set it up? Just create multiple Apache server authentication records - 1 record for each host instance. In each record, a host instance is defined by a unique IP address and configuration file pair. You can create 2 records for the same IP address, but the config file can't be the same in the 2 records.

## Server Record: List

See [List Authentication Records by Type](#)

## Server Record: Create / Update

These parameters are used to create and update a Server authentication record.

Parameter	Description
<code>action=create update</code>	(Required) Specify “create” to create a new record, or “update” to update an existing record.
<code>echo_request={0 1}</code>	(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.

Parameter	Description
title={value}	(Required) 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.
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.
unix_install_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record). The directory where the WebSphere application is installed.
installation_path={value}	(Required to create a 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/update a 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 <b>auto_discover_instances=0</b> ), or multiple instances (use with <b>auto_discover_instances=1</b> ). 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/update a Tomcat Server record; valid only for this record). Specify <b>auto_discover_instances=1</b> 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 ( <b>auto_discover_instances=0</b> ), we will not auto discover instances. Applies to Apache Tomcat or when you've specified a single instance.
ips={value}	(Required to create a record) Add IP addresses of the hosts you want to scan using this record.
ids={value}	(Required to update a record; invalid when creating a record) Update Server 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, 1359-1407). Valid IDs are required.
add_ips={value}	(Optional and valid only when updating a record; invalid when creating a 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 when updating a record; invalid when creating a record). Remove IP address(es) from the IP list for an existing record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled). The network ID for the record.

## Server Record: Delete

These parameters are used to delete an existing Server authentication record.

Parameter	Description
action=delete	(Required) The action required for the API request: delete.
echo_request={0   1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output.
ids={value}	(Required) Delete only Server 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.

## Server Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details.

## Server Record: Sample API Request

### Create an Apache record:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d  
"action=create&title=Apache+Record&unix_apache_config_file=/opt/IBM/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/"
```

### Update an Apache record:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d  
"action=update&ids=1234&unix_apache_config_file=/opt/IBM/HTTPServer/conf/httpd.conf2" "https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

## Docker Record (PC, SCA)

The Docker Record API (`/api/2.0/fo/auth/docker/`) lets you to create, update, list and delete Docker records for compliance scans (using PC or SCA). Create a Docker record in order to authenticate to a Docker daemon (version 1.9 to 1.12) running on a Linux host. Unix authentication is required so you'll also need a Unix record for the asset running the docker.

This record type is available only in accounts with PC or SCA enabled and is supported only for compliance scans.

See [User Permissions Summary](#)

### List Docker Records

See [List Authentication Records by Type](#)

#### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d  
"action=list&ids=72685"  
"https://qualysapi.qualys.com/api/2.0/fo/auth/docker/"
```

#### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE AUTH_DOCKER_LIST_OUTPUT SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/auth/docker/auth_docker_list_out  
put.dtd">  
<AUTH_DOCKER_LIST_OUTPUT>  
  <RESPONSE>  
    <DATETIME>2017-03-09T06:11:39Z</DATETIME>  
    <AUTH_DOCKER_LIST>  
      <AUTH_DOCKER>  
        <ID>72685</ID>  
        <TITLE><![CDATA[docker_sample]]></TITLE>  
  
      <DAEMON_CONFIGURATION_FILE>/etc/docker/daemon.json</DAEMON_CONFIGURATION_  
FILE>  
  
        <DOCKER_COMMAND>/usr/bin/docker</DOCKER_COMMAND>  
        <IP_SET>  
          <IP>10.10.30.159</IP>  
        </IP_SET>  
        <CREATED>  
          <DATETIME>2017-03-09T06:09:46Z</DATETIME>  
          <BY>username</BY>  
        </CREATED>  
        <LAST_MODIFIED>
```



```

    <DATETIME>2017-03-09T06:09:46Z</DATETIME>
  </LAST_MODIFIED>
</AUTH_DOCKER>
</AUTH_DOCKER_LIST>
</RESPONSE>
</AUTH_DOCKER_LIST_OUTPUT>
```

Create Docker Record

Use these parameters to create a new Docker record in your account.

Parameter	Description
action=create	(Required)
title={value}	(Required) The record title.
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) User defined comments.
docker_deamon_conf_file={value}	(Optional) Location of the configuration file for the docker daemon.
docker_command={value}	(Optional) The docker command to connect to a local docker daemon.
ips={value}	(Required) IPs to add to your docker record.
network_id={1   0}	(Optional) By default, the parameter is set to 0

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&echo_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>2017-03-09T06:09:46Z</DATETIME>
    <USER_LOGIN>username</USER_LOGIN>
  </REQUEST>
  <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/docker/</RESOURCE>
  <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_daemon_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>2017-03-09T06:09:46Z</DATETIME>
  <BATCH_LIST>
    <BATCH>
      <TEXT>Successfully Created</TEXT>
      <ID_SET>
        <ID>72685</ID>
      </ID_SET>
    </BATCH>
  </BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

## Update Docker Record

Use these parameters to update an existing Docker record.

Parameter	Description
action=update	(Required)
ids={value}	(Required) ID of the record you're updating.
title={value}	(Optional) The record title.

Parameter	Description
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) User defined comments.
docker_daemon_conf_file={value}	(Optional) Location of the configuration file for the docker daemon.
docker_command={value}	(Optional) The docker command to connect to a local docker daemon.
network_id={1   0}	(Optional) By default, the parameter is set to 0
add_ips={value}	(Optional) IPs to be added to your record.
remove_ips={value}	(Optional) IPs to be removed from your 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>2017-03-09T06:12:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

## Delete Docker Record

Use these parameters to delete a Docker record.

Parameter	Description
action=delete	(Required)
ids={value}	(Required) ID of the record you're deleting.
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 in output.

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d  
"action=delete&ids=72685"  
"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>2017-03-09T06:13:57Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Deleted</TEXT>  
        <ID_SET>  
          <ID>72685</ID>  
        </ID_SET>  
      </BATCH>  
    </BATCH_LIST>  
  </RESPONSE>  
</BATCH_RETURN>
```

# HTTP Record

You have the option to choose HTTP authentication for vulnerability scans using Qualys Vulnerability Management (VM). Use the HTTP Record API (`/api/2.0/fo/auth/http/`) for scanning protected portions of web sites and devices like printers and routers that require HTTP protocol level authentication. (Note this is not Form-based authentication). By authenticating we can perform additional vulnerability tests that we couldn't do otherwise.

How it works – During a vulnerability 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.

See [User Permissions Summary](#)

## HTTP Record: Requests

Use the parameters below to make requests to list, create, update and delete HTTP records..

Parameter	Description
action={value}	(Required) An action for the request. One of: list - list HTTP records (GET or POST) create - create a new HTTP record (POST) update - update 1 or more HTTP records (POST) delete - delete 1 or more HTTP records (POST)
title={value}	(Required for a create request; Optional for an update request; otherwise invalid) The HTTP record title.
username={value}	(Required for a create request; Optional for update request; otherwise invalid). The user name to be used for authentication.
password={value}	(Required for a create request; Optional for update request; otherwise invalid) The password to be used for authentication.
vhost={value} - or - realm={value}	(Required for create request; Optional for update request) 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).
ssl={0   1}	(Optional for create or update request; otherwise invalid) 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://...

Parameter	Description
comments={value}	(Optional for create or update request) User-defined comments.
ids={value}	(Required for update or delete request; Optional for list request; otherwise invalid) One or more HTTP record IDs.

### HTTP Record: XML Output

DTD: `https://<base_url>/api/2.0/batch_return.dtd`

Please see Appendix A for details.

### HTTP Record: Sample API Requests

Create a new HTTP record - realm

API request:

```
curl -k -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d  
"action=create&username=jsmith&password=abc123&title=My+HTTP+Record+1&rea  
lm=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>2014-01-03T07:51:48Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Created</TEXT>  
        <ID_SET>  
          <ID>55111</ID>  
        </ID_SET>  
      </BATCH>  
    </BATCH_LIST>  
  </RESPONSE>  
</BATCH_RETURN>
```

Create a new HTTP record - virtual host

API request:

```
curl -k -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d  
"action=create&username=jsmith&password=abc123&title=My+HTTP+Record+2&vho  
st=bank.us.corpl.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>2014-01-03T08:02:44Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>55112</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### List HTTP records

#### API request:

```
curl -k -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=55111"
"https://qualysapi.qualys.com/api/2.0/fo/auth/http/"
```

### XML output:

```
?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_HTTP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/http/auth_http_list_output.
dtd">
<AUTH_HTTP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-01-03T08:08:19Z</DATETIME>
    <AUTH_HTTP_LIST>
      <AUTH_HTTP>
        <ID>55111</ID>
        <TITLE><![CDATA[My HTTP Record]]></TITLE>
        <USERNAME><![CDATA[jsmith]]></USERNAME>
        <SSL>0</SSL>
        <REALM><![CDATA[My Homepage]]></REALM>
        <CREATED>
          <DATETIME>2014-01-03T07:51:48Z</DATETIME>
          <BY>acme_ab1</BY>
        </CREATED>
      </AUTH_HTTP>
    </AUTH_HTTP_LIST>
  </RESPONSE>
</AUTH_HTTP_LIST_OUTPUT>
```

```
<LAST_MODIFIED>  
  <DATETIME>2014-01-03T07:51:48Z</DATETIME>  
</LAST_MODIFIED>  
</AUTH_HTTP>  
</AUTH_HTTP_LIST>  
</RESPONSE>  
</AUTH_HTTP_LIST_OUTPUT>
```



# IBM DB2 Record

The IBM DB2 Record API (`/api/2.0/fo/auth/ibm_db2/`) allows you to manage DB2 authentication records. You can submit API requests to view DB2 records, add new records, update records and delete records. Authentication is required for each API request.

During scanning the service will authenticate to one or more DB2 instances on a single host using all the DB2 records in your account. See “Multiple DB2 Instances.”

See [User Permissions Summary](#)

## List DB2 Records

See [List Authentication Records by Type](#)

## Create DB2 Record

The parameters described below are used to specify a request that creates a new DB2 record.

Parameter	Description
action=create	(Required) The POST method is 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.
title={value}	(Required) The title for 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. 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.
{login credentials}	(Required) See “DB2 Record: Login Credentials.”
ips={value}	(Required) Add IP address(es) to the IP list for a new authentication record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
pc_only={0   1}	(Optional) Specify pc_only=1 if the record will be used for compliance scans only. See “Multiple DB2 Instances.”
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Update DB2 Record

The parameters listed below are used to specify a request to update one or more existing DB2 records. Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
action=update	(Required) The POST method is 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.
ids={value}	(Required) Update 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, 1359-1407). Valid IDs are required.
title={value}	(Optional) Overwrites the existing record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).  When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.
comments={value}	(Optional) User defined notes about the record. A maximum of 1999 characters (ascii) may be specified.
{login credentials}	(Optional) See "DB2 Record: Login Credentials."
ips={value}	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. Multiple entries are comma separated. See "Multiple DB2 Instances" below.
add_ips={value}	(Optional) Add IP address(es) to the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated. See "Multiple DB2 Instances." below.
remove_ips={value}	(Optional) Remove IP address(es) from the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
pc_only={0   1}	(Optional) Specify pc_only=1 if the record will be used for compliance scans only. See "Multiple DB2 Instances."
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Delete DB2 Record

The parameters listed below are used to specify a request that deletes one or more DB2 records.

Parameter	Description
action=delete	(Required) The POST method is required.
echo_request={0   1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output.
ids={value}	(Required) Delete 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.

## DB2 Record: Login Credentials

The following parameters are used to define the login credentials. Parameters specified in an update request are optional and will overwrite any existing parameters (previously defined).

Parameter	Description
username={value}	(Required for a create request; optional for an update request) The user name for a DB2 database account. A maximum of 13 characters (ascii) may be specified.
password={value}	(Required for a create request; optional for an update request) The password for a DB2 database account. A maximum of 13 characters (ascii) may be specified.
database={value}	(Required for a create request; optional for an update request) The name of the DB2 database. A maximum of 8 characters (ascii) may be specified. See "Multiple DB2 Instances" below.
port={value}	(Required for a create request; optional for an update request) The port the database instance is running on. See "Multiple DB2 Instances" below.

## 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
<b>Record 1</b>	10.10.31.178	5000	SAMPLE	pc_only=0
<b>Record 2</b>	10.10.30.159	5000	TOOLS	pc_only=0
<b>Record 3</b>	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 Record: OS Parameters

The parameters described below are used to define the Windows and/or Unix record(s) in your account for your DB2 hosts if you want the service to perform OS-dependent compliance checks. Provide all the following Windows parameters if you want the service to gather DB2 compliance data from Windows hosts. Provide all the following Unix parameters if you want the service to gather DB2 compliance data from Unix hosts.

Parameter	Description
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. A maximum of 255 characters may be specified. See "DB2 Paths" below.
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. A maximum of 255 characters may be specified. See "DB2 Paths" below.
win_seclogfile={value} unix_seclogfile={value}	The path to the secondary archive location if you want the service to perform OS-dependent compliance checks. 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. A maximum of 255 characters may be specified. See "DB2 Paths" below.

Parameter	Description
win_terlogfile={value} unix_terlogfile={value}	The path to the tertiary archive location if you want the service to perform OS-dependent compliance checks. This parameter specifies a path to which DB2 will try to archive log files if the log files cannot be archived to either the primary or the secondary (if set) archive destinations because of a media problem affecting those destinations. It is set by the DB2 failarchpath parameter. A maximum of 255 characters may be specified. See “DB2 Paths” below.
win_mirlogfile={value} unix_mirlogfile={value}	The path to the mirror archive location if you want the service to perform OS-dependent compliance checks. 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. A maximum of 255 characters may be specified. See “DB2 Paths” below.

## DB2 Paths

When specifying the path to configuration files, these special characters are not allowed:

For Windows:

; & | # % ? ! \* ` ( ) [ ] " ' > < = ^ /

For Unix:

; & | # % ? ! \* ` ( ) [ ] " ' > < = ^ \

## IBM DB2 Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details.

# MongoDB Record

The MongoDB Record API ([/api/2.0/fo/auth/mongodb/](#)) allows you manage MongoDB records for performing authenticated scans of MongoDB instances running on Unix. Vulnerability scans and compliance scans are supported. You can perform these actions: create, update, list, delete.

- Technologies supported: MongoDB 3.x
- Unix authentication is required for compliance scans using the PC app. 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.

See [User Permissions Summary](#)

## List MongoDB records

See [List Authentication Records by Type](#)

### 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_o  
utput.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_CONFIGURA  
TION_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>  
...
```

### Create / Update MongoDB record

Use these parameters to create or update a MongoDB record. For an update request, all parameters are optional except “ids” which is required.

Parameter	Description
action=create   update	(Required) The action for the API call, create or update.
ids={id1,id2,...}	(Required for update request, Invalid for create request) The IDs of the MongoDB records you want to update. Valid IDs are required. Multiple IDs are comma separated.
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 for create request) A title for the Sybase record. The title must be unique. Maximum 255 characters (ascii).
ips={value}	(Required for a create request) A single IP, multiple IPs and/or ranges. Multiple entries are comma separated.
add_ips={value}	(Optional for an update request) A single IP, multiple IPs and/or ranges to be added to this record. Multiple entries are comma separated.
remove_ips={value}	(Optional for an update request) A single IP, multiple IPs and/or ranges to be removed from this record. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
comments={value}	(Optional) Specifies user defined notes about the MongoDB 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.
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).

Parameter	Description
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.
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_type={ <b>basic</b>   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}	(For create request, required 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}	(For create request, required when login_type=basic) The password of the MongoDB account to be used for authentication. Maximum 100 characters (ascii).
vault_type={value}	(For create request, required when login_type=vault) The vault type to be used for authentication. See <a href="#">Vault Support matrix</a>
vault_id={value}	(For create request, required when login_type=vault) The vault record ID to be used for authentication.
{vault parameters}	For create request, required when login_type=vault Vault specific parameters required depend on the vault type you've selected. See <a href="#">Vault Definition</a>
private_key_vault_id={value}	(For create request, required 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. See <a href="#">Vault Support matrix</a>
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 <a href="#">Vault Support matrix</a>
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 <a href="#">Vault Support matrix</a>



Parameter	Description
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 <a href="#">Vault Support matrix</a>
certificate={value}	(For create request, optional when login_type=pkcert ) The passphrase X.509 certificate content.

**Example: 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=mlqa&password=12345
abc&ips=10.20.32.239&comments=mongo-basic-login&unix_conf_path=/etc/mongo
d3.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>2017-09-12T22:43:27Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125709</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

**Example: Create MongoDB record - use 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=test123&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>2017-09-12T22:45:06Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125710</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

**Example: Create MongoDB record - use 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=mlqa"
"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>2017-09-12T22:46:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>125711</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

## Delete MongoDB records

Use these parameters to delete one or more MongoDB records.

Parameter	Description
action=delete	(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.
ids={value}	(Required) Delete only MongoDB records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.

### Example: Delete MongoDB records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=delete&ids=125708,125709"
"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>2017-09-12T23:00:48Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID_RANGE>125708-125709</ID_RANGE>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

# MS SQL Record (PC, SCA)

The MS SQL Record API (`/api/2.0/fo/auth/ms_sql/`) allows you to manage MS SQL Server authentication records for compliance scanning only (PC or SCA scans). You can submit API requests to view MS SQL Server records, add new records, update records and delete records. Authentication is required for each API request.

See [User Permissions Summary](#)

## Recommended

Before you create authentication records, you must configure authentication credentials on target hosts. Please refer to the *MS SQL Server Trusted Scanning: Setup for Compliance Scans* document for further information. This document may be downloaded (in PDF) when you are logged into your Qualys account (go to Help > Resources > Tips and Techniques).

## List MS SQL Records

See [List Authentication Records by Type](#)

## Create MS SQL Record

The parameters described below are used to specify a request that creates a new MS SQL Server authentication record.

Parameter	Description
action=create	(Required) Specifies the create action type for the request.
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) Specifies a title for the authentication record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional) Specifies user defined notes about the authentication 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.
{login credentials}	Define login credentials for authentication to target hosts. See "MS SQL Record: Login Credentials."
{target hosts}	See "MS SQL Record: Target Hosts."

Parameter	Description
{protocols}	See "MS SQL Record: Enable Protocols."
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Update MS SQL Record

The parameters described below are used to specify a request to update one or more existing MS SQL Server authentication records. Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
action=update	(Required) Specifies the update action type for the request.
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.
ids={value}	(Required) Update 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, 1359-1407). Valid IDs are required.
title={value}	(Optional) Overwrites (replaces) the existing record title with a new title. The title may include a maximum of 255 characters (ascii).  When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.
comments={value}	(Optional) Specifies user defined notes about the authentication 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.
{login credentials}	Define login credentials for authentication to target hosts. See "MS SQL Record: Login Credentials."
{target hosts}	See "MS SQL Record: Target Hosts."

Parameter	Description
{protocols}	See "MS SQL Record: Enable Protocols."
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

### Delete MS SQL Record

Use these parameters to delete one or more MS SQL Server authentication records.

Parameter	Description
action=delete	(Required) Specifies the delete action type for the request.
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.
ids={value}	(Required) Delete only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.

### MS SQL Record: Login Credentials

The following parameters are used to define the login credentials. Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
username={value}* 	(Required for create request; Optional for update request) The user account to be used for authentication. The username may include 1-128 characters (ascii).
password={value}* 	(Required for create request; Optional for update request) The password corresponding to the user account defined in the record for authentication. The password may include 1-128 characters (ascii).
db_local={0   1}* 	(Optional) A flag indicating the authentication type. 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. For a create request if the <b>db_local</b> parameter is unspecified, the flag is set to 1.

Parameter	Description
<code>windows_domain={value}</code>	<p>(Required when <b>db_local=0</b>; 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).</p> <p>For an update request when the credentials for the record are for a Microsoft Windows account (<b>db_local=0</b>) and you want to change the record to use credentials for a MS SQL Server account (<b>db_local=1</b>) note the following. You must set <b>windows_domain=''</b> (the empty string) to clear the current parameter setting.</p>
<code>instance={value}* {0   1}</code>	<p>(Optional) 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). For a create request if the instance parameter is unspecified, the instance name is set to “MSSQLSERVER”.</p> <p>These parameters are mutually exclusive: instance and auto_discover_instances=1.</p>
<code>auto_discover_instances= {0   1}</code>	<p>Set <b>auto_discover_instances=1</b> and we’ll find all MS SQL Server instance names on each host. Note Windows authentication is required in order for us to auto discover instance names - be sure you set up Windows authentication records for your hosts running MS SQL Server</p> <p>These parameters are mutually exclusive: instance and auto_discover_instances=1.</p>
<code>database={value}* {0   1}</code>	<p>(Optional) 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”.</p> <p>These parameters are mutually exclusive: database and auto_discover_databases=1.</p>
<code>auto_discover_databases= {0   1}</code>	<p>Set <b>auto_discover_databases=1</b> and we’ll find all MS SQL Server database names on each host.</p> <p>These parameters are mutually exclusive: database and auto_discover_databases=1.</p>

Parameter	Description
port={value}*  	(Required for create request; Optional for update request) 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.
auto_discover_ports={0   1}	Set <b>auto_discover_ports=1</b> and for each host we'll find all ports MS SQL Server is running on. Note Windows authentication is required for us to auto discover ports - be sure you set up 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.

### MS SQL Record: Target Hosts

For an MS SQL authentication record, the combination of each login type (Windows or MS SQL Server), account login name, database information (instance name, database name, port) and IP addresses or member domain name must be unique.

You can create either IP based or domain based MS SQL authentication records. For domain based MS SQL authentication records, just add the member domain to your MS SQL record and we'll auto discover MS SQL servers for authentication.

The following parameters are used to define the target compliance hosts that the scanning engine should log into with the specified credentials. Only compliance hosts can be added to an MS SQL Server authentication record.



Parameter	Description
ips={value}	<p>Defines an IP list for the authentication record.</p> <p>(Optional for update request) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.</p> <p>You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.</p> <p>For create request, it is required to specify either this parameter or <b>member_domain</b> parameter.</p> <p>This parameter and the <b>add_ips</b> or <b>remove_ips</b> or <b>member_domain</b> parameter cannot be specified in the same request.</p>
add_ips={value}	<p>(Optional for update request only) 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.</p> <p>You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> or <b>member_domain</b> parameter cannot be specified in the same request.</p>
remove_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to remove from the IP list for an existing authentication record.</p> <p>You may enter a combination of IPs and IP ranges to identify compliance hosts. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> or <b>member_domain</b> parameter cannot be specified in the same request.</p>
member_domain={value}	<p>Defines the domain of the MS SQL server for the authentication record.</p> <p>For create request, it is required to specify either this parameter or <b>ips</b> or <b>add_ips</b> parameter.</p> <p>This parameter and the <b>ips</b> or <b>add_ips</b> or <b>remove_ips</b> parameter cannot be specified in the same request.</p>

API request (list record for windows using member domain):

```
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_list_out  
put.dtd">  
<AUTH_MS_SQL_LIST_OUTPUT>  
  <REQUEST>  
    <DATETIME>2016-09-20T05:34:37Z</DATETIME>  
    <USER_LOGIN>user_john</USER_LOGIN>  
    <RESOURCE>  
      https://qualysapi.qualys.com/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>2016-09-20T05:34:37Z</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>2016-09-20T05:26:31Z</DATETIME>
      <BY>user_john</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2016-09-20T05:26:31Z</DATETIME>
    </LAST_MODIFIED>
    <COMMENTS><![CDATA[authcreated]]></COMMENTS>
  </AUTH_MS_SQL>
</AUTH_MS_SQL_LIST>
</RESPONSE>
</AUTH_MS_SQL_LIST_OUTPUT>

```

### API request (create request for windows using member domain):

```

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=mssqlvt1&username=administrator&password=abc123&db_lo
cal=1&port=8012&member_domain=sitedomain.com&echo_request=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>2016-09-20T05:26:31Z</DATETIME>
    <USER_LOGIN>user_john</USER_LOGIN>
    <RESOURCE>
      https://qualysapi.qualys.com/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_LIST>
  </REQUEST>
</BATCH_RETURN>

```

```
<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>2016-09-20T05:26:31Z</DATETIME>
  <BATCH_LIST>
    <BATCH>
      <TEXT>Successfully Created</TEXT>
      <ID_SET>
        <ID>13907</ID>
      </ID_SET>
    </BATCH>
  </BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

API request (update request for windows using member domain):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&echo_request=1&ids=13907&member_domain=webdomain.com"
"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>2016-09-20T05:37:13Z</DATETIME>
    <USER_LOGIN>user_john</USER_LOGIN>
    <RESOURCE>https://qualysapi.qualys.com/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>2016-09-20T05:37:13Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET><ID>13907</ID>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

## MS SQL Record: Enable Protocols

Use these input parameters to enable authentication protocols in MS SQL records.

For MS SQL Server records (PC only), all three authentication protocols are supported. Kerberos and NTLMv2 are enabled by default in new records. MS SQL records created prior to this release will have all three protocols enabled.

Parameter	Description
kerberos={0   1}	(Optional) When not specified, Kerberos is enabled allowing the scanning engine to try Kerberos when negotiating authentication to target hosts. Specify <b>kerberos=0</b> if you do not want Kerberos attempted.
ntlmv2={0   1}	(Optional) When not specified, NTLMv2 is enabled allowing the scanning engine to try NTLMv2 when negotiating authentication to target hosts. Specify <b>ntlmv2=0</b> if you do not want NTLMv2 attempted.
ntlmv1={0   1}	(Optional) When not specified, NTLMv1 will not be attempted. Specify <b>ntlmv1=1</b> to try NTMLv1 when negotiating authentication to target hosts.

## MS SQL Record: XML Output

The XML output returned by an MS SQL Server record API request (create, edit or delete) uses the DTD at the following URL (where qualysapi.qualys.com is the API server URL where your account is located):

`http://qualysapi.qualys.com/api/2.0/batch_return.dtd`

Want to learn more? See Appendix D.

# MySQL Record

The MySQL Record API ([/api/2.0/fo/auth/mysql/](#)) lets you to list, create, update and delete MySQL authentication records. User permissions for this API are the same as other authentication record APIs.

See [User Permissions Summary](#)

## List MySQL records

See [List Authentication Records by Type](#)

### API request:

```
curl -u USERNAME:PASSWORD -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/?action=list&details=
All"
```

### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VAULT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/auth_mysql_list_outpu
t.dtd">
<AUTH_MYSQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2015-02-02T19:31:42Z</DATETIME>
    <AUTH_MYSQL_LIST>
      <AUTH_MYSQL>
        <ID>2040156540</ID>
        <TITLE><![CDATA[MY SQL RedHat 5 CentOS 6]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <DATABASE><![CDATA[mysql]]></DATABASE>
        <PORT>3307</PORT>
        <IP_SET>
          <IP>10.10.33.226</IP>
        </IP_SET>
        <SSL_VERIFY>false</SSL_VERIFY>
        <WINDOWS_CONF_FILE><![CDATA[C:\Program Files\MySQL\MySQL Server
5.5\test\my.ini]]></WINDOWS_CONF_FILE>
        <UNIX_CONF_FILE><![CDATA[/etc/my.cnf]]></UNIX_CONF_FILE>
        <CREATED>
          <DATETIME>2015-01-27T22:28:51Z</DATETIME>
          <BY>seenu_as</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2015-01-29T20:13:24Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MYSQL>
    </AUTH_MYSQL_LIST>
  </RESPONSE>
</AUTH_MYSQL_LIST_OUTPUT>
```

```
<AUTH_MYSQL>
  <ID>2040166540</ID>
  <TITLE><![CDATA[MySQL (Unix)]]></TITLE>
  <USERNAME><![CDATA[root]]></USERNAME>
  <DATABASE><![CDATA[mysql]]></DATABASE>
  <PORT>3306</PORT>
  <IP_SET>
    <IP>10.10.10.76</IP>
    <IP>10.10.26.238</IP>
    <IP>10.10.30.132</IP>
    <IP>10.10.32.121</IP>
  </IP_SET>
  <SSL_VERIFY>false</SSL_VERIFY>
  <WINDOWS_CONF_FILE><![CDATA[]]></WINDOWS_CONF_FILE>
  <UNIX_CONF_FILE><![CDATA[/etc/my.cnf]]></UNIX_CONF_FILE>
  <CREATED>
    <DATETIME>2015-01-27T23:17:45Z</DATETIME>
    <BY>seenu_as</BY>
  </CREATED>
  <LAST_MODIFIED>
    <DATETIME>2015-01-27T23:17:45Z</DATETIME>
  </LAST_MODIFIED>
</AUTH_MYSQL>
</AUTH_MYSQL_LIST>
</AUTH_MYSQL_LIST_OUTPUT>
```

## Create / Update MySQL records

Use these parameters:

Parameter	Description
action=create   update	(Required) POST method may be used.
title={value}	(Required for create request) The title for the new MySQL record. The title must be unique and must contain 255 characters (ascii).
username={value}	(Required for create request) The username to be used for authentication to MySQL server.
ips={value}	(Required for create request) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated.  (Optional for update request) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.



Parameter	Description
ids={value}	(Required for update request; invalid for create request) The IDs of the MySQL authentication records that you want to update. Multiple IDs are comma separated
add_ips={value}	(Optional for update request; invalid for create request) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional for update request; invalid for create request) Remove IPs from the IPs list for this record. Multiple IPs/ranges are comma separated.
password={value}	(Optional) The password to be used for authentication to MySQL server.
comments={value}	(Optional) User-defined comments. 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.
ssl_verify={0   1}	(Optional 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) 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}	(Optional) The database name to authenticate to. Specify a valid MySQL database name. The default is "mysql".
port={value}	(Optional) The port the database name is running on. The default is 3306.
windows_config_file={value}	(Optional) The path to the Windows MySQL config file. Access to this config file is required to run certain checks on Windows hosts.
unix_config_file={value}	(Optional) The path to the Unix MySQL config file. Access to this config file is required to run certain checks on Unix hosts.

Parameter	Description
client_cert={value}	(Optional) PEM-encoded X.509 certificate. Specify if certificate authentication is required by your server to establish an SSL connection.
client_key={value}	(Optional) PEM-encoded RSA private key. Specify if certificate authentication is required by your server to establish an SSL connection.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

API request (create new record):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d "action=create&title=NewMySQLRecord&username=USERNAME&password=PASSWORD&ips=10.10.10.2-10.10.10.4&unix_config_file=/xyz/config/mysql.config" "https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2015-02-03T17:08:34Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>137296922</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

API request (update record):

```
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>2015-01-23T17:14:28Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
```

```

        <ID_SET>
        <ID>137296922</ID>
    </ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>

```

## Delete MySQL records

Use these parameters:

Parameter	Description
action=delete	(Required) POST method may be used.
ids={value}	(Required) MySQL authentication record IDs for the records you want to delete. Multiple records are comma separated.

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=delete&ids=137296922"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"

```

### XML output:

```

<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2015-02-03T17:14:28Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>137296922</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>

```

# Oracle Record

The Oracle Record API (`/api/2.0/fo/auth/oracle/`) allows you to manage Oracle authentication records for authenticated scanning. You can submit API requests to view Oracle authentication records, add new records, update records and delete records. Authentication is required for each API request.

During scanning the service will authenticate to one or more Oracle instances on a single host using all the Oracle records in your account. For compliance scans, the user can allow the service to authenticate to multiple Oracle instances on a single host and port combination. See the topic “Oracle Use Cases” in the Qualys online help.

See [User Permissions Summary](#)

## Account Set Up

The service provides a collection of scripts for successfully setting up Oracle trusted scanning for vulnerability scans and compliance scans. The scripts guide you through creating a user account with required privileges for authenticated scanning. Scripts and step-by-step instructions are described in the following documents:

*Oracle Trusted Scanning: Setup for Vulnerability Scans*

*Oracle Trusted Scanning: Setup for Compliance Scans*

Both documents may be downloaded (in PDF) when you are logged into your Qualys account. Go to Help > Resources > Tips and Techniques and click the download link provided.

## List Oracle Records

See [List Authentication Records by Type](#)

## Create Oracle Record

Parameter	Description
action=create	(Required) Specifies the create action type for the request.
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) A title for the authentication 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 authentication record. A maximum of 1999 characters (ascii) may be specified; 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.
{login credentials}	Define login credentials for authentication to target hosts. See “Oracle Record: Login Credentials.”
{target hosts}	Define the target hosts for authentication. See “Oracle Record: Target Hosts.”
{OS properties}	Define operating system properties for compliance scans. See “Oracle Record: OS Parameters.”
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Update Oracle Record

Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
action=update	(Required) Specifies the update action type for the request.
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.
ids={value}	(Required) Update 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, 1359-1407). Valid IDs are required.
title={value}	(Optional) Overwrites the existing record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).  When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.

Parameter	Description
comments={value}	(Optional) User defined notes about the authentication 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.
{login credentials}	Define login credentials for authentication to target hosts. See “Oracle Record: Login Credentials.”
{target hosts}	Define the target hosts for authentication. See “Oracle Record: Target Hosts.”
{OS properties}	Define operating system properties for compliance scans. See “Oracle Record: OS Parameters.”
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Delete Oracle Record

Parameter	Description
action=delete	(Required) Specifies the delete action type for the request.
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.
ids={value}	(Required) Delete 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.

## Oracle Record: Login Credentials

Parameters specified in an update request are optional and will overwrite any existing parameters (previously defined).

Parameter	Description
username={value}	(Required to create a 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 a record) The password corresponding to the user account defined in the record for authentication. The password may include 1-31 characters (ascii).
sid={value}	<div>(To create a new record <b>sid</b> or <b>servicename</b> is required) The Oracle System ID (SID) that identifies the database instance to be authenticated to.</div> <div>The parameters <b>sid</b> and <b>servicename</b> cannot be specified in the same request.</div>
servicename={value}	<div>(To create a new record <b>sid</b> or <b>servicename</b> is required) The Oracle service name that identifies the database instance to be authenticated to. A maximum of 30 characters may be specified.</div> <div>The parameters <b>sid</b> and <b>servicename</b> cannot be specified in the same request.</div>
port={value}	(Optional to create a 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. See “All Ports” below for information.
pc_only={0   1}	(Optional to create a 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 <b>pc_only=1</b> 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.

### All Ports

The “All Ports” option is used when the **port** parameter is not specified (the default). When specified, 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. You may only create one Oracle authentication record with this setting for each host.

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.

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.

### Oracle Use Cases

See the topic “Oracle Use Cases” in the Qualys online help to learn more about how to define Oracle records for various network configurations.

### Oracle Record: Target Hosts

The same IP may be included in multiple Oracle records as long as different ports are specified. Each IP may be included in one record with the “All Ports” setting.

Parameter	Description
ips={value}	(Required for create request) Defines an IP list for the authentication record.  (Optional for update request) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.  You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.  This parameter and the <b>add_ips</b> parameter or the <b>remove_ips</b> parameter cannot be specified in the same request.



Parameter	Description
add_ips={value}	<p>(Optional for update request only) 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.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>
remove_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to remove from the IP list for the authentication record.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>

## Oracle Record: OS Parameters

OS parameters are used by compliance scans only.

Define Windows parameters to be used for Windows compliance scans.

Parameter	Description
perform_windows_os_checks={0   1}	<p>(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 "Database Settings" in the sub-category "DB OS-dependent Controls".</p>
win_ora_home_name={value}	<p>(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The Windows Oracle Home name. Example: OraHome1</p>
win_ora_home_path={value}	<p>(Required if perform_windows_os_checks=1 is specified; otherwise invalid) The Windows Oracle Home path. Example: c:\Program Files\Oracle\10</p>
win_init_ora_path={value}	<p>(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\dfs\initORA10.ora</p>

Parameter	Description
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

Define Unix parameters to be used for Unix compliance scans.

Parameter	Description
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 “Database Settings” 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

Oracle Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details

# Oracle Listener Record

The Oracle Listener Record API (`/api/2.0/fo/auth/oracle_listener/`) allows you to manage Oracle Listener authentication records for authenticated scanning. You can submit API requests to view Oracle Listener authentication records, add new records, update records and delete records. Authentication is required for each API request. Multiple Oracle Listener records with different passwords may be created for each host.

See [User Permissions Summary](#)

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 vulnerability 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).

## List Oracle Listener Records

See [List Authentication Records by Type](#)

## Create Oracle Listener Record

Parameter	Description
action=create	(Required) POST method must be used.
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) Specifies a title for the authentication record. The title must be unique and may include a maximum of 255 characters (ascii).
comments={value}	(Optional) Specifies user defined notes about the authentication 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.
password={value}	(Required) 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. The password may include 1-31 characters (ascii).

Parameter	Description
{target hosts}	Define the target hosts for authentication. See “Oracle Listener Record: Target Hosts.”
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Update Oracle Listener Record

Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
action=update	(Required) POST method must be used.
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.
ids={value}	(Required) Update 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, 1359-1407). Valid IDs are required.
title={value}	(Optional) Overwrites the existing record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).  When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.
comments={value}	(Optional) Specifies user defined notes about the authentication 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.
password={value}	(Optional) 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. The password may include 1-31 characters (ascii).

Parameter	Description
{target hosts}	Define the target hosts for authentication. See “Oracle Listener Record: Target Hosts.”
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

### Delete Oracle Listener Record

Parameter	Description
action=delete	(Required) POST method must be used.
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.
ids={value}	(Required) Delete 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.

### Oracle Listener Record: Target Hosts

Each IP address in your account may be included in one Oracle Listener record.

The following parameters are used to define the target hosts that the scanning engine should log into with the specified credentials.

Parameter	Description
ips={value}	(Required for create request) Defines an IP list for the authentication record.  (Optional for update request) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.  You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.  This parameter and the <b>add_ips</b> parameter or the <b>remove_ips</b> parameter cannot be specified in the same request.

Parameter	Description
add_ips={value}	<p>(Optional for update request only) 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.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>
remove_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to remove from the IP list for the authentication record.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>

**Oracle Listener Record: XML Output**

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix D for details.

# Oracle WebLogic Server Record (PC, SCA)

The Oracle WebLogic Server Record API (`/api/2.0/fo/auth/oracle_weblogic/`) lets you list, create, update and delete Oracle WebLogic Server authentication records for compliance scans (using PC or SCA).

### Good to Know

- The Oracle WebLogic Server record type is only available in accounts with PC (Policy Compliance) and is only supported for compliance scans.
- 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.
- User permissions for this API are the same as other authentication record APIs. Want to know more? See "User Permissions Summary."

### List WebLogic Server Records

See [List Authentication Records by Type](#)

### Create / Update WebLogic Server Record

Use these parameters:

Parameter	Description
action=create   update	(Required) POST method may be used.
title={value}	(Required for create request) The title for the new Oracle WebLogic Server record. The title must be unique and must contain 255 characters (ascii).
installation_path={value}	(Required for create request) 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 <b>auto_discover=1</b> , which means we will use auto discovery to find all domains for you. Specify <b>auto_discover=0</b> and we will not auto discover domains. For an update request, we will keep the record's settings as is unless you overwrite them.  <b>auto_discover=0</b> must be specified with the <b>domain</b> parameter in the same request.



Parameter	Description
domain={value}	(Optional) A single Oracle WebLogic Server domain name.  Example: website  The <b>domain</b> parameter must be specified with <b>auto_discover=0</b> in the same request.
ips={value}	(Required for create request) The IP address(es) for the Unix hosts where Oracle WebLogic servers are installed. Multiple entries are comma separated.  (Optional for update request) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
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
add_ips={value}	(Optional for update request; invalid for create request) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
remove_ips={value}	(Optional for update request; invalid for create request) Remove IPs from the IPs list for this record. Multiple IPs/ranges are comma separated.
comments={value}	(Optional) User-defined comments. 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.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

#### API request (create record without Auto Discover):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&installation_path=/u01/app/oracle&auto_discover=0&domain=ww.qualys.com&ips=10.10.10.23&title=WEB_ORA_CREATE"
"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>2016-05-10T13:30:49Z</DATETIME>
```

```
<BATCH_LIST>
  <BATCH>
    <TEXT>Successfully Created</TEXT>
    <ID_SET>
      <ID>2707632279</ID>
    </ID_SET>
  </BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

API request (create record with Auto Discover):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&installation_path=/u01/app/oracle&auto_discover=1&ips=10.1
0.10.23&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>2016-05-10T13:42:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2707642279</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

**Delete WebLogic Server Record**

Use these parameters:

Parameter	Description
action=delete	(Required) POST method may be used.
ids={value}	(Required) Oracle WebLogic Server authentication record IDs for the records you want to delete. Multiple records are comma separated.

# Palo Alto Firewall Record

The Palo Alto Firewall API ([/api/2.0/fo/auth/palo\\_alto\\_firewall](#)) allows you to manage Palo Alto Firewall records for authenticated scanning. You can perform these actions: create, update, list, delete.

See [User Permissions Summary](#)

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.

## List Palo Alto Firewall records

See [List Authentication Records by Type](#)

### 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/auth_pal
o_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>
        ...
```

## Create / Update Palo Alto Firewall record

Use these parameters to create or update a Palo Alto Firewall record. For an update request, all parameters are optional except “ids” which is required.

Parameter	Description
action=create   update	(Required) The action for the API call, create or update.
ids={id1,id2,...}	(Required for update request, Invalid for create request) The IDs of the Palo Alto Firewall records you want to update. Valid IDs are required. Multiple IDs are comma separated.
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 for create request) A title for the Palo Alto Firewall record. The title must be unique. Maximum 255 characters (ascii).
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 Palo Alto Firewall 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 Palo Alto Firewall account to be used for authentication. Maximum 100 characters (ascii).
login_type=vault	(For create request, password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters will need to be provided. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a>
comments={value}	(Optional) Specifies user defined notes about the Palo Alto Firewall 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.

### Example: 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=123123"  
"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>2017-09-13T06:29:41Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Created</TEXT>  
        <ID_SET>  
          <ID>125727</ID>  
        </ID_SET>  
      </BATCH>  
    </BATCH_LIST>  
  </RESPONSE>  
</BATCH_RETURN>
```

### Example: Create Palo Alto Firewall Record using Cyber-Ark PIM Suite 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=Cyber-Ark  
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>2017-09-13T06:22:01Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Created</TEXT>  
        <ID_SET>  
          <ID>125726</ID>
```

```
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

### Delete Palo Alto Firewall records

Use these parameters to delete a Palo Alto Firewall record.

Parameter	Description
action=delete	(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.
ids={value}	(Required) Delete only Palo Alto Firewall records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.

### Example: Delete Palo Alto Firewall Record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=delete&ids=125753"
"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>2017-09-15T12:10:26Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>125753</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

# PostgreSQL Record (PC, SCA)

The PostgreSQL Record API ([/api/2.0/fo/auth/postgresql/](#)) allows you create, update, delete and list PostgreSQL records for performing authenticated scans of PostgreSQL Version 9.0 instances running on Unix. This record type is only available in accounts with PC or SCA enabled, and only supported for compliance scans.

See [User Permissions Summary](#)

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.

## List PostgreSQL Records

See [List Authentication Records by Type](#)

### 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_postgresql_
list_output.dtd">
<AUTH_POSTGRESQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-24T22:01:50Z</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>
      </AUTH_POSTGRESQL>
    </AUTH_POSTGRESQL_LIST>
  </RESPONSE>
</AUTH_POSTGRESQL_LIST_OUTPUT>
<UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]></UNIX_
_CONF_FILE>
  <NETWORK_ID>0</NETWORK_ID>
  <CREATED>
    <DATETIME>2017-04-13T23:42:50Z</DATETIME>
    <BY>acme_as1</BY>
  </CREATED>
```

```
<LAST_MODIFIED>
  <DATETIME>2017-04-20T23:35:42Z</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.vuln.qa.qualys.com]]></HOST>
  </HOSTS>
  <IP_SET>
    <IP>10.20.31.107</IP>
  </IP_SET>
<UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]></UNIX_CONF_FILE>
  <NETWORK_ID>0</NETWORK_ID>
  <CREATED>
    <DATETIME>2017-04-20T20:12:48Z</DATETIME>
    <BY>acme_as1</BY>
  </CREATED>
  ...
</AUTH_POSTGRESQL_LIST>
</RESPONSE>
</AUTH_POSTGRESQL_LIST_OUTPUT>
```

## Create / Update PostgreSQL record

Use these parameters to create or update a PostgreSQL record. For an update request, all parameters are optional except “ids” which is required.

Parameter	Description
action=create   update	(Required) The action for the API call, create or update.
ids={id1,id2,...}	(Required for update request, Invalid for create request) The IDs of the PostgreSQL records you want to update. Valid IDs are required. Multiple IDs are comma separated.
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 for create request) A title for the Sybase record. The title must be unique. Maximum 255 characters (ascii).



Parameter	Description
ips={value}	(Required for a create request) A single IP, multiple IPs and/or ranges. Multiple entries are comma separated.
add_ips={value}	(Optional for an update request) A single IP, multiple IPs and/or ranges to be added to this record. Multiple entries are comma separated.
remove_ips={value}	(Optional for an update request) A single IP, multiple IPs and/or ranges to be removed from this record. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
pgsql_unix_conf_file={value}	(Required for create request) 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.
comments={value}	(Optional) Specifies user defined notes about the PostgreSQL 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.
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).
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.
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_type=vault	(For create request, password or login_type=vault is required) Set to vault if a third party vault will be used to retrieve password. Vault parameters are required if login_type=vault. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a>

Parameter	Description
client_key_type={value}	(Optional) Client key type basic (default) or vault.
client_key={value}	(Optional for create request if client_key_type=basic) Client key content, if private key not in vault.
client_key_vault_type={value}	(Required for create request if client_key_type=vault) The third party vault to be used to retrieve the private key. Certain vaults support this capability. See <a href="#">Vault Support matrix</a>
client_key_vault_id={value}	(Required for create request if client_key_type=vault) The ID of the vault to get the private key from. <u>Vault parameters:</u> 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 for create request if passphrase_type=basic) The passphrase value.
client_cert={value}	(Optional for create request 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: CA Access Control   Cyber-Ark PIM Suite   Cyber-Ark AIM   Hitachi ID PAM   Quest Vault   Thycotic Secret Server
passphrase_vault_id={value}	(Required if passphrase_type=vault) The ID of the vault to get the passphrase from.

**Example: Create PostgreSQL record**

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d  
"action=create&title=API_POSTGRE_2&username=root&password=abc123&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>2017-04-27T20:17:42Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Created</TEXT>  
        <ID_SET>
```

```
<ID>84307</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

**Example: Update PostgreSQL record**

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>2017-04-10T21:01:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

**Delete PostgreSQL records**

Use these parameters to delete a PostgreSQL record.

Parameter	Description
action=delete	(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.
ids={value}	(Required) Delete only PostgreSQL records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.

### **Example: Delete PostgreSQL record**

#### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d  
"action=delete&ids=78187,78783-78784&echo_request=1"  
"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>  
  <REQUEST>  
    <DATETIME>2017-04-10T21:27:22Z</DATETIME>  
    <USER_LOGIN>enter_ss</USER_LOGIN>  
  <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/</RESOU  
RCE>  
  <PARAM_LIST>  
    <PARAM>  
      <KEY>action</KEY>  
      <VALUE>delete</VALUE>  
    </PARAM>  
    <PARAM>  
      <KEY>ids</KEY>  
      <VALUE>78187,78783-78784</VALUE>  
    </PARAM>  
    <PARAM>  
      <KEY>echo_request</KEY>  
      <VALUE>1</VALUE>  
    </PARAM>  
  </PARAM_LIST>  
</REQUEST>  
<RESPONSE>  
  <DATETIME>2017-04-10T21:27:22Z</DATETIME>  
  <BATCH_LIST>  
    <BATCH>  
      <TEXT>Successfully Deleted</TEXT>  
      <ID_SET>  
        <ID>78187</ID>  
        <ID_RANGE>78187,78783-78784</ID_RANGE>  
      </ID_SET>  
    </BATCH>  
  </BATCH_LIST>  
</RESPONSE>  
</BATCH_RETURN>
```

# SNMP Record

The SNMP Record API (`/api/2.0/fo/auth/snmp/`) allows you to manage SNMP authentication records for authenticated scanning. Authentication is required for each API request.

Using this API resource you can submit API requests to view SNMP authentication records, add new records, update records and delete records. Authenticated scanning using these SNMP versions is supported: SNMPv1, SNMPv2 and SNMPv3.

For vulnerability scans, privileged admin access is optional; when provided the service has the ability to perform more in depth security analysis. For compliance scans, privileged admin access is required.

See [User Permissions Summary](#)

## List SNMP Records

See [List Authentication Records by Type](#)

## Create / Update SNMP Record

Parameter	Description
action=create   update	(Required) POST method is 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}	(Required) Specifies a title for the authentication record. The title must be unique and may include a maximum of 255 characters (ascii).

Parameter	Description
comments={value}	<p>(Optional) Specifies user defined notes about the authentication 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 &lt;script&gt;) cannot be included; if tags are included an error is returned and the request fails.</p> <p>For an update request: Overwrites the existing record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).</p> <p>When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.</p>
version={v1   v2c   v3}	<p>(Optional) Specifies the SNMP protocol version. A valid value is: v1 = SNMPv1 (the default) v2c = SNMPv2c v3 = SNMPv3 For an update request, this parameter overwrites the existing SNMP version with a new version.</p>
{login credentials}	See “SNMP Record: Login Credentials.”
{target hosts}	See “SNMP Record: Target Hosts.” Each IP address in your account may be included in one SNMP record.
ids={value}	(Required for update request) Update only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Delete SNMP Record

Parameter	Description
action=delete	(Required) POST method is 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.
ids={value}	(Required) Delete only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.

## SNMP Record: Login Credentials

The **community\_strings** parameter may be used for SNMPv1 and SNMPv2c. This parameter is not valid for records set to SNMPv3.

Parameter	Description
community_strings={value}	<p>(Optional) Specifies the SNMP community strings to be used for authentication to target hosts. Multiple entries are comma separated.</p> <p>The service attempts authentication using several common default community strings. When <b>community_strings</b> is specified, the user-provided community strings are used for authentication before the default community strings.</p>

The following parameters may be used for SNMPv3.

Parameter	Description
username={value}	<p>(Optional) Specifies the user account for authentication to target hosts. A maximum of 128 characters may be specified.</p> <p>These three parameters are used to specify authentication: <b>username</b>, <b>password</b> and <b>auth_alg</b>.</p> <p>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.</p>

Parameter	Description
password={value}	<p>(Optional) Specifies a password for authentication to target hosts. A maximum of 128 characters may be specified.</p> <hr/> <p>These three parameters are used to specify authentication: <b>username</b>, <b>password</b> and <b>auth_alg</b>.</p> <p>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.</p>
auth_alg={MD5   SHA1}	<p>(Optional) Specifies the algorithm for authentication: MD5 or SHA1. This algorithm is used to safely prove to the SNMP server knowledge of the password without sending the password.</p> <hr/> <p>These three parameters are used to specify authentication: <b>username</b>, <b>password</b> and <b>auth_alg</b>.</p> <p>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.</p>
encrypt_password={value}	<p>(Optional) Specifies the password if privacy (data encryption) is to be used for SNMP communication. A maximum of 128 characters may be specified.</p> <hr/> <p>These two parameters are used to specify privacy: <b>encrypt_password</b> and <b>priv_alg</b>.</p> <p>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.</p>



Parameter	Description
priv_alg={DES   AES}	<p>(Optional) Specifies the algorithm to be used for privacy: DES or AES. This algorithm is used to encrypt and decrypt SNMP messages.</p> <hr/> <p>These two parameters are used to specify privacy: <b>encrypt_password</b> and <b>priv_alg</b>.</p> <p>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.</p>
security_engine_id={value}	<p>(Optional) Specifies 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.</p> <hr/> <p>If a security engine ID is part of the target host configuration, the parameter <b>security_engine_id</b> must be defined for the record in order for authentication to be successful.</p> <p>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.</p>
context_engine_id={value}	<p>(Optional) Specifies 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.</p> <hr/> <p>If an SNMP context is part of the target host configuration, the parameters <b>context_engine_id</b> and/or <b>context</b> must be defined for the record in order for the scanning engine to retrieve context-sensitive information from the target host.</p>
context={value}	<p>(Optional) Specifies 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.</p> <hr/> <p>If an SNMP context is part of the target host configuration, the parameters <b>context_engine_id</b> and/or <b>context</b> must be defined for the record in order for the scanning engine to retrieve context-sensitive information from the target host.</p>

## SNMP Record: Target Hosts

Each IP address in your account may be included in one SNMP record.

The following parameters are used to define the target hosts that the scanning engine should log into with the specified credentials.

Parameter	Description
ips={value}	<p>(Required for create request) Defines an IP list for the authentication record.</p> <p>(Optional for update request) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>add_ips</b> parameter or the <b>remove_ips</b> parameter cannot be specified in the same request.</p>
add_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list an existing authentication record. Specifies one or more IP addresses to add to the IP list for the authentication record.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>
remove_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to remove from the IP list for the authentication record.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>

### SNMP Record: Sample API Requests

These sample API requests work on Qualys US Platform 1 where the FQDN in the API server URL is qualysapi.qualys.com. Please be sure to replace the FQDN with the proper API server URL for your platform. For the EU platform, use qualysapi.qualys.eu. For a partner platform, use the URL for your @customer platform API server.

The header parameter “X-Requested-With” is also provided as an example. Please change this parameter according to your need. This parameter is exposed in the activity log (only displayed when used with session cookie authentication - does not apply for basic authentication as used in the following examples) and it is useful for API monitoring API activity.

**Sample 1.** Use the URL shown below to create a new record for SNMPv3:

```
curl -H 'X-Requested-With: Curl Sample' -d
'action=create&title=My+Record&version=v3&username=user&password=password
&auth_alg=MD5&encrypt_password=passwordabcde123456&priv_alg=DES&security_
engine_id=0x80001F88805131F121BD9B194B&context_engine_id=0x80001F88805131
F121BD9B194B&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/'
```

**Sample 2.** Use the URL shown below to update an existing SNMP record to change the user name and password for authentication and the IPs in the record:

```
curl -H 'X-Requested-With: Curl Sample' -d
'action=update&ids=65319&username=user2&password=password2&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/'
```

## SNMP Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details.

## Sybase Record (PC, SCA)

The Sybase Record API ([/api/2.0/fo/auth/sybase/](#)) allows you to create, update, delete and list Sybase records for authenticating to Sybase Adaptive Server Enterprise (ASE) instances. This record type is only available in accounts with PC or SCA enabled, and only supported for compliance scans.

See [User Permissions Summary](#)

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.

[Click here](#) for Sybase Authentication Set Up Instructions

### List Sybase Records

See [List Authentication Records by Type](#)

#### 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/sybase/" > file.xml
```

#### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE AUTH_SYBASE_LIST_OUTPUT SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/auth_sybase_list_out  
put.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>
...

```

### Create / Update Sybase record

Use these parameters to create or update a Sybase record. For an update request, all parameters are optional except “ids” which is required.

Parameter	Description
action=create   update	(Required) The action for the API call, create or update.
ids={id1,id2,...}	(Required for update request, Invalid for create request) The IDs of the Sybase records you want to update. Valid IDs are required. Multiple IDs are comma separated.
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.
title={value}	(Required for create request) A title for the Sybase record. The title must be unique. Maximum 255 characters (ascii).
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 Sybase 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 Sybase account to be used for authentication. Maximum 100 characters (ascii).

Parameter	Description
login_type=vault	(For create request, password or login_type=vault is required) Set to vault if you want to retrieve the password from a third party vault. The password can have a maximum 100 characters (ascii). Vault parameters are required when login_type=vault. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a>
port={value}	(Required for create request) The port the Sybase database is on.
database={value}	(Required for create request) The name of the Sybase database you want to authenticate to.
install_dir={value}	(Required for create request if this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.
ips={value}	(Required for a create request) A single IP, multiple IPs and/or ranges. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
comments={value}	(Optional) Specifies user defined notes about the Sybase 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.

**Example: 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&pa
ssword=password&port=444&database=sybaseDB1&ips=10.10.24.12,10.10.24.13,1
0.10.24.15&installation_dir=/dir123&comments=This%20Sybase%20comments"
"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://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-10T20:52:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
```

```
<ID>78782</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

### Example: Create Sybase Record using Cyber-Ark PIM Suite 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=139249&l
ogin_type=vault&vault_type=Cyber-Ark%20PIM%20Suite&folder=Root&file=passw
d_abc123&installation_dir=C://dir1/win/vault&username=Syb_User&port=456&d
atabase=Syb_db_Cyber-ArkSuite&ips=10.10.25.81-
10.10.25.82&comments=sybase_vault_comments"
"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://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-13T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>88888</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### Example: 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/d
ir" "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://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2017-04-10T21:01:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### Delete Sybase record

Use these parameters to delete one or more Sybase records.

Parameter	Description
action=delete	(Required)
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) Delete only Sybase records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.

#### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=delete&ids=78187,78783-78784&echo_request=1"
"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://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <REQUEST>
    <DATETIME>2017-04-10T21:27:22Z</DATETIME>
    <USER_LOGIN>enter_ss</USER_LOGIN>
  </REQUEST>
  <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/</RESOURCE>
  <PARAM_LIST>
    <PARAM>
      <KEY>action</KEY>
      <VALUE>delete</VALUE>
```



```
</PARAM>
<PARAM>
  <KEY>ids</KEY>
  <VALUE>78187,78783-78784</VALUE>
</PARAM>
<PARAM>
  <KEY>echo_request</KEY>
  <VALUE>1</VALUE>
</PARAM>
</PARAM_LIST>
</REQUEST>
<RESPONSE>
  <DATETIME>2017-04-10T21:27:22Z</DATETIME>
  <BATCH_LIST>
    <BATCH>
      <TEXT>Successfully Deleted</TEXT>
      <ID_SET>
        <ID>78187</ID>
        <ID_RANGE>78783-78784</ID_RANGE>
      </ID_SET>
    </BATCH>
  </BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

# Unix Record

The Unix Record API ([/api/2.0/fo/auth/unix/](#)) allows you to manage Unix, Cisco and Checkpoint Firewall authentication records for authenticated scanning. The Checkpoint Firewall record type is only available in accounts with PC (Policy Compliance) and is only supported for compliance scans.

See [User Permissions Summary](#)

## List Unix Records

See [List Authentication Records by Type](#)

## Create / Update Unix record

Use the following parameters to create or update an authentication record for Unix or Cisco or Checkpoint Firewall.

Parameters: [Request](#) | [Login Credentials for Unix](#) | [Login Credentials for Cisco and Checkpoint Firewall](#) | [Scanning Options](#) | [Target Hosts](#)

Request:

Parameter	Description
action=create   update	(Required) POST method must be used.
sub_type={cisco   checkpoint_firewall}	(Required for Cisco or Checkpoint Firewall) For a Cisco record, specify <b>sub_type=cisco</b> For a Checkpoint Firewall record, specify <b>sub_type=checkpoint_firewall</b>
echo_request={0   1}	(Optional) Specify 1 to 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.
title={value}	(Required for create request) A title for the authentication record. The title must be unique and may include a maximum of 255 characters (ascii).

Parameter	Description
ids={value}	(Required for update request) Update 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, 1359-1407). Valid IDs are required.
comments={value}	(Optional) Specifies user defined notes about the authentication 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.

### Login Credentials for Unix:

Parameter	Description
username={value}	(Required for create request) The user account to be used for authentication on target hosts. The username may include 1-31 characters (ascii).
password={value}	(Required for create request if cleartext_password=1) The password for the user account to be used for authentication when the account is not defined in a vault. The password may include 1-31 characters (ascii).
login_type={ <b>basic</b>   vault}	(Optional) Set vault to use a third-party vault to retrieve the password. Vault parameters are required if login_type=vault is specified. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a> <a href="#">Unix Record Samples</a>
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 details, see “Clear Text Password” in the online help or refer to the <i>Unix Trusted Scanning</i> document (log into your account and go to Help > Resources).  For a create request, if cleartext_password=1, then the <b>password</b> 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*.

Parameter	Description
skip_password={0   1}	(Optional) For Unix record only. 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.
{XML File}	(Optional) For Unix record only. XML file where you define private-key certificates and root delegations.

### Login Credentials for Cisco and Checkpoint Firewall:

Parameter	Description
username={value}	(Required for a create request) For Cisco or Checkpoint Firewall
password={value}	(Required for create request if cleartext_password=1) The password for the user account to be used for authentication when the account is not defined in a vault. The password may include 1-31 characters (ascii).
login_type={ <b>basic</b>   vault}	(Optional) Set to vault to use a third-party vault to retrieve the password. Vault parameters are required if login_type=vault is specified. By default, a vault is not used. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a> <a href="#">Unix Record Samples</a>
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 details, see "Clear Text Password" in the online help or refer to the <i>Unix Trusted Scanning</i> document (log into your account and go to Help > Resources).
enable_password={value}	(Optional) For Cisco only. The password required for executing the "enable" command on the target hosts. The password may include 1-31 characters (ascii). Note: The pooled credentials feature is not supported if the "enable" command requires a password and it is specified using the <b>enable_password</b> parameter.
expert_password={value}	(Optional) For Checkpoint Firewall only. The password required for executing the "expert" command on the target hosts. The password may include 1-31 characters (ascii).

### Scanning Options:

Parameter	Description
port={value}	(Optional) For compliance scanning only. Custom ports to be used to perform authenticated compliance assessment (control testing). <a href="#">Ports Used For Unix Compliance Scanning</a>
use_agentless_tracking=[0   1]	(Optional) For Unix only. Specify "1" to enable Agentless Tracking.
agentless_tracking_path={value}	(Required if use_agentless_tracking=1). For Unix only (not supported for Cisco or Checkpoint Firewall) 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:

Important: Each IP address may be included in one Unix or one Cisco or one Checkpoint Firewall record within one Qualys user account.

Parameter	Description
ips={value}	(Required for create request) Add IP address(es) for this record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.  (Optional for update request) Overwrites (replaces) all the IP address(es) in the existing authentication record. The IPs you specify are added, and any existing IPs are removed.  This parameter cannot be specified in the same request with <b>add_ips</b> parameter or <b>remove_ips</b> parameter.
add_ips={value}	(Optional for update request; Invalid for create request) Add IP address(es) to the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated. See "Important Note About IPs" above.  This parameter and the <b>ips</b> parameter cannot be specified in the same request.

Parameter	Description
remove_ips={value}	(Optional for update request, Invalid for create request) Remove IP address(es) from the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.  This parameter and the <b>ips</b> 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.

### Ports Used For Unix Compliance Scanning

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

### Delete Unix record

Use these parameters to delete one or more Unix records (i.e. Unix, Cisco and/or Checkpoint Firwall).

Parameter	Description
action=delete	(Required) POST method must be used.
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.
ids={value}	(Required) IDs for records to be deleted. One or more IDs/ranges may be specified. Multiple entries are comma separated. Valid IDs are required.

## Unix Record Samples

### Create Unix Record

#### API request 1:

Create a Unix record and add the password for login, without adding any root delegation tools or private-key certificates. Applies to record type Unix, Cisco, Checkpoint Firewall.

```
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&password=crazy8!&ips=10.10.36.63"
```

#### API request 2:

(Applies to record type Unix only) Create a Unix record without adding any root delegation tools or private-key certificates AND set skip\_password=1 if the login account does not have a password. (If this account has the empty password, just enter the required parameters title, username and ips as in previous releases and the empty password will be used for login).

```
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&skip_password=1&ips=10.10.36.63"
```

#### API request 3:

(Applies to record type Unix only) Create a Unix record and add multiple root delegation tools and private-key certificates AND use the Lieberman ERPM vault for login.

```
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=Un
ix&vault&username=Qualys&ips=10.113.195.152&port=5857&login_type=vault&va
ult_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
```

File add\_params.xml contains multiple root delegation tools and private-key certificates:

```
<?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>
        </DIGITAL_VAULT>
      </PASSWORD_INFO>
    </ROOT_TOOL>
  </ROOT_TOOLS>
  <SECRET_NAME><![CDATA[super_secret_name]]></SECRET_NAME>
</UNIX_AUTH_PARAMS>
```

```
        </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>Cyber-Ark 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
FiLfGH0c0rREmC0cBPsiyqqaitPNYTGeqKRmSBwGNrAzNTAcSkslsoY/WkMDW6QD
dLZNiGB0CFag94zyoMyCjyrdpayACAOWfH5w8VixxHF16Vxx5b6foLBE40FOYAIP
sdmlHvCfSFaN2dPflUnb0erwjigjJNwYIV78529eLE+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
AAAAHhNzaCl1yc2EtY2Vydc12MDFAb3BlbnZac5jb20AAAagwR4bJSiBtJlOgCAQUF3yZ6Io2
```



```

WYfnBiOEsQ45RKbqLgAAAAAQABAAABAQC5sVLb7emh8/v2uHp6xlpN5R+MHQwz3A5M3GRKtu
uu1Njc/XYgqeWLM0JpbVtCVXwUcPgKt4Q0DmlGqc4uhZhZrdtpQGHRiEivndNNLY9NQj7LozE7
x/sGiWdtmLucUh1teXMaBpM4aER9Y6uW5wv6ZylY7CAV9bcVz/ljlSympjzkPjJ39AJq+QxZk
Iv+H4uh/T05LwHdilFrjWWwEoI8DV/DRlw3h8o4jhnjlQxBxyjad3efmFaejgRnY6cBW82lgm
...
    </CERTIFICATE>
  </PRIVATE_KEY_CERTIFICATE>
<PRIVATE_KEY_CERTIFICATE>
  <PRIVATE_KEY_INFO type="basic">
    <PRIVATE_KEY type="rsa">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaClrZXktcjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABCPiEUH5L3LZ
GInEw+h/m4+AAAAEAAAAEAAAEXAAAAB3NzaClyc2EAAAADAQABAAABAQCpuwFVTYVmske0bd
FjSlYgsfvyCr7e5irIfow7B8hNY0XJWyOEqZ5BzwPAEtzjua6m3vnqKPEQD1HyFdLse62JE7x
0jDXLr9bZ64THFpogERC/gI2aorrrLKLxdr0K7u5wQUTm1L0xO7Y0hE9Bbi8ok++xTW+Ymf7Lb
VRLWVdN6kUBunIGow3W+tHIohPoUlw82QayZRa4iXpqpWVbh/9OMnblraC
....
-----END OPENSSH PRIVATE KEY-----]]></PRIVATE_KEY>
    </PRIVATE_KEY_INFO>
  </PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>"

```

## Samples for Creating Unix records with Private Keys

### Example 1: RSA authentication (Non-encrypted)

#### API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u  
USERNAME:PASSWORD -X POST  
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?  
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"  
--data-binary @add_pk_Valid.xml
```

#### POST Data Request (Contents of add\_pk\_Valid.xml)

```
<?xml version="1.0" encoding="UTF-8" ?>  
<UNIX_AUTH_PARAMS>  
  <PRIVATE_KEY_CERTIFICATES>  
    <PRIVATE_KEY_CERTIFICATE>  
      <PRIVATE_KEY_INFO type="basic">  
        <PRIVATE_KEY type="rsa">  
          <![CDATA[-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAsOYRhrZjV6QuC5uar6EeO3Qw3M5mzgei+6o8TEIN/dAY/aVw  
4Sw6h+YKfzuSxmAmwsRWmswUTB7BbY4Kg/h/6GFZuX/a3u9VTgg23mST3tWcGieJ  
AsCLK5Fh6pxrgheMuqrUIs2T5iJ688n1VF/UveI0OkfcEhBOt0X0At1F8rl6G1EP  
C5WEk+4HG3F03iYrm7t/ehnlJGg6k7QAnSi0FwExfcAk+LUzk+3C6MXIXADnHT1e  
YtIkNK2ptssf489pm7j/V/4DOTKsgXq505BTYzQyKBUXsy7qi yg11RcgExNi/++J  
...  
9gklhwZ6hfuIw1GtZkYBoN5qKBLFytw8VTWqmH/QvPKGrdxMHV6MoTtuLBKxmpRz  
q2KBAoGBALNNrtixyALuxvk3BjYewygPPyguV4Zlp5BglPkB0bOqCIhY1ukBjuf/  
jCp0wuY+DdahHeLw9FK6L8GzmnB8lzpSMxM6NZHlxA+y1sw7pR2TCnees6JQ5J4  
CqhNu2tprpTGm4KzFG8Oxa0BJcC9KUOuhVDAbFUs1A+o56JcWzNs  
-----END RSA 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>2017-04-19T14:58:49Z</DATETIME>  
    <BATCH_LIST>  
      <BATCH>  
        <TEXT>Successfully Created</TEXT>  
        <ID_SET>
```

```

        <ID>80729</ID>
    </ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>

```

## Example 2: RSA authentication (Encrypted)

### API request:

```

curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml

```

### POST Data Request (Contents of add\_pk\_Valid.xml)

```

<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <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, 4035E2A17376E0EB20A1305C36B503BB

BPmQr8lHc2ZZsLYc6meyPS+oLRI2QIFtEBdf4EDvYWL1c5q50zoJKi6RpCJXQiIR
XBxaALWoipR3Zj1Xwa6330Txz6+jLxLMI6wh75cJlAMxxmR1klElr0DjvmFFh/B2
ExS2/10KQBSc57bmK0xW82509i2/ECFh0Co3pI5VxtnXA/MSN1DHE2oITYu0aXd/
P7CUmdIEOc157d27GtcaWwejd3j2v9C/NHDxrlG1AW4xplxuLZIUqyUNCuFYv5kt
+Qx0/fWE7jb49P4AshE3vhB5b7vbNubxKTXNI9ffYlsxOHxPQaVz jTh1tvLA0UBS
...
5ozY5s7bCDN/Tz7Wf16tXgvdArT8HQHok8w7ONcJZlatokI/K+WpPru/tkWlStPI
GgI4U9J0Gt58A1Lw3iBbjgd74fdsJ9SHEbSeoUB0MJQIMbjn69fcZTg53/cBvn2s
vAJSoLm0FRL/QoWLDQMXORlUZHbv2JMN83nj3LCFrAKeQdAK7LAQ79Ci+arZbNNj
PluSMGFQgtxSc5wJUHG1It9DSW0hTap02rLXR6V4m2cY+pbISrptcTTP58IcYm1Q
s7YXJ6WSAPchSH/GyLoQKiU1vESLRNHlXbtKZJrMb1JV6F3mR7P75dYinaKTSE2g
-----END RSA PRIVATE KEY-----]]></PRIVATE_KEY>
      </PRIVATE_KEY_INFO>
      <PASSPHRASE_INFO type="basic">
        <PASSPHRASE><![CDATA[12345]]></PASSPHRASE>
      </PASSPHRASE_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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

**Example 3: DSA authentication (Non- encrypted)**

API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml
```

POST Data Request (Contents of add\_pk\_Valid.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="dsa">
<![CDATA[-----BEGIN DSA PRIVATE KEY-----
MIIBugIBAAKBgQCBbVl2OJB3e8PHLBDxtZZHbop7fuyyP/LT0mFhjUxDXWCVlFU
8k7uiYkZwhq2qYybx4/NmbCYKhqLfoQqcI30AoA+1II6lOkwhCRPX6fsnUibZiRQ
E4ovzZmr4JQ+gNRdpdeXMqvKuYGs3jkrJCCwA/NPaSTBbDYh5KRbRtAa0wIVAiaI
...
HQEjdR3+RvJgYgZ90NeyUakb/mI+2aMJZChWWiPzNax4cLez+eDYuJoX/d3V3FEwo
slczdclubhco++DutAauryRN3lAFhd+n7J53ZyuDx+UkgxJU+K6MVxQIUOe6QwZTP
3dIZGq43D5BAbOrjJAI=
-----END DSA 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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET><ID>80729</ID></ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### **Example 4: DSA authentication (Encrypted)**

#### API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml
```

#### POST Data Request (Contents of add\_pk\_Valid.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="dsa">
<![CDATA[-----BEGIN DSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 0366F5DE27F248E78C604D62184C3E83

0WUxcCPotHK70i5LMW7ZmtTtFE0b3ebcaJUBtnD3M0gomdQAz+ZZmv0Ap4PNsPJN
KCJAcyI0vgbxna3f3xlyAY3FoWLVrmOJ33WX+CUC/aNrDud+2Qh9DKHdJfF6xqR+
4270kR/pHvYfhxafcsr5EziWwSt6twicTYsvZ+YaPX96OJcBG+N5HCFZ2zyxoJ/S
...
Zj0lnbJAHeBUVBZGZG6qFt92fsqyUbjNj4tTXBATnVy2LVcdQ5LKZ20r6RihcdNj
U4ZKZSag2WHGUctS/uj4TGDeIpy/ewyUxejjKaGH+yHrwUz1/Y3ppzw0g+mmptp6
CLverSuW82p2bUB3P8cL8A==
-----END DSA PRIVATE KEY-----]]></PRIVATE_KEY>
      </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic">
      <PASSPHRASE><![CDATA[12345]]></PASSPHRASE>
```

```
</PASSPHRASE_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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### **Example 5 : ECDSA authentication (Non- encrypted)**

#### API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml
```

#### POST Data Request (Contents of add\_pk\_Valid.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="ecdsa">
          <![CDATA[-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIGgeck27ONbtL+653a5tDzcEwl6ILc8HHmM6jKKWlxhjoAoGCCqGSM49
AwEHoUQDQgAE4TuLCxvVN6Djk0irhDRHhpgHUhd2c+A/7Vm1ERHtWc jnvJ7CVQzi
GCPPQkEUKUxg7hKYkFXJuF8lLzfYZwcolQ==
-----END EC 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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### **Example 6: ECDSA authentication (Encrypted)**

#### API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml
```

#### POST Data Request (Contents of add\_pk\_Valid.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="ecdsa">
<![CDATA[-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 519724814D193C308249D9EA36104118

VfvH3paq+P8UWCvhg0t40VWBpw9gHDtiVwphVXmaSxiEJhwddwjOfsM5ulqZeHfV
/lfegkRGdv70IdV8sze2bAx170lEWChrOuWrNqiW8KhrkHbFKS3maI6sR85rQIgM
ROQ7TMfuXJ86ry54jp+goRvdxCL7q6FGIfgayHTxfrm=
-----END EC PRIVATE KEY-----]]></PRIVATE_KEY>
      </PRIVATE_KEY_INFO>
      <PASSPHRASE_INFO type="basic">
        <PASSPHRASE><![CDATA[12345]]></PASSPHRASE>
```

```
        </PASSPHRASE_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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

### **Example 7: ED25519 authentication (Non-encrypted)**

#### API request:

```
curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml
```

#### POST Data Request (Contents of add\_pk\_Valid.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="ed25519">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaClrZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAAAAwAAAtzc2gtZW
QyNTUxOQAAACDj3hMJHUS+/mDU4UDkbe/Q0oKMpwFRPdFd1X6Dhvhv6wAAAJiMsmtzjLJr
cwAAAtzc2gtZWQyNTUxOQAAACDj3hMJHUS+/mDU4UDkbe/Q0oKMpwFRPdFd1X6Dhvhv6w
AAAEYxN0lcCTGDew9Y2XMT+Y35CGEWZq7ZusLV1d8v2ZY3ePeEwkdRL7+YNThQOrt79DS
goynAVE90V2VfOOG+g/rAAAAD3JtZWWh0YUBtYWlpc3RyeQECAwQFBg==
-----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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>

```

### **Example 8: ED25519 authentication (Encrypted)**

#### API request:

```

curl -H "X-Requested-With: curl demo" -H "Content-type: text/xml" -u
USERNAME:PASSWORD -X POST
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?
action=create&title=Auth_Private_Key&username=root&ips=10.20.31.244"
--data-binary @add_pk_Valid.xml

```

#### POST Data Request (Contents of add\_pk\_Valid.xml)

```

<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="ed25519">
<![CDATA[-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAACmFlczI1Ni1jYmMAAAAGYmNyeXB0AAAAGAAAABAszHwIYP
g2XSX6PQCAWxxzAAAAEAAAAEAAAAzAAAAC3NzaC1lZDI1NTE5AAAAII37ri31dHt8Tk7l
fyLOXOQJ3FFzL8G+VridaHs43aUbAAAAoCKqy7tDvxpvcvo8Yl1lAO614KHMfsI6OGFtpUM
WpOoE8XLepoVGzvOJv1BlcKlKasmuMO2FODN0iBedu4AnUUfbIaUpyb/AiIu2XQwjTT+LE
slu9T94h41ohOZQ5indnXBy6w0iko49wgZxZCl536ZTVsxNTGH/ZBrmqSgmEJAoF8AE40W
RL6WvTy1npDh7pOZCD40JkXS6vxc7hvrRqNCQ=
-----END OPENSSH PRIVATE KEY-----]]></PRIVATE_KEY>
      </PRIVATE_KEY_INFO>
    </PRIVATE_KEY_CERTIFICATE>
  </PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>

```

```
<PASSPHRASE_INFO type="basic">
  <PASSPHRASE><![CDATA[12345]]></PASSPHRASE>
</PASSPHRASE_INFO>
</PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATES>
</UNIX_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>2017-04-19T14:58:49Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>80729</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

## **Edit Root Delegations and Private Keys**

(Applies to record type Unix only) Use an update request including XML binary data like this:

```
curl -H "X-Requested-With: curl" -H "Content-type:text/xml"
-u "USERNAME:PASSWORD" -X "POST"
"http://qualysapi.qualys.com/api/2.0/fo/auth/unix/action=update&id=12345
67" --data-binary @edit_params.xml
```

### Edit root tools:

Root tools in file binary\_input\_params.xml will be added. Any existing root tools will be deleted from the Unix record.

where edit\_params.xml is:

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <ROOT_TOOLS>
    <ROOT_TOOL>
      <ID>140016922</ID>
      <STANDARD_TYPE type="pimsu"/>
    </ROOT_TOOL>
  </ROOT_TOOLS>
</UNIX_AUTH_PARAMS>
```

```

    <PASSWORD_INFO type="vault">
      <DIGITAL_VAULT>
        <VAULT_USERNAME><![CDATA[root]]></VAULT_USERNAME>
        <VAULT_TYPE>Thycotic Secret Server</VAULT_TYPE>
        <VAULT_ID>25026922</VAULT_ID>
      </DIGITAL_VAULT>
    </PASSWORD_INFO>
  </ROOT_TOOL>
  <!-- in add_root_tools.xml we had created two root-tools; here we
are specifying only one item to edit, so the other record will be deleted!
-->
  </ROOT_TOOLS>
</UNIX_AUTH_PARAMS>

```

### Edit private-key certificates:

Private-key certificates in file binary\_input\_params.xml will be added. Any existing private-key certificates will be deleted from the Unix record.

where edit\_params.xml is:

```

<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
  <PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
      <ID>110066922</ID>
      <PRIVATE_KEY_INFO type="vault">
        <DIGITAL_VAULT>
          <VAULT_TYPE>Cyber-Ark 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>
      <ID>110076922</ID>
      <PRIVATE_KEY_INFO type="basic">
        <PRIVATE_KEY type="rsa">
          <![CDATA[-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,F9A653E2D12E019357B349B6EEE068B1

FiLfGH0c0rREmC0cBPsiyqqaitPNYTGeqKRmSBwGNrAzNTAcSkslsoY/WkMDW6QD
dLZNiGB0CFag94zyoMyCjyrdpayACAOWfH5w8VixxHF16Vxx5b6foLBE40FOYAIP

```

```
sdmlHvCfSFaN2dPflUnb0erwjigjJNwYIV78529e1E+2+dZIemi90ibh0R35NB60
TLeS3UUVEzp/O9ZPLf0pqPPHnWgfW4GXp/SUpwojES9fCQE+BW4MMWHWu8XKtytt
DcUtGNQlrT205Eg2D/GOWXla//CTHpiP6Zs0pWw/Ohmw1AkPWQa5iGAmCOWqRSFr
...
-----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
AAAAHhNzaClYc2EtY2VyZC12MDFAb3BlbnNzaC5jb20AAAAGwR4bJSiBtJlOgCAQUF3yZ6Io2
WYfnBioESQ45RkbqLgAAAAQAQABAAABQC5sVLb7emh8/v2uHp6xlpN5R+MHQwz3A5M3GRKtu
uulNjc/XYgqeWLM0JpbVtCVXwUcPgKt4Q0DmlGqc4uhZhZrdtpQGHrEivndNNLY9NQj7LozE7
x/sGiWdtmlucUh1teXMaBpM4aER9Y6uW5wv6ZylY7CAV9bcVz/ljlSympjzkPjJ39AJq+QxZk
Iv+H4uh/T05LwHdilFrjWWwEoI8DV/DRIw3h8o4jhnjlQxBxyjad3efmFaejgRnY6cBW82lgm
J3ODQMG96EbWHF6m0vAtmAelx9bahJD8adgu6EF
...
    </CERTIFICATE>
</PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

Edit root tools and private-key certificates:

Root tools and private-key certificates in file `binary_input_params.xml` will be added. Any existing private-key certificates and/or root tools will be deleted from the Unix record.

where `edit_params.xml` is:

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS>
        <ROOT_TOOL>
            <ID>140016922</ID>
            <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_TOOLS>
<PRIVATE_KEY_CERTIFICATES>
    <PRIVATE_KEY_CERTIFICATE>
        <ID>110066922</ID>
        <PRIVATE_KEY_INFO type="vault">
            <DIGITAL_VAULT>
                <VAULT_TYPE>Cyber-Ark 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>
        <ID>110076922</ID>
        <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
sdmlHvCfSFaN2dPflUnb0erwjigjJNwYIV78529e1E+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
AAAAHHNzaClYc2EtY2VydC12MDFab3BlbnNzaC5jb20AAAAGwR4bJSiBtJlJlOGCAQUF3yZ6Io2
WYfnBiOEsQ45RKbqLgAAAADAQABAAABAQC5sVLb7emh8/v2uHp6x1pN5R+MHQwz3A5M3GRKtu
uulNjc/XYgqeWLMOJpbVtCVXwUcPgKt4Q0DmlGqc4uhZhzrdtpQGHrEi...

```

```
        </CERTIFICATE>
    </PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

## Delete Root Delegations and Private Keys

(Applies to record type Unix only) Use a Unix record update request including XML binary data like this:

```
curl -H "X-Requested-With: curl" -H "Content-type:text/xml"
-u "USERNAME:PASSWORD" -X "POST"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/action=update&id=12345
67" --data-binary @delete_params.xml
```

### Delete all root delegations:

where delete\_params.xml is:

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

### Delete all private-key certificates:

where delete\_params.xml is:

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

### Delete all private-key certificates and root delegations:

where delete\_params.xml is:

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
    <ROOT_TOOLS></ROOT_TOOLS>
    <PRIVATE_KEY_CERTIFICATES></PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

## Unix Record List

### API request:

```
curl -u "USERNAME:PASSWORD" -X "GET" -H "Content-Type: text/xml"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/?action=list"
```

### 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>2016-09-01T15:59:40Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>1116826922</ID>
        <TITLE>
          <![CDATA[ssh2]]>
        </TITLE>
        <USERNAME>
          <![CDATA[root]]>
        </USERNAME>
        <SKIP_PASSWORD>1</SKIP_PASSWORD>
        <ROOT_TOOL_INFO_LIST>
          <ROOT_TOOL_INFO>
            <ID>100016922</ID>
            <ROOT_TOOL>PowerBroker</ROOT_TOOL>
            <PASSWORD_INFO type="vault">
              <DIGITAL_VAULT>
                <DIGITAL_VAULT_ID>
                  <![CDATA[25026922]]>
                </DIGITAL_VAULT_ID>
                <DIGITAL_VAULT_TYPE>
                  <![CDATA[Cyber-Ark PIM Suite]]>
                </DIGITAL_VAULT_TYPE>
                <DIGITAL_VAULT_TITLE>
                  <![CDATA[CyberArk]]>
                </DIGITAL_VAULT_TITLE>
                <VAULT_USERNAME>
                  <![CDATA[aaa]]>
                </VAULT_USERNAME>
                <VAULT_FOLDER>
                  <![CDATA[aaa]]>
                </VAULT_FOLDER>
                <VAULT_FILE>
                  <![CDATA[bbb]]>
                </VAULT_FILE>
              </DIGITAL_VAULT>
            </PASSWORD_INFO>
          </ROOT_TOOL_INFO>
        </ROOT_TOOL_INFO_LIST>
      </AUTH_UNIX>
    </AUTH_UNIX_LIST>
  </RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>
```

```
</VAULT_FILE>
</DIGITAL_VAULT>
</PASSWORD_INFO>
</ROOT_TOOL_INFO>
<ROOT_TOOL_INFO>
  <ID>100006922</ID>
  <ROOT_TOOL>PowerBroker</ROOT_TOOL>
  <PASSWORD_INFO type="basic" />
</ROOT_TOOL_INFO>
</ROOT_TOOL_INFO_LIST>
<PRIVATE_KEY_CERTIFICATE_LIST>
  <PRIVATE_KEY_CERTIFICATE>
    <ID>70016922</ID>
    <PRIVATE_KEY_INFO type="vault">
      <DIGITAL_VAULT>
        <DIGITAL_VAULT_ID>
          <![CDATA[25026922]]>
        </DIGITAL_VAULT_ID>
        <DIGITAL_VAULT_TYPE>
          <![CDATA[Cyber-Ark PIM Suite]]>
        </DIGITAL_VAULT_TYPE>
        <DIGITAL_VAULT_TITLE>
          <![CDATA[CyberArk]]>
        </DIGITAL_VAULT_TITLE>
        <VAULT_FOLDER>
          <![CDATA[fff]]>
        </VAULT_FOLDER>
        <VAULT_FILE>
          <![CDATA[gggg]]>
        </VAULT_FILE>
      </DIGITAL_VAULT>
    </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic" />
    <CERTIFICATE type="x.509" />
  </PRIVATE_KEY_CERTIFICATE>
  <PRIVATE_KEY_CERTIFICATE>
    <ID>70006922</ID>
    <PRIVATE_KEY_INFO type="basic">
      <PRIVATE_KEY type="rsa" />
    </PRIVATE_KEY_INFO>
    <PASSPHRASE_INFO type="basic" />
    <CERTIFICATE type="openssh" />
  </PRIVATE_KEY_CERTIFICATE>
</PRIVATE_KEY_CERTIFICATE_LIST>
<PORT>22, 23</PORT>
<IP_SET>
  <IP>10.10.35.253</IP>
</IP_SET>
<NETWORK_ID>0</NETWORK_ID>
```



```

    <CREATED>
      <DATETIME>2016-09-01T09:22:01Z</DATETIME>
      <BY>quays_asll</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2016-09-01T15:59:00Z</DATETIME>
    </LAST_MODIFIED>
    <COMMENTS>
      <![CDATA[vai API cooolio!yay!!!]]>
    </COMMENTS>
    <USE_AGENTLESS_TRACKING>1</USE_AGENTLESS_TRACKING>
    <AGENTLESS_TRACKING_PATH>
      <![CDATA[/usr/local]]>
    </AGENTLESS_TRACKING_PATH>
  </AUTH_UNIX>
</AUTH_UNIX_LIST>
</RESPONSE>
</AUTH_UNIX_LIST_OUTPUT>

```

## Unix Record: Input Parameters

For a Unix type record, root delegation tools and private-key certificates are specified using the DTD at `<platformURL>/api/2.0/fo/auth/unix/unix_auth_params.dtd`. Recent DTD is below.

```

<!-- QUALYS UNIX_AUTH_PARAMS DTD -->
<!ELEMENT UNIX_AUTH_PARAMS (ROOT_TOOLS?, PRIVATE_KEY_CERTIFICATES?)>
<!ELEMENT ROOT_TOOLS (ROOT_TOOL)*>
<!ELEMENT ROOT_TOOL (ID?, (STANDARD_TYPE|CUSTOM_TYPE), PASSWORD_INFO)>
<!-- ID may not be specified for any applicable in edit mode-->
<!ELEMENT ID (#PCDATA)>
<!ELEMENT STANDARD_TYPE (#PCDATA)>
<!ATTLIST STANDARD_TYPE
    type (sudo|pimsu|powerbroker) #REQUIRED>
<!ELEMENT CUSTOM_TYPE (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PASSWORD_INFO (DIGITAL_VAULT|PASSWORD)>
<!ATTLIST PASSWORD_INFO
    type (basic|vault) #REQUIRED>
<!ELEMENT DIGITAL_VAULT (VAULT_INFO_ID?, VAULT_USERNAME?, VAULT_TYPE?,
VAULT_ID?, FOLDER?, FILE?, SECRET_NAME?, SYSTEM_NAME?, END_POINT_NAME?,
END_POINT_TYPE?, END_POINT_CONTAINER?, AUTO_DISCOVER_SYSTEM_NAME?,
SYSTEM_NAME_SINGLE_HOST?, SYSTEM_TYPE?, CUSTOM_SYSTEM_TYPE?)>
<!-- VAULT_USERNAME may ONLY be used if used within PASSPHRASE_INFO or
PASSWORD_INFO -->
<!ELEMENT VAULT_INFO_ID (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_TYPE (#PCDATA)>
<!ELEMENT VAULT_ID (#PCDATA)>

```

```
<!-- Cyber-Ark PIM Suite/ Cyber-Ark AIM -->
<!ELEMENT FOLDER (#PCDATA)>
<!ELEMENT FILE (#PCDATA)>
<!-- -->
<!-- Thycotic Secret Server -->
<!ELEMENT SECRET_NAME (#PCDATA)>
<!-- -->
<!-- Quest Vault -->
<!ELEMENT SYSTEM_NAME (#PCDATA)>
<!-- -->
<!-- CA Access Control -->
<!ELEMENT END_POINT_NAME (#PCDATA)>
<!ELEMENT END_POINT_TYPE (#PCDATA)>
<!ELEMENT END_POINT_CONTAINER (#PCDATA)>
<!-- -->
<!-- Lieberman ERP -->
<!ELEMENT AUTO_DISCOVER_SYSTEM_NAME (#PCDATA)>
<!ELEMENT SYSTEM_NAME_SINGLE_HOST (#PCDATA)>
<!ELEMENT SYSTEM_TYPE (#PCDATA)>
<!ELEMENT CUSTOM_SYSTEM_TYPE (#PCDATA)>
<!-- -->
<!ELEMENT PASSWORD (#PCDATA)>
<!ELEMENT PRIVATE_KEY_CERTIFICATES (PRIVATE_KEY_CERTIFICATE)*>
<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID?, PRIVATE_KEY_INFO,
PASSPHRASE_INFO?, CERTIFICATE?)>
<!ELEMENT PRIVATE_KEY_INFO (DIGITAL_VAULT|PRIVATE_KEY)>
<!ATTLIST PRIVATE_KEY_INFO
    type (basic|vault) #REQUIRED>
<!ELEMENT PASSPHRASE_INFO (PASSPHRASE|DIGITAL_VAULT)>
<!ATTLIST PASSPHRASE_INFO
    type (basic|vault) #REQUIRED>
<!ELEMENT PASSPHRASE (#PCDATA)>
<!ELEMENT CERTIFICATE (#PCDATA)>
<!ATTLIST CERTIFICATE
    type (x.509|openssh) #REQUIRED>
<!ELEMENT PRIVATE_KEY (#PCDATA)>
<!ATTLIST PRIVATE_KEY
    type (rsa|dsa|ecdsa|ed25519) #REQUIRED>
<!-- EOF -->
```

## Unix Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details.

# VMware Record

The VMware authentication record type 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. The existence of this authentication module immediately enables several Qualys capabilities for Mapping, Vulnerability Management, and Policy Compliance for vSphere; and will support more vSphere-focused capabilities and integrations in the future.

The VMware Record API (`/api/2.0/fo/auth/vmware/`) allows you to manage VMware authentication records. You can submit API requests to view VMware authentication records, add new records, update records and delete records. Authentication is required for each API request. See Chapter 2, “Authentication Using the V2 APIs.”

See [User Permissions Summary](#)

## Create / Update VMware Record

Parameter	Description
action=create   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.
title={value}	<p>(Required for create request) The title of the VMware record. The title must be unique and may include a maximum of 255 characters (ascii).</p> <p>(Optional for update request) Overwrites the existing VMware record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).</p> <p>When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.</p>
comments={value}	(Optional) User defined notes about the VMware 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.

Parameter	Description
{login credentials}	(Required) See “VMware Record: Login Credentials.”
ips={value}	(Required) Add IP address(es) of the ESXi servers that the scanning engine should log into using the record’s credentials. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
ips={value}	(Optional for update request) Overwrites (replaces) the IP address(es) in the IP list for an existing VMware record. The IPs you specify are added, and any existing IPs are removed. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
ids={value}	(Required for update request) Update VMware records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.
add_ips={value}	(Optional for update request) Add IP address(es) to the IP list for an existing VMware record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
remove_ips={value}	(Optional for update request) Remove IP address(es) from the IP list for an existing VMware record. You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## VMware Record: Login Credentials

The login credentials for authenticating to a VMware ESXi server are described below.

Parameter	Description
username={value}	(Required for a create request; optional for an update request) The user name for a VMware account. A maximum of 13 characters (ascii) may be specified.
password={value}	(Required for a create request; optional for an update request) The password for a VMware account. A maximum of 13 characters (ascii) may be specified.
login_type={ <b>basic</b>   vault}	(Optional) Set to vault to use a third-party vault to retrieve the password. Vault parameters are required if login_type=vault is specified. By default, a vault is not used. <a href="#">Vault Support matrix</a> <a href="#">Vault Definition</a>
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.

Parameter	Description
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.

## VMware Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix D for details.

## VMware Record: Sample API Request

### API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=NewVMwareRecordWithAPI&username=USERNAME&password=PA
SSWORD&ips=10.10.10.2-10.10.10.4"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/" >
apiOutputCreateVMwareRecord.txt
```

### XML Output:

```
cat apiOutputCreateVMwareRecord.txt

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2012-02-03T21:16:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>30486</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

## Delete VMware Record

Parameter	Description
action=delete	(Required) The action required for the API request: delete.
echo_request={0   1}	(Optional) Show (echo) the request's input parameters (names and values) in the XML output.
ids={value}	(Required) Delete only VMware 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.

# Windows Record

The Windows Record API (`/api/2.0/fo/auth/windows/`) allows you to manage Windows authentication records for authenticated scanning. You can submit API requests to view Windows authentication records, add new records, update records and delete records.

See [User Permissions Summary](#)

Please refer to the *Windows Trusted Scanning* document for information, including account requirements and setup instructions. This document may be downloaded (in PDF) when you are logged into your Qualys account. Go to Help > Resources > Tips and Techniques and click the download link provided.

## List Windows Records

See [List Authentication Records by Type](#)

## Create Windows Record

Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
action=create   update	(Required) POST method must be used.
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}	<p>(Required for create request) Specifies a title for the authentication record. The title must be unique and may include a maximum of 255 characters (ascii).</p> <p>(Optional for update request) Overwrites the existing record title with a new title. The title must be unique and may include a maximum of 255 characters (ascii).</p> <p>When multiple IDs are specified for a batch update, the title is only replaced in the first record ID in the action since the title must be unique across records. The update will fail for the remaining IDs included in the action.</p>

Parameter	Description
comments={value}	(Optional) Specifies user defined notes about the authentication 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.
{login credentials}	Define login credentials for authentication to target hosts. See “Windows Record: Login Credentials.”
{target hosts}	See “Windows Record: Target Hosts.”
{protocols}	See “Windows Record: Enable Protocols” and “Windows Record: SMB Signing.”
use_agentless_tracking={0   1}	Specify “1” to enable Agentless Tracking.
ids={value}	(Required for update request) Update only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.

## Windows Record: Login Credentials

When defining login credentials for Windows authentication, you must supply a username and password for a Windows account.

These domain types are supported: Active Directory, NetBIOS User-Selected IPs, NetBIOS Service-Selected IPs.

Once a record is saved, you cannot change the domain type from Active Directory to NetBIOS or from NetBIOS to Active Directory.

Authentication is performed at the local host level when neither of these parameters are specified: **windows\_ad\_domain** and **windows\_domain**

Parameters specified in an update request will overwrite any existing parameters (previously defined).

Parameter	Description
username={value}	(Required for create request; Optional for update request) Specifies the user account to be used for authentication on target hosts. The username may include 1-31 characters (ascii).
password={value}	(Required for create request; Optional for update request) Specifies the password corresponding to the user account defined in the record for authentication. The password may include 1-31 characters (ascii).



Parameter	Description
login_type={ <b>basic</b>   vault}	<p>(Optional) Set to vault to use a third-party vault to retrieve the password. Vault parameters are required if login_type=vault is specified. By default, a vault is not used.</p> <p><a href="#">Vault Support matrix</a>  <a href="#">Vault Definition</a>  <a href="#">Unix Record Samples</a></p>
windows_ad_domain={value}	<p>(Optional) Specifies a 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).</p> <hr/> <p>This parameter and the <b>windows_domain</b> parameter cannot be specified in the same request.</p> <hr/> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>
windows_domain={value}	<p>(Optional) Specifies a Windows NetBIOS domain name for domain level authentication.</p> <hr/> <p>This parameter and the <b>windows_ad_domain</b> parameter cannot be specified in the same request.</p> <hr/> <p>When the <b>ips</b> 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.</p> <hr/> <p>When the <b>ips</b> 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.</p>
ntlm={0   1}	<p>(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 <b>ntlm=0</b> 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.</p>

## Windows Record: Target Hosts

Each IP address in your account may be included in one Windows record.

Parameter	Description
ips={value}	<p>(Optional for create request) When specified, the <b>ips</b> parameter defines an IP list for the authentication record. These are the hosts to be authenticated to with the login credentials. When not specified, the service uses the authentication credentials stored on the domain to authenticate to hosts that are members of the domain.</p> <p>(Optional for update request) Overwrites (replaces) the IP list for the authentication record. The IPs you specify are added and any existing IPs are removed.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>add_ips</b> parameter or the <b>remove_ips</b> parameter cannot be specified in the same request.</p>
add_ips={value}	<p>(Optional for update request only) 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.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>
remove_ips={value}	<p>(Optional for update request only) This parameter is used to update an existing IP list in an existing authentication record. Specifies one or more IP addresses to remove from the IP list for the authentication record.</p> <p>You may enter a combination of IPs and IP ranges. Multiple entries are comma separated.</p> <p>This parameter and the <b>ips</b> parameter cannot be specified in the same request.</p>

## Windows Record: Enable Protocols

Use these parameters to enable authentication protocols in Windows records.

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.

Parameter	Description
kerberos={0   1}	(Optional) When not specified, Kerberos is enabled allowing the scanning engine to try Kerberos when negotiating authentication to target hosts. Specify <b>kerberos=0</b> if you do not want Kerberos attempted.  Kerberos is supported for domain authentication only. When <b>kerberos=1</b> you must include <b>windows_ad_domain</b> or <b>windows_domain</b> in the same request.
ntlmv2={0   1}	(Optional) When not specified, NTLMv2 is enabled allowing the scanning engine to try NTLMv2 when negotiating authentication to target hosts. Specify <b>ntlmv2=0</b> if you do not want NTLMv2 attempted.
ntlm={0   1}	(Optional) When not specified, NTLMv1 will not be attempted. Specify <b>ntlm=1</b> to allow the scanning engine to try NTLMv1 when negotiating authentication to target hosts.

## Windows Record: SMB Signing

Define if the SMB protocol is required for Windows authentication or what should the minimum version of SMB be. You can set the minimum required SMB version for authentication without enabling SMB signing required.

Authentication will fail for target hosts that have an SMB version that is older than the minimum version selected. For example, if you set a minimum of 2.0.2 and you scan a Windows host with version 1.0 then authentication will fail and the host will not be scanned.

## Should I require SMB Signing?

The answer is No for most cases. This 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.

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.

Parameter	Description
require_smb_signing={0   1}	Set value to 0 (default) when SMB signing is not required. Set value to 1 to require SMB signing.
minimum_smb_version={value}	Specify 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 Record: XML Output

DTD: [https://<base\\_url>/api/2.0/batch\\_return.dtd](https://<base_url>/api/2.0/batch_return.dtd)

Please see Appendix A for details.

### Delete Windows Record

Parameter	Description
action=delete	(Required) POST method must be used.
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.
ids={value}	(Required) Delete only authentication records with certain IDs and/or ID ranges. Multiple entries are comma separated. Valid IDs are required.

## Vault Support API

The Vault Support API is used to manage integration with third party password vaults, an option when enabling authenticated scanning (e.g. trusted scanning).

<b>Vault summary</b>	
<a href="#">Vault Support matrix</a>	View supported vaults by OS and supported features (i.e. password, key passphrase, private key)
<b>Vault settings</b>	
<a href="#">Vault Definition</a>	Use Authentication API (/api/2.0/fo/auth/*) to add vault definition in authentication records
<a href="#">List Vaults</a>	Use Vault API (/api/2.0/fo/vault) to list vault records
<a href="#">Manage Vaults</a>	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). [Learn more](#)

password	private key	key passphrase	root delegation passwd
Cisco			
Cyber-Ark AIM Cyber-Ark PIM Suite			
Checkpoint Firewall (compliance scans only)			
Cyber-Ark AIM Cyber-Ark PIM Suite			
IBM DB2			
(UI support only) CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
MongoDB			
BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Quest Vault Thycotic Secret Server	BeyondTrust PBPS Cyber-Ark AIM Thycotic Secret Server	CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	
MS SQL (compliance scans only)			
(UI support only) BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			

password	private key	key passphrase	root delegation passwd
MySQL			
(UI support only) BeyondTrust PBPS Cyber-Ark AIM Cyber-Ark PIM Suite Quest Vault Thycotic Secret Server			
Oracle			
(UI support only) BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server			
Oracle Listener			
(UI support only) BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
Palo Alto Firewall			
BeyondTrust PBPS Cyber-Ark AIM Cyber-Ark PIM Suite Quest Vault Thycotic Secret Server			
PostgreSQL (compliance scans only)			
CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Quest Vault Thycotic Secret Server	Cyber-Ark AIM Thycotic Secret Server	CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Quest Vault Thycotic Secret Server	

password	private key	key passphrase	root delegation passwd
Sybase (compliance scans only)			
Cyber-Ark AIM Cyber-Ark PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
Unix			
BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	BeyondTrust PBPS CyberArk AIM Thycotic Secret Server	CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server	BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server
VMware			
BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Lieberman ERPM Quest Vault Thycotic Secret Server			
Windows			
BeyondTrust PBPS CA Access Control Cyber-Ark PIM Suite Cyber-Ark AIM Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server			



# 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={ <b>basic</b>   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) Want to know what vaults support what technologies and capabilities? See <a href="#">Vault Support matrix</a> Choose one: BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM (no parameters specific to this vault type.) Lieberman ERPM Quest Vault Thycotic Secret Server
<b>BeyondTrust PBPS</b>	
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 for you 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
<b>CA Access Control</b>	
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).
<b>CyberArk AIM</b>	
folder={value}	(Required if vault type is Cyber-Ark 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>
file={value}	(Required if vault type is Cyber-Ark 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>

Parameter	Description
<b>CyberArk PIM Suite</b>	
folder={value}	(Required if vault type is 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 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>
<b>Lieberman ERPm</b>	
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, mssql, ldap, cisco, custom

Parameter	Description
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.
<b>Quest Vault</b>	
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.
<b>Thycotic Secret Server</b>	
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.

# 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[Cyber-Ark 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[Cyber-Ark 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: BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server
modified={date}	(Optional) Include vaults modified on or after a certain date/time, in this format: YYYY-MM-DD[THH:MM:SSZ] (UTC/GMT).
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 <b>orderby</b> parameter. One of: asc (for ascending order) or desc (for descending order).

Parameter	Description
limit={value}	<p>(Optional) The maximum number of vault records processed for the request, starting at the record number specified by the <b>offset</b> parameter. These parameters must be specified together: <b>limit</b> and <b>offset</b>.</p> <p>When not specified, default limit is set to 1,000 vault records. You can specify a value less than or greater than the default.</p> <p>It's possible to specify "limit=0" for no limit. In this case the output is not paginated and all records are returned in a single output. Warning: This is not recommended since it may generate a very large output and processing large XML files can consume a lot of resources on the client side.</p>
offset={value}	<p>(Optional) The starting vault record number, used only when the request includes the <b>limit</b> parameter.</p>

### 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.eng.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

Use the parameter “action=create”.

Parameters:

Parameter	Description
action=create	(Required)
title={value}	(Required) The vault title.
type={value}	(Required) The vault type. A valid value is: BeyondTrust PBPS CA Access Control Cyber-Ark AIM Cyber-Ark PIM Suite Hitachi ID PAM Lieberman ERPM Quest Vault Thycotic Secret Server
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=Cyber-Ark AIM&title=New-CyberArk-
AIM&appid=CyberArk007&safe=Vaultsafe&url=https://afco.com&ssl_verify=1&
cert=-----BEGIN+CERTIFICATE-----
%0D%0AMIIDxzCCAkCQAQEWdQYJKoZIwdjELMAkGA1UEBhM%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

Use the parameter “action=update”.

### 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

Use the parameter “action=view”.

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[Cyber-Ark 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

Use the parameter “action=delete”.

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.

### **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}	<p>(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.</p> <p>Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).</p> <p>For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.</p>
private_key={value}	<p>(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-----).</p> <p>For a create/update request, if the private_key parameter is specified, then the cert parameter must also be specified.</p>
private_key_pwd={value}	(Optional) Specify a password for your private key if it's encrypted.
<b>CA Access Control</b>	
ca_url={value}	<p>(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.</p> <p>Sample web services URL: http://caac126u-32-235.caac125.domain.com:18080/iam/TEWS6/ac</p> <p>Sample web management URL: http://caac126p-33-166.caac125.domain.com:18080/iam/ac/</p>
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.
<b>CyberArk AIM</b>	
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.
<b>CyberArk PIM Suite</b>	
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.
<b>Hitachi ID PAM</b>	
url={value}	(Required for new vault) The HTTP or HTTPS URL of the Hitachi ID PAM webservice.
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.
<b>Lieberman ERPM</b>	
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 webservice. 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.
----------------	---

---

## Option Profile API

The Option Profile API is used to manage scan settings saved as option profiles in the user's subscription.

These topics are covered:

- Option Profile - Export
- Option Profile - Import



# Option Profile - Export

The Option Profile API v2 (the resource `/api/2.0/fo/subscription/option_profile/` with the parameter `action=export`) gives you the ability to export option profiles. The Option Profile API allows customers to import/export option profiles from one subscription to another in XML format. The API user must have the Manager role.

## Export API

The Export Option Profile API (`/api/2.0/fo/subscription/option_profile/?action=export`) allows the user to export one option profile or all option profiles in the subscription to an XML file. The output of an Export Option Profile API call is proving as POST Raw Data.

Parameters:

Parameter	Description
<code>action=export</code>	(Required) The GET or POST method may be used.
<code>output_format={XML}</code>	(Optional) XML format is supported. When unspecified, output format is XML.
<code>option_profile_id={value}</code>	(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.
<code>option_profile_title={value}</code>	(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.
<code>option_profile_type={value}</code>	(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".

## XML Output

An API request for a option profile XML output using the DTD which can be found at the following URL:

`https://<qualysapi.qualys.com>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd`

where `<qualysapi.qualys.com>` is the API server URL where your account is located. The DTD for the option profile XML is provided in Appendix G.

Example 1: Export Option Profile

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_profile/  
"
```

All the option profiles in the user's account get exported in XML format.

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE OPTION_PROFILES SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/  
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_DIS
COVERY>
  </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>
```

```

<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>
</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_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_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>
```

### Example 2: 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_profile/"
```

The option profile with the specified id and title in the user's account get exported in XML format.

#### XML Response:

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

```
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/
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>
      </PERFORMANCE>
      <PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_DISCOVERY>
      <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_ENABLE>
      </DISSOLVABLE_AGENT>
      <WINDOWS_DIRECTORY_SEARCH_ENABLE>1</WINDOWS_DIRECTORY_SEARCH_ENABLE>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>1</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>1</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

```
</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>
  <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_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_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>
```

### Example 3: Export Option Profile of type PCI

#### API request (export with option profile type):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
-X GET "action=export&option_profile_type=pci"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/"
```

The option profile with PCI type in the user's account get exported in XML format.

#### XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/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>
  </PERFORMANCE>
</SCAN>
<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>

```

# Option Profile - Import

The Import Option Profile API (/api/2.0/fo/subscription/option\_profile/?action=import) allows the user to import all option profiles defined in input XML file.

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](#) file 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.

Parameters:

Parameter	Description
action=import	(Required) The POST method must be used.

Example: Import option profiles in the input file into the user's account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @Export_OP.xml
"https://qualysapi.qualys.com/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
"https://qualysapi.qualys.com/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_DIS
COVERY>
</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>
    </CUSTOM>
  </CUSTOM_LIST>
<LOGIN_PASSWORD><![CDATA[L:temp,P:123123123]]></LOGIN_PASSWORD>
  </CUSTOM>
</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>
<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>
</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_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>

```

### 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>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>

```

## Report Template API

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

The API `/api/2.0/fo/report/template/scan/` allows you to 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	<code>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</code> <u>Required parameters:</u> <code>action=create</code> <code>report_format=xml</code>	POST
Update Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=update</code> <code>report_format=xml</code>	PUT
Delete Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=delete</code>	POST
Export Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</code> <u>Required parameters:</u> <code>action=export</code> <code>report_format=xml</code> <u>Optional parameter:</u> <code>template_id={value}</code> 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.

Parameter	Description
owner={value}	<p>Username of the owner of this template.</p> <p>Validity of the owner to create reports is based on the user role or business unit.</p> <p>See <a href="#">About template owner</a>.</p>
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}	<p>Specify 1 to include trending. Choose a timeframe (daily, weekly or monthly) to analyze the vulnerability status for the timeframe selected.</p> <p>This parameter is required only if scan_selection=HostBased.</p>
limit_timeframe={0   1}	<p>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.</p> <p>This parameter is required only if scan_selection=HostBased.</p>
selection_type={day   month   weeks   date   none   scans}	<p>Specify whether to include trending information for number of weeks, days or months or a specific date.</p> <p>Specifying none will create a report without any trending information included.</p> <p>Specifying scans will include trending information for the last two detections.</p> <p>This parameter is required only if scan_selection=HostBased.</p>
selection_range={value}	<p>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.</p> <p>Trending information since the last number of units or the specified date will be included.</p> <p>This parameter is required only if scan_selection=HostBased.</p>
asset_groups={value}	<p>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.</p> <p>This parameter is required only if scan_selection=HostBased.</p>

Parameter	Description
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.
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)

Parameter	Description
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.
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

Parameter	Description
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 include metadata information for each EC2 asset. This could be EC2 instance information such as accountId, region, availabilityZone, instanceId, instanceType, imageId, and kernelId.
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_solution={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_compliance={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_malware={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_reopened={0 1}	Specify 1 to include information related to reopened vulnerabilities.

Parameter	Description
include_vuln_details_appendix={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).
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.
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 <a href="#">Identified OS</a> .
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.
vuln_active={0   1}	Specify 1 to filter confirmed vulnerabilities in your report based on the state - Active.

Parameter	Description
vuln_disabled={0   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 <a href="#">Categories</a> .
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 <a href="#">Identified Services</a> .
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 <a href="#">Identified Services</a> .
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.

## Scan Template examples

### Example: 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/?action=cre
ate&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>
```

### **Example: 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/?action=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>
```

### **Example: 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>
```

**Example: Export Scan template**API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?action=exp
ort&template_id=89470&report_format=xml"
```

Exports the report template based on the template ID. When the template ID is not specified, exports all templates for the report type.

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/scanreportt
emplate_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="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[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]]></IN
FO>
```

```

    <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>

```

## Scan template DTD

[https://<base\\_url>/api/2.0/fo/report/template/scan/scanreporttemplate\\_info.dtd](https://<base_url>/api/2.0/fo/report/template/scan/scanreporttemplate_info.dtd)

For details see Appendix G, [Scan Report Template Output](#)

# PCI Scan Template

The API `/api/2.0/fo/report/template/pciscan/` allows you to 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	<code>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</code> <u>Required parameters:</u> <code>action=create</code> <code>report_format=xml</code>	POST
Update PCI Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=update</code> <code>report_format=xml</code>	PUT
Delete PCI Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=delete</code>	POST
Export PCI Scan Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</code> <u>Required parameters:</u> <code>action=export</code> <code>report_format=xml</code> <u>Optional parameter:</u> <code>template_id={value}</code> 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.

Parameter	Description
PCI Risk Ranking	Configure PCI Risk Ranking.
<code>custom_pci_ranking={0   1}</code>	Specify 1 to enable custom PCI risk ranking. When disabled Qualys will use default PCI ASV risk rankings.

Parameter	Description
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"

## Examples

Refer to [Scan template examples](#) for create, update, delete and export sample requests. Requests and outputs for PCI Scan template are similar.

## PCI Scan template DTD

`https://<base_url>/api/2.0/fo/report/template/pciscan/pciscanreporttemplate_info.dtd`

For details see Appendix G, [PCI Scan Template Output](#)

# Patch Template

The API `/api/2.0/fo/report/template/patch/` allows you to 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	<code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code> <u>Required parameters:</u> <code>action=create</code> <code>report_format=xml</code>	POST
Update Patch Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=update</code> <code>report_format=xml</code>	PUT
Delete Patch Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code> <u>Required parameters:</u> <code>template_id={value}</code> <code>action=delete</code>	POST
Export Patch Template	<code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code> <u>Required parameters:</u> <code>action=export</code> <code>report_format=xml</code> <u>Optional parameter:</u> <code>template_id={value}</code> 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.



Parameter	Description
owner={value}	<p>Username of the owner of this template.</p> <p>Validity of the owner to create reports is based on the user role or business unit.</p> <p>See <a href="#">About template owner</a>.</p>
Target	What target assets to include in the report.
patch_evaluation={ <b>qidbased</b>   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   <b>ANY</b> }	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}	<p>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.</p> <p>Multiple tags can be provided using comma separated values.</p>
tag_exclude_selector={ALL   <b>ANY</b> }	<p>Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation).</p> <p>Specifying ANY will match any of the assets tags (This is an OR operation).</p>
tag_set_exclude={value}	<p>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.</p> <p>Multiple tags can be provided using comma separated values.</p>
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.

Parameter	Description
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
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.
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.

Parameter	Description
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.
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.

Parameter	Description
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.

## Examples

Refer to [Scan template examples](#) for create, update, delete and export sample requests. Requests and outputs for Patch template are similar.

## Patch template DTD

`https://<base_url>/api/2.0/fo/report/template/patch/patchreporttemplate_info.dtd`

For details see Appendix G, [Patch Template Output](#)

# Map Template

The API /api/2.0/fo/report/template/map/ allows you to 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/ <u>Required parameters:</u> action=create report_format=xml	POST
Update Map Template	<base_url>/api/2.0/fo/report/template/map/ <u>Required parameters:</u> template_id={value} action=update report_format=xml	PUT
Delete Map Template	<base_url>/api/2.0/fo/report/template/map/ <u>Required parameters:</u> template_id={value} action=delete	POST
Export Map Template	<base_url>/api/2.0/fo/report/template/map/ <u>Required parameters:</u> action=export report_format=xml <u>Optional parameter:</u> template_id={value} When unspecified all templates for the report type get exported.	GET

## Map Template settings

These parameters (all are optional) are used for a create or update request to define Map 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.

Parameter	Description
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 <a href="#">About template owner</a> .
global={0   1}	Share this report template with other users by making it global. Specify 1 to make it global.
Display	Display options to include in the report.
map_sort_by={ipaddress   dns   netbios   router   operating system}	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.

Parameter	Description
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_rouge={0   1}	Specify 1 to filter the report by host types - Rouge.
Included Discovery Methods	Specify at least one.
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 <a href="#">Identified OS</a> .

## Examples

Refer to [Scan template examples](#) for create, update, delete and export sample requests. Requests and outputs for Map template are similar.

## Map template DTD

`https://<base_url>/api/2.0/fo/report/template/map/mapreporttemplate_info.dtd`

For details see Appendix G, [Map Template Output](#)

## 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  
3Com HomeConnect  
3Com NBX  
3Com OfficeConnect  
3Com SuperStack  
3Com Switch  
3Com Wireless Access Point  
AB  
AB ControlLogix  
Adic  
Adic Scalar  
Adic Storage  
ADIC Storage  
Adtran  
Adtran Device  
Adtran NetVanta  
Adtran TSUIQ  
ADTX  
ADTX ArrayMasStor  
AIX  
AIX 4.2-4.3  
AIX 4.3  
AIX 4.3.2.0-4.3.3.0  
AIX 4.33  
AIX 4.3-5.1  
AIX 4.x  
AIX 4.x-5.x  
AIX 5.1  
AIX 5.1-5.2  
AIX 5.1-5.3  
AIX 5.2  
AIX 5.3  
AIX 5.3.0.4  
AIX 5.x  
AIX 6.x  
Alcatel

Alcatel OmniStack  
Alcatel OmniSwitch  
Allied  
Allied Telesyn Switch  
Alteon  
Alteon ACE Switch  
Alteon Switch  
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 Airport Wireless Access Point  
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  
Avaya IP Phone  
Avaya Wireless Access Point  
Avocent  
Avocent CCM Appliance  
Axis  
Axis Network Camera

Axis Printer	Cisco Content Engine
Axis Storpoint CD	Cisco Content Services Switch
Axis Video Server	Cisco Content Switching Solution
Axis Wireless Access Point	Cisco Content/File Engine
Axonix SuperCD	Cisco Controller
Bay Networks	Cisco File Engine
Bay Networks Router	Cisco Firewall Services Module
Bay Networks Switch	Cisco IOS
Belkin	Cisco IP Phone
Belkin Wireless Access Point	Cisco IP/TV Program Manager
BeOS 5	Cisco Local Director
BlueCoat Security Gateway	Cisco PIX
BlueSocket Embedded Linux 2.4-2.6	Cisco VPN
BorderWare Firewall	Cisco WGB350
Brocade Device	Cisco Wireless Access Point
Brother Printer	ClearPath MCP
BSD	CNT UltraNet Edge
BSD Unix	Cognitive Printer
BSDI BSD	CometLabs Switch
BT Voyager	Compaq
Buffalo Wireless Access Point	Compaq Insight Manager
Cabletron	Compaq Switch
Cabletron SmartSTACK	Computone Device
Cabletron Switch	Connect2Air Wireless Access Point
Caldera	ControlLogix ENET
Caldera Open Linux	Crossroads Storage Router
Caldera Open UNIX 7	Custom Micro Device
Caldera Open UNIX 8	CyberGuard Firewall
Canon	CyberGuard Firewall
Canon Network Printer	Datamax I-Class
Canon Print Server	Datamax Printer
Canon Printer	Dawning SNI
Cayman3000	Debian
CEKAB Device	Dell
CentOS	Dell Laser
CentOS	Dell PowerConnect
CheckPoint	Dell PowerVault
CheckPoint FW1	Dell Remote Access Controller
CheckPoint FW1 NG	Digi
CheckPoint FW1 on Solaris	Digi One PortServer
CheckPoint SecurePlatform	Digi One SP
Cintech Switch	Digi Port Server
Cirronet Wireless Access Point	Divar Video Camera
Cisco	D-Link
Cisco Analog Phone Gateway	D-Link DSL Modem
Cisco Analog Telephone Adaptor	D-Link Print Server
Cisco Arrowpoint WebNS	D-Link Router
Cisco ASA	D-Link Switch
Cisco Catalyst	D-Link Wireless Access Point

Draytek Router	HP Tru64
DVD Server	HP-UX
Efficient Router	HP-UX 10
EFI Printer	HP-UX 10.20
EMC's Network-Attached Storage Device	HP-UX 11
Enterasys	Huawei Switch
Entry-Master Card Access Control System	HVAC controller
Epson Printer	IBM
ExtendedNet Print Server	IBM 2210
Extreme	IBM 4400 Printer
Extreme Alpine	IBM 4690
Extreme Networks Device	IBM Infoprint
Extreme Networks ExtremeWare	IBM Mainframe
Extreme Networks Switch	IBM Network Printer
F5 Networks Big-IP	IBM OS/2
Fabric OS	IBM OS/390
FaxPress	IBM OS/400
Fiery Printer	IBM Printer
File Engine	IBM Remote Supervisor Adapter
Fortigate	IBM Remote Supervisor Adapter II
Foundry Networks	IBM Tape Library
FreeBSD	IBM Token-Ring Stackable Hub
Fujitsu	IBM z/VM
Fujitsu Blade	i-data Print Server
Gestetner	Indyme MTS Messaging Telephony Server CU4400
Gestetner Printer	Infinity Embedded Device
Gigafast	Infotrend Serial ATA Storage Subsystem
Gigafast Wireless Access Point	Intel
Gigafast Wireless Access Point	Intel NetportExpress Print Server
Google Appliance	Intel Switch
Hawking Wireless Access Point	Intel Wireless Access Point
Honeyd HoneyPot	Intergy Network Energy Source System
HP	Intermate
HP 3000 MPE	Intermate Print Server
HP AdvanceStack Switch	Intermate Print Server
HP Deskjet Printer	Intermec
HP Fabric OS	Intermec EasyLAN Printer
HP Guardian Service Processor	Intermec Wireless Access Point
HP iLO	Inter-Tel IP Phone
HP Inkjet Printer	IP Phone
HP JetDirect	IRIX
HP LaserJet	IRIX 6.2
HP OpenVMS	IRIX 6.5
HP ProCurve	IRIX behind Firewall or Load Balancer
HP RILO	IronPort
HP Surestore Library	
HP Switch	

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	OkilAN Print Server
NETBuilder Bridge	Open Networks Router
Netgear	OpenBSD
Netgear GSM	Oracle Enterprise Linux
Netgear Print Server	Oracle Enterprise Linux 4.5
Netgear Printer	Oracle Enterprise Linux 5.2
Netgear Router	ORiNOCO Wireless Access Point
Netgear Smart Switch	Orinoco Wireless Access Point
Netgear Switch	Packeteer
Netgear Wireless Access Point	Packeteer PacketSeeker
Netopia	Packeteer PacketShaper
Netopia Router	Panasonic Network Camera
Netphone	Paradyne Device
Netphone IP Phone	Perle Jetstream
NetScaler	PocketPro Print Server
NetScaler VPN Device	Point Six Point Server
NetScreen	Polycom
NetScreen 100	Polycom Device
NetScreen 50	Polycom MGC
NetScreen 5XP	Polycom VSX
NetSilicon Device	Power Measurement ION Meter
Netsilicon Device	Powerware
NetWare	Powerware ConnectUPS
NetWare 4.11-5.0 SP5	Powerware UPS Device
NetWare 5	Precidia Device
NetWare 5.0	Primergy RSB
NetWare 5.1	Printronix Printer
NetWare 6	Procom NetFORCE
NetWare 6.5	pSOSystem
NetWare Print Server	QNX
Network Camera	Quantum
Network Print Server	Quantum NAS SnapServer
Network Printer	Quantum PX506 Tape Library
Network Scanner	Quick Eagle Device
NGS 500 Router	RadiSys iRMX
NIB Network Printer	Radware Device
Nokia	Raptor Firewall
Nokia IPSO	Red Hat
Nokia Wireless Access Point	Redline
Nortel	Redline Networks Processor
Nortel Device	Redline Wireless Access Point
Nortel Networks BayStack	Ricoh
Nortel Passport	RICOH Aficio
Nortel Router	Ricoh Aficio
Nortel Switch	Ricoh Printer
NRG	Ringdale Device
NRG Network	RIO Xtreme
NRG Printer	RiverStone Networks Router
Okidata Printer	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 11  
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	Windows ME
Ubuntu	Windows NT
Ubuntu Linux 10	Windows NT4
Ubuntu Linux 11	Windows RT
Ubuntu Linux 7	Windows Vista
Ubuntu Linux 8	Windows XP
Ubuntu Linux 9	WKTl RDS Encoder
Ubuntu Linux LTS	Xerox
Uninterruptible Power Supply Device	Xerox Device
UNIX System V	Xerox DocuColor Printer
UNIX System V Release 4.2	Xerox Document Centre
UNIX SystemUNIX System V 4	Xerox DocuPrint Printer
Uptime Devices Monitoring System	Xerox Phaser Printer
UptimeDevices Sensorprobe	Xerox Plotter
VAX	Xerox Printer
VAX VMS 6.1	Xerox WorkCentre
VAX VMS 6.1 behind Sidewinder G2	Xerox WorkCentre Printer
VAX VMS 6.2	XES Printer
VAX VMS 7.1	XJet Print Server
VAX VMS 7.1 behind Sidewinder G2	ZebraNet Print Server
Verilink WANSuite Router	ZOT Print Server
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 9x	
Windows CE	
Windows Longhorn	

## 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_TMI_Admin_Server
Applix_TMI_Server
Arkeiad_Network_Backup
ARUGIZER_BACKDOOR
auth
Berlios_Global_Positioning_System_D
aemon
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	mssql
http	mssql_monitor
http_over_ssl	MYDESKTOP
IBM_SolidDB	mysql
IBM_DB2_Universal_Database	named_udp
IBM_TIVOLI_STORAGE_MANAGER	ncp
icecast	nessus
ident	netbios_ns
imap	netbios_ssn
INDUSOFT	netbus
Infopulse_Gatekeeper	netop
ipmi	netstat
ipp	Netviewer_PC_Duo
irc	nfs
ISA_Proxy	nntp
isakmp	ntp
ISAKMP_over_TCP	ocsp
iSCSI	ocssd
iSNS	Omniquad_Server
jabber	open_vpn
Kadmin-4	opennap
kazaa	oracle
Kerberos-5	Oracle_Express_Server
l2tp	Oracle_Express_Server_xsagent
LANDesk	Oracle_Express_Server_xsdaemon
LANDESK_CBA_PDS	oracle_intelligent_agent
LANDESK_MANAGEMENT_AGENT	ORACLE_RMI
LANDESK_MANAGEMENT_AGENT	pcanywhere
ldap	pen
ldap_over_ssl	Polycom_MGC_Management
limewire	pop2
linuxconf	pop3
lpd	PostgreSQL
managesoft	pptp
McAfee_ePolicy_Orchestrator	PRORAT_TROJAN
melange_chat	proxy_http
MERCUR_Control-Service	proxy_telnet
Micromuse_Netcool_Object_Server	psmond
microsoft-ds	pvserver
Microsoft_Message_Queue_Server	Quote_of_the_Day
minisql	quote_of_the_day_udp
modbus	radius
MODBUS_UDP	radius_tcp
mqseries	radmin
msdtc	rccmd
MSMQ_Ping	RealMedia_EncoderServer
msrpc	Red_Carpet_Daemon
msrpc-over-http	RELIABLE DATAGRAM SOCKETS OVER TCP
msrpc_udp	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  
SAPgui  
SGI\_Performance\_Copilot  
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\_Administrato  
r  
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**

Proxy  
RedHat  
RPC  
Security Policy  
SNMP  
Solaris  
SMB / NETBIOS  
SUSE  
TCP/IP  
Ubuntu  
VMware  
Web Application  
Web Application Firewall  
Web server  
Windows  
X-Window

AIX  
Amazon Linux  
Backdoors and trojan horses  
Brute Force Attack  
CentOS  
CGI  
Cisco  
Database  
Debian  
DNS and BIND  
E-Commerce  
Fedora  
File Transfer Protocol  
Finger  
Firewall  
Forensics  
General remote services  
Hardware  
HP-UX  
Information gathering  
Internet Explorer  
Local  
Mail services  
Malware  
News Server  
NFS  
OEL  
Office Application

## Activity Log API

The Export Activity Log API (/api/2.0/fo/activity\_log/) allows users to export the user activity log for a subscription to CSV format.

### Export user activity log for subscription

#### Parameters

These parameters are used to export the user activity log for a subscription.

Parameter	Description
action=list	(Required) The action required for the API request: list. The POST or GET method can be used.
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. 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”.

Parameter	Description
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 format YYYY-MM-DD HH:ii:ss, 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 format YYYY-MM-DD HH:ii:ss, and must be more than or equal to since_datetime, and less than or equal to today's date.
user_role={value}	<p>(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.</p> <p>User roles you can specify:</p> <ul style="list-style-type: none"> <li>- Manager</li> <li>- Unit Manager</li> <li>- Auditor</li> <li>- Scanner</li> <li>- Reader</li> <li>- KnowledgeBase Only</li> <li>- Remediation User</li> <li>- Contact</li> </ul> <p>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).</p>
output_format=CSV	(Optional) CSV (default)
truncation_limit={value}	(Optional) Limit the number of log records to include in the CSV output.

## Sample API Request

### API request:

```
curl -u "username:password" -k -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/activity_log/?action=list"
```

The activity log gets exported in CSV format.

### 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","10.113.195.136"
"2017-02-02T13:31:19Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:28:38Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:28:17Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:27:27Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:26:41Z","request","auth","API:
/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"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"
```

## Network API

The Network API is used to manage networks when the Network Support feature is enabled in the user's subscription.

These topics are covered:

- Network List
- Create Network
- Update Network
- Assign Scanner Appliance to Network

# Network List

The Network List API v2 (resource `/api/2.0/fo/network/` with parameter `action=list`) is used to list custom networks in your account. The optional “ids” input parameter can be used to filter the list.

Supported methods	GET and POST
Permissions	This API is available to all users with the API access permission. 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.

## Sample

### API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/network/?action=list&ids=734
3,7345,7350"
```

### XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NETWORK_LIST SYSTEM
"https://qualysapi.qualys.com/network_list_output.dtd">
<RESPONSE>
  <DATETIME>2013-07-28T01:06:45Z</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>
```



# Create Network

The Create Network API v2 (resource /api/2.0/fo/network/ with action=create) is used to create a new network. The input parameter “name” (required) is a user-defined friendly name. A successful request will return a unique network ID and this is used to manage your network using the API.

Supported methods	POST
Permissions	This API is available to Managers only

## Next steps

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).

## Sample

### 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>2014-01-14T04:37:24Z</DATETIME>  
    <TEXT>Network created with ID</TEXT>  
    <ITEM_LIST>  
      <ITEM>  
        <KEY>id</KEY>  
        <VALUE>1103</VALUE>  
      </ITEM>  
    </ITEM_LIST>  
  </RESPONSE>  
</SIMPLE_RETURN>
```

# Update Network

The Update Network API v2 (resource /api/2.0/fo/network/ with parameter action=update) is used to change the name for a network. Use the “name” parameter to specify a new network name. (The network ID is assigned by our service and it can’t be changed.)

Supported methods	POST
Permissions	This API is available to Managers only

## Sample

### 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>2014-01-20T06:17:06Z</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>
```

# Assign Scanner Appliance to Network

The Assign Scanner Appliance to Network API v2 (resource /api/2.0/fo/appliance/ with action=assign\_network\_id) is used to 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.

Supported methods	POST
Permissions	This API is available to Managers only
Required input parameters	action=assign_network_id appliance_id={id} network_id={id}

## Sample

### API request:

```
curl -k -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:

The simple return DTD is used. The response will look like this, if successful:

```
<?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>2013-12-16T22:50:49Z</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>2013-12-16T22:53:41Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT>parameter network_id has invalid value: 1103 (No such
```

```
network ID)</TEXT>  
</RESPONSE>  
</SIMPLE_RETURN>
```

## Scan XML

This appendix describes the XML output returned from API V2 requests. The following topics are included:

- Simple Return
- Batch Return
- Scan List Output
- SCAP Scan List Output
- Scheduled Scan List Output
- Vulnerability Scan Results
- Compliance Scan Results
- VM Recrypt Results (Scan Statistics)
- PCI Scan Share Status Output
- Network List
- KnowledgeBase Output
- Customized Vulnerability List Output

## Simple Return

The simple return is XML output returned from several API V2 calls. The DTD “simple\_return.dtd” can be found at the following URL:

[https://qualysapi.qualys.com/api/2.0/simple\\_return.dtd](https://qualysapi.qualys.com/api/2.0/simple_return.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Simple Return

A recent DTD for the simple return output (simple\_return.dtd) is shown below.

```
<!-- QUALYS SIMPLE_RETURN DTD -->

<!ELEMENT SIMPLE_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, CODE?, TEXT, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
```

## XPaths for Simple Return

This section describes the XPaths for the simple return output (simple\_return.dtd).

XPath	element specifications / notes
/SIMPLE_RETURN	(REQUEST?, RESPONSE)
/SIMPLE_RETURN/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SIMPLE_RETURN/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/SIMPLE_RETURN/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/SIMPLE_RETURN/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/SIMPLE_RETURN/REQUEST/PARAM_LIST	(PARAM+)
/SIMPLE_RETURN/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/SIMPLE_RETURN/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/SIMPLE_RETURN/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/SIMPLE_RETURN/REQUEST/POST_DATA	(#PCDATA) The POST data.
/SIMPLE_RETURN/RESPONSE	(DATETIME, CODE?, TEXT, ITEM_LIST?)
/SIMPLE_RETURN/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/SIMPLE_RETURN/RESPONSE/CODE	(#PCDATA) The response error code.
/SIMPLE_RETURN/RESPONSE/TEXT	(#PCDATA) The response error text.
/SIMPLE_RETURN/RESPONSE/ITEM_LIST	(ITEM+)
/SIMPLE_RETURN/RESPONSE/ITEM_LIST/ITEM	(KEY, VALUE+)
/SIMPLE_RETURN/RESPONSE/ITEM_LIST/ITEM/KEY	(#PCDATA) The response item keyword.
/SIMPLE_RETURN/RESPONSE/ITEM_LIST/ITEM/VALUE	(#PCDATA) The response item value.

## Batch Return

The batch return is XML output returned from several API V2 calls. The DTD “batch\_return.dtd” can be found at the following URL:

[https://qualysapi.qualys.com/api/2.0/batch\\_return.dtd](https://qualysapi.qualys.com/api/2.0/batch_return.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Batch Return

A recent DTD for the simple return output (batch\_return.dtd) is shown below.

```
<!-- QUALYS BATCH_RETURN DTD -->
<!ELEMENT BATCH_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, BATCH_LIST?)>
<!ELEMENT BATCH_LIST (BATCH+)>
<!ELEMENT BATCH (CODE?, TEXT?, ID_SET?)>

<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!-- EOF -->
```



## XPaths for Batch Return

This section describes the XPaths for the simple return output (batch\_return.dtd).

XPath	element specifications / notes
/BATCH_RETURN	(REQUEST?, RESPONSE)
/BATCH_RETURN/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/BATCH_RETURN/REQUEST/DATETIME	(#PCDATA)
	The date and time of the request.
/BATCH_RETURN/REQUEST/USER_LOGIN	(#PCDATA)
	The user login ID of the user who made the request.
/BATCH_RETURN/REQUEST/RESOURCE	(#PCDATA)
	The resource specified for the request.
/BATCH_RETURN/REQUEST/PARAM_LIST	(PARAM+)
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA)
	The input parameter name.
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA)
	The input parameter value.
/BATCH_RETURN/REQUEST/POST_DATA	(#PCDATA)
	The POST data.
/BATCH_RETURN/RESPONSE	(DATETIME, BATCH_LIST?)
/BATCH_RETURN/RESPONSE/DATETIME	(#PCDATA)
	The date and time of the response.
/BATCH_RETURN/RESPONSE/BATCH_LIST	(BATCH+)
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH	(CODE?, TEXT?, ID_SET?)
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/CODE	(#PCDATA)
	A batch code.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/TEXT	(#PCDATA)
	A batch text description.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/ID_SET	(ID   ID_RANGE)
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/ID_SET/ID	(#PCDATA)
	A batch ID number.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/ID_SET/ID_RANGE	(#PCDATA)
	A batch ID range.

## Scan List Output

The scan list output is an XML report returned from the VM and PC scan list API calls. The DTD “scan\_list\_output.dtd” can be found at the following URL (when your account is located on US Platform 1):

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

### DTD for Scan List Output

A recent DTD for the scan list output (scan\_list\_output.dtd) is shown below.

```
<!-- QUALYS SCAN_LIST_OUTPUT DTD -->  
  
<!ELEMENT SCAN_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, SCAN_LIST?)>  
<!ELEMENT SCAN_LIST (SCAN+)>  
<!ELEMENT SCAN (ID?, REF, SCAN_TYPE?, TYPE, TITLE, USER_LOGIN,  
                LAUNCH_DATETIME,DURATION, PROCESSING_PRIORITY?, PROCESSED,  
                STATUS?, TARGET, ASSET_GROUP_TITLE_LIST?,  
                OPTION_PROFILE?)>  
<!ELEMENT ID (#PCDATA)>  
<!ELEMENT REF (#PCDATA)>  
<!ELEMENT SCAN_TYPE (#PCDATA)>  
<!ELEMENT TYPE (#PCDATA)>  
<!ELEMENT TITLE (#PCDATA)>  
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>  
<!ELEMENT DURATION (#PCDATA)>  
<!ELEMENT PROCESSING_PRIORITY (#PCDATA)>  
<!ELEMENT PROCESSED (#PCDATA)>  
<!ELEMENT STATUS (STATE, SUB_STATE?)>  
<!ELEMENT STATE (#PCDATA)>  
<!ELEMENT SUB_STATE (#PCDATA)>  
<!ELEMENT TARGET (#PCDATA)>
```

```

<!ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>
<!ELEMENT DEFAULT_FLAG (#PCDATA)>
<!-- EOF -->

```

## XPaths for Scan List Output

This section describes the XPaths for the scan list output (scan\_list\_output.dtd).

XPath	element specifications / notes
/SCAN_LIST_OUTPUT	(REQUEST?, RESPONSE)
/SCAN_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCAN_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCAN_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/SCAN_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/SCAN_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/SCAN_LIST_OUTPUT/RESPONSE	(DATETIME, SCAN_LIST?)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST (SCAN+)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN	(ID?, REF, SCAN_TYPE?, TYPE, TITLE, USER_LOGIN, LAUNCH_DATETIME, DURATION, PROCESSING_PRIORITY?, PROCESSED, STATUS?, TARGET, ASSET_GROUP_TITLE_LIST?, OPTION_PROFILE?)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ID (#PCDATA)	The scan ID.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/REF (#PCDATA)	The scan reference code.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/SCAN_TYPE (#PCDATA)	For a CertView VM scan this is set to "CertView".

<b>XPath</b>	<b>element specifications / notes</b>
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TYPE (#PCDATA)	The scan type: On-Demand, Scheduled or API.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TITLE (#PCDATA)	The scan title.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/USER_LOGIN (#PCDATA)	The user login ID of the user who launched the scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/LAUNCH_DATETIME (#PCDATA)	The date and time when the scan was launched.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/DURATION (#PCDATA)	The time it took to perform the scan - when the scan status is Finished. For a scan that has not finished (queued, running), the duration is set to "Pending".
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/PROCESSING_PRIORITY (#PCDATA)	(Applicable for VM scans only) The processing priority setting for the scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/PROCESSED (#PCDATA)	A flag that specifies whether the scan results have been processed. A value of 1 is returned when the scan results have been processed. A value of 0 is returned when the results have not been processed.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS	(STATE, SUB-STATE?)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS/STATE (#PCDATA)	The scan state: 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).
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS/SUB_STATE (#PCDATA)	The sub-state related to the scan state, if any. For scan state Finished, value can be: No_Vuln (no vulnerabilities found) or No_Host (no host alive). For scan state Queued, value can be: Launching (service received scan request), Pausing (service received pause scan request), or Resuming (service received resume scan request).
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TARGET (#PCDATA)	The scan target hosts. This element does not appear when API request includes ignore_target=1.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST/ASSET_GROUP_TITLE (#PCDATA)	The asset group title specified for the scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE (TITLE, DEFAULT_FLAG?)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE/TITLE (#PCDATA)	The option profile title specified for the scan.

XPath	element specifications / notes
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE/DEFAULT_FLAG	(#PCDATA)
	A flag that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.

## SCAP Scan List Output

The SCAP scan list output is an XML report returned from the SCAP scan list API call. The DTD can be found at the following URL (when your account is located on US Platform 1):

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

### DTD for SCAP Scan List Output

A recent DTD for the SCAP scan list output (qscap\_scan\_list\_output.dtd) is shown below.

```
<!-- QUALYS QSCAP SCAN_LIST_OUTPUT DTD -->  
  
<!ELEMENT SCAN_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, SCAN_LIST?)>  
<!ELEMENT SCAN_LIST (SCAN+)>  
<!ELEMENT SCAN (ID?, REF, TYPE, TITLE, POLICY, USER_LOGIN,  
                LAUNCH_DATETIME, STATUS?, TARGET, ASSET_GROUP_TITLE_LIST?,  
                OPTION_PROFILE?)>  
  
<!ELEMENT ID (#PCDATA)>  
<!ELEMENT REF (#PCDATA)>  
<!ELEMENT TYPE (#PCDATA)>  
<!ELEMENT TITLE (#PCDATA)>  
<!ELEMENT POLICY (ID, TITLE)>  
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>  
<!ELEMENT STATUS (STATE, SUB_STATE?)>  
<!ELEMENT STATE (#PCDATA)>  
<!ELEMENT SUB_STATE (#PCDATA)>  
<!ELEMENT TARGET (#PCDATA)>  
<!ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>  
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>  
<!ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>  
<!ELEMENT DEFAULT_FLAG (#PCDATA)>
```

## XPaths for SCAP Scan List Output

This section describes the XPaths for the SCAP scan list output (scap\_scan\_list\_output.dtd).

XPath	element specifications / notes
/SCAN_LIST_OUTPUT	(REQUEST?, RESPONSE)
/SCAN_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCAN_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCAN_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/SCAN_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/SCAN_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/SCAN_LIST_OUTPUT/RESPONSE (DATETIME, SCAN_LIST?)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST (SCAN+)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN	(ID?, REF, TYPE, TITLE, USER_LOGIN, LAUNCH_DATETIME, STATUS?, TARGET, ASSET_GROUP_TITLE_LIST?, OPTION_PROFILE?)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ID (#PCDATA)	The SCAP scan ID.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/REF (#PCDATA)	The SCAP scan reference code.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TYPE (#PCDATA)	The scan type: On-Demand, Scheduled or API.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TITLE (#PCDATA)	The SCAP scan title.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/POLICY (ID, TITLE)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/POLICY/ID (#PCDATA)	The SCAP policy ID.

<b>XPath</b>	<b>element specifications / notes</b>
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/POLICY/TITLE (#PCDATA)	The SCAP policy title.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/USER_LOGIN (#PCDATA)	The user login ID of the user who launched the SCAP scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/LAUNCH_DATETIME (#PCDATA)	The date and time when the SCAP scan was launched.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS (STATE, SUB-STATE?)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS/STATE (#PCDATA)	The scan state: 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).
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/STATUS/SUB_STATE (#PCDATA)	The sub-state related to the scan state, if any. For scan state Finished, value can be: No_Vuln (no vulnerabilities found) or No_Host (no host alive). For scan state Queued, value can be: Launching (service received scan request), Pausing (service received pause scan request), or Resuming (service received resume scan request).
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/TARGET (#PCDATA)	The target hosts selected for the SCAP scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST/ASSET_GROUP_TITLE (#PCDATA)	The asset group title selected for the SCAP scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE (TITLE, DEFAULT_FLAG?)	
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE/TITLE (#PCDATA)	The option profile title selected for the SCAP scan.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/OPTION_PROFILE/DEFAULT_FLAG (#PCDATA)	A flag that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.



# Scheduled Scan List Output

The scheduled scan list output is an XML report returned from scheduled scan API calls. The DTD can be found at the following URL (when your account is located on US Platform 1):

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

## DTD for Scheduled Scan List Output

A recent DTD for the scheduled scan list output (scheduled\_scan\_list\_output.dtd) is shown below.

```
<!-- QUALYS SCHEDULE_SCAN_LIST_OUTPUT DTD -->

<!ELEMENT SCHEDULE_SCAN_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, SCHEDULE_SCAN_LIST?)>
<!ELEMENT SCHEDULE_SCAN_LIST (SCAN+)>
<!ELEMENT SCAN (ID, SCAN_TYPE?, ACTIVE, TITLE?, USER_LOGIN, TARGET,
NETWORK_ID?, ISCANNER_NAME?, EC2_INSTANCE?, CLOUD_DETAILS?,
ASSET_GROUP_TITLE_LIST?, ASSET_TAGS?, EXCLUDE_IP_PER_SCAN?,
USER_ENTERED_IPS?, OPTION_PROFILE?, PROCESSING_PRIORITY?, SCHEDULE,
NOTIFICATIONS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TARGET (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT ISCANNER_NAME (#PCDATA)>
<!ELEMENT EC2_INSTANCE (CONNECTOR_UUID, EC2_ENDPOINT, EC2_ONLY_CLASSIC?)>
<!ELEMENT CONNECTOR_UUID (#PCDATA)>
<!ELEMENT EC2_ENDPOINT (#PCDATA)>
<!ELEMENT EC2_ONLY_CLASSIC (#PCDATA)>
```

```
<!ELEMENT CLOUD_DETAILS (PROVIDER, CONNECTOR, SCAN_TYPE, CLOUD_TARGET)>
<!ELEMENT PROVIDER (#PCDATA)>
<!ELEMENT CONNECTOR (ID?, UUID, NAME)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT REGION (UUID, CODE?, NAME?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT VPC_SCOPE (#PCDATA)>
<!ELEMENT VPC_LIST (VPC+)>
<!ELEMENT VPC (UUID)>

<!ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT ASSET_TAGS (TAG_INCLUDE_SELECTOR, TAG_SET_INCLUDE,
TAG_EXCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, USE_IP_NT_RANGE_TAGS)>
<!ELEMENT TAG_INCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_INCLUDE (#PCDATA)>
<!ELEMENT TAG_EXCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_EXCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS (#PCDATA)>
<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ELEMENT USER_ENTERED_IPS (RANGE+)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
<!ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>
<!ELEMENT DEFAULT_FLAG (#PCDATA)>
<!ELEMENT PROCESSING_PRIORITY (#PCDATA)>

<!ELEMENT SCHEDULE ((DAILY|WEEKLY|MONTHLY), START_DATE_UTC, START_HOUR,
START_MINUTE, END_AFTER_HOURS?, END_AFTER_MINUTES?, PAUSE_AFTER_HOURS?,
PAUSE_AFTER_MINUTES?, RESUME_IN_DAYS?, RESUME_IN_HOURS?, NEXTLAUNCH_UTC?,
TIME_ZONE, DST_SELECTED, MAX_OCCURRENCE?)>
<!ELEMENT DAILY EMPTY>
<!ATTLIST DAILY
    frequency_days CDATA #REQUIRED>

<!-- weekdays is comma-separated list of weekdays e.g. 0,1,4,5 -->
<!ELEMENT WEEKLY EMPTY>
<!ATTLIST WEEKLY
    frequency_weeks CDATA #REQUIRED
    weekdays CDATA #REQUIRED>
```

```

<!-- either day of month, or (day of week and week of month) must be
provided -->
<!ELEMENT MONTHLY EMPTY>
<!ATTLIST MONTHLY
    frequency_months CDATA #REQUIRED
    day_of_month CDATA #IMPLIED
    day_of_week (0|1|2|3|4|5|6) #IMPLIED
    week_of_month (1|2|3|4|5) #IMPLIED>

<!-- start date of the task in UTC -->
<!ELEMENT START_DATE_UTC (#PCDATA)>
<!-- User Selected hour -->
<!ELEMENT START_HOUR (#PCDATA)>
<!-- User Selected Minute -->
<!ELEMENT START_MINUTE (#PCDATA)>
<!ELEMENT END_AFTER_HOURS (#PCDATA)>
<!ELEMENT END_AFTER_MINUTES (#PCDATA)>
<!ELEMENT PAUSE_AFTER_HOURS (#PCDATA)>
<!ELEMENT PAUSE_AFTER_MINUTES (#PCDATA)>
<!ELEMENT RESUME_IN_DAYS (#PCDATA)>
<!ELEMENT RESUME_IN_HOURS (#PCDATA)>
<!ELEMENT NEXTLAUNCH_UTC (#PCDATA)>
<!ELEMENT TIME_ZONE (TIME_ZONE_CODE, TIME_ZONE_DETAILS)>

<!-- timezone code like US-CA -->
<!ELEMENT TIME_ZONE_CODE (#PCDATA)>

<!-- timezone details like (GMT-0800) United States (California): Los
Angeles, Sacramento, San Diego, San Francisco-->
<!ELEMENT TIME_ZONE_DETAILS (#PCDATA)>

<!-- Did user select DST? 0-not selected 1-selected -->
<!ELEMENT DST_SELECTED (#PCDATA)>
<!ELEMENT MAX_OCCURRENCE (#PCDATA)>

<!-- notifications -->
<!ELEMENT NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?,
DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>

```

## XPaths for Scheduled Scan List Output

This section describes the XPaths for the scheduled scan list output (scheduled\_scan\_list\_output.dtd).

<b>XPath</b>	<b>element specifications / notes</b>
/SCHEDULE_SCAN_LIST_OUTPUT (REQUEST?, RESPONSE)	
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE	(DATETIME, SCHEDULE_SCAN_LIST?)
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST (SCAN+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN	(ID, SCAN_TYPE?, ACTIVE, TITLE?, USER_LOGIN, TARGET, NETWORK_ID?, ISCANNER_NAME?, EC2_INSTANCE?, CLOUD_DETAILS?, ASSET_GROUP_TITLE_LIST?, ASSET_TAGS?, EXCLUDE_IP_PER_SCAN?, USER_ENTERED_IPS?, OPTION_PROFILE?, PROCESSING_PRIORITY?, SCHEDULE, NOTIFICATIONS?)
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ID (#PCDATA)	The scan ID.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ACTIVE (#PCDATA)	1 for an active schedule, or 0 for a deactivated schedule.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/TITLE (#PCDATA)	The scan title.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/USER_LOGIN (#PCDATA)	The user login ID for the user who owns the scan schedule.

<b>XPath</b>	<b>element specifications / notes</b>
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/TARGET (#PCDATA)	The target hosts for the scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NETWORK_ID (#PCDATA)	The network ID for the target hosts, if custom networks are defined.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ISCANNER_NAME (#PCDATA)	The name of the scanner appliance used for the scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/EC2_INSTANCE (CONNECTOR_UUID, EC2_ENDPOINT, EC2_ONLY_CLASSIC?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/EC2_INSTANCE/CONNECTOR_UUID (#PCDATA)	The connector uuid for the AWS integration used for the EC2 scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/EC2_INSTANCE/EC2_ENDPOINT (#PCDATA)	The EC2 region code, or the ID of the Virtual Private Cloud (VPC) zone.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/EC2_INSTANCE/EC2_ONLY_CLASSIC (#PCDATA)	1 means the EC2 scan is configured to scan EC2 classic hosts in the region.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCAN_TYPE (#PCDATA)	For a CertView VM scan this is set to “CertView”.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS (PROVIDER, CONNECTOR, SCAN_TYPE, CLOUD_TARGET)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/PROVIDER (#PCDATA)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CONNECTOR (ID?, UUID, NAME)	Qualys connector ID used for scheduled scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CONNECTOR/ID (#PCDATA)	Qualys connector ID.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CONNECTOR/UUID (#PCDATA)	Qualys connector UUID.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CONNECTOR/NAME (#PCDATA)	Qualys connector user defined name.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/SCAN_TYPE (#PCDATA)	Set to “Internal” for an internal scan.

<b>XPath</b>	<b>element specifications / notes</b>
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/PLATFORM (#PCDATA)	The target cloud portal platform. For example AWS for Amazon Web Services.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/REGION (UUID, CODE?, NAME?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/REGION/UUID (#PCDATA)	The target cloud portal region UUID.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/REGION/CODE (#PCDATA)	The target cloud portal region code.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/REGION/NAME (#PCDATA)	The target cloud portal region name.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/VPC_SCOPE (#PCDATA)	The target cloud portal VPC scope: All, Selected or None.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/VPC_LIST (VPC+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/CLOUD_TARGET/VPC_LIST/VPC (#PCDATA)	The VPC ID in the target portal VPC list.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_GROUP_TITLE_LIST/ASSET_GROUP_TITLE (#PCDATA)	The asset group title specified for the scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS (TAG_INCLUDE_SELECTOR, TAG_SET_INCLUDE, TAG_EXCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, USE_IP_NT_RANGE_TAGS)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS/TAG_INCLUDE_SELECTOR (#PCDATA)	Include any of the selected tags (any) or all of the selected tags (all).
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS/TAG_SET_INCLUDE (#PCDATA)	Tag set to include from the scan target.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS/TAG_EXCLUDE_SELECTOR (#PCDATA)	Exclude any of the selected tags (any) or all of the selected tags (all).

XPath	element specifications / notes
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS/TAG_SET_EXCLUDE (#PCDATA)	Tag set to exclude from the scan target.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ASSET_TAGS/USE_IP_NT_RANGE_TAGS (#PCDATA)	0 means select from all tags (tags with any tag rule). 1 means scan all IP addresses defined in tags with the rule “IP address in Network Range(s)”.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/EXCLUDE_IP_PER_SCAN (#PCDATA)	When the scan target has excluded hosts, the target hosts that were excluded.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/USER_ENTERED_IPS (RANGE+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/RANGE (START, END)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/RANGE/START (#PCDATA)	When the scan target includes user entered IPs, the start of an IP range.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/RANGE/END (#PCDATA)	When the scan target includes user entered IPs, the end of an IP range.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/OPTION_PROFILE (TITLE, DEFAULT_FLAG?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/OPTION_PROFILE/TITLE (#PCDATA)	The option profile title specified for the scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/OPTION_PROFILE/DEFAULT_FLAG (#PCDATA)	A flag that specifies whether the option profile was defined as the default option profile in the user account. A value of 1 is returned when this option profile is the default. A value of 0 is returned when this option profile is not the default.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/PROCESSING_PRIORITY (#PCDATA)	(Applicable for VM scans only) The processing priority setting for the scan.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE ((DAILY WEEKLY MONTHLY), START_DATE_UTC, START_HOUR, START_MINUTE, END_AFTER_HOURS?, END_AFTER_MINUTES?, PAUSE_AFTER_HOURS?, PAUSE_AFTER_MINUTES?, RESUME_IN_DAYS?, RESUME_IN_HOURS?, NEXTLAUNCH_UTC?, TIME_ZONE, DST_SELECTED, MAX_OCCURRENCE?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /DAILY	attribute: <b>frequency_days</b> <b>frequency_days</b> is <i>required</i> for a scan that runs after some number of days (from 1 to 365)
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /WEEKLY	attribute: <b>frequency_weeks</b> <b>frequency_weeks</b> is <i>required</i> for a scan that runs after some number of weeks (from 1 to 52)

XPath	element specifications / notes
attribute: <b>weekdays</b>	<b>weekdays</b> is <i>required</i> for a scan that runs after some number of weeks on a particular weekday (from 0 to 6), where 0 is Sunday and 6 is Saturday, multiple weekdays are comma separated
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /MONTHLY	
attribute: <b>frequency_months</b>	<b>frequency_months</b> is <i>required</i> for a scan that runs after some number of months (from 1 to 12)
attribute: <b>day_of_month</b>	<b>day_of_month</b> is <i>implied</i> and, if present, indicates the scan runs on the Nth day of the month (from 1 to 31)
attribute: <b>day_of_week</b>	<b>day_of_week</b> is <i>implied</i> and, if present, indicates the scan runs on the Nth day of the month on a particular weekday (from 0 to 6), where 0 is Sunday and 6 is Saturday
attribute: <b>week_of_month</b>	<b>week_of_month</b> is <i>implied</i> and, if present, indicates the scan runs on the Nth day of the month on the Nth week of the month (from 1 to 5), where 1 is the first week of the month and 5 is the fifth week of the month
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /START_DATE_UTC (#PCDATA)	
The start date (in UTC format) defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /START_HOUR (#PCDATA)	
The start hour defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /START_MINUTE (#PCDATA)	
The start minute defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /END_AFTER_HOURS (#PCDATA)	
The “end after number of hours” setting defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /END_AFTER_MINUTES (#PCDATA)	
The “end after number of minutes” setting defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /PAUSE_AFTER_HOURS (#PCDATA)	
The “pause after number of hours” setting defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /PAUSE_AFTER_MINUTES (#PCDATA)	
The “pause after number of minutes” setting defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /RESUME_IN_DAYS (#PCDATA)	
The “resume in number of days” setting defined for the scan schedule.	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE /RESUME_IN_HOURS (#PCDATA)	
The “resume in number of hours” setting defined for the scan schedule.	



<b>XPath</b>	<b>element specifications / notes</b>
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / NEXTLAUNCH_UTC (#PCDATA)	The next launch date and time for the scan schedule.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / SCHEDULE/TIME_ZONE (TIME_ZONE_CODE, TIME_ZONE_DETAILS)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / TIME_ZONE/TIME_ZONE_CODE (#PCDATA)	The time zone code defined for the scan schedule. For example: US-CA.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / TIME_ZONE/TIME_ZONE_DETAILS (#PCDATA)	The time zone details (description) for the local time zone, identified in the <TIME_ZONE_CODE> element. For example:, (GMT-0800) United States (California): Los Angeles, Sacramento, San Diego, San Francisco.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / DST_SELECTED (#PCDATA)	When set to 1, Daylight Saving Time (DST) is enabled for the scan schedule.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/SCHEDULE / MAX_OCCURRENCE (#PCDATA)	The number of times the scan schedule will be run before it is deactivated (from 1 to 99).
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?, DISTRIBUTION_GROUPS?)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ BEFORE_LAUNCH (TIME, UNIT, MESSAGE)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ BEFORE_LAUNCH/TIME (#PCDATA)	The number of days, hours or minutes before the scan starts when the notification will be sent.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ BEFORE_LAUNCH/UNIT (#PCDATA)	The time unit (days, hours or minutes) set for the before scan notification.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ BEFORE_LAUNCH/MESSAGE (#PCDATA)	A user-provided custom message added to the before scan notification.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ AFTER_COMPLETE (MESSAGE)	A user-provided custom message added to the after scan notification.

XPath	element specifications / notes
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/DISTRIBUTION_GROUPS/DISTRIBUTION_GROUP (ID, TITLE)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/DISTRIBUTION_GROUPS/DISTRIBUTION_GROUP/ID (#PCDATA)	The ID of a distribution group that will receive notifications.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/DISTRIBUTION_GROUPS/DISTRIBUTION_GROUP/TITLE (#PCDATA)	The title of a distribution group that will receive notifications.

# Vulnerability Scan Results

The vulnerability scan results is returned from the download vulnerability scan results API call. Vulnerability scan results can be downloaded in these formats: CSV and JSON (JavaScript Object Notation).

**mode set to brief or extended** This information is returned:

Field	Description
IP	IP address.
DNS Name	DNS hostname when available.
Netbios Name	NetBIOS hostname when available.
QID	Qualys vulnerability ID (QID).
Result	Scan test result returned by the scanning engine.

**mode set to brief or extended** This information is returned:

Field	Description
Protocol	Protocol used to detect the vulnerability.
Port	Port used to detect the vulnerability.
SSL	A flag indicating whether SSL was used to detect the vulnerability: “yes” indicates SSL was used to detect the vulnerability, “no” indicates SSL was not used to detect the vulnerability.
FQDN	Fully qualified domain name for the host, when defined.

**output\_format set to json\_extended or csv\_extended** This information is returned:

Scan Summary section includes: company details (name, address), user details (name, login, role), scan date, number of active hosts, number of total hosts, scan type (On Demand or Scheduled), status, scan reference, scanner appliance, scan duration, scan title, asset groups, IPs, excluded IPs, and the option profile used.

Scan Results section includes: operating system, IP status, vulnerability title, type, severity, port, protocol, FQDN, SSL, CVE ID, vendor reference, Bugtraq ID, CVSS scores, threat, impact, solution, exploitability, associated malware, PCI vuln flag, OS CPE and category.

## Compliance Scan Results

The compliance scan results output XML is returned from an API request to fetch (download) a compliance scan using the PC scan API (/api/2.0/fo/scan/compliance/?action=fetch). The DTD can be found at the following URL (when your account is located on US Platform 1):

[https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/compliance\\_scan\\_result\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/compliance_scan_result_output.dtd)

### DTD for Compliance Scan Result Output

The PC scan results output DTD (compliance\_scan\_result\_output.dtd) is below.

```
<!ELEMENT COMPLIANCE_SCAN_RESULT_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)>
<!ATTLIST KEY
    value CDATA #IMPLIED
>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, COMPLIANCE_SCAN)>
<!ELEMENT COMPLIANCE_SCAN ((HEADER, ERROR?, AUTH_SCAN_ISSUES?,
                             APPENDIX)+)>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR
    number CDATA #IMPLIED
>
<!-- INFORMATION ABOUT THE SCAN -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO,
                  KEY+, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ELEMENT NAME (#PCDATA)*>
<!ELEMENT GENERATION_DATETIME (#PCDATA)*>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
```

```

<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)*>
<!ELEMENT ROLE (#PCDATA)*>

<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANNER) -->
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
<!ELEMENT AUTH_SCAN_ISSUES (AUTH_SCAN_FAILED*, AUTH_SCAN_INSUFFICIENT*)>
<!ELEMENT AUTH_SCAN_FAILED (HOST_INFO*)>
<!ELEMENT AUTH_SCAN_INSUFFICIENT (HOST_INFO*)>
<!ELEMENT HOST_INFO (DNS, IP, NETBIOS, INSTANCE, CAUSE)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>

<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?,
    AUTHENTICATION?)>
<!ELEMENT TARGET_HOSTS (HOSTS_SCANNED?, EXCLUDED_HOSTS?,
    HOSTS_NOT_ALIVE?, PAUSE_CANCEL_ACTION?,
    HOSTNAME_NOT_FOUND?, HOSTS_SCAN_ABORTED?)>
<!ELEMENT HOSTS_SCANNED (#PCDATA)>
<!ELEMENT HOSTNAME_NOT_FOUND (#PCDATA)>
<!ELEMENT EXCLUDED_HOSTS (#PCDATA)>
<!ELEMENT HOSTS_NOT_ALIVE (#PCDATA)>
<!ELEMENT HOSTS_SCAN_ABORTED (#PCDATA)>
<!ELEMENT PAUSE_CANCEL_ACTION (HOSTS, ACTION, BY)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT BY (#PCDATA)>

<!ELEMENT TARGET_DISTRIBUTION (SCANNER+)>
<!ELEMENT SCANNER (NAME, HOSTS)>
<!ELEMENT HOSTS (#PCDATA)>

<!ELEMENT AUTHENTICATION (AUTH+)>
<!ELEMENT AUTH (TYPE?, (FAILED | SUCCESS | INSUFFICIENT)+)>
<!ELEMENT TYPE (#PCDATA)>

```

```

<!ELEMENT FAILED (IP,INSTANCE?)>
<!ELEMENT SUCCESS (IP,INSTANCE?)>
<!ELEMENT INSUFFICIENT (IP,INSTANCE?)>
<!-- EOF -->

```

**XPaths for Compliance Scan Result Output**

This section describes the XPaths for the compliance scan results output.

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT (REQUEST?, RESPONSE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA)
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time the scan was launched.
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The login ID of the user who launched the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name.
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/COMPLIANCE_SCAN_RESULT_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE (DATETIME, COMPLIANCE_SCAN)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN	((HEADER, ERROR?, AUTH_SCAN_ISSUES?, APPENDIX)+)
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO, KEY+ ASSET_GROUPS?, OPTION PROFILE?)

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/NAME (#PCDATA)	The name of the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the scan was launched.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/NAME (#PCDATA)	The company name associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/ADDRESS (#PCDATA)	The street address associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/CITY (#PCDATA)	The city associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/STATE (#PCDATA)	The city associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/COUNTRY (#PCDATA)	The country associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/COMPANY_INFO/ZIP_CODE (#PCDATA)	The zip code associated with the account used to launch the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/USER_INFO (NAME, USERNAME, ROLE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/USER_INFO/NAME (#PCDATA)	The name of the user who launched the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/USER_INFO/USERNAME (#PCDATA)	The user login of the user who launched the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/USER_INFO/ROLE (#PCDATA)	The user role assigned to the user who launched the scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/ASSET_GROUPS /ASSET_GROUP_TITLE (#PCDATA)	The title of an asset group in the scan target.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	The title of the option profile used.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/ERROR (#PCDATA)	An error description.
attribute: number	An error number (implied)
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES (AUTH_SCAN_FAILED, AUTH_SCAN_INSUFFICIENT)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED (HOST_INFO)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO (DNS, IP, NETBIOS, INSTANCE, CAUSE)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO/DNS (#PCDATA)	The DNS name of a host that failed authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO/IP (#PCDATA)	The IP address of a host that failed authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO/NETBIOS (#PCDATA)	The NetBIOS hostname of a host that failed authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO/INSTANCE (#PCDATA)	The instance of a host that failed authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_FAILED/HOST_INFO/CAUSE (#PCDATA)	Additional information for a host that failed authentication. This may include the login ID used during the authentication attempt.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT (HOST_INFO)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO (DNS, IP, NETBIOS, INSTANCE, CAUSE)	



XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO/DNS (#PCDATA)	The DNS name of a host that failed authentication due to insufficient privileges.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO/IP (#PCDATA)	The IP address of a host that failed authentication due to insufficient privileges.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO/NETBIOS (#PCDATA)	The NetBIOS hostname of a host that failed authentication due to insufficient privileges.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO/INSTANCE (#PCDATA)	The instance of the host that failed authentication due to insufficient privileges..
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO/CAUSE (#PCDATA)	Additional information for a host that failed authentication due to insufficient privileges. This may include the login ID used during the authentication attempt.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?, AUTHENTICATION?)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS (HOSTS_SCANNED?, EXCLUDED_HOSTS?, HOSTS_NOT_ALIVE?, PAUSE_CANCEL_ACTION?, HOSTNAME_NOT_FOUND?, HOSTS_SCAN_ABORTED?)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/HOSTS_SCANNED (#PCDATA)	Target hosts that were scanned.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/EXCLUDED_HOSTS (#PCDATA)	Target hosts that were excluded from the scan target.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/HOSTS_NOT_ALIVE (#PCDATA)	Target hosts that were not alive.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/HOSTNAME_NOT_FOUND (#PCDATA)	Target hosts that were not found.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/HOSTS_SCAN_ABORTED (#PCDATA)	Target hosts on which the scan was aborted.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/PAUSE_CANCEL_ACTION (HOSTS, ACTION, BY)	

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/PAUSE_CANCEL_ACTION/HOSTS (#PCDATA)	The target hosts that an action (pause or cancel) was taken on.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/PAUSE_CANCEL_ACTION/ACTION (#PCDATA)	An action (pause or cancel) taken by a user on a scan.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_HOSTS/PAUSE_CANCEL_ACTION/BY (#PCDATA)	The user who took an action (pause or cancel).
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_DISTRIBUTION (SCANNER+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_DISTRIBUTION/SCANNER (NAME, HOSTS)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_DISTRIBUTION/SCANNER/NAME (#PCDATA)	The name of a scanner appliance used.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/TARGET_DISTRIBUTION/SCANNER/HOSTS (#PCDATA)	The compliance hosts that were scanned.

## VM Recrypt Results (Scan Statistics)

The VM Recrypt Results output is returned from a VM Scan Statistics API request. The DTD “vm\_recrypt\_results.dtd” can be found at the following URL:

[https://qualysapi.qualys.com/api/2.0/fo/scan/stats/vm\\_recrypt\\_results.dtd](https://qualysapi.qualys.com/api/2.0/fo/scan/stats/vm_recrypt_results.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

### DTD for VM Recrypt Results

A recent DTD (vm\_recrypt\_results.dtd) is shown below.

```
<!ELEMENT TASK_PROCESSING (UNPROCESSED_SCANS?, VM_RECRYPT_BACKLOG?,
VM_RECRYPT_BACKLOG_BY_SCAN?, VM_RECRYPT_BACKLOG_BY_TASK?)>

<!ELEMENT UNPROCESSED_SCANS (#PCDATA)>
<!ELEMENT VM_RECRYPT_BACKLOG (#PCDATA)>
<!ELEMENT VM_RECRYPT_BACKLOG_BY_SCAN (SCAN*)>
<!ELEMENT VM_RECRYPT_BACKLOG_BY_TASK (SCAN*)>

<!ELEMENT SCAN (ID?, TITLE?, STATUS?, PROCESSING_PRIORITY?, COUNT?,
NBHOST?, TO_PROCESS?, PROCESSED?, SCAN_DATE?, SCAN_UPDATED_DATE?,
TASK_TYPE?, TASK_STATUS?, TASK_UPDATED_DATE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT PROCESSING_PRIORITY (#PCDATA)>
<!ELEMENT COUNT (#PCDATA)>
<!ELEMENT NBHOST (#PCDATA)>
<!ELEMENT TO_PROCESS (#PCDATA)>
<!ELEMENT PROCESSED (#PCDATA)>
<!ELEMENT SCAN_DATE (#PCDATA)>
<!ELEMENT SCAN_UPDATED_DATE (#PCDATA)>
<!ELEMENT TASK_TYPE (#PCDATA)>
<!ELEMENT TASK_STATUS (#PCDATA)>
<!ELEMENT TASK_UPDATED_DATE (#PCDATA)>
```

# XPaths for VM Recrypt Results

This section describes the XPaths for VM Recrypt Results (vm\_recrypt\_results.dtd).

XPath	element specifications / notes
/TASK_PROCESSING	(UNPROCESSED_SCANS?, VM_RECRYPT_BACKLOG?, VM_RECRYPT_BACKLOG_BY_SCAN?, VM_RECRYPT_BACKLOG_BY_TASK?)
/TASK_PROCESSING/UNPROCESSED_SCANS (#PCDATA)	The total number of scans that are not processed, including scans that are queued, running, loading, finished, etc.
/TASK_PROCESSING/VM_RECRYPT_BACKLOG (#PCDATA)	The total number of assets across your finished scans that are waiting to be processed.
/TASK_PROCESSING/VM_RECRYPT_BACKLOG_BY_SCAN (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.
/TASK_PROCESSING/VM_RECRYPT_BACKLOG_BY_TASK (SCAN*)	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.
/TASK_PROCESSING/.../SCAN	(ID?, TITLE?, STATUS?, PROCESSING_PRIORITY?, COUNT?, NBHOST?, TO_PROCESS?, PROCESSED?, SCAN_DATE?, SCAN_UPDATED_DATE?, TASK_TYPE?, TASK_STATUS?, TASK_UPDATED_DATE?)
/TASK_PROCESSING/.../SCAN/ID (#PCDATA)	The scan ID.
/TASK_PROCESSING/.../SCAN/TITLE (#PCDATA)	The scan title.
/TASK_PROCESSING/.../SCAN/STATUS (#PCDATA)	The scan status.
/TASK_PROCESSING/.../SCAN/PROCESSING_PRIORITY (#PCDATA)	The processing priority setting for the scan.
/TASK_PROCESSING/.../SCAN/COUNT (#PCDATA)	The number of hosts that the scan finished but not processed.
/TASK_PROCESSING/.../SCAN/NBHOST (#PCDATA)	The number of total hosts alive for the scan.
/TASK_PROCESSING/.../SCAN/TO_PROCESS (#PCDATA)	The number of hosts waiting to be processed.

XPath	element specifications / notes
/TASK_PROCESSING/.../SCAN/PROCESSED (#PCDATA)	The number of hosts from the scan that have been processed.
/TASK_PROCESSING/.../SCAN/SCAN_DATE (#PCDATA)	The scan start date.
/TASK_PROCESSING/.../SCAN/SCAN_UPDATED_DATE (#PCDATA)	The scan updated date.
/TASK_PROCESSING/.../SCAN/TASK_TYPE (#PCDATA)	The task type “VM Scan Processing”.
/TASK_PROCESSING/.../SCAN/TASK_STATUS (#PCDATA)	The task processing status.
/TASK_PROCESSING/.../SCAN/TASK_UPDATED_DATE (#PCDATA)	The task updated date.

## PCI Scan Share Status Output

The PCI scan share status output is an XML report returned from an API request for the share status of a PCI scan that's already been shared with a PCI Merchant account.

The DTD “pci\_scan\_share\_status.dtd” can be found at the following URL:

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

where <qualysapi.qualys.com> is the API server URL where your account is located.

### DTD for PCI Scan Share Status Output

A recent DTD for the PCI scan share status output (pci\_scan\_share\_status.dtd) is shown below.

```
<!-- QUALYS PCI_SCAN_SHARE_STATUS DTD -->  
  
<!ELEMENT PCI_SCAN_SHARE_STATUS (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 (SCAN)>  
<!ELEMENT SCAN (MERCHANT_USERNAME, SCAN_REF, STATUS, LAST_SHARED)>  
<!ELEMENT MERCHANT_USERNAME (#PCDATA)>  
<!ELEMENT SCAN_REF (#PCDATA)>  
<!ELEMENT LAST_SHARED (#PCDATA)>  
<!ELEMENT STATUS (#PCDATA)>  
<!-- EOF -->
```

## XPaths for PCI Scan Share Status Output

This section describes the XPaths for the PCI scan share status output (pci\_scan\_share\_status.dtd).

XPath	element specifications / notes
/PCI_SCAN_SHARE_STATUS	(REQUEST?, RESPONSE)
/PCI_SCAN_SHARE_STATUS/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/PCI_SCAN_SHARE_STATUS/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/PCI_SCAN_SHARE_STATUS/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/PCI_SCAN_SHARE_STATUS/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/PCI_SCAN_SHARE_STATUS/REQUEST/PARAM_LIST (PARAM+)	
/PCI_SCAN_SHARE_STATUS/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/PCI_SCAN_SHARE_STATUS/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/PCI_SCAN_SHARE_STATUS/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/PCI_SCAN_SHARE_STATUS/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/PCI_SCAN_SHARE_STATUS/RESPONSE (SCAN)	
/PCI_SCAN_SHARE_STATUS/RESPONSE/SCAN	(MERCHANT_USERNAME, SCAN_REF, STATUS, LAST_SHARED)
/PCI_SCAN_SHARE_STATUS/RESPONSE/SCAN/MERCHANT_USERNAME (#PCDATA)	The user name for a target PCI Merchant account. This account is associated with a share PCI scan request.
/PCI_SCAN_SHARE_STATUS/RESPONSE/SCAN/SCAN_REF (#PCDATA)	The scan reference ID for the PCI scan associated. This PCI scan is associated with a share PCI scan request.
/PCI_SCAN_SHARE_STATUS/RESPONSE/SCAN/STATUS (#PCDATA)	The share status of a share PCI scan request for a PCI Merchant account and a PCI scan: Queued (request was received and sharing has not started yet), In Progress, Finished (request was successful and the scan was shared/exported to the PCI Merchant account successfully), or Error (request was not successful and the scan was not shared/exported).
/PCI_SCAN_SHARE_STATUS/RESPONSE/SCAN/LAST_SHARED (#PCDATA)	The most recent date and time of a share PCI scan request for a PCI Merchant account and a PCI scan.

# Map Report Output

The map report output XML is returned when you launch and then fetch a map report using the Report APIv2.

The DTD can be found at the following URL (where <baseURL> is the API server URL where your account is located):

[https://<baseURL>/map\\_report.dtd](https://<baseURL>/map_report.dtd)

## DTD for Map Report Output

A recent DTD is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS MAP REPORT DTD -->
<!ELEMENT MAPREPORT (HEADER, HOST_LIST)>
<!ELEMENT HEADER (DOMAIN, NETWORK?, USERNAME, REPORT_TEMPLATE,
REPORT_TITLE, RESTRICTED_IPS?, MAP_RESULT_LIST, NETWORK?)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT REPORT_TEMPLATE (#PCDATA)>
<!ELEMENT REPORT_TITLE (#PCDATA)>
<!ELEMENT RESTRICTED_IPS (#PCDATA)>
<!ELEMENT MAP_RESULT_LIST (MAP_RESULT+)>
<!ELEMENT MAP_RESULT (MAP_RESULT_TITLE, MAP_DATE, OPTION_PROFILE,
MAP_REFERENCE)>
<!ELEMENT MAP_RESULT_TITLE (#PCDATA)>
<!ELEMENT MAP_DATE (#PCDATA)>
<!ELEMENT OPTION_PROFILE (#PCDATA)>
<!ELEMENT MAP_REFERENCE (#PCDATA)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (IP, HOSTNAME, NETBIOS, ROUTER, OS, APPROVED?, SCANNABLE?,
IN_NETBLOCK?, LIVE?, DISCOVERY_LIST?, ASSET_GROUPS?,
AUTHENTICATION_RECORDS?, HOST_STATUS?, LAST_SCAN_DATE?)>
<!ELEMENT IP (#PCDATA)>
    <!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT HOSTNAME (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT ROUTER (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT APPROVED (#PCDATA)>
<!ELEMENT SCANNABLE (#PCDATA)>
<!ELEMENT IN_NETBLOCK (#PCDATA)>
<!ELEMENT LIVE (#PCDATA)>
<!ELEMENT DISCOVERY_LIST (DISCOVERY*)>
```



```

<!ELEMENT DISCOVERY (DISCOVERY_NAME*, PORT*)>
<!ELEMENT DISCOVERY_NAME (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT ASSET_GROUPS (AG_NAME*)>
<!ELEMENT AG_NAME (#PCDATA)>
<!ELEMENT AUTHENTICATION_RECORDS (AUTHENTICATION*)>
<!ELEMENT AUTHENTICATION (#PCDATA)>
<!ELEMENT HOST_STATUS (#PCDATA)>
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>

```

## XPaths for Map Report Output

This section describes the XPaths for map report output.

XPath	element specifications / notes
/MAPREPORT	(HEADER, HOST_LIST)
/MAPREPORT/HEADER	(DOMAIN, NETWORK?, USERNAME, REPORT_TEMPLATE, REPORT_TITLE, RESTRICTED_IPS?, MAP_RESULT_LIST, NETWORK?)
/MAPREPORT/HEADER/DOMAIN (#PCDATA)	Target domain name for the map report.
/MAPREPORT/HEADER/NETWORK (#PCDATA)	Target network if any for the map report.
/MAPREPORT/HEADER/USERNAME, (#PCDATA)	Username who fetched the map report.
/MAPREPORT/HEADER/REPORT_TEMPLATE (#PCDATA)	Report template used to run the map report.
/MAPREPORT/HEADER/REPORT_TITLE (#PCDATA)	Title of the map report.
/MAPREPORT/HEADER/RESTRICTED_IPS (#PCDATA)	IPs selected for inclusion in the map report.
/MAPREPORT/HEADER/MAP_RESULT_LIST (MAP_RESULT+)	
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT (MAP_RESULT+)	
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT (MAP_RESULT_TITLE, MAP_DATE, OPTION_PROFILE, MAP_REFERENCE)	
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT/MAP_RESULT_TITLE #PCDATA	Title of the map task/result.
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT/MAP_DATE (#PCDATA)	Date when the map was launched.
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT/OPTION_PROFILE (#PCDATA)	Option profile used to run the map.

<b>XPath</b>	<b>element specifications / notes</b>
/MAPREPORT/HEADER/MAP_RESULT_LIST/MAP_RESULT/MAP_REFERENCE (#PCDATA)	Map reference code.
/MAPREPORT/HOST_LIST (HOST+)	
/MAPREPORT/HOST_LIST/HOST	(IP, HOSTNAME, NETBIOS, ROUTER, OS, APPROVED?, SCANNABLE?, IN_NETBLOCK?, LIVE?, DISCOVERY_LIST?, ASSET_GROUPS?, AUTHENTICATION_RECORDS?, HOST_STATUS?, LAST_SCAN_DATE?)
/MAPREPORT/HOST_LIST/HOST/IP (#PCDATA)	IP address of host discovered.
attribute: network_id	The network ID of the discovered host if any.
/MAPREPORT/HOST_LIST/HOST/HOSTNAME (#PCDATA)	DNS hostname of host discovered if any.
/MAPREPORT/HOST_LIST/HOST/NETBIOS (#PCDATA)	NetBIOS hostname of host discovered if any.
/MAPREPORT/HOST_LIST/HOST/ROUTER (#PCDATA)	Router used to discover host.
/MAPREPORT/HOST_LIST/HOST/OS (#PCDATA)	Operating system detected on host.
/MAPREPORT/HOST_LIST/HOST/APPROVED (#PCDATA)	1 means the host was marked as approved host at the time of the map, and 0 means it was not marked as approved.
/MAPREPORT/HOST_LIST/HOST/SCANNABLE (#PCDATA)	1 means the host was marked as scannable since it was in your subscription at the time of the map, and 0 means it was not marked as scannable.
/MAPREPORT/HOST_LIST/HOST/IN_NETBLOCK (#PCDATA)	1 means the host was defined in a netblock within the map target, and 0 means it was not defined in a netblock.
/MAPREPORT/HOST_LIST/HOST/LIVE (#PCDATA)	1 means host was found to be alive (up and running), and 0 means it was found to be not alive.
/MAPREPORT/HOST_LIST/HOST/DISCOVERY_LIST (DISCOVERY*)	
/MAPREPORT/HOST_LIST/HOST/DISCOVERY_LIST/DISCOVERY (DISCOVERY_NAME*, PORT*)	
/MAPREPORT/HOST_LIST/HOST/DISCOVERY_LIST/DISCOVERY/DISCOVERY_NAME (#PCDATA)	The name of discovery.
/MAPREPORT/HOST_LIST/HOST/PORT (#PCDATA)	The port where discovery was made.
/MAPREPORT/HOST_LIST/HOST/ASSET_GROUPS (AG_NAME*)	
/MAPREPORT/HOST_LIST/HOST/ASSET_GROUPS/AG_NAME (#PCDATA)	The name of an asset group containing the host.

XPath	element specifications / notes
/MAPREPORT/HOST_LIST/HOST/AUTHENTICATION_RECORDS	(AUTHENTICATION*)
/MAPREPORT/HOST_LIST/HOST/AUTHENTICATION_RECORDS/AUTHENTICATION	(#PCDATA)
	The name of an authentication record containing the host.
/MAPREPORT/HOST_LIST/HOST/HOST_STATUS	(#PCDATA)
	The host status.
/MAPREPORT/HOST_LIST/HOST/LAST_SCAN_DATE	(#PCDATA)
	The last date the host was scanned.

## Network List

The network list XML output is returned from a network list API v2 request. The DTD can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

[https://qualysapi.qualys.com/network\\_list\\_output.dtd](https://qualysapi.qualys.com/network_list_output.dtd)

### DTD for Network List Output

A recent DTD for network list output (network\_list\_output.dtd) is below.

```

<!-- QUALYS NETWORK_LIST_OUTPUT DTD -->
<!ELEMENT NETWORK_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, NETWORK_LIST?)>
<!ELEMENT NETWORK_LIST (NETWORK+)>
<!ELEMENT NETWORK (ID, NAME, SCANNER_APPLIANCE_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCE_LIST (SCANNER_APPLIANCE+)>
<!ELEMENT SCANNER_APPLIANCE (ID, FRIENDLY_NAME)>
<!ELEMENT FRIENDLY_NAME (#PCDATA)>
<!-- EOF -->

```

### XPaths for Network List Output

This section describes the XPathS for network list output (network\_list\_output.dtd).

XPath	element specifications / notes
/NETWORK_LIST_OUTPUT	(REQUEST?, RESPONSE)
/NETWORK_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/NETWORK_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA)
	The date and time of the request.

XPath	element specifications / notes
/NETWORK_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/NETWORK_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/NETWORK_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/NETWORK_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/NETWORK_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/NETWORK_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/NETWORK_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data.
/NETWORK_LIST_OUTPUT/RESPONSE (DATETIME, NETWORK_LIST?)	
/NETWORK_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST (NETWORK+)	
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK (ID, NAME, SCANNER_APPLIANCE_LIST?)	
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/ID (#PCDATA)	The network ID.
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/NAME (#PCDATA)	The network name.
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/SCANNER_APPLIANCE_LIST (SCANNER_APPLIANCE+)	
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/SCANNER_APPLIANCE_LIST/SCANNER_APPLIANCE (ID, FRIENDLY_NAME)	
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/SCANNER_APPLIANCE_LIST/SCANNER_APPLIANCE/ID (#PCDATA)	The ID of a scanner appliance assigned to the network.
/NETWORK_LIST_OUTPUT/RESPONSE/NETWORK_LIST/NETWORK/SCANNER_APPLIANCE_LIST/SCANNER_APPLIANCE/FRIENDLY_NAME (#PCDATA)	The name of a scanner appliance assigned to the network.

# KnowledgeBase Output

The KnowledgeBase XML output provides information about vulnerabilities in the Qualys KnowledgeBase. The KnowledgeBase output is returned from a KnowledgeBase API request.

DTD:

[https://<baseurl>/api/2.0/fo/knowledge\\_base/vuln/knowledge\\_base\\_vuln\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd)

## DTD for KnowledgeBase Output

A recent DTD for the KnowledgeBase output is shown below.

```
<!-- QUALYS KNOWLEDGE_BASE_VULN_LIST_OUTPUT DTD -->
<!ELEMENT KNOWLEDGE_BASE_VULN_LIST_OUTPUT (REQUEST?,RESPONSE)>

  <!-- REQUEST -->
  <!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
    POST_DATA?)>
    <!-- DATETIME -->
    <!ELEMENT DATETIME (#PCDATA)>
    <!-- USER_LOGIN -->
    <!ELEMENT USER_LOGIN (#PCDATA)>
    <!-- RESOURCE -->
    <!ELEMENT RESOURCE (#PCDATA)>
    <!-- PARAM_LIST -->
    <!ELEMENT PARAM_LIST (PARAM+)>
      <!-- PARAM -->
      <!ELEMENT PARAM (KEY, VALUE)>
        <!-- KEY -->
        <!ELEMENT KEY (#PCDATA)>
        <!-- VALUE -->
        <!ELEMENT VALUE (#PCDATA)>
    <!-- if returned, POST_DATA will be urlencoded -->
    <!ELEMENT POST_DATA (#PCDATA)>

  <!-- RESPONSE -->
  <!ELEMENT RESPONSE (DATETIME, (VULN_LIST|ID_SET)?, WARNING?)>
    <!-- DATETIME already defined -->
    <!-- VULN_LIST -->
    <!ELEMENT VULN_LIST (VULN*)>
      <!-- VULN -->
      <!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY?,
        DETECTION_INFO?, LAST_CUSTOMIZATION?,
        LAST_SERVICE_MODIFICATION_DATETIME?,
        PUBLISHED_DATETIME, BUGTRAQ_LIST?, PATCHABLE,
        SOFTWARE_LIST?, VENDOR_REFERENCE_LIST?, CVE_LIST?,
        DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
        CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
        COMPLIANCE_LIST?, CORRELATION?, CVSS?, CVSS_V3?,
        PCI_FLAG?, AUTOMATIC_PCI_FAIL?, PCI_REASONS?,
        THREAT_INTELLIGENCE?, SUPPORTED_MODULES?,
        DISCOVERY, IS_DISABLED?, CHANGE_LOG_LIST? )>
        <!-- QID -->
        <!ELEMENT QID (#PCDATA)>
        <!-- VULN_TYPE -->
        <!ELEMENT VULN_TYPE (#PCDATA)>
        <!-- SEVERITY_LEVEL -->
        <!ELEMENT SEVERITY_LEVEL (#PCDATA)>
        <!-- TITLE -->
        <!ELEMENT TITLE (#PCDATA)>
```

```

<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT DETECTION_INFO (#PCDATA)>
<!ELEMENT LAST_CUSTOMIZATION (DATETIME, USER_LOGIN?)>
  <!-- USER_LOGIN already defined (no USER_LOGIN for OVAL Vulns) -
->

<!ELEMENT LAST_SERVICE_MODIFICATION_DATETIME (#PCDATA)>
<!ELEMENT PUBLISHED_DATETIME (#PCDATA)>
<!ELEMENT BUGTRAQ_LIST (BUGTRAQ+)>
  <!ELEMENT BUGTRAQ (ID, URL)>
    <!ELEMENT ID (#PCDATA)>
    <!ELEMENT URL (#PCDATA)>
<!ELEMENT PATCHABLE (#PCDATA)>
<!ELEMENT SOFTWARE_LIST (SOFTWARE+)>
  <!ELEMENT SOFTWARE (PRODUCT, VENDOR)>
    <!ELEMENT PRODUCT (#PCDATA)>
    <!ELEMENT VENDOR (#PCDATA)>
<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
  <!ELEMENT VENDOR_REFERENCE (ID, URL)>
<!ELEMENT CVE_LIST (CVE+)>
  <!ELEMENT CVE (ID, URL)>
  <!-- ID, URL already defined -->
<!ELEMENT DIAGNOSIS (#PCDATA)>
<!ELEMENT DIAGNOSIS_COMMENT (#PCDATA)>
<!ELEMENT CONSEQUENCE (#PCDATA)>
<!ELEMENT CONSEQUENCE_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>
<!ELEMENT COMPLIANCE_LIST (COMPLIANCE+)>
  <!ELEMENT COMPLIANCE (TYPE, SECTION, DESCRIPTION)>
    <!ELEMENT TYPE (#PCDATA)>
    <!ELEMENT SECTION (#PCDATA)>
    <!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT CORRELATION (EXPLOITS?, MALWARE?)>
  <!ELEMENT EXPLOITS (EXPLT_SRC+)>
    <!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
      <!ELEMENT SRC_NAME (#PCDATA)>
      <!ELEMENT EXPLT_LIST (EXPLT+)>
        <!ELEMENT EXPLT (REF, DESC, LINK?)>
          <!ELEMENT REF (#PCDATA)>
          <!ELEMENT DESC (#PCDATA)>
          <!ELEMENT LINK (#PCDATA)>
    <!ELEMENT MALWARE (MW_SRC+)>
      <!ELEMENT MW_SRC (SRC_NAME, MW_LIST)>
        <!ELEMENT MW_LIST (MW_INFO+)>
          <!ELEMENT MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?,
MW_ALIAS?, MW_RATING?, MW_LINK?)>
            <!ELEMENT MW_ID (#PCDATA)>
            <!ELEMENT MW_TYPE (#PCDATA)>
            <!ELEMENT MW_PLATFORM (#PCDATA)>

```

```
<!ELEMENT MW_ALIAS (#PCDATA)>
<!ELEMENT MW_RATING (#PCDATA)>
<!ELEMENT MW_LINK (#PCDATA)>
<!ELEMENT CVSS (BASE, TEMPORAL?, ACCESS?, IMPACT?,
AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
  <!ELEMENT BASE (#PCDATA)>
    <!ATTLIST BASE source CDATA #IMPLIED>
  <!ELEMENT TEMPORAL (#PCDATA)>
  <!ELEMENT ACCESS (VECTOR?, COMPLEXITY?)>
    <!ELEMENT VECTOR (#PCDATA)>
    <!ELEMENT COMPLEXITY (#PCDATA)>
  <!ELEMENT IMPACT (CONFIDENTIALITY?, INTEGRITY?, AVAILABILITY?)>
    <!ELEMENT CONFIDENTIALITY (#PCDATA)>
    <!ELEMENT INTEGRITY (#PCDATA)>
    <!ELEMENT AVAILABILITY (#PCDATA)>
  <!ELEMENT AUTHENTICATION (#PCDATA)>
  <!ELEMENT EXPLOITABILITY (#PCDATA)>
  <!ELEMENT REMEDIATION_LEVEL (#PCDATA)>
  <!ELEMENT REPORT_CONFIDENCE (#PCDATA)>
  <!ELEMENT CVSS_V3 (BASE, TEMPORAL?, ACCESS?, IMPACT?,
AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>

  <!ELEMENT PCI_FLAG (#PCDATA)>
  <!ELEMENT AUTOMATIC_PCI_FAIL (#PCDATA)>
  <!ELEMENT PCI_REASONS (PCI_REASON+)>
  <!ELEMENT PCI_REASON (#PCDATA)>
  <!ELEMENT THREAT_INTELLIGENCE (THREAT_INTEL+)>
  <!ELEMENT THREAT_INTEL (#PCDATA)>
  <!ATTLIST THREAT_INTEL
    id CDATA #REQUIRED>
  <!ELEMENT SUPPORTED_MODULES (#PCDATA)>

  <!ELEMENT DISCOVERY (REMOTE, AUTH_TYPE_LIST?, ADDITIONAL_INFO?)>
    <!ELEMENT REMOTE (#PCDATA)>
    <!ELEMENT AUTH_TYPE_LIST (AUTH_TYPE+)>
      <!ELEMENT AUTH_TYPE (#PCDATA)>
    <!ELEMENT ADDITIONAL_INFO (#PCDATA)>
  <!ELEMENT IS_DISABLED (#PCDATA)>
  <!ELEMENT CHANGE_LOG_LIST (CHANGE_LOG_INFO+)>
    <!ELEMENT CHANGE_LOG_INFO (CHANGE_DATE, COMMENTS)>
      <!ELEMENT CHANGE_DATE (#PCDATA)>
      <!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT ID_SET ((ID|ID_RANGE)+)>
  <!-- ID already defined -->
  <!ELEMENT ID_RANGE (#PCDATA)>
```



```
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
  <!ELEMENT CODE (#PCDATA)>
  <!ELEMENT TEXT (#PCDATA)>
  <!-- URL already defined -->

<!-- EOF -->
```

## XPaths for KnowledgeBase Output

This section describes the XPaths for the KnowledgeBase output.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT (REQUEST?, RESPONSE)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA? )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+))	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE))	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1.</b>
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE	(DATETIME, (VULN_LIST ID_SET)?, WARNING?)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST (VULN+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN	

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/QID (#PCDATA)	(QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY, LAST_CUSTOMIZATION?, LAST_SERVICE_MODIFICATION_DATETIME?, PUBLISHED_DATETIME, BUGTRAQ_LIST?, PATCHABLE, SOFTWARE_LIST?, VENDOR_REFERENCE_LIST?, CVE_LIST?, DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE_LIST?, CORRELATION?, CVSS?, CVSS_V3?, PCI_FLAG, AUTOMATIC_PCI_FAIL?, PCI_REASONS?, SUPPORTED_MODULES?, DISCOVERY, IS_DISABLED?, CHANGE_LOG_LIST?)
	The vulnerability QID (Qualys ID), assigned by the service.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VULN_TYPE (#PCDATA)	
	The vulnerability type: Vulnerability, Potential Vulnerability or Information Gathered. The type "Vulnerability or Potential Vulnerability" corresponds to the half red/half yellow icon in the QualyGuard user interface. If confirmed to exist on a host during a scan, the vulnerability is classified as a confirmed vulnerability in your account; if not the vulnerability is classified as a potential vulnerability in your account.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SEVERITY_LEVEL (#PCDATA)	
	The severity level of the vulnerability. A valid value for a confirmed or potential vulnerability is an integer 1 to 5, where 5 represents the most serious risk if exploited. A valid value for information gathered is a value 1 to 3, where 3 represents the most serious risk if exploited.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/TITLE (#PCDATA)	
	The vulnerability title.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CATEGORY (#PCDATA)	
	The vulnerability category.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/LAST_CUSTOMIZATION (DATETIME, USER_LOGIN)	
	The date this vulnerability was last customized by a user, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/LAST_SERVICE_MODIFIDATION_DATETIME (#PCDATA)	
	The date this vulnerability was last updated by the service, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PUBLISHED_DATETIME (#PCDATA)	
	The date this vulnerability was published by the service, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST (BUGTRAQ+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST/BUGTRAQ (ID, URL)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST/BUGTRAQ/ID (#PCDATA)	A Bugtraq ID for a vulnerability.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST/BUGTRAQ/URL (#PCDATA)	The URL to a Bugtraq ID.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PATCHABLE (#PCDATA)	A flag indicating whether there is a patch available to fix the vulnerability. The value 1 indicates a patch is available to fix the vulnerability. The value 0 indicates a patch is not available to fix the vulnerability.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOFTWARE_LIST (SOFTWARE+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOFTWARE_LIST/SOFTWARE (PRODUCT, VENDOR)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOFTWARE_LIST/SOFTWARE/PRODUCT (#PCDATA)	Software product information associated with the vulnerability. This information is provided by NIST as a part of CVE information. (This element appears only when the API request includes the parameter <b>details=All</b> .)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOFTWARE_LIST/SOFTWARE/VENDOR (#PCDATA)	Software vendor information associated with the vulnerability. This information is provided by NIST as a part of CVE information. (This element appears only when the API request includes the parameter <b>details=All</b> .)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST (VENDOR, REFERENCE+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST/VENDOR (ID, URL)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST/VENDOR/ID (#PCDATA)	A name of a vendor reference.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST/VENDOR/URL (#PCDATA)	The URL to a vendor reference.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVE (ID, URL)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVE/ID (#PCDATA)	A CVE name assigned to the vulnerability. CVE (Common Vulnerabilities and Exposures) is a list of common names for publicly known vulnerabilities and exposures. Through open and collaborative discussions, the CVE Editorial Board determines which vulnerabilities or exposures are included in CVE. If the CVE name starts with CAN (candidate) then it is under consideration for entry into CVE.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVE/URL (#PCDATA)	The URL to a CVE name.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ DIAGNOSIS (#PCDATA)	A service-provided description of the threat posed by the vulnerability if successfully exploited.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ DIAGNOSIS_COMMENT (#PCDATA)	A user-customized description of the threat posed by the vulnerability if successfully exploited.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CONSEQUENCE (#PCDATA)	A service-provided description of the consequences that may occur if this vulnerability is successfully exploited.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CONSEQUENCE_COMMENT (#PCDATA)	A user-customized description of the consequences that may occur if this vulnerability is successfully exploited.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ SOLUTION (#PCDATA)	A service-provided description of a verified solution to fix the vulnerability.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ SOLUTION_COMMENT (#PCDATA)	A user-customized description of a verified solution to fix the vulnerability.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ COMPLIANCE_LIST (COMPLIANCE+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ COMPLIANCE_LIST (TYPE, SECTION, DESCRIPTION)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ COMPLIANCE_LIST/TYPE (#PCDATA)	A type of a compliance information associated with the vulnerability: HIPAA, GLBA, CobIT or SOX.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/COMPLIANCE_LIST/SECTION (#PCDATA)	A section of a compliance policy or regulation.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/COMPLIANCE_LIST/DESCRIPTION (#PCDATA)	A description of a compliance policy or regulation.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION (EXPLOITS?, MALWARE?)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS (EXPL_SRC+)	The <EXPLOITS> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC (SRC_NAME, EXPLT_LIST)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/SRC_NAME (#PCDATA)	A name of a third party vendor or publicly available source whose exploitability information is correlated with the vulnerability.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/EXPLT_LIST (EXPLT+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	A CVE reference for the exploitability information.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	A description of the exploitability information provided by the source (third party vendor or publicly available source).
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPL_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	A link to the exploit for the vulnerability, when available from the source.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE (MW_SRC+)	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/SRC_NAME (#PCDATA)	The name of the source of the malware information: Trend Micro.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST (MW_INFO+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_ID (#PCDATA)	A malware name/ID assigned by Trend Micro.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_TYPE (#PCDATA)	A type of malware, such as Backdoor, Virus, Worm or Trojan.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_PLATFORM (#PCDATA)	A list of the platforms that may be affected.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_ALIAS (#PCDATA)	A list of other names used by different vendors and/or publicly available sources that refer to the same threat.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_RATING (#PCDATA)	An overall risk rating as determined by Trend Micro: Low, Medium or High.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/MALWARE/MW_SRC/MW_LIST/MW_INFO/MW_LINK (#PCDATA)	A link to malware details.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS (BASE, TEMPORAL?, ACCESS?, IMPACT?, AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?)	CVSS2 subelements for CVSS Sub Metrics appear only when the CVSS Scoring feature is turned on in the user's subscription and the API request includes the parameter <b>details=All.</b> )
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_BASE (#PCDATA)	CVSS base score assigned to the vulnerability.
attribute: <b>source</b>	<b>source</b> is <i>implied</i> and, if present, is "service" to indicate that the CVSS base score for the vulnerability is supplied by Qualys. The service displays a CVSS base score provided by NIST whenever available. In a case where NIST lists a CVSS base score of 0 or does not provide a score for a vulnerability in the NVD, the service determines whether the severity of the vulnerability warrants a higher CVSS base score.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/TEMPORAL (#PCDATA)	CVSS2 temporal score.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/ACCESS (VECTOR?, COMPLEXITY?)	

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/ACCESS/VECTOR (#PCDATA)	CVSS access vector metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/ACCESS/COMPLEXITY (#PCDATA)	CVSS access complexity metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/IMPACT (CONFIDENTIALITY?, INTEGRITY?, AVAILABILITY?)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/IMPACT/CONFIDENTIALITY (#PCDATA)	CVSS confidentiality impact metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/IMPACT/INTEGRITY (#PCDATA)	CVSS integrity impact metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/IMPACT/AVAILABILITY (#PCDATA)	CVSS availability impact metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/AUTHENTICATION (#PCDATA)	CVSS authentication metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/EXPLOITABILITY (#PCDATA)	CVSS exploitability metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/REMEDIATION_LEVEL (#PCDATA)	CVSS remediation level metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/REPORT_CONFIDENCE (#PCDATA)	CVSS report confidence metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS_V3	(BASE, TEMPORAL?, ACCESS?, IMPACT?, AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?)  CVSS3 subelements for CVSS Sub Metrics appear only when the CVSS Scoring feature is turned on in the user’s subscription and the API request includes the parameter <b>details=All</b> .)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ PCI_FLAG (#PCDATA)	A flag indicating whether the vulnerability must be fixed to pass PCI compliance. The value 1 indicates the vulnerability must be fixed to pass PCI compliance. The value 0 indicates the vulnerability does not need to be fixed to pass PCI compliance.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/AUTOMATIC_PCI_FAIL (#PCDATA)	This flag is for internal use only.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PCI_REASONS (PCI_REASON+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PCI_REASONS/PCI_REASON (#PCDATA)	A reason why the vulnerability passed or failed PCI compliance. This appears only when the CVSS Scoring feature is turned on in the user's subscription and the API request includes the parameter <b>show_pci_reasons=1</b> .
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SUPPORTED_MODULES (#PCDATA)	One or more Qualys modules that can be used to detect the vulnerability. This appears only when the API request includes the parameter <b>show_supported_modules_info=1</b> .
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY (REMOTE, AUTH_TYPE_LIST?)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/REMOTE (#PCDATA)	A flag indicating whether the discovery method is remotely detectable. The value 0 indicates the vulnerability cannot be detected remotely (authentication is required). The value 1 indicates the vulnerability can be detected in two ways: 1) remotely without using authentication, and 2) using authentication.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/AUTH_TYPE_LIST (AUTH_TYPE+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/AUTH_TYPE_LIST/AUTH_TYPE (#PCDATA)	An authentication type used to detect the vulnerability using trusted scanning.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/IS_DISABLED (#PCDATA)	A flag indicating whether the vulnerability is disabled. A value of 1 means it is disabled. A value of 0 means it is not disabled.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CHANGE_LOG_LIST (CHANGE_LOG_INFO+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CHANGE_LOG_LIST/CHANGE_LOG_INFO (CHANGE_DATE, COMMENTS)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CHANGE_LOG_LIST/CHANGE_LOG_INFO/CHANGE_DATE (#PCDATA)	The date of a QID change.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CHANGE_LOG_LIST/CHANGE_LOG_INFO/COMMENTS (#PCDATA)	Comments provided at the time of the QID change.



## CVSS Sub Metrics Mapping

A mapping of the CVSS sub metric values, as returned in the KnowledgeBase output, and the CVSS sub metric names, as defined by the CVSS standard, is provided below.

### Base Family

Metric Value	KnowledgeBase Output XML Element and Value
<b>Access Vector (AV)</b>	
Local (L)	<VECTOR>1</VECTOR>
Adjacent Network (A)	<VECTOR>2</VECTOR>
Network (N)	<VECTOR>3</VECTOR>
<b>Access Complexity</b>	
Low (L)	<COMPLEXITY>1</COMPLEXITY>
Medium (M)	<COMPLEXITY>2</COMPLEXITY>
High (H)	<COMPLEXITY>3</COMPLEXITY>
<b>Authentication (Au)</b>	
None (N)	<AUTHENTICATION>1</AUTHENTICATION>
Single (S)	<AUTHENTICATION>2</AUTHENTICATION>
Multiple (M)	<AUTHENTICATION>3</AUTHENTICATION>
<b>Confidentiality Impact (C)</b>	
None (N)	<CONFIDENTIALITY>1</CONFIDENTIALITY>
Partial (P)	<CONFIDENTIALITY>2</CONFIDENTIALITY>
Complete (C)	<CONFIDENTIALITY>3</CONFIDENTIALITY>
<b>Integrity Impact (I)</b>	
None (N)	<INTEGRITY>1</INTEGRITY>
Partial (P)	<INTEGRITY>2</INTEGRITY>
Complete (C)	<INTEGRITY>3</INTEGRITY>
<b>Availability Impact (A)</b>	
None (N)	<AVAILABILITY>1</AVAILABILITY>
Partial (P)	<AVAILABILITY>2</AVAILABILITY>
Complete (C)	<AVAILABILITY>3</AVAILABILITY>

**Temporal Metrics Family**

Metric Value	KnowledgeBase Download XML Element and Value
<b>Exploitability (E)</b>	
Unproven (U)	<EXPLOITABILITY>1</EXPLOITABILITY>
Proof-of-Concept (POC)	<EXPLOITABILITY>2</EXPLOITABILITY>
Functional (F)	<EXPLOITABILITY>3</EXPLOITABILITY>
High (H)	<EXPLOITABILITY>4</EXPLOITABILITY>
Not Defined (ND)	<EXPLOITABILITY>0</EXPLOITABILITY>
<b>Remediation Level (RL)</b>	
Official Fix (OF)	<REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
Temporary Fix (TF)	<REMEDIATION_LEVEL>2</REMEDIATION_LEVEL>
Workaround (W)	<REMEDIATION_LEVEL>3</REMEDIATION_LEVEL>
Unavailable (U)	<REMEDIATION_LEVEL>4</REMEDIATION_LEVEL>
Not Defined (ND)	<REMEDIATION_LEVEL>0</REMEDIATION_LEVEL>
<b>Report Confidence (RC)</b>	
Unconfirmed (UC)	<REPORT_CONFIDENCE>1</REPORT_CONFIDENCE>
Uncorroborated (UR)	<REPORT_CONFIDENCE>2</REPORT_CONFIDENCE>
Confirmed (C)	<REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>
Not Defined (ND)	<REPORT_CONFIDENCE>0</REPORT_CONFIDENCE>

# Customized Vulnerability List Output

The Customized Vulnerability List XML output provides information about vulnerabilities in the Qualys KnowledgeBase that have been edited.

DTD:

[https://<baseurl>/api/2.0/fo/knowledge\\_base/vuln/kb\\_custom\\_vuln\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_list_output.dtd)

## DTD for Vulnerability List Output

A recent DTD is shown below.

```
<!-- QUALYS KB_CUSTOM_VULN_LIST_OUTPUT DTD -->

<!ELEMENT KB_CUSTOM_VULN_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, (CUSTOM_VULN_LIST)?, WARNING?)>
<!-- DATETIME already defined -->
<!ELEMENT CUSTOM_VULN_LIST (CUSTOM_VULN_DATA*)>
<!ELEMENT CUSTOM_VULN_DATA (QID, SEVERITY_LEVEL, ORIGINAL_SEVERITY_LEVEL,
IS_DISABLED, UPDATED_DATETIME, UPDATED_BY, THREAT_COMMENT?,
IMPACT_COMMENT?, SOLUTION_COMMENT?)>

<!ELEMENT QID (#PCDATA)>
<!ELEMENT ORIGINAL_SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT UPDATED_DATETIME (#PCDATA)>
<!ELEMENT THREAT_COMMENT (#PCDATA)>
<!ELEMENT IMPACT_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT UPDATED_BY (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
```

```
<!ELEMENT URL (#PCDATA)>
<!-- URL already defined -->
<!-- EOF -->
```

## XPaths for Vulnerability List Output

This section describes the XPaths.

XPath	element specifications / notes
/KB_CUSTOM_VULN_LIST_OUTPUT (REQUEST?, RESPONSE)	
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. (This element appears only when the API request includes the parameter <b>echo_request=1</b> .)
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The Qualys login ID of the user who made the request. (This element appears only when the API request includes the parameter <b>echo_request=1</b> .)
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. (This element appears only when the API request includes the parameter <b>echo_request=1</b> .)
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. (This element appears only when the API request includes the parameter <b>echo_request=1</b> .)
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/KB_CUSTOM_VULN_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. (This element appears only when the API request includes the parameter <b>echo_request=1</b> .)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE	(DATETIME, (CUSTOM_VULN_LIST)?, WARNING?)
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/CUSTOM_VULN_LIST (CUSTOM_VULN_DATA*)	

XPath	element specifications / notes
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA	(QID, SEVERITY_LEVEL, ORIGINAL_SEVERITY_LEVEL, IS_DISABLED, UPDATED_DATETIME, UPDATED_BY, THREAT_COMMENT?, IMPACT_COMMENT?, SOLUTION_COMMENT?)
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/QID (#PCDATA)	The vulnerability QID assigned by Qualys.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/SEVERITY_LEVEL (#PCDATA)	The severity level of the vulnerability. For a confirmed or potential vulnerability this is an integer 1 to 5, where 5 represents the most serious risk if exploited. For information gathered is an integer 1 to 3, where 3 represents the most serious risk.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/ORIGINAL_SEVERITY_LEVEL (#PCDATA)	The original severity level of the vulnerability. See SEVERITY_LEVEL above.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/IS_DISABLED (#PCDATA)	A flag indicating whether the vulnerability is disabled. A value of 1 means it is disabled. A value of 0 means it is not disabled.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/UPDATED_DATETIME (#PCDATA)	The date this vulnerability was last edited by a user, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/UPDATED_BY (#PCDATA)	The Qualys login ID of the user who last edited the vulnerability.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/THREAT_COMMENT (#PCDATA)	A user-customized description of the threat the vulnerability poses.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/IMPACT_COMMENT (#PCDATA)	A user-customized description of the impact of the vulnerability if exploited
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/CUSTOM_VULN_DATA/SOLUTION_COMMENT (#PCDATA)	A user-customized description of a verified solution to fix the vulnerability.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/WARNING (CODE?, TEXT, URL?)	
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	A warning code.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	Warning message text.
/KB_CUSTOM_VULN_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	Warning URL. This element will not be returned (it is not implemented).

## Asset XML

This appendix describes the XML output returned from API V2 requests for host and IP address data using the Asset API functions.

- IP List Output
- Host List Output
- Host List VM Detection Output
- Excluded Hosts List Output
- Excluded Hosts Change History Output
- Virtual Host List Output
- IPv6 Mapping Records List Output
- Restricted IPs List Output
- Duplicate Hosts Error Output
- Asset Group List Output
- Asset Search Report

# IP List Output

The IP list output identifies IP addresses in the user account. The IP list XML is returned from a IP list API request.

The DTD can be found at the following URL (where <baseurl> is the API server URL where your account is located):

[https://<baseurl>/api/2.0/fo/asset/ip/ip\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/asset/ip/ip_list_output.dtd)

## DTD for IP List Output

A recent DTD for the IP list output is shown below.

```
<!-- QUALYS IP_OUTPUT DTD -->
<!ELEMENT IP_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, IP_SET?)>

<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!-- EOF -->
```

**XPaths for IP List Output**

This section describes the XPaths for the IP list output.

XPath	element specifications / notes
/IP_LIST_OUTPUT	(REQUEST?, RESPONSE)
/IP_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST, POST_DATA?)
/IP_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/IP_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login of the user who made the request.
/IP_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/IP_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/IP_LIST_OUTPUT/RESPONSE	(DATETIME, IP_SET)
/IP_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the Qualys response.
/IP_LIST_OUTPUT/RESPONSE/IP_SET	((IP   IP_RANGE)+)
/IP_LIST_OUTPUT/RESPONSE/IP_SET/IP	(#PCDATA) An IP address.
/IP_LIST_OUTPUT/RESPONSE/IP_SET/IP_RANGE	(#PCDATA) An IP address range.



# Host List Output

The host list XML output provides information about hosts in the user account that have been scanned. The host list output is returned from a host list API request.

The DTD can be found at the following URL where `<baseurl>` is the API server URL where your account is located):

`https://<baseurl>/api/2.0/fo/asset/host/host_list_output.dtd`

## DTD for Host List Output

A recent DTD for the host list output is shown below.

```
<!-- QUALYS HOST_OUTPUT DTD -->

<!ELEMENT HOST_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, (HOST_LIST|ID_SET)?, WARNING?, GLOSSARY?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, IP?, TRACKING_METHOD?, NETWORK_ID?,
DNS?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?, TAGS?, METADATA?,
LAST_VULN_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?,
LAST_VM_AUTH_SCANNED_DURATION?, LAST_COMPLIANCE_SCAN_DATETIME?, OWNER?,
COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
```

```

<!ELEMENT TAGS (TAG*)>
<!ELEMENT TAG (TAG_ID?, NAME?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT LAST_VULN_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT USER_DEF (LABEL_1?, LABEL_2?, LABEL_3?, VALUE_1?, VALUE_2?,
VALUE_3?)>
<!ELEMENT LABEL_1 (#PCDATA)>
<!ELEMENT LABEL_2 (#PCDATA)>
<!ELEMENT LABEL_3 (#PCDATA)>
<!ELEMENT VALUE_1 (#PCDATA)>
<!ELEMENT VALUE_2 (#PCDATA)>
<!ELEMENT VALUE_3 (#PCDATA)>

<!ELEMENT METADATA (EC2|GOOGLE|AZURE)+>
<!ELEMENT EC2 (ATTRIBUTE*)>
<!ELEMENT GOOGLE (ATTRIBUTE*)>
<!ELEMENT AZURE (ATTRIBUTE*)>
<!ELEMENT ATTRIBUTE
(NAME, LAST_STATUS, VALUE, LAST_SUCCESS_DATE?, LAST_ERROR_DATE?, LAST_ERROR?)>
<!ELEMENT LAST_STATUS (#PCDATA)>
<!ELEMENT LAST_SUCCESS_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR (#PCDATA)>

<!ELEMENT ASSET_GROUP_IDS (#PCDATA)>

<!ELEMENT ID_SET ((ID|ID_RANGE)+)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT GLOSSARY (USER_DEF?, USER_LIST?, ASSET_GROUP_LIST?)>

<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

```

```
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, TITLE)>
<!ELEMENT TITLE (#PCDATA)>
<!-- EOF -->
```

## XPaths for Host List Output

This section describes the XPaths for the host list output.

XPath	element specifications / notes
/HOST_OUTPUT	(REQUEST?,RESPONSE)
/HOST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/HOST_OUTPUT/REQUEST/DATETIME	(#PCDATA)  The date and time of the API request.
/HOST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA)  The user login ID of the user who made the request.
/HOST_OUTPUT/REQUEST/RESOURCE	(#PCDATA)  The resource specified for the request.
/HOST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+))
/HOST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/HOST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA)  An input parameter name.
/HOST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA)  An input parameter value.
/HOST_OUTPUT/REQUEST/POST_DATA	(#PCDATA)  The POST data, if any.
/HOST_OUTPUT/RESPONSE	(DATETIME, (HOST_LIST ID_SET)?, WARNING?, GLOSSARY?)
/HOST_OUTPUT/RESPONSE/DATETIME	(#PCDATA)  The date and time of the Qualys response.
/HOST_OUTPUT/RESPONSE/HOST_LIST	(HOST+)
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST	(ID, IP?, TRACKING_METHOD?, NETWORK_ID?, DNS?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?, TAGS?, METADATA?, LAST_VULN_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?, LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?, LAST_VM_AUTH_SCANNED_DURATION?, LAST_COMPLIANCE_SCAN_DATETIME?, OWNER?, COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)  The HOST element is returned when the “details” input parameter is set to “basic” or “all” or if the parameter is unspecified.

<b>XPath</b>	<b>element specifications / notes</b>
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/ID (#PCDATA)	The host ID.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/IP (#PCDATA)	The asset's IP address.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The tracking method assigned to the asset: IP, DNS, NETBIOS, EC2.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/NETWORK_ID (#PCDATA)	The network ID of the asset, if the Networks feature is enabled.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS (#PCDATA)	DNS name for the asset. For an EC2 asset this is the private DNS name.
/HOST_OUTPUT/RESPONSE/HOST_LIST/EC2_INSTANCE_ID (#PCDATA)	EC2 instance ID for the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/NETBIOS (#PCDATA)	NetBIOS host name for the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/OS (#PCDATA)	Operating system detected on the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/QG_HOSTID (#PCDATA)	The Qualys host ID assigned to the asset when Agentless Tracking is used or when a cloud agent is installed.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS (TAG_ID?, NAME?)	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG_ID (#PCDATA)	A tag ID associated with the asset when show_tags=1 is specified.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/NAME (#PCDATA)	A tag name associated with the asset when show_tags=1 is specified.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA (EC2 GOOGLE AZURE)+	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 (ATTRIBUTE*)	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/GOOGLE (ATTRIBUTE*)	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/AZURE (ATTRIBUTE*)	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE (NAME, LAST_STATUS, VALUE, LAST_SUCCESS_DATE?, LAST_ERROR_DATE?, LAST_ERROR?)	
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/ NAME (#PCDATA)	Attribute name, fetched from instance metadata.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/ LAST_STATUS (#PCDATA)	Attribute last status, fetched from instance metadata.

XPath	element specifications / notes
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/VALUE (#PCDATA)	Attribute value fetched, from instance metadata.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_SUCCESS_DATE (#PCDATA)	Attribute last success date/time, fetched from instance metadata.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_ERROR_DATE (#PCDATA)	Attribute last error date/time, fetched from instance metadata.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_ERROR (#PCDATA)	Attribute last error, fetched from instance metadata.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VULN_SCAN_DATETIME (#PCDATA)	The date and time of the most recent vulnerability scan.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_SCANNED_DATE (#PCDATA)	The scan end date/time for the most recent unauthenticated vulnerability scan on the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_SCANNED_DURATION (#PCDATA)	The scan duration (in seconds) for the most recent unauthenticated vulnerability scan on the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_AUTH_SCANNED_DATE (#PCDATA)	The scan end date/time for the last successful authenticated vulnerability scan on the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)	The scan duration (in seconds) for the last successful authenticated vulnerability scan on the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)	The date and time of the most recent compliance scan.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/OWNER (#PCDATA)	The asset owner.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/COMMENTS (#PCDATA)	The comments defined for the asset.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/USER_DEF	(LABEL_1?, LABEL_2?, LABEL_3?, VALUE_1?, VALUE_2?, VALUE_3?) A set of host attributes assigned to the host. Three user-defined attributes are defined for the subscription.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/USER_DEF/LABEL_n (#PCDATA)	Not returned inside the <HOST> element. Returned inside <GLOSSARY>.

<b>XPath</b>	<b>element specifications / notes</b>
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/USER_DEF/VALUE_n (#PCDATA)	A host attribute value. Three elements are returned, one element for each of the three values. The elements are: <VALUE_1>, <VALUE_2> and <VALUE_3>.
/HOST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_GROUP_IDS (#PCDATA)	The asset group IDs for the asset groups which the host belongs to.
/HOST_OUTPUT/RESPONSE/ID_SET ((ID ID_RANGE)+)	The ID_SET element is returned when the “details” input parameter is set to “none”.
/HOST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	A host ID.
/HOST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	A host ID range.
/HOST_OUTPUT/RESPONSE/WARNING (CODE?, TEXT, URL?)	
/HOST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	The warning code. This code appears when the API request identifies more than 1,000 records (hosts) or the custom truncation limit.
/HOST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	The warning message text. This message appears when the API request identifies more than 1,000 records (hosts) or the custom truncation limit.
/HOST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL for making another request for the next batch of host records.
/HOST_OUTPUT/RESPONSE/GLOSSARY (USER_DEF?, USER_LIST?, ASSET_GROUP_LIST?)	
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_DEF (#PCDATA)	(LABEL_1?, LABEL_2?, LABEL_3?, VALUE_1?, VALUE_2?, VALUE_3?)  A set of host attributes assigned to the host. Three user-defined attributes are defined for the subscription.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_DEF/LABEL_n (#PCDATA)	A host attribute label, as defined for the subscription. When the default labels are used the elements are: <LABEL_1>Location, <LABEL_2>Function and <LABEL_3>Asset Tag. The labels may be customized within Qualys.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_DEF/VALUE_n (#PCDATA)	Not returned inside the <GLOSSARY> element. Returned inside <HOST>.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST (USER+)	A list of users who are asset owners for the hosts in the host list output.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER (USER_LOGIN, FIRST_NAME, LAST_NAME)	A user who is an asset owner for a host in the host list output.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER_LOGIN (#PCDATA)	A user login ID.
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER/FIRST_NAME (#PCDATA)	A user’s first name.

XPath	element specifications / notes
/HOST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/LAST_NAME	A user's last name.
/HOST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST (ASSET_GROUP+)	A list of asset groups which hosts in the host list output belong to.
/HOST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP (ID, TITLE)	
/HOST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP/ID	An asset group ID.
/HOST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP/TITLE	An asset group title.

## Host List VM Detection Output

The host list detection XML output provides information about VM scanned hosts in the user account, including “automatic” data. The host list detection output is returned from a host list detection API request.

The DTD can be found at the following URL (where <baseurl> is the API server URL where your account is located):

```
https://<baseurl>/api/2.0/fo/asset/host/vm/detection/host_list_
vm_detection_output.dtd
```

## DTD for Host List VM Detection Output

A recent DTD for the host list detection output is shown below.

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT HOST_LIST_VM_DETECTION_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, HOST_LIST?, WARNING?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?,
                OS?, OS_CPE?, DNS?, EC2_INSTANCE_ID?, NETBIOS?, QG_HOSTID?,
                LAST_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
                LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?,
                LAST_VM_AUTH_SCANNED_DURATION?, LAST_PC_SCANNED_DATE?,
                TAGS?, METADATA?, DETECTION_LIST)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
```



```

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_PC_SCANNED_DATE (#PCDATA)>
<!ELEMENT TAGS (TAG+)>
<!ELEMENT TAG (TAG_ID?, NAME, COLOR?, BACKGROUND_COLOR?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COLOR (#PCDATA)>
<!ELEMENT BACKGROUND_COLOR (#PCDATA)>
<!ELEMENT METADATA (EC2|GOOGLE|AZURE)+>
<!ELEMENT EC2 (ATTRIBUTE*)>
<!ELEMENT GOOGLE (ATTRIBUTE*)>
<!ELEMENT AZURE (ATTRIBUTE*)>
<!ELEMENT ATTRIBUTE
(NAME, LAST_STATUS, VALUE, LAST_SUCCESS_DATE?, LAST_ERROR_DATE?, LAST_ERROR?)>
<!ELEMENT LAST_STATUS (#PCDATA)>
<!ELEMENT LAST_SUCCESS_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR (#PCDATA)>
<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?,
    INSTANCE?,
    RESULTS?, STATUS?,
    FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?,
    TIMES_FOUND?,
    LAST_TEST_DATETIME?,
    LAST_UPDATE_DATETIME?,
    LAST_FIXED_DATETIME?,
    FIRST_REOPENED_DATETIME?, LAST_REOPENED_DATETIME?,
    TIMES_REOPENED?,
    SERVICE?, IS_IGNORED?, IS_DISABLED?,
    AFFECT_RUNNING_KERNEL?, AFFECT_RUNNING_SERVICE?,
    AFFECT_EXPLOITABLE_CONFIG?,
    LAST_PROCESSED_DATETIME? )>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT RESULTS (#PCDATA)>

```

```

<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT LAST_TEST_DATETIME (#PCDATA)>
<!ELEMENT LAST_UPDATE_DATETIME (#PCDATA)>
<!ELEMENT LAST_FIXED_DATETIME (#PCDATA)>
<!ELEMENT FIRST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT LAST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT IS_IGNORED (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_KERNEL (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_SERVICE (#PCDATA)>
<!ELEMENT AFFECT_EXPLOITABLE_CONFIG (#PCDATA)>
<!ELEMENT LAST_PROCESSED_DATETIME (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->

```

**XPaths for Host List VM Detection Output**

This section describes the XPaths for the host list detection output.

XPath	element specifications / notes
/HOST_LIST_VM_DETECTION_OUTPUT	(REQUEST?,RESPONSE)
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request.
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE))	
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name.

<b>XPath</b>	<b>element specifications / notes</b>
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/HOST_LIST_VM_DETECTION_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE	(DATETIME, HOST_LIST?, WARNING?)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST (HOST+)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST	(ID, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?, OS?, OS_CPE?, DNS?, EC2_INSTANCE_ID?, NETBIOS?, QG_HOSTID?, LAST_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?, LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?, LAST_VM_AUTH_SCANNED_DURATION?, LAST_PC_SCANNED_DATE?, TAGS?, METADATA?, DETECTION_LIST)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/ID (#PCDATA)	Host ID for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/IP (#PCDATA)	IPv4 address for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/IPV6 (#PCDATA)	IPv6 address for the asset. This appears only if the IPv6 feature is enabled for the subscription.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The tracking method assigned to the asset: IP, DNS, NETBIOS, EC2.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/OS (#PCDATA)	The operating system detected on the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/OS_CPE (#PCDATA)	The OS CPE name assigned to the operating system detected on the asset. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS (#PCDATA)	DNS name for the asset. For an EC2 asset this is the private DNS name.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/EC2_INSTANCE_ID (#PCDATA)	EC2 instance ID for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/NETBIOS (#PCDATA)	NetBIOS name for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/QG_HOSTID (#PCDATA)	The Qualys host ID assigned to the asset when Agentless Tracking is used or when a cloud agent is installed.

<b>XPath</b>	<b>element specifications / notes</b>
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_SCAN_DATETIME (#PCDATA)	The date and time of the most recent vulnerability scan of the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_SCANNED_DATE (#PCDATA)	The scan end date/time for the most recent unauthenticated vulnerability scan of the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_SCANNED_DURATION (#PCDATA)	The scan duration (in seconds) for the most recent unauthenticated vulnerability scan of the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_AUTH_SCANNED_DATE (#PCDATA)	The scan end date/time for the last successful authenticated vulnerability scan of the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)	The scan duration (in seconds) for the last successful authenticated vulnerability scan of the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_PC_SCANNED_DATE (#PCDATA)	The scan end date/time for the most recent compliance scan on the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS (TAG+)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG (TAG_ID?, NAME, COLOR?, BACKGROUND_COLOR?)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG/TAG_ID (#PCDATA)	The ID of a tag associated with the asset when show_tags=1 is specified.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG/NAME (#PCDATA)	The name of a tag associated with the asset when show_tags=1 is specified.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG/COLOR (#PCDATA)	The color of a tag associated with the asset when show_tags=1 is specified.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG/BACKGROUND_COLOR (#PCDATA)	The background color of a tag associated with the asset when show_tags=1 is specified.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA (EC2 GOOGLE AZURE)+	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE (ATTRIBUTE*)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE	(NAME, LAST_STATUS, VALUE, LAST_SUCCESS_DATE?, LAST_ERROR_DATE?, LAST_ERROR?)

## XPath

## element specifications / notes

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/NAME (#PCDATA)

Attribute name, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/LAST\_STATUS (#PCDATA)

Attribute last status, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/VALUE (#PCDATA)

Attribute value, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/LAST\_SUCCESS\_DATE (#PCDATA)

Attribute last success date/time, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/LAST\_ERROR\_DATE (#PCDATA)

Attribute last error date/time, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/METADATA/  
EC2|GOOGLE|AZURE/ATTRIBUTE/LAST\_ERROR (#PCDATA)

Attribute last error, fetched from instance metadata.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST (DETECTION+)

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION  
(QID,TYPE,SEVERITY?,PORT?,PROTOCOL?,FQDN?,SSL?,INSTANCE?,  
RESULTS?,STATUS?,FIRST\_FOUND\_DATETIME?,  
LAST\_FOUND\_DATETIME?,TIMES\_FOUND?,  
LAST\_TEST\_DATETIME?,LAST\_UPDATE\_DATETIME?,  
LAST\_FIXED\_DATETIME?,FIRST\_REOPENED\_DATETIME?,  
LAST\_REOPENED\_DATETIME?,TIMES\_REOPENED?,SERVICE?,  
IS\_IGNORED?,IS\_DISABLED?,AFFECT\_RUNNING\_KERNEL?,  
AFFECT\_RUNNING\_SERVICE?,AFFECT\_EXPLOITABLE\_CONFIG?,  
LAST\_PROCESSED\_DATETIME?)

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/  
DETECTION/QID (#PCDATA)

The QID for the vulnerability in the detection record.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/  
DETECTION/TYPE (#PCDATA)

The type of vulnerability in the detection record: Confirmed for a confirmed vulnerability, Potential for a potential vulnerability, and Info for an information gathered.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/  
DETECTION/SEVERITY (#PCDATA)

The severity of the vulnerability.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/  
DETECTION/PORT (#PCDATA)

The port number that the vulnerability was detected on.

<b>XPath</b>	<b>element specifications / notes</b>
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/PROTOCOL (#PCDATA)	The protocol the vulnerability was detected on.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/FQDN (#PCDATA)	The Fully Qualified Domain Name (FQDN) of the host.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/SSL (#PCDATA)	The value 1 is returned if the vulnerability was detected over SSL. The value 0 is returned if the vulnerability was not detected over SSL. This element is not returned for information gathered.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/INSTANCE (#PCDATA)	The Oracle DB instance the vulnerability was detected on.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/RESULTS (#PCDATA)	The scan test results, if any, returned by the service for the detection record.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/STATUS (#PCDATA)	The current vulnerability status of the vulnerability in the detection record.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/FIRST_FOUND_DATETIME (#PCDATA)	The date/time when the vulnerability was first found.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/LAST_FOUND_DATETIME (#PCDATA)	The most recent date/time when the vulnerability was found.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/TIMES_FOUND (#PCDATA)	The number of times the vulnerability was detected on the host.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/LAST_TEST_DATETIME (#PCDATA)	The most recent date/time when the vulnerability was tested.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/LAST_UPDATE_DATETIME (#PCDATA)	The most recent date/time when the detection record was updated.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/LAST_FIXED_DATETIME (#PCDATA)	The date/time when the vulnerability was verified fixed by a scan.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/FIRST_REOPENED_DATETIME (#PCDATA)	The date/time when the vulnerability was reopened by a scan.

**XPath**

**element specifications / notes**

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/LAST\_REOPENED\_DATETIME (#PCDATA)

The date/time when the vulnerability was last reopened by a scan.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/TIMES\_REOPENED (#PCDATA)

The number of times the vulnerability was reopened by a scan.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/SERVICE (#PCDATA)

The service the vulnerability was detected on, if applicable.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/IS\_IGNORED (#PCDATA)

A flag indicating whether the vulnerability is ignored for the particular host. A value of 1 means it is ignored, a value of 0 means it is not ignored.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/IS\_DISABLED (#PCDATA)

A flag indicating whether the vulnerability is globally disabled for all hosts. A value of 1 means it is disabled, a value of 0 means it is not disabled.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/AFFECT\_RUNNING\_KERNEL (#PCDATA)

A flag identifying vulnerabilities found on running or non-running Linux kernels. A value of 1 indicates that the QID is exploitable because it was found on a running kernel. A value of 0 indicates that it is not exploitable because it was found on a non-running kernel. This element is returned only if the API request includes the parameter `arf_kernel_filter` set to 0, 1, 2, 3 or 4 or `active_kernels_only` set to 0, 1, 2 or 3.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/AFFECT\_RUNNING\_SERVICE (#PCDATA)

A flag identifying vulnerabilities found on running or non-running services. A value of 1 indicates that the QID is exploitable because it was found on a running port/service. A value of 0 indicates that it is not exploitable because it was found on a non-running port/service. This element is returned only if the API request includes the parameter `arf_service_filter` set to 0, 1, 2, 3 or 4.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/AFFECT\_EXPLOITABLE\_CONFIG (#PCDATA)

A flag identifying vulnerabilities that may or may not be exploitable due to the current host configuration. A value of 1 indicates that the QID is exploitable due to the current host configuration. A value of 0 indicates that it is not exploitable due to the current host configuration. This element is returned only if the API request includes the parameter `arf_config_filter` set to 0, 1, 2, 3 or 4.

/HOST\_LIST\_VM\_DETECTION\_OUTPUT/RESPONSE/HOST\_LIST/HOST/DETECTION\_LIST/DETECTION/LAST\_PROCESSED\_DATETIME (#PCDATA)

The date/time when the detection was last processed.

XPath	element specifications / notes
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/WARNING	(CODE?, TEXT, URL?)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/WARNING/CODE	(#PCDATA)
	The warning code. This code appears when the API request identifies more than 1,000 host records.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/WARNING/TEXT	(#PCDATA)
	The warning message text. This message appears when the API request identifies more than 1,000 host records.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/WARNING/URL	(#PCDATA)
	The URL for making another request for the next batch of host records.



# Excluded Hosts List Output

The excluded hosts list XML output provides information about excluded hosts in the user's account. The excluded host list output is returned from an excluded host list API request.

The DTD can be found at the following URL (where `<baseurl>` is the API server URL where your account is located):

```
https://<baseurl>/api/2.0/fo/asset/excluded_ip/
ip_list_output.dtd
```

## DTD for Excluded Host List Output

A recent DTD for the excluded hosts list output is shown below.

```
<!-- QUALYS IP_OUTPUT DTD -->

<!ELEMENT IP_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, IP_SET?)>

<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ATTLIST IP expiration_date CDATA #IMPLIED>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE
  network_id CDATA #IMPLIED
  expiration_date CDATA #IMPLIED
>
<!-- EOF -->
```

**XPaths for Excluded Hosts List Output**

This section describes the XPaths for the excluded hosts list output.

XPath	element specifications / notes
/IP_LIST_OUTPUT	(REQUEST?, RESPONSE)
/IP_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST, POST_DATA?)
/IP_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/IP_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login of the user who made the request.
/IP_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/IP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/IP_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/IP_LIST_OUTPUT/RESPONSE	(DATETIME, IP_SET)
/IP_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the Qualys response.
/IP_LIST_OUTPUT/RESPONSE/IP_SET	((IP IP_RANGE)+)
/IP_LIST_OUTPUT/RESPONSE/IP_SET/IP	(#PCDATA) An IP address, identifying an excluded host. If the Networks feature is enabled in your subscription, the attribute “network_id” is the network ID associated with this IP address. If an expiration date was specified when this IP was added to the list, the attribute “expiration_date” is the date when the IP will be removed from the list.
/IP_LIST_OUTPUT/RESPONSE/IP_SET/IP_RANGE	(#PCDATA) An IP address range, identifying excluded hosts. If the Networks feature is enabled in your subscription, the attribute “network_id” is the network ID associated with this IP range. If an expiration date was specified when this IP range was added to the list, the attribute “expiration_date” is the date when the IP range will be removed from the list.

# Excluded Hosts Change History Output

The excluded hosts change history XML output provides information about excluded hosts change history in the user's account. The excluded host change history output is returned from an excluded host change history API request.

The DTD can be found at the following URL (where `<baseurl>` is the API server URL where your account is located):

`https://<baseurl>/api/2.0/fo/asset/excluded_ip/history/history_list_output.dtd`

## DTD for Excluded Host Change History Output

A recent DTD for the excluded hosts change history output is shown below.

```
<!-- QUALYS HISTORY_LIST_OUTPUT DTD -->

<!ELEMENT HISTORY_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, HISTORY_LIST?, WARNING?, GLOSSARY?)>
<!ELEMENT HISTORY_LIST (HISTORY+)>
<!ELEMENT HISTORY (ID, IP_SET, ACTION, DATETIME, USER_LOGIN, COMMENTS)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
```

```

<!ELEMENT GLOSSARY (USER_LIST)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME, ROLE)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>
<!-- EOF -->

```

**XPaths for Excluded Hosts Change History Output**

This section describes the XPaths for the excluded hosts change history output.

XPath	element specifications / notes
/HISTORY_LIST_OUTPUT	(REQUEST?, RESPONSE)
/HISTORY_LIST_OUTPUT /REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST, POST_DATA?)
/HISTORY_LIST_OUTPUT /REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/HISTORY_LIST_OUTPUT /REQUEST/USER_LOGIN	(#PCDATA) The user login of the user who made the request.
/HISTORY_LIST_OUTPUT /REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/HISTORY_LIST_OUTPUT /REQUEST/PARAM_LIST	(PARAM+)
/HISTORY_LIST_OUTPUT /REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/HISTORY_LIST_OUTPUT /REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/HISTORY_LIST_OUTPUT /REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/HISTORY_LIST_OUTPUT /REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/HISTORY_LIST_OUTPUT/RESPONSE	(DATETIME, HISTORY_LIST? WARNING?, GLOSSARY?)
/HISTORY_LIST_OUTPUT/RESPONSE /DATETIME	(#PCDATA) The date and time of the Qualys response.
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST	(HISTORY+)
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY	(ID, IP_SET, ACTION, DATETIME, USER_LOGIN, COMMENTS))
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/ID	(#PCDATA) An ID for an excluded hosts change history record.

**XPath**

**element specifications / notes**

/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/IP_SET ((IP, IP_RANGE)+)	
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/IP_SET/IP (#PCDATA)	An IP address range, identifying excluded hosts.
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/IP_SET/RANGE (#PCDATA)	An IP address range, identifying excluded hosts.
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/ACTION (#PCDATA)	An action associated with the change: Added for added excluded hosts, or Removed for removed excluded hosts.
/HISTORY_LIST_OUTPUT/RESPONSE /HISTORY_LIST/HISTORY/COMMENTS (#PCDATA)	User comments entered during the action associated with excluded hosts.
/HISTORY_LIST_OUTPUT /RESPONSE/WARNING (CODE?, TEXT, URL?)	
/HISTORY_LIST_OUTPUT /RESPONSE/WARNING/CODE (#PCDATA)	The warning code. This code appears when the API request identifies more than 1,000 excluded hosts change history records.
/HISTORY_LIST_OUTPUT /RESPONSE/WARNING/TEXT (#PCDATA)	The warning message text. This message appears when the API request identifies more than 1,000 excluded hosts change history records.
/HISTORY_LIST_OUTPUT /RESPONSE/WARNING/TEXT/URL (#PCDATA)	The URL for making another request for the next batch of excluded hosts change history records. The URL includes the “id_max” parameter for change history records with an ID less than or equal to a specified ID.
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY (USER_LIST)	
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY/USER_LIST (USER+)	
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY/USER_LIST/USER (USER_LOGIN, FIRST_NAME, LAST_NAME, ROLE)	
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY/USER_LIST/USER/FIRST_NAME (#PCDATA)	The first name of a user who performed an action on excluded hosts included in the XML output.
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY/USER_LIST/USER/LAST_NAME (#PCDATA)	The last name of a user who performed an action on excluded hosts included in the XML output.
/HISTORY_LIST_OUTPUT /RESPONSE/GLOSSARY/USER_LIST/USER/ROLE (#PCDATA)	The role of a user who performed an action on excluded hosts included in the XML output.

## Virtual Host List Output

The virtual host list output identifies virtual hosts in the user account.

The DTD can be found at the following URL (where <baseurl> is the API server URL where your account is located):

[https://<baseurl>/api/2.0/fo/asset/vhost/vhost\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/asset/vhost/vhost_list_output.dtd)

### DTD for Virtual Host List Output

A recent DTD for the virtual host list output is shown below.

```
<!-- QUALYS VIRTUAL_HOST_OUTPUT DTD -->

<!ELEMENT VIRTUAL_HOST_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, (VIRTUAL_HOST_LIST)?, WARNING?)>
<!ELEMENT VIRTUAL_HOST_LIST (VIRTUAL_HOST+)>
<!ELEMENT VIRTUAL_HOST (IP, PORT, FQDN+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
```

## XPaths for Virtual Host List Output

This section describes the XPaths for the virtual host list output.

XPath	element specifications / notes
/VIRTUAL_HOST_LIST_OUTPUT (REQUEST?,RESPONSE)	
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA? )
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+))	
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE))	
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE	(DATETIME, (VIRTUAL_HOST_LIST)?, WARNING?)
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/VIRTUAL_HOST_LIST (VIRTUAL_HOST+)	
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/VIRTUAL_HOST_LIST/VIRTUAL_HOST	(IP, PORT, FQDN+)
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/VIRTUAL_HOST_LIST/VIRTUAL_HOST/IP (#PCDATA)	The IP address for the virtual host configuration.
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/VIRTUAL_HOST_LIST/VIRTUAL_HOST/PORT (#PCDATA)	The port for the virtual host configuration.
/VIRTUAL_HOST_LIST_OUTPUT/RESPONSE/VIRTUAL_HOST_LIST/VIRTUAL_HOST/FQDN (#PCDATA)	One FQDN for the virtual host configuration.

## IPv6 Mapping Records List Output

The IPv6 mapping records list output identifies IPv6 mapping records in the subscription.

The DTD can be found at the following URL (where <baseurl> is the API server URL where your account is located):

[https://<baseurl>/api/2.0/fo/asset/ip/v4\\_v6/ip\\_map\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/asset/ip/v4_v6/ip_map_list_output.dtd)

### DTD for IPv6 Mapping Records List Output

A recent DTD for the IPv6 mapping records list output is shown below.

```
<!-- QUALYS IP_MAP_LIST_OUTPUT DTD -->

<!ELEMENT IP_MAP_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, IP_MAP_LIST?)>

<!ELEMENT IP_MAP_LIST (IP_MAP+)>
<!ELEMENT IP_MAP (ID, V4, V6, NETWORK_ID?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT V4 (#PCDATA)>
<!ELEMENT V6 (#PCDATA)>

<!-- EOF -->
```



## XPaths for IPv6 Mapping Records List Output

This section describes the XPaths for the IPv6 mapping records list output.

XPath	element specifications / notes
/IP_MAP_LIST_OUTPUT	(REQUEST?,RESPONSE)
/IP_MAP_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/IP_MAP_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/IP_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/IP_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/IP_MAP_LIST_OUTPUT/RESPONSE (DATETIME, IP_MAP_LIST?)	
/IP_MAP_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/IP_MAP_LIST_OUTPUT/RESPONSE/IP_MAP_LIST_LIST (IP_MAP+)	
/IP_MAP_LIST_OUTPUT/RESPONSE/IP_MAP_LIST_LIST/IP_MAP (ID, V4, V6)	
/IP_MAP_LIST_OUTPUT/RESPONSE/IP_MAP_LIST_LIST/IP_MAP/ID (#PCDATA)	A service-assigned ID for a mapping record.
/IP_MAP_LIST_OUTPUT/RESPONSE/IP_MAP_LIST_LIST/IP_MAP/V4 (#PCDATA)	An IPv4 address for a mapping record.
/IP_MAP_LIST_OUTPUT/RESPONSE/IP_MAP_LIST_LIST/IP_MAP/V6 (#PCDATA)	An IPv6 address for a mapping record.

## Restricted IPs List Output

The DTD for the restricted IPs list output can be found at the following URL (where `<baseurl>` is the API server URL where your account is located):

`https://qualysapi.qualys.com/api/2.0/fo/setup/restricted\_ips/restricted\_ips\_output.dtd`

### DTD for Restricted IPs List Output

A recent DTD for the restricted IPs list output is shown below.

```
<!-- QUALYS RESTRICTED_IPS_OUTPUT DTD -->

<!ELEMENT RESTRICTED_IPS_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, IP_SET?, STATUS?)>

<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!-- EOF -->
```

## XPaths for Restricted IPs List Output

This section describes the XPaths for the restricted IPs list output.

XPath	element specifications / notes
/RESTRICTED_IPS_OUTPUT	(REQUEST?,RESPONSE)
/RESTRICTED_IPS_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/RESTRICTED_IPS_OUTPUT/REQUEST/DATETIME	(#PCDATA)  The date and time of the API request to download the restricted IPs list. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA)  The user login ID of the user who made the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/REQUEST/RESOURCE	(#PCDATA)  The resource specified for the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/RESTRICTED_IPS_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/RESTRICTED_IPS_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA)  An input parameter name. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA)  An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/REQUEST/POST_DATA	(#PCDATA)  The POST data, if any. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/RESTRICTED_IPS_OUTPUT/RESPONSE	(DATETIME, IP_SET?, STATUS?)
/RESTRICTED_IPS_OUTPUT/RESPONSE/DATETIME	(#PCDATA)  The date and time of the Qualys response.
/RESTRICTED_IPS_OUTPUT/RESPONSE/IP_SET	((IP IP_RANGE)+)
/RESTRICTED_IPS_OUTPUT/RESPONSE/IP_SET/IP	(#PCDATA)  An IP address in the restricted IPs list.
/RESTRICTED_IPS_OUTPUT/RESPONSE/IP_SET/IP_RANGE	(#PCDATA)  An IP address range in the restricted IPs list.
/RESTRICTED_IPS_OUTPUT/RESPONSE/STATUS	(#PCDATA)  The status of the restricted IPs list: enabled or disabled. When enabled a user who attempts to log in to Qualys from an IP in the restricted IPs list will be denied access.

## Duplicate Hosts Error Output

Duplicate hosts error is returned with instructions in cases where you try to update hosts with multiple scan data entries using the IP Update API. This can happen when scans identified multiple hostnames for the same IP address.

### DTD for Duplicate Hosts Error Output

A recent DTD is shown below.

```
<!-- QUALYS DUPLICATE_HOSTS_ERROR_OUTPUT DTD -->

<!ELEMENT DUPLICATE_HOSTS_ERROR_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 (CODE?, DATETIME, WARNING?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT WARNING (TEXT, DUPLICATE_HOSTS, URL)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT DUPLICATE_HOSTS (DUPLICATE_HOST*)>

<!ELEMENT DUPLICATE_HOST (IP, DNS_HOSTNAME, NETBIOS_HOSTNAME,
                          LAST_SCANDATE, TRACKING)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS_HOSTNAME (#PCDATA)>
<!ELEMENT NETBIOS_HOSTNAME (#PCDATA)>
<!ELEMENT LAST_SCANDATE (#PCDATA)>
<!ELEMENT TRACKING (#PCDATA)>

<!-- EOF -->
```

## XPaths for Duplicate Hosts Error Output

This section describes the XPaths.

XPath	element specifications / notes
/DUPLICATE_HOSTS_ERROR_OUTPUT (REQUEST?,RESPONSE)	
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request to download the restricted IPs list. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/PARAM_LIST (PARAM+))	
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE))	
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE (CODE?, DATETIME, WARNING?)	
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/CODE (#PCDATA)	Qualys response code.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/WARNING (TEXT, DUPLICATE_HOSTS, URL)	
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	A warning description with instructions on how to resolve the issue.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/WARNING/DUPLICATE_HOSTS (DUPLICATE_HOST*)	
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST	(IP, DNS_HOSTNAME, NETBIOS_HOSTNAME, LAST_SCANDATE, TRACKING)

XPath	element specifications / notes
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST/ IP (#PCDATA)	The IP address of the duplicate asset.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST/ DNS_HOSTNAME (#PCDATA)	The DNS name of the duplicate asset.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST/ NETBIOS_HOSTNAME (#PCDATA)	The NetBIOS hostname of the duplicate asset.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST/ LAST_SCANDATE (#PCDATA)	The date/time when the duplicate asset was last scanned.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/DUPLICATE_HOSTS /HOST/ TRACKING (#PCDATA)	The tracking method of the duplicate asset: IP, DNS, NETBIOS, EC2.
/DUPLICATE_HOSTS_ERROR_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL to use to log in to the Qualys Cloud Platform where you can edit the duplicate asset per the warning instructions provided.

# Asset Group List Output

The DTD for the asset group list output can be found at the following URL (where `<baseurl>` is the API server URL where your account is located):

`https://<baseurl>/api/2.0/fo/asset/group/asset_group_list_output.dtd`

## DTD for Asset Group List Output

A recent DTD for the asset group list output is below.

```
<!-- QUALYS ASSET_GROUP_LIST_OUTPUT DTD -->

<!ELEMENT ASSET_GROUP_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, (ASSET_GROUP_LIST|ID_SET)?, WARNING?)>
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT ASSET_GROUP (ID, TITLE?,
    OWNER_USER_ID?, OWNER_UNIT_ID?, (NETWORK_ID|NETWORK_IDS)?,
    LAST_UPDATE?, BUSINESS_IMPACT?,
    CVSS_ENVIRO_CDP?, CVSS_ENVIRO_TD?, CVSS_ENVIRO_CR?, CVSS_ENVIRO_IR?,
    CVSS_ENVIRO_AR?,
    DEFAULT_APPLIANCE_ID?, APPLIANCE_IDS?,
    IP_SET?, DOMAIN_LIST?, DNS_LIST?, NETBIOS_LIST?,
    HOST_IDS?, EC2_IDS?,
    ASSIGNED_USER_IDS?, ASSIGNED_UNIT_IDS?, COMMENTS?
)>

<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT OWNER_USER_ID (#PCDATA)>
<!ELEMENT OWNER_UNIT_ID (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
```

```
<!ELEMENT NETWORK_IDS (#PCDATA)>
<!ELEMENT LAST_UPDATE (#PCDATA)>
<!ELEMENT BUSINESS_IMPACT (#PCDATA)>

<!-- CVSS -->
<!ELEMENT CVSS_ENVIRO_CDP (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_TD (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_CR (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_IR (#PCDATA)>
<!ELEMENT CVSS_ENVIRO_AR (#PCDATA)>

<!-- APPLIANCE_LIST -->
<!ELEMENT DEFAULT_APPLIANCE_ID (#PCDATA)>
<!ELEMENT APPLIANCE_IDS (#PCDATA)>

<!-- IP_SET -->
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE network_id CDATA #IMPLIED>

<!-- DOMAIN_LIST -->
<!ELEMENT DOMAIN_LIST (DOMAIN+)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ATTLIST DOMAIN netblock CDATA ">
<!ATTLIST DOMAIN network_id CDATA #IMPLIED>

<!-- DNS_LIST -->
<!ELEMENT DNS_LIST (DNS+)>
<!ELEMENT DNS (#PCDATA)>
<!ATTLIST DNS network_id CDATA "0">

<!-- NETBIOS_LIST -->
<!ELEMENT NETBIOS_LIST (NETBIOS+)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ATTLIST NETBIOS network_id CDATA "0">

<!-- EC2_IDS -->
<!ELEMENT EC2_IDS (#PCDATA)>

<!-- HOST_IDS -->
<!ELEMENT HOST_IDS (#PCDATA)>

<!-- USER_IDS -->
<!ELEMENT ASSIGNED_USER_IDS (#PCDATA)>

<!-- UNIT_IDS -->
<!ELEMENT ASSIGNED_UNIT_IDS (#PCDATA)>
```



```
<!-- COMMENTS -->
<!ELEMENT COMMENTS (#PCDATA)>

<!-- WARNING -->
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
```

## XPaths for Asset Group List Output

This section describes the XPaths for the asset group list output.

XPath	element specifications / notes
/ASSET_GROUP_LIST_OUTPUT (REQUEST?,RESPONSE)	
/ASSET_GROUP_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/ASSET_GROUP_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/ASSET_GROUP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/ASSET_GROUP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter <b>echo_request=1</b> .
/ASSET_GROUP_LIST_OUTPUT/RESPONSE (DATETIME, (ASSET_GROUP_LIST ID_SET)?, WARNING?)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.

XPath	element specifications / notes
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST (ASSET_GROUP+)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP (ID, TITLE?, OWNER_USER_ID?, OWNER_UNIT_ID?, (NETWORK_ID NETWORK_IDS)?, LAST_UPDATE?, BUSINESS_IMPACT?, CVSS_ENVIRO_CDP?, CVSS_ENVIRO_TD?, CVSS_ENVIRO_CR?, CVSS_ENVIRO_IR?, CVSS_ENVIRO_AR?, DEFAULT_APPLIANCE_ID?, APPLIANCE_IDS?, IP_SET?, DOMAIN_LIST?, DNS_LIST?, NETBIOS_LIST?, HOST_IDS?, EC2_IDS?, ASSIGNED_USER_IDS?, ASSIGNED_UNIT_IDS?, COMMENTS?)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ID_SET (ID ID_RANGE)+	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	The ID of included asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	The ID range of included asset groups.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/TITLE (#PCDATA)	The title of the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/OWNER_USER_ID (#PCDATA)	The ID of the asset group's owner.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/OWNER_UNIT_ID (#PCDATA)	The business unit ID of the asset group's owner.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/NETWORK_ID (#PCDATA)	(Appears only if the Networks feature is enabled for your subscription) The asset group will be assigned to a custom network ID or 0 (the Global Default Network).
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/NETWORK_IDS(#PCDATA)	(Appears only if the Networks feature is enabled for your subscription) This element lists custom network IDs that include the All asset group. Have multiple All asset groups? Yes you might. There is 1 All group for the subscription, and 1 All group for each custom business unit.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/ LAST_UPDATE (#PCDATA)	The date/time the asset group was last updated.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/ BUSINESS_IMPACT (#PCDATA)	The business impact assigned to the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/CVSS<value> (#PCDATA)	The CVSS environmental metrics assigned to the asset group. CVSS_ENVIRO_CDP (Collateral Damage Potential) CVSS_ENVIRO_TD (Target Distribution) CVSS_ENVIRO_CR (Confidentiality Requirement) CVSS_ENVIRO_IR (Integrity Requirement) CVSS_ENVIRO_AR (Availability Requirement)

XPath	element specifications / notes
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/DEFAULT_APPLIANCE_ID (#PCDATA)	The ID of the asset group's default scanner appliance.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/APPLIANCE_IDS (#PCDATA)	The IDs of the scanner appliances assigned to the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/IP_SET (IP IP_RANGE)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/IP_SET/IP (#PCDATA)	An IP address assigned to the asset group. If the Networks feature is enabled in your subscription, the attribute "network_id" is the network ID associated with this IP address.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/IP_SET/IP_RANGE (#PCDATA)	An IP address range assigned to the asset group. If the Networks feature is enabled in your subscription, the attribute "network_id" is the network ID associated with this IP range.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/DOMAIN_LIST (DOMAIN+)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/DOMAIN_LIST/DOMAIN (#PCDATA)	A domain assigned to the asset group. The attribute "netblock" is the netblock assigned to this domain, if any. If the Networks feature is enabled in your subscription, the attribute "network_id" is the network ID associated with this IP address.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/DNS_LIST (DNS+)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/DNS_LIST/DNS (#PCDATA)	A DNS name assigned to the asset group. If the Networks feature is enabled in your subscription, the attribute "network_id" is the network ID associated with the DNS host.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/NETBIOS_LIST (NETBIOS+)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/NETBIOS_LIST/NETBIOS (#PCDATA)	A NetBIOS name assigned to the asset group. If the Networks feature is enabled in your subscription, the attribute "network_id" is the network ID associated with the NetBIOS host.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/EC2_IDS (#PCDATA)	EC2 IDs associated with the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/HOST_IDS (#PCDATA)	The host IDs associated with the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/EC2_IDS (#PCDATA)	The EC2 instance IDs associated with the asset group.

<b>XPath</b>	<b>element specifications / notes</b>
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_USER_IDS (#PCDATA)	The asset group is visible to users with these user IDs.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/ASSIGNED_UNIT_IDS (#PCDATA)	The asset group is assigned to business units with these unit IDs.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/ASSET_GROUP_LIST/ASSET_GROUP/COMMENTS (#PCDATA)	User defined comments for the asset group.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/WARNING (CODE?, TEXT, URL?)	
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	The warning code. This code appears when the API request finds more than 1,000 asset group records.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	The warning message text. This message appears when the API request finds more than 1,000 asset group records.
/ASSET_GROUP_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL for making another request for the next batch of asset group records.

# Asset Search Report

The DTD for the asset search report output can be found at the following URL (where `<base_url>` is the API server base URL where your account is located):

`https://<base_url>/asset_search_report_v2.dtd`

## DTD for Asset Search Report

A recent DTD for asset search report output is below.

```
<!-- QUALYS ASSET SEARCH REPORT DTD -->

<!ELEMENT ASSET_SEARCH_REPORT (ERROR | (HEADER, HOST_LIST?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- HEADER -->

<!ELEMENT HEADER (REQUEST?, COMPANY, USERNAME, GENERATION_DATETIME,
TOTAL?, FILTERS)>

<!-- REQUEST Header -->
<!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 COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT FILTERS
((IP_LIST|ASSET_GROUPS|ASSET_TAGS|FILTER_DNS|FILTER_NETBIOS|
TRACKING_METHOD|FILTER_OPERATING_SYSTEM|FILTER_OS_CPE|FILTER_PORT|
FILTER_SERVICE|FILTER_QID|FILTER_RESULT|FILTER_LAST_SCAN_DATE|
FILTER_FIRST_FOUND_DATE|NETWORK|FILTER_DISPLAY_AG_TITLES|FILTER_QID_WITH_
TEXT|FILTER_LAST_COMPLIANCE_SCAN_DATE)+)>

<!ELEMENT IP_LIST (RANGE*)>
```

```
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT ASSET_TAGS (INCLUDED_TAGS, EXCLUDED_TAGS?)>

<!ELEMENT INCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST INCLUDED_TAGS scope CDATA #IMPLIED>

<!ELEMENT EXCLUDED_TAGS (ASSET_TAG*)>
<!ATTLIST EXCLUDED_TAGS scope CDATA #IMPLIED>

<!ELEMENT ASSET_TAG (#PCDATA)>

<!ELEMENT FILTER_DNS (#PCDATA)>
<!ATTLIST FILTER_DNS criterion CDATA #IMPLIED>

<!ELEMENT FILTER_NETBIOS (#PCDATA)>
<!ATTLIST FILTER_NETBIOS criterion CDATA #IMPLIED>

<!ELEMENT TRACKING_METHOD (#PCDATA)>

<!ELEMENT FILTER_OPERATING_SYSTEM (#PCDATA)>
<!ATTLIST FILTER_OPERATING_SYSTEM criterion CDATA #IMPLIED>
<!ELEMENT FILTER_OS_CPE (#PCDATA)>
<!ELEMENT FILTER_PORT (#PCDATA)>
<!ELEMENT FILTER_SERVICE (#PCDATA)>
<!ELEMENT FILTER_QID (#PCDATA)>
<!ELEMENT FILTER_RESULT (#PCDATA)>
<!ATTLIST FILTER_RESULT criterion CDATA #IMPLIED>
<!ELEMENT FILTER_LAST_SCAN_DATE (#PCDATA)>
<!ATTLIST FILTER_LAST_SCAN_DATE criterion CDATA #IMPLIED>
<!ELEMENT FILTER_LAST_COMPLIANCE_SCAN_DATE (#PCDATA)>
<!ATTLIST FILTER_LAST_COMPLIANCE_SCAN_DATE criterion CDATA #IMPLIED>
<!ELEMENT FILTER_FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT FILTER_DISPLAY_AG_TITLES (#PCDATA)>
<!ELEMENT FILTER_QID_WITH_TEXT (#PCDATA)>
<!ELEMENT TOTAL (#PCDATA)>
<!-- HOST_LIST -->

<!ELEMENT HOST_LIST ((HOST|WARNING)*)>

<!ELEMENT HOST (ERROR | (IP, HOST_TAGS?, TRACKING_METHOD,
DNS?, EC2_INSTANCE_ID?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?, QID_LIST?,
PORT_SERVICE_LIST?, ASSET_GROUPS?, NETWORK?, LAST_SCAN_DATE?,
LAST_COMPLIANCE_SCAN_DATE?, FIRST_FOUND_DATE?))>
```

```
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT HOST_TAGS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT QID_LIST (QID+)>
<!ELEMENT QID (ID, RESULT?)>
<!ELEMENT ID (#PCDATA)>
<!-- if format is set to "table" -->
<!-- tab '\t' is the col separator -->
<!-- and new line '\n' is the end of row -->
<!ELEMENT RESULT (#PCDATA)>
<!-- ATTLIST RESULT
      format CDATA #IMPLIED
-->
<!ELEMENT PORT_SERVICE_LIST (PORT_SERVICE+)>
<!ELEMENT PORT_SERVICE (PORT, SERVICE, DEFAULT_SERVICE?)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT DEFAULT_SERVICE (#PCDATA)>
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>
<!ELEMENT LAST_COMPLIANCE_SCAN_DATE (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>

<!ELEMENT WARNING (#PCDATA)>
<!-- ATTLIST WARNING number CDATA #IMPLIED -->
```

## XPaths for Asset Search Report

This section describes the XPaths for the asset search report output.

XPath	element specifications / notes
/ASSET SEARCH REPORT	(ERROR   (HEADER, HOST_LIST?))
/ASSET SEARCH REPORT/ERROR (#PCDATA)	
	An error message.
attribute: <b>number</b>	An error code, when available.
/ASSET SEARCH REPORT/ERROR/HEADER	
	(REQUEST?, COMPANY, USERNAME, GENERATION_DATETIME, TOTAL?, FILTERS)
/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST	
	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/DATETIME (#PCDATA)	

## XPath

### element specifications / notes

The date and time of the request.

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/USER\_LOGIN (#PCDATA)

The login ID of the user who made the request.

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/RESOURCE (#PCDATA)

The resource specified for the request.

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/PARAM\_LIST (PARAM+))

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/PARAM\_LIST/PARAM (KEY, VALUE))

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/PARAM\_LIST/PARAM/KEY (#PCDATA)

The input parameter name.

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/PARAM\_LIST/PARAM/VALUE (#PCDATA)

The input parameter value.

/ASSET SEARCH REPORT/ERROR/HEADER/REQUEST/POST\_DATA (#PCDATA)

The POST data.

/ASSET SEARCH REPORT/ERROR/HEADER/COMPANY (#PCDATA)

The user's company name as defined in the user's account.

/ASSET SEARCH REPORT/ERROR/HEADER/USERNAME (#PCDATA)

The login ID of the user, who generated the asset search report.

/ASSET SEARCH REPORT/ERROR/HEADER/GENERATION\_DATETIME (#PCDATA)

The date and time when the report was generated.

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS

(IP\_LIST | ASSET\_GROUPS | ASSET\_TAGS | FILTER\_DNS | FILTER\_NETBIOS |  
TRACKING\_METHOD | FILTER\_OPERATING\_SYSTEM | FILTER\_OS\_CPE |  
FILTER\_PORT | FILTER\_SERVICE | FILTER\_QID | FILTER\_RESULT |  
FILTER\_LAST\_SCAN\_DATE | FILTER\_FIRST\_FOUND\_DATE | NETWORK |  
FILTER\_DISPLAY\_AG\_TITLES | FILTER\_QID\_WITH\_TEXT |  
FILTER\_LAST\_COMPLIANCE\_SCAN\_DATE)

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/IP\_LIST (RANGE\*)

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/IP\_LIST/RANGE (START, END)

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/IP\_LIST/RANGE/START (#PCDATA)

When the asset search report includes user entered IPs, the start of an IP range.

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/IP\_LIST/RANGE/END (#PCDATA)

When the asset search report includes user entered IPs, the end of an IP range.

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET\_GROUPS (ASSET\_GROUP\_TITLE+)

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET\_GROUPS/ASSET\_GROUP\_TITLE (#PCDATA)

An asset group title.

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET\_GROUPS/NETWORK (#PCDATA)

Restrict the request to a certain custom network ID.

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET\_TAGS (INCLUDED\_TAGS, EXCLUDED\_TAGS?)

/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET\_TAGS/ INCLUDED\_TAGS (ASSET\_TAG\*)



XPath	element specifications / notes
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ INCLUDED_TAGS	
attribute: <b>scope</b>	The list of asset tags included in the report source. The <b>scope</b> “all” means hosts matching all tags; <b>scope</b> “any” means hosts matching at least one of the tags.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ EXCLUDED_TAGS (ASSET_TAG*)	
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ EXCLUDED_TAGS	
attribute: <b>scope</b>	The list of asset tags excluded from the report source. The <b>scope</b> “all” means hosts matching all tags; <b>scope</b> “any” means hosts matching at least one of the tags.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS (#PCDATA)	
	The asset tags selected for the report.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_DNS (#PCDATA)	
	The DNS hostname.
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_NETBIOS (#PCDATA)	
	The NetBIOS hostname.
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/TRACKING_METHOD (#PCDATA)	
	The tracking method for a host in a posture info record: IP, DNS, NETBIOS, EC2.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_OPERATING_SYSTEM (#PCDATA)	
	The operating system on a host in a posture info record, when available.
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_OS_CPE (#PCDATA)	
	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_PORT (#PCDATA)	
	Hosts with the specified open ports.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_SERVICE (#PCDATA)	
	Hosts that has the specified services running on it.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_QID (#PCDATA)	
	The QID assigned to the asset.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_RESULT (#PCDATA)	
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_LAST_SCAN_DATE (#PCDATA)	
	The date and time of the most recent vulnerability scan.
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_LAST_COMPLIANCE_SCAN_DATE (#PCDATA)	
	The date and time of the most recent compliance scan.
attribute: <b>criterion</b>	<b>criterion</b> is deprecated.

XPath	element specifications / notes
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_FIRST_FOUND_DATE (#PCDATA)	The date when the asset was first detected.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_DISPLAY_AG_TITLES (#PCDATA)	AssetGroup Titles for each host.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_QID_WITH_TEXT (#PCDATA)	Vulnerabilities (QIDs) with the specified text in the KnowledgeBase applicable to the host.
/ASSET SEARCH REPORT/ERROR/HEADER/TOTAL (#PCDATA)	Total number of hosts in the asset search report.
/ASSET SEARCH REPORT/ERROR/HOST_LIST ((HOST   WARNING)*)	
/ASSET SEARCH REPORT/ERROR/HOST_LIST/HOST	(ERROR   (IP, HOST_TAGS?, TRACKING_METHOD, DNS?, EC2_INSTANCE_ID?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?, QID_LIST?, PORT_SERVICE_LIST?, ASSET_GROUPS?, NETWORK?, LAST_SCAN_DATE?, LAST_COMPLIANCE_SCAN_DATE?, FIRST_FOUND_DATE?))
/ASSET SEARCH REPORT/ERROR/HOST_LIST/HOST IP (#PCDATA)	The IP address for the host.
attribute: <b>network_id</b>	<b>network_id</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/HOST_TAGS (#PCDATA)	All the tags associated with the host.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/DNS (#PCDATA)	DNS hostname for the asset. For an EC2 asset this is the private DNS name .
/ASSET SEARCH REPORT/ERROR/HOST_LIST/EC2_INSTANCE_ID (#PCDATA)	EC2 instance ID for the asset.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/NETBIOS (#PCDATA)	NetBIOS hostname for the asset, when available.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/OPERATING_SYSTEM (#PCDATA)	The operating system detected on the host.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/OS_CPE (#PCDATA)	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/ASSET SEARCH REPORT/ERROR/HOST_LIST/QID_LIST (QID+)	
/ASSET SEARCH REPORT/ERROR/HOST_LIST/QID_LIST/QID (ID, RESULT?)	
/ASSET SEARCH REPORT/ERROR/HOST_LIST/QID_LIST/QID/ID (#PCDATA)	The vulnerability QID (Qualys ID).
/ASSET SEARCH REPORT/ERROR/HOST_LIST/QID_LIST/QID/RESULT (#PCDATA)	
attribute: <b>format</b>	<b>format</b> is deprecated.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST (PORT_SERVICE+)	

XPath	element specifications / notes
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE (PORT, SERVICE, DEFAULT_SERVICE?)	
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/PORT (#PCDATA)	Hosts that has the specified open ports.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/SERVICE (#PCDATA)	Hosts that has the specified services running on it.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/DEFAULT_SERVICE (#PCDATA)	Expected service to be running on the open ports
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/LAST_SCAN_DATE (#PCDATA)	The date and time of the most recent vulnerability scan.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/ LAST_COMPLIANCE_SCAN_DATE (#PCDATA)	The date and time of the most recent compliance scan.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/FIRST_FOUND_DATE (#PCDATA)	The date and time the host was first detected.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/WARNING (#PCDATA)	A warning message.
attribute: <b>number</b>	A warning code, when available.

## Compliance Data XML

This appendix describes the XML output returned from API V2 requests for compliance data using the Policy Compliance API functions.

- Compliancea Control List Output
- Compliance Policy List Output
- Compliance Policy Export Output
- Compliance Posture Information Output
- Compliance Policy Report
- Compliance Authentication Report
- Compliance Scorecard Report
- Exception List Output
- Exception Batch Return Output
- SCAP Policy List Output

# Compliance Control List Output

The compliance control list XML is returned from a compliance control list API call.

DTD: [https://<baseurl>/api/2.0/fo/compliance/control/control\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/compliance/control/control_list_output.dtd)

## DTD for Compliance Control List Output

A recent DTD for the compliance control list is shown below.

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->

<!ELEMENT CONTROL_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, (CONTROL_LIST|ID_SET)?, WARNING?)>
<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, UPDATE_DATE, CREATED_DATE, CATEGORY, SUB_CATEGORY,
STATEMENT, CRITICALITY?, DEPRECATED?, DEPRECATED_DATE?,
CHECK_TYPE?, COMMENT?, IGNORE_ERROR?, IGNORE_ITEM_NOT_FOUND?,
SCAN_PARAMETERS?, TECHNOLOGY_LIST, FRAMEWORK_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>
<!ELEMENT CREATED_DATE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT SUB_CATEGORY (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT DEPRECATED (#PCDATA)>
<!ELEMENT DEPRECATED_DATE (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
```

```
<!ELEMENT SCAN_PARAMETERS (REG_HIVE?, REG_KEY?, REG_VALUE_NAME?,  
FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?, WMI_QUERY?, SHARE_USER?,  
PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,  
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,  
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,  
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,  
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,  
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,  
TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?,  
INTEGRITY_CHECK_TIME_LIMIT?, INTEGRITY_CHECK_MATCH_LIMIT?, DIGEST_HASH?,  
DATA_TYPE, DESCRIPTION)>  
  
<!ELEMENT REG_HIVE (#PCDATA)>  
<!ELEMENT REG_KEY (#PCDATA)>  
<!ELEMENT REG_VALUE_NAME (#PCDATA)>  
<!ELEMENT FILE_PATH (#PCDATA)>  
<!ELEMENT FILE_QUERY (#PCDATA)>  
<!ELEMENT HASH_TYPE (#PCDATA)>  
<!ELEMENT WMI_NS (#PCDATA)>  
<!ELEMENT WMI_QUERY (#PCDATA)>  
<!ELEMENT SHARE_USER (#PCDATA)>  
<!ELEMENT PATH_USER (#PCDATA)>  
<!ELEMENT GROUP_NAME (#PCDATA)>  
<!ELEMENT GROUP_NAME_LIMIT (#PCDATA)>  
<!ELEMENT BASE_DIR (#PCDATA)>  
<!ELEMENT DEPTH_LIMIT (#PCDATA)>  
<!ELEMENT INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)>  
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>  
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>  
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>  
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>  
<!ELEMENT TIME_LIMIT (#PCDATA)>  
<!ELEMENT MATCH_LIMIT (#PCDATA)>  
<!ELEMENT WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)>  
<!ELEMENT MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN (#PCDATA)>  
<!ELEMENT WIN_PERMISSION_USERS (#PCDATA)>  
<!ELEMENT WIN_PERMISSION_MATCH (#PCDATA)>  
<!ELEMENT SHOULD_DESCEND (#PCDATA)>  
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>  
<!ELEMENT PERMISSIONS (SPECIAL, USER, GROUP, OTHER)>  
<!ELEMENT PERM_COND (#PCDATA)>  
<!ELEMENT TYPE_MATCH (#PCDATA)>  
<!ELEMENT USER_OWNER (#PCDATA)>  
<!ELEMENT GROUP_OWNER (#PCDATA)>  
  
<!ELEMENT WIN_PERMISSIONS (WIN_BASIC_PERMISSIONS?,  
WIN_ADVANCED_PERMISSIONS?)>  
<!ELEMENT WIN_BASIC_PERMISSIONS (WIN_BASIC_PERMISSION_TYPE+)>  
<!ELEMENT WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSION_TYPE+)>
```

```

<!ELEMENT WIN_BASIC_PERMISSION_TYPE (#PCDATA)>
<!ELEMENT WIN_ADVANCED_PERMISSION_TYPE (#PCDATA)>

<!ELEMENT SPECIAL (USER, GROUP, DELETION)>
<!ELEMENT USER (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT GROUP (#PCDATA|READ|WRITE|EXECUTE)*>
<!ELEMENT OTHER (READ, WRITE, EXECUTE)>
<!ELEMENT DELETION (#PCDATA)>
<!ELEMENT READ (#PCDATA)>
<!ELEMENT WRITE (#PCDATA)>
<!ELEMENT EXECUTE (#PCDATA)>

<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
<!ELEMENT DIGEST_HASH (#PCDATA)>

<!ELEMENT DATA_TYPE (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT DATAPOINT (CARDINALITY, OPERATOR, DEFAULT_VALUES)>
<!ELEMENT USE_SCAN_VALUE (#PCDATA)>
<!ELEMENT CARDINALITY (#PCDATA)>
<!ELEMENT OPERATOR (#PCDATA)>
<!ELEMENT DEFAULT_VALUES (DEFAULT_VALUE+)>
<!ATTLIST DEFAULT_VALUES total CDATA "0">
<!ELEMENT DEFAULT_VALUE (#PCDATA)>
<!ELEMENT FRAMEWORK_LIST (FRAMEWORK+)>
<!ELEMENT FRAMEWORK (ID, NAME, REFERENCE_LIST)>
<!ELEMENT REFERENCE_LIST (REFERENCE+)>
<!ELEMENT REFERENCE (SECTION, COMMENTS)>
<!ELEMENT SECTION (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->

```

**XPaths for Control List Output**

This section describes the XPaths for the compliance control list output.

**Control List Output: Request**

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT	(REQUEST?, RESPONSE)
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/COMPLIANCE_CONTROL_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.



## Control List Output: Response

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT (REQUEST?, RESPONSE)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE	(DATETIME, CONTROL_LIST   ID_SET?, WARNING?)
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST (CONTROL+)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL	(ID, UPDATE_DATE, CREATED_DATE, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?, DEPRECATED?, DEPRECATED_DATE?, CHECK_TYPE?, COMMENT?, IGNORE_ERROR?, IGNORE_ITEM_NOT_FOUND?, SCAN_PARAMETERS?, TECHNOLOGY_LIST, FRAMEWORK_LIST?)
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/ID (#PCDATA)	A compliance control ID.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/UPDATE_DATE (#PCDATA)	The date and time when the control was last updated.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CREATED_DATE (#PCDATA)	The date and time when the control was created.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CATEGORY (#PCDATA)	A category for a compliance control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SUB-CATEGORY (#PCDATA)	A sub-category for a compliance control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	A statement for a compliance control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY/LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/DEPRECATED (#PCDATA)	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/DEPRECATED_DATE (#PCDATA)	For a deprecated control, the date the control was deprecated. This element appears only for a deprecated control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CHECK_TYPE (#PCDATA)	The check type: Registry Key Existence, Registry Value Existence, Registry Value Content Check, Registry Permission, etc
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/COMMENT (#PCDATA)	User defined comments.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/IGNORE_ERROR (#PCDATA)	Set to 1 when the ignore error option is enabled for the control. When enabled, the service marks control instances as Passed in cases where an error occurs during control evaluation.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/IGNORE_ITEM_NOT_FOUND (#PCDATA)	Set to 1 when the ignore item not found option is enabled for the control. When enabled the service will show a status of Passed or Failed in cases where a control returns error code 2 “item not found” (e.g. scan did not find file, registry, or related data, as appropriate for the control type), depending on the status you prefer (defined in the policy).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS	(REG_HIVE?, REG_KEY?, REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?, WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?, BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?, FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?, DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?, MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?, WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?, INTEGRITY_CHECK_MATCH_LIMIT?, DIGEST_HASH?, DATA_TYPE, DESCRIPTION)

## XPath

## element specifications / notes

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/REG\_HIVE (#PCDATA)

A Windows registry hive: HKEY\_CLASSES\_ROOT (HKCR) |  
HKEY\_CURRENT\_USER (HKCU) | HKEY\_LOCAL\_MACHINE (HKLM) |  
HKEY\_USERS (HKU).

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/REG\_KEY (#PCDATA)

A Windows registry key.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/REG\_VALUE\_NAME (#PCDATA)

A value for a Windows registry key.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/FILE\_PATH (#PCDATA)

A pathname to a file or directory.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/FILE\_QUERY (#PCDATA)

A query for a file content check.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/HASH\_TYPE (#PCDATA)

An algorithm to be used for computing a file hash: MD5 | SHA-1 | SHA-256.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WMI\_NS (#PCDATA)

A WMI namespace for a WMI query check.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WMI\_QUERY (#PCDATA)

A WMI query for a WMI query check.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/SHARE\_USER (#PCDATA)

A user name who can access a share for a share access check.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PATH\_USER (#PCDATA)

A user name who can access a directory for a share access check.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/GROUP\_NAME (#PCDATA)

Windows local group name to get a list of members for.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/GROUP\_NAME\_LIMIT (#PCDATA)

The maximum number of results (1 to 1000) to be returned for Windows group  
name

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/BASE\_DIR (#PCDATA)

For directory search, the base directory to start search from.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/SHOULD_DESCEND (#PCDATA)	For directory search, set to “true” when search extends into other file systems found; otherwise set to “false”.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DEPTH_LIMIT (#PCDATA)	For directory search, depth level for searching each directory: only directory properties (0), directory contents (1) or multiple levels below the base directory (2-10).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/INTEGRITY_CHECK_DEPTH_LIMIT (#PCDATA)	For directory integrity content check (Unix or Windows), depth level for searching the directory. Only directory properties (0), directory contents (1) or multiple levels below the directory (2-10).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FOLLOW_SYMLINK (#PCDATA)	For directory search, set to “true” when target destination files and directories will be analyzed; otherwise set to “false”.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_NAME_MATCH (#PCDATA)	For directory search, a filename to match, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_NAME_SKIP (#PCDATA)	For directory search, a filename to skip, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DIR_NAME_MATCH (#PCDATA)	For directory search, a directory name to match, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DIR_NAME_SKIP (#PCDATA)	For directory search, a directory name to skip, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)	For Windows directory search, types of system objects to search: DIRECTORY, FILE or DIRECTORY FILE (i.e. both directory and file).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN (#PCDATA)	For Windows directory search, when set to “Yes” we’ll perform a look up of the users set in <WIN_PERMISSION_USERS> and match against well-known users, groups and aliases. <a href="#">Click here to find abbreviated SDDL names for well-known users and groups.</a>

## XPath

## element specifications / notes

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSION\_USERS (#PCDATA)

For Windows directory search, comma separated list of principals with permissions to the files/directories to match.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSION\_MATCH (#PCDATA)

For Windows directory search, match “Any” (i.e. at least one of the permissions set or “All” (i.e. files that match all of the permissions set) in WIN\_BASIC\_PERMISSIONS.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSIONS (WIN\_BASIC\_PERMISSIONS?, WIN\_ADVANCED\_PERMISSIONS?)

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSIONS/WIN\_BASIC\_PERMISSIONS (WIN\_BASIC\_PERMISSIONS\_TYPE+)

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSIONS/WIN\_BASIC\_PERMISSIONS /  
WIN\_BASIC\_PERMISSIONS\_TYPE (#PCDATA)

For Windows directory search, match basic permission: Full Control | Modify | List Folder | Content | Read & Execute | Write | Read

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSIONS/WIN\_ADVANCED\_PERMISSIONS  
(WIN\_ADVANCED\_PERMISSIONS\_TYPE+)

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/WIN\_PERMISSIONS/WIN\_BASIC\_PERMISSIONS (WIN\_BASIC\_PERMISSIONS\_TYPE+)

For Windows directory search, match advanced permission: Full Control | Traverse Folder | Execute Files | List Folder/Read Data | Read Attributes | Read Extended Attributes | Create Files/Write Data | Create Folders/Append Data | Write Attributes | Write Extended Attributes | Delete Sub-folders & Files | Delete | Read Permissions | Change Permissions | Take Ownership

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PERMISSIONS (SPECIAL, USER, GROUP, OTHER)

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PERMISSIONS/SPECIAL (USER, GROUP, DELETION)

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PERMISSIONS/USER (#PCDATA | READ | WRITE | EXECUTE)

For Unix directory search, match files with these user permissions.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PERMISSIONS /GROUP (#PCDATA | READ | WRITE | EXECUTE)

For Unix directory search, match files with these group permissions.

/COMPLIANCE\_CONTROL\_LIST\_OUTPUT/RESPONSE/CONTROL\_LIST/CONTROL/  
SCAN\_PARAMETERS/PERMISSIONS/OTHER (#PCDATA | READ | WRITE | EXECUTE)

For Unix directory search, match files with these other permissions.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/PERM_COND (#PCDATA)	For Unix directory search, match “all” permissions or “some” permissions set in PERMISSIONS, or “exclude” (i.e. ignore files with certain permissions).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/TYPE_MATCH (#PCDATA)	For Unix directory search, match system objects specified as string of comma separated codes: d (directory), f (regular file), l (symbolic link), p (named pipe, FIFO), b (block special - buffered), c (character special - unbuffered), s (socket), D (door, Solaris only). Sample string: d,f,l
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/USER_OWNER (#PCDATA)	For Unix directory search, match files owned by certain users specified as comma separated list of user names and/or UUIDs.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/GROUP_OWNER (#PCDATA)	For Unix directory search, match files owned by certain groups specified as comma separated list of group names and/or GUIDs.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/TIME_LIMIT (#PCDATA)	For a Unix directory search, the search time limit in seconds.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/MATCH_LIMIT (#PCDATA)	For a Unix directory search, the maximum number of objects matched.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)	For integrity content check of directory / file (Unix or Windows), the integrity check time limit.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)	For integrity content check of directory / file (Unix or Windows), the integrity check match limit.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DIGEST_HASH (#PCDATA)	For integrity content check of directory / file (Unix or Windows), the digest hash.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DATA_TYPE (#PCDATA)	A scan parameter that identifies a valid data type for the actual value provided by the service: Boolean   Integer   String   String List   Line List
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DESCRIPTION (#PCDATA)	A description of the check’s scan parameters.

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST (TECHNOLOGY+)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/ID (#PCDATA)	A technology ID for a technology in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/NAME (#PCDATA)	A technology name for a technology in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/RATIONALE (#PCDATA)	The rationale description for a technology in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/DATAPOINT (CARDINALITY, OPERATOR, DEFAULT_VALUES)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/DATAPOINT/CARDINALITY (#PCDATA)	A cardinality used to calculate the expected value for a technology based on DATA_TYPE. String List: contains   does not contain   matches   is contained in   intersect. Line List: match any   match all   match none   empty   not empty. Boolean or Integer: no cd.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/DATAPOINT/OPERATOR (#PCDATA)	A name of an operator used to calculate the expected value for a technology: ge (greater than or equal to)   gt (greater than)   le (less than or equal to)   lt (less than)   ne (not equal to)   eq (equal to)   in   range (in range)   re (regular expression)   xre (regular expression list)   xeq (string list)   no op (no operator).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/DATAPOINT/DEFAULT_VALUES (DEFAULT_VALUE+)	<b>total</b> is the total number of default values
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/DATAPOINT/DEFAULT_VALUES/DEFAULT_VALUE (#PCDATA)	A default value for each technology this is used to calculate the expected value for a technology, specified as a regular expression or a string depending on the check type.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/ TECHNOLOGY/USE_SCAN_VALUE (#PCDATA)	Indicates whether the “Use scan data as expected value” option is enabled for the technology in a File Integrity check. A value of “1” means it is enabled. A value of “0” means it’s not enabled.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST (FRAMEWORK+)	

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework (ID, NAME, REFERENCE_LIST)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/ID (#PCDATA)	A framework ID for a framework reference in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/NAME (#PCDATA)	A framework name for a framework reference in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST (REFERENCE+)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST/REFERENCE (SECTION, COMMENTS)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST/REFERENCE/SECTION (#PCDATA)	A framework section for a framework reference in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST/REFERENCE/COMMENTS (#PCDATA)	A framework description (comments) for a framework reference in a control.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/ID_SET (ID ID_RANGE)+	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	A compliance control ID.
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	A range of compliance control IDs.

### Control List Output: Warning

XPath	element specifications / notes
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/WARNING (CODE, TEXT, URL?)	
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	A warning code. A warning code appears when the API request identifies more than 1,000 records (controls).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	A warning message. A warning message appears when the API request identifies more than 1,000 records (controls).
/COMPLIANCE_CONTROL_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL for making another API request for the next batch of compliance control records.



# Compliance Policy List Output

The compliance policy list XML is returned from an API request for a compliance policy list.

DTD: [https://<basurl>/api/2.0/fo/compliance/policy/policy\\_list\\_output.dtd](https://<basurl>/api/2.0/fo/compliance/policy/policy_list_output.dtd)

## DTD for Compliance Policy List Output

A recent DTD for the compliance policy list is shown below.

```
<!-- QUALYS POLICY_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT POLICY_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, (POLICY_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT POLICY_LIST (POLICY+)>
<!ELEMENT POLICY (ID, TITLE, CREATED?, LAST_MODIFIED?, LAST_EVALUATED?,
STATUS?, IS_LOCKED?, EVALUATE_NOW?, ASSET_GROUP_IDS?,
TAG_SET_INCLUDE?, TAG_INCLUDE_SELECTOR?,
INCLUDE_AGENT_IPS?, CONTROL_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>

<!ELEMENT LAST_MODIFIED (DATETIME, BY)>

<!ELEMENT LAST_EVALUATED (DATETIME)>

<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT IS_LOCKED (#PCDATA)>
<!ELEMENT EVALUATE_NOW (#PCDATA)>
```

```
<!ELEMENT ASSET_GROUP_IDS (#PCDATA)>
<!ATTLIST ASSET_GROUP_IDS has_hidden_data CDATA #IMPLIED>

<!ELEMENT TAG_SET_INCLUDE (TAG_ID+)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT TAG_INCLUDE_SELECTOR (#PCDATA)>

<!ELEMENT INCLUDE_AGENT_IPS (#PCDATA)>

<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, STATEMENT, CRITICALITY?, DEPRECATED?,
                    TECHNOLOGY_LIST?)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT DEPRECATED (#PCDATA)>

<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (ID, NAME, RATIONALE, CUSTOMIZED)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT CUSTOMIZED (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT GLOSSARY (ASSET_GROUP_LIST?, ASSET_TAG_LIST?, USER_LIST?)>

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, TITLE, NETWORK_ID?, IP_SET?)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>

<!ELEMENT ASSET_TAG_LIST (TAG+)>
<!ELEMENT TAG (TAG_ID?, TAG_NAME?)>
<!ELEMENT TAG_NAME (#PCDATA)>

<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
```

```
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

## XPaths for Compliance Policy List Output

This section describes the XPaths for the compliance policy list output.

### Compliance Policy List Output: Request

XPath	element specifications / notes
/COMPLIANCE_POLICY_LIST_OUTPUT	(REQUEST?, RESPONSE)
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/COMPLIANCE_POLICY_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.

### Compliance Policy List Output: Response

XPath	element specifications / notes
/COMPLIANCE_POLICY_LIST_OUTPUT	(REQUEST?, RESPONSE)
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE	(DATETIME, (POLICY_LIST   ID_SET)?, WARNING?, GLOSSARY?)
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST	(POLICY+)
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY	

XPath	element specifications / notes
	(ID, TITLE, CREATED?, LAST_MODIFIED?, LAST_EVALUATED?, STATUS?, IS_LOCKED?, EVALUATE_NOW?, ASSET_GROUP_IDS?, TAG_SET_INCLUDE?, TAG_INCLUDE_SELECTOR?, INCLUDE_AGENT_IPS?, CONTROL_LIST?)
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/ID (#PCDATA)	
	A compliance policy ID.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TITLE (#PCDATA)	
	A compliance policy title.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CREATED (#PCDATA)	
	The date/time when the policy was created.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED (DATETIME, BY)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED/DATETIME (#PCDATA)	
	The date/time when the policy was last updated.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED/BY (#PCDATA)	
	The user login ID of the user who last modified the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_EVALUATED (DATETIME)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_EVALUATED/DATETIME (#PCDATA)	
	The date/time when the policy was last evaluated.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/STATUS (#PCDATA)	
	The current status of the policy: active or inactive.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/IS_LOCKED (#PCDATA)	
	The current status of the policy: locked or unlocked.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/EVALUTE_NOW (#PCDATA)	
	Indicates whether the Evaluate Now option was selected in the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/ASSET_GROUP_IDS (#PCDATA)	
	A list of asset group IDs for the asset groups assigned to a policy.
attribute: <b>has_hidden_data</b>	<b>has_hidden_data</b> is <i>implied</i> and, if present, has the value 1. This flag 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.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_INCLUDE (TAG_ID+)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_INCLUDE/TAG_ID (#PCDATA)	
	A tag set ID.

XPath	element specifications / notes
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_INCLUDE_SELECTOR (#PCDATA)	The value “any” means the hosts included in the policy match at least one of the selected tags, and “all” means the hosts match all of the selected tags.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/INCLUDE_AGENT_IPS (#PCDATA)	The value 1 means the policy includes agent IPs, and 0 means the policy doesn’t include them.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST (CONTROL+)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL (ID, STATEMENT, CRITICALITY?, DEPRECATED?, TECHNOLOGY_LIST?)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/ID (#PCDATA)	A compliance control ID.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	A control statement.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/CRITICALITY/LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/DEPRECATED (#PCDATA)	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST (TECHNOLOGY+)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY (ID, NAME, RATIONALE, CUSTOMIZED)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/ID (#PCDATA)	A technology ID for a control.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/NAME (#PCDATA)	A technology name for a control.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/RATIONALE (#PCDATA)	The rationale description for a control technology.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/CUSTOMIZED (#PCDATA)	A value indicating whether the default value was customized for a control technology. The value 1 indicates the default value was customized. The value 0 indicates the default value was not customized. The value 0 always is present for a locked control (a control that cannot be customized).
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/ID_SET (ID ID_RANGE)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	A policy ID.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	A range policy IDs.

## Compliance Policy List Output: Warning

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST (WARNING+)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING (CODE?, TEXT, URL?)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	A warning code. A warning code appears when the API request identifies more than 1,000 records (policies).
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	A warning message. A warning message appears when the API request identifies more than 1,000 records (policies).
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL for making another API request for the next batch of policy records.

## Compliance Policy List: Glossary

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY (ASSET_GROUP_LIST?, ASSET_TAG_LIST?, USER_LIST?)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST (ASSET_GROUP+)	A list of asset groups assigned to policies in the policy list output.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP (ID, TITLE, IP_SET?)	

XPath	element specifications / notes
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/ID (#PCDATA)	An asset group ID for an asset group assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/TITLE (#PCDATA)	An asset group title for an asset group assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/IP_SET (IP IP_RANGE)+	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/IP_SET/IP (#PCDATA)	An IP address in an asset group that is assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/IP_SET/IP_RANGE (#PCDATA)	An IP address range in an asset group that is assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST (TAG+)	A list of asset tags assigned to policies in the policy list output.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST/TAG (TAG_ID?, TAG_NAME?)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST /TAG/TAG_ID (#PCDATA)	An asset tag ID for an asset tag assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST /TAG/TAG_NAME (#PCDATA)	An asset tag name for an asset tag assigned to the policy.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST (USER+)	A list of users who created or edited exceptions in compliance policies in the policy list output. For a policy that was edited, the user who most recently edited the exception is included in the output.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER (USER_LOGIN, FIRST_NAME, LAST_NAME)	
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER (#PCDATA)	A user login ID.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /FIRST_NAME (#PCDATA)	The first name of the account user.
/COMPLIANCE_POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /LAST_NAME (#PCDATA)	The last name of the account user.

# Compliance Policy Export Output

The compliance policy export XML is returned from an API request for a compliance policy export.

DTD: [https://<baseurl>/api/2.0/fo/compliance/policy/policy\\_export\\_output.dtd](https://<baseurl>/api/2.0/fo/compliance/policy/policy_export_output.dtd)

## DTD for Compliance Policy Export Output

A recent DTD is shown below.

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->

<!ELEMENT POLICY_EXPORT_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, POLICY)>
<!ELEMENT POLICY (TITLE, DESCRIPTION?, LOCKED?, EXPORTED, COVER_PAGE?,
    STATUS?, TECHNOLOGIES, SECTIONS, APPENDIX?)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT LOCKED (#PCDATA)>
<!ELEMENT EXPORTED (#PCDATA)>
<!ELEMENT COVER_PAGE (#PCDATA)>

<!ELEMENT SECTIONS (SECTION*)>
<!ATTLIST SECTIONS total CDATA #IMPLIED>
<!ELEMENT SECTION (NUMBER, HEADING, CONTROLS)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT HEADING (#PCDATA)>

<!ELEMENT CONTROLS ((CONTROL|USER_DEFINED_CONTROL)*)>
<!ATTLIST CONTROLS total CDATA #IMPLIED>
<!ELEMENT CONTROL (ID, CRITICALITY?, IS_CONTROL_DISABLE?,
    REFERENCE_TEXT?, TECHNOLOGIES)>
<!ELEMENT ID (#PCDATA)>
```



```

<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT IS_CONTROL_DISABLE (#PCDATA)>
<!ELEMENT REFERENCE_TEXT (#PCDATA)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY*)>
<!ATTLIST TECHNOLOGIES total CDATA #IMPLIED>
<!ELEMENT TECHNOLOGY (ID, NAME?, EVALUATE?, RATIONALE?, DATAPOINT?,
    USE_SCAN_VALUE?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EVALUATE (CTRL*)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT CTRL (AND|OR|NOT|DP)+>
<!ELEMENT AND (AND|OR|NOT|DP)+>
<!ELEMENT OR (AND|OR|NOT|DP)+>
<!ELEMENT NOT (AND|OR|NOT|DP)+>
<!ELEMENT DP (K|OP|CD|L|V|FV)+>
<!ELEMENT K (#PCDATA)>
<!ELEMENT OP (#PCDATA)>
<!ELEMENT CD (#PCDATA)>
<!ELEMENT L (#PCDATA)>
<!ELEMENT V (#PCDATA)>
<!ELEMENT FV (#PCDATA)>
<!ATTLIST FV set CDATA #IMPLIED>

<!ELEMENT DATAPOINT (CARDINALITY?, OPERATOR?, DEFAULT_VALUES?)>
<!ELEMENT CARDINALITY (#PCDATA)>
<!ELEMENT OPERATOR (#PCDATA)>
<!ELEMENT DEFAULT_VALUES (DEFAULT_VALUE*)>
<!ATTLIST DEFAULT_VALUES total CDATA #IMPLIED>
<!ELEMENT DEFAULT_VALUE (#PCDATA)>

<!ELEMENT USE_SCAN_VALUE (#PCDATA)>

<!ELEMENT USER_DEFINED_CONTROL (ID, UDC_ID, CHECK_TYPE, CATEGORY,
    SUB_CATEGORY, STATEMENT, CRITICALITY?,
    COMMENT?, IGNORE_ERROR,
    IGNORE_ITEM_NOT_FOUND?, SCAN_PARAMETERS,
    REFERENCE_TEXT?, TECHNOLOGIES,
    REFERENCE_LIST)>
<!ELEMENT UDC_ID (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>

<!ELEMENT CATEGORY (ID, NAME)>
<!ELEMENT SUB_CATEGORY (ID, NAME)>

<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>

```

```
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
<!ELEMENT REFERENCE_LIST (REFERENCE*)>
<!ELEMENT REFERENCE (REF_DESCRIPTION?, URL?)>
<!ELEMENT REF_DESCRIPTION (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT SCAN_PARAMETERS (REG_HIVE?, REG_KEY?, REG_VALUE_NAME?,
    FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
    WMI_QUERY?, SHARE_USER?, PATH_USER?,
    BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?,
    FOLLOW_SYMLINK?, FILE_NAME_MATCH?,
    FILE_NAME_SKIP?, DIR_NAME_MATCH?,
    DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?,
    TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?,
    TIME_LIMIT?, MATCH_LIMIT?,
    WIN_FILE_SYS_OBJECT_TYPES?,
    MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?,
    WIN_PERMISSION_USERS?, WIN_PERMISSION_MATCH?,
    WIN_PERMISSIONS?, GROUP_NAME?,
    GROUP_NAME_LIMIT?, DATA_TYPE, DESCRIPTION)>

<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
<!ELEMENT FOLLOW_SYMLINK (#PCDATA)>
<!ELEMENT FILE_NAME_MATCH (#PCDATA)>
<!ELEMENT FILE_NAME_SKIP (#PCDATA)>
<!ELEMENT DIR_NAME_MATCH (#PCDATA)>
<!ELEMENT DIR_NAME_SKIP (#PCDATA)>
<!ELEMENT PERM_COND (#PCDATA)>
<!ELEMENT TYPE_MATCH (#PCDATA)>
<!ELEMENT USER_OWNER (#PCDATA)>
<!ELEMENT GROUP_OWNER (#PCDATA)>
<!ELEMENT TIME_LIMIT (#PCDATA)>
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT WIN_PERMISSION_MATCH (#PCDATA)>
<!ELEMENT MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN (#PCDATA)>
<!ELEMENT WIN_PERMISSION_USERS (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_NAME_LIMIT (#PCDATA)>
```

```
<!ELEMENT DATA_TYPE (#PCDATA)>

<!ELEMENT PERMISSIONS (SPECIAL, USER, GROUP, OTHER)>
<!ELEMENT SPECIAL (SPECIAL_USER, SPECIAL_GROUP, SPECIAL_DELETION)>
<!ELEMENT SPECIAL_USER (#PCDATA)>
<!ELEMENT SPECIAL_GROUP (#PCDATA)>
<!ELEMENT SPECIAL_DELETION (#PCDATA)>

<!ELEMENT USER (READ, WRITE, EXECUTE)>
<!ELEMENT GROUP (READ, WRITE, EXECUTE)>
<!ELEMENT OTHER (READ, WRITE, EXECUTE)>
<!ELEMENT READ (#PCDATA)>
<!ELEMENT WRITE (#PCDATA)>
<!ELEMENT EXECUTE (#PCDATA)>

<!ELEMENT WIN_PERMISSIONS (WIN_BASIC_PERMISSIONS?,
                           WIN_ADVANCED_PERMISSIONS?)>
<!ELEMENT WIN_BASIC_PERMISSIONS (WIN_BASIC_PERMISSION_TYPE+)>
<!ELEMENT WIN_BASIC_PERMISSION_TYPE (#PCDATA)>
<!ELEMENT WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSION_TYPE+)>
<!ELEMENT WIN_ADVANCED_PERMISSION_TYPE (#PCDATA)>

<!ELEMENT WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)>

<!ELEMENT APPENDIX (OP_ACRONYMS, DATA_POINT_ACRONYMS+)>
<!ELEMENT OP_ACRONYMS (OP+)>
<!ATTLIST OP id CDATA #IMPLIED>
<!ELEMENT DATA_POINT_ACRONYMS (DP+)>
<!ATTLIST K id CDATA #IMPLIED>
<!ATTLIST FV id CDATA #IMPLIED>

<!-- EOF -->
```

## XPaths for Compliance Policy Export Output

This section describes the XPathS for the compliance policy export output.

### Compliance Policy Export Output: Request

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT	(REQUEST?, RESPONSE)
/POLICY_EXPORT_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/OLICY_EXPORT_OUTPUT/REQUEST/DATETIME	(#PCDATA)
The date and time of the request.	

<b>XPath</b>	<b>element specifications / notes</b>
/POLICY_EXPORT_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/POLICY_EXPORT_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/POLICY_EXPORT_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/POLICY_EXPORT_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/POLICY_EXPORT_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name.
/POLICY_EXPORT_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/POLICY_EXPORT_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.

## Compliance Policy Export Output: Response

<b>XPath</b>	<b>element specifications / notes</b>
/POLICY_EXPORT_OUTPUT/RESPONSE (REQUEST?, RESPONSE)	
/POLICY_EXPORT_OUTPUT/RESPONSE (DATETIME, POLICY)	
/POLICY_EXPORT_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/POLICY_EXPORT_OUTPUT/RESPONSE /POLICY (TITLE, DESCRIPTION?, LOCKED?, EXPORTED, COVER_PAGE?, STATUS?, TECHNOLOGIES, SECTIONS, APPENDIX?)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/TITLE (#PCDATA)	A compliance policy title.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/POLICY/DESCRIPTION (#PCDATA)	A compliance policy description.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/POLICY/LOCKED (#PCDATA)	A flag indicating that the policy is locked.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/EXPORTED (#PCDATA)	The date/time when the policy was exported.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/COVER_PAGE (#PCDATA)	Content for the cover page.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/STATUS (#PCDATA)	The current policy status: active or inactive.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS (SECTION+)	<b>total</b> is the total number of sections

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION	(NUMBER, HEADING, CONTROLS)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/NUMBER	(#PCDATA)
	A section number.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/HEADING	(#PCDATA)
	A section heading.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS	((CONTROL USER_DEFINED_CONTROL)*)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS	(CONTROL*)
	<b>total</b> is the total number of controls
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL	(ID, CRITICALITY?, IS_CONTROL_DISABLE?, REFERENCE_TEXT?, TECHNOLOGIES)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/ID	(#PCDATA)
	A control ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/CRITICALITY	(LABEL, VALUE)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/CRITICALITY/LABEL	(#PCDATA)
	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/IS_CONTROL_DISABLE	(#PCDATA)
	1 means the control is disabled; 0 means the control is enabled.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES	(TECHNOLOGY+)
	<b>total</b> is the total number of technologies
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY	(ID, NAME?, EVALUATE?, RATIONALE?, DATAPOINT?, USE_SCAN_VALUE?)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/ID	(#PCDATA)
	A technology ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/NAME	(#PCDATA)
	A technology name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE	(CTRL*)
	The control evaluation logic.
attribute: checksum	This attribute is no longer returned in the XML output. However, you can still include it in policy export XML and import it into your account.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL (AND OR NOT DP)+	The root tag for control evaluation.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /AND (AND OR NOT DP)+	Indicates a logical AND relationship between its children.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /OR (AND OR NOT DP)+	Indicates a logical OR relationship between its children.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /NOT (AND OR NOT DP)+	Indicates negation of evaluation logic represented by its child tag.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP (K OP CD L V FV)+	The evaluation logic for a data point in the compliance policy.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/K (#PCDATA)	A service-defined, unique name for the data point.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/OP (#PCDATA)	The operator option set in the compliance policy for the data point, if applicable. Possible values depending on the data type: ge   gt   le   lt   eq   ne   in   range   re   xre   xeq   no op. See “Operator Names” below.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/CD (#PCDATA)	The cardinality option set in the compliance policy for the data point, if applicable. Possible values depending on the data type: contains   does not contain   matches   is contained in   intersect   match any   match all   match none   empty   not empty   no cd.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/L (#PCDATA)	Identifies attributes of the data point that are locked and cannot be changed in the compliance policy. These data point attributes may be locked: OP (operator), CD (cardinality), V (expected value).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/V (#PCDATA)	The user-provided “expected” value for the data point, as defined in the policy.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/EVALUATE/CTRL /DP/FV (#PCDATA)	A fixed expected value for the data point in the compliance policy. A fixed value cannot be changed in the policy. It can only be selected/deselected.
attribute: set	<b>set</b> indicates whether the fixed value is selected in the compliance policy. When set=1 the fixed value is selected. When set=0 the fixed value is not selected.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/RATIONALE (#PCDATA)	A rationale statement describing how the control should be implemented for each technology.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/DATAPOINT	(CARDINALITY?, OPERATOR?, DEFAULT_VALUES?)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/DATAPOINT/CARDINALITY (#PCDATA)	A cardinality used to calculate the expected value for a technology. When DATA_TYPE is “String List”: contains   does not contain   matches   is contained in   intersect. When DATA_TYPE is “Line List”: match any   match all   match none   empty   not empty. When DATA_TYPE is “Boolean” or “Integer”: no cd.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/DATAPOINT/OPERATOR (#PCDATA)	A name of an operator used to calculate the expected value for a technology: ge   gt   le   lt   ne   eq   in   range   re   xre   xeq   no op.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/DATAPOINT/DEFAULT_VALUES (DEFAULT_VALUE*)	<b>total</b> is the total number of default values.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/DATAPOINT/DEFAULT_VALUES/DEFAULT_VALUE (#PCDATA)	A default value for each technology this is used to calculate the expected value for a technology, specified as a regular expression or a string depending on the check type. This value can be a maximum of 4000 alphanumeric characters. A regular expression must follow the PCRE Standard.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY/USE_SCAN_VALUE (#PCDATA)	Indicates whether the “Use scan data as expected value” option is enabled for the technology in a File Integrity check. A value of “1” means it is enabled. A value of “0” means it’s not enabled.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL	(ID, UDC_ID, CHECK_TYPE, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?, COMMENT?, IGNORE_ERROR, IGNORE_ITEM_NOT_FOUND?, SCAN_PARAMETERS, REFERENCE_TEXT?, TECHNOLOGIES, REFERENCE_LIST)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/ID (#PCDATA)	Control ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/UDC_ID (#PCDATA)	User-defined control ID (UCD ID) for Qualys Custom Control.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/ USER_DEFINED_CONTROL/CHECK_TYPE (#PCDATA)	The check type: Registry Key Existence   Registry Value Existence   Registry Value Content Check   Registry Permission   Window File/Directory Existence   Window File/Directory Permission   Unix File/Directory Permission   Unix File Content Check   Unix File/Directory Existence   Window File Integrity Check   Unix File Integrity Check   WMI Query Check   Share Access Check   Unix Directory Search Check   Windows Directory Search Check   Windows Group Membership Check
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/ USER_DEFINED_CONTROL/CATEGORY (ID, NAME)	A category for a compliance control.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/ USER_DEFINED_CONTROL/CATEGORY/ID (#PCDATA)	The category ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/CATEGORY/NAME (#PCDATA)	The category name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/SUB_CATEGORY (ID, NAME)	A sub-category for the control.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/SUB_CATEGORY/ID (#PCDATA)	The sub-category ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/SUB_CATEGORY/NAME (#PCDATA)	The sub-category name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/STATEMENT (#PCDATA)	A control statement that describes how the control should be implemented in the environment.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/COMMENT (#PCDATA)	User defined comments.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONT ROL/IGNORE_ERROR (#PCDATA)	Set to 1 when the ignore error option is enabled for the control. When enabled, the service marks control instances as Passed in cases where an error occurs during control evaluation.



XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/IGNORE_ITEM_NOT_FOUND (#PCDATA)	Set to 1 when the ignore item not found option is enabled for the control. When enabled the service will show a status of Passed or Failed in cases where a control returns error code 2 “item not found” (e.g. scan did not find file, registry, or related data, as appropriate for the control type), depending on the status you prefer (defined in the policy).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/REFERENCE_LIST (REFERENCE*)	A list of user-defined references.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/REFERENCE_LIST/REFERENCE (REF_DESCRIPTION?, URL?)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/REFERENCE_LIST/REFERENCE/REF_DESCRIPTION (#PCDATA)	A user-defined description for a reference to an internal policy or document.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/REFERENCE_LIST/REFERENCE/URL (#PCDATA)	A URL for a reference to an internal policy or document
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS	(REG_HIVE?, REG_KEY?, REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?, WMI_QUERY?, SHARE_USER?, PATH_USER?, BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?, DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?, WIN_FILE_SYS_OBJECT_TYPES?, MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?, WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?, GROUP_NAME_LIMIT?, DATA_TYPE, DESCRIPTION)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/REG_HIVE (#PCDATA)	A Windows registry hive: HKEY_CLASSES_ROOT (HKCR)   HKEY_CURRENT_USER (HKCU)   HKEY_LOCAL_MACHINE (HKLM)   HKEY_USERS (HKU).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/REG_KEY (#PCDATA)	A Windows registry key.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/REG_VALUE_NAME (#PCDATA)	A value for a Windows registry key.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FILE_PATH (#PCDATA)	A pathname to a file or directory.

<b>XPath</b>	<b>element specifications / notes</b>
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FILE_QUERY (#PCDATA)	A query for a file content check.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/HASH_TYPE (#PCDATA)	An algorithm to be used for computing a file hash: MD5   SHA-1   SHA-256.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WMI_NS (#PCDATA)	A WMI namespace for a WMI query check.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WMI_QUERY (#PCDATA)	A WMI query for a WMI query check.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/SHARE_USER (#PCDATA)	A user name who can access a share for a share access check.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PATH_USER (#PCDATA)	A user name who can access a directory for a share access check.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/BASE_DIR (#PCDATA)	For directory search, the base directory to start search from.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/SHOULD_DESCEND (#PCDATA)	For directory search, set to “true” when search extends into other file systems found; otherwise set to “false”.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/DEPTH_LIMIT (#PCDATA)	For directory search, depth level for searching each directory: only directory properties (0), directory contents (1) or multiple levels below the base directory (2-10).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FOLLOW_SYMLINK (#PCDATA)	For directory search, set to “true” when target destination files and directories will be analyzed; otherwise set to “false”.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FILE_NAME_MATCH (#PCDATA)	For directory search, a filename to match, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FILE_NAME_SKIP (#PCDATA)	For directory search, a filename to skip, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.

## XPath

## element specifications / notes

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/DIR\_NAME\_MATCH (#PCDATA)

For directory search, a directory name to match, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/DIR\_NAME\_SKIP (#PCDATA)

For directory search, a directory name to skip, i.e. a Windows wildcard expression or a Unix globbing (wildcard) expression.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERM\_COND (#PCDATA)

For Unix directory search, match “all” permissions or “some” permissions set in PERMISSIONS, or “exclude” (i.e. ignore files with certain permissions).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/TYPE\_MATCH (#PCDATA)

For Unix directory search, match system objects specified as string of comma separated codes: d (directory), f (regular file), l (symbolic link), p (named pipe, FIFO), b (block special - buffered), c (character special - unbuffered), s (socket), D (door, Solaris only). Sample string: d,f,l

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/USER\_OWNER (#PCDATA)

For Unix directory search, match files owned by certain users specified as comma separated list of user names and/or UUIDs.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/GROUP\_OWNER (#PCDATA)

For Unix directory search, match files owned by certain groups specified as comma separated list of group names and/or GUIDs.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/TIME\_LIMIT (#PCDATA)

For a Unix directory search, the search time limit in seconds.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/MATCH\_LIMIT (#PCDATA)

For a Unix directory search, the maximum number of objects matched.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/WIN\_PERMISSION\_MATCH (#PCDATA)

For Windows directory search, match “Any” (i.e. at least one of the permissions set or “All” (i.e. files that match all of the permissions set) in WIN\_BASIC\_PERMISSIONS.

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/MATCH\_WELL\_KNOWN\_USERS\_FOR\_ANY\_DOMAIN (#PCDATA)

For Windows directory search, when set to “Yes” we’ll perform a look up of the users set in <WIN\_PERMISSION\_USERS> and match against well-known users, groups and aliases.

<b>XPath</b>	<b>element specifications / notes</b>
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WIN_PERMISSION_USERS (#PCDATA)	For Windows directory search, comma separated list of principals with permissions to the files/directories to match.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/GROUP_NAME (#PCDATA)	Windows local group name to get a list of members for.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/GROUP_NAME_LIMIT (#PCDATA)	The maximum number of results (1 to 1000) to be returned for Windows group name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/DATA_TYPE (#PCDATA)	A scan parameter that identifies a valid data type for the actual value provided by the service: Boolean   Integer   String   String List   Line List
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS	(SPECIAL, USER, GROUP, OTHER)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/SPECIAL	(SPECIAL_USER, SPECIAL_GROUP, SPECIAL_DELETION)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/SPECIAL/SPECIAL_USER (#PCDATA)	For Unix directory search, indicates whether the special set user ID on execution permission is set on the file: Yes, No or Any (either setting is fine).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/SPECIAL/SPECIAL_GROUP (#PCDATA)	For Unix directory search, indicates whether the special set group ID on execution permission is set on the file: Yes, No or Any (either setting is fine).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/SPECIAL/SPECIAL_DELETION (#PCDATA)	For Unix directory search, indicates whether the special restricted deletion (directory) or sticky bit (file) permission is set: Yes, No or Any (either setting is fine).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/USER (READ,WRITE, EXECUTE)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PERMISSIONS/USER/READ (#PCDATA)	For Unix directory search, indicates whether Read permission is set for User: Yes, No or Any (either setting is fine).

## XPath

## element specifications / notes

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/USER/WRITE (#PCDATA)

For Unix directory search, indicates whether Write permission is set for User: Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/USER/EXECUTE (#PCDATA)

For Unix directory search, indicates whether Execute permission is set for User: Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/GROUP (READ,WRITE, EXECUTE)

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/GROUP/READ (#PCDATA)

For Unix directory search, indicates whether Read permission is set for Group: Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/GROUP/WRITE (#PCDATA)

For Unix directory search, indicates whether Write permission is set for Group: Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/GROUP/EXECUTE (#PCDATA)

For Unix directory search, indicates whether Execute permission is set for Group: Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/OTHER (READ,WRITE, EXECUTE)

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/OTHER/READ (#PCDATA)

For Unix directory search, indicates whether Read permission is set for Others (all other users of the system): Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/OTHER/WRITE (#PCDATA)

For Unix directory search, indicates whether Write permission is set for Others (all other users of the system): Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/PERMISSIONS/OTHER/EXECUTE (#PCDATA)

For Unix directory search, indicates whether Execute permission is set for Others (all other users of the system): Yes, No or Any (either setting is fine).

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/WIN\_PERMISSIONS

(WIN\_BASIC\_PERMISSIONS?, WIN\_ADVANCED\_PERMISSIONS?)

/POLICY\_EXPORT\_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER\_DEFINED\_CONTROL/SCAN\_PARAMETERS/WIN\_PERMISSIONS/WIN\_BASIC\_PERMISSIONS

(WIN\_BASIC\_PERMISSION\_TYPE+)

**XPath**

**element specifications / notes**

/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS/WIN_BASIC_PERMISSIONS/WIN_BASIC_PERMISSION_TYPE (#PCDATA)	For Windows directory search, match basic permission: Full Control   Modify   List Folder   Content   Read & Execute   Write   Read
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS/WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSION_TYPE+)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS/WIN_ADVANCED_PERMISSIONS/WIN_ADVANCED_PERMISSION_TYPE (#PCDATA)	For Windows directory search, match advanced permission: Full Control   Traverse Folder   Execute Files   List Folder/Read Data   Read Attributes   Read Extended Attributes   Create Files/Write Data   Create Folders/Append Data   Write Attributes   Write Extended Attributes   Delete Sub-folders & Files   Delete   Read Permissions   Change Permissions   Take Ownership
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/WIN_FILE_SYS_OBJECT_TYPES (#PCDATA)	For Windows directory search, types of system objects to search: DIRECTORY, FILE or DIRECTORY FILE (i.e. both directory and file).
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/ (OP_ACRONYMS, DATA_POINT_ACRONYMS+)>	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/OP_ACRONYMS (OP+)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/OP_ACRONYMS/ OP	The acronym for operator option set in the compliance policy for the data point, if applicable. Possible values depending on the data type: ge   gt   le   lt   eq   ne   in   range   re   xre   xeq   no op. See “Operator Names” below.
attribute: id	Indicates operator <b>id</b> .
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/DATA_POINT_ACRONYMS/ (DP+)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/DATA_POINT_ACRONYMS/ K	The acronym for the service-defined, unique name for the data point.
attribute: id	Indicates <b>id</b> of the service-defined, unique name for the data point.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/APPENDIX/DATA_POINT_ACRONYMS/ FV	A fixed expected value for the data point in the compliance policy. A fixed value cannot be changed in the policy. It can only be selected/deselected.
attribute: id	Indicates <b>id</b> of the fixed expected value for the data point in the compliance policy.

## Operator Names

Operator	Description	Operator	Description
ge	greater than or equal to	in	in
gt	greater than	range	in range
le	less than or equal to	re	regular expression
lt	less than	xre	regular expression list
eq	equal to	xeq	string list
ne	not equal to	no op	no operator

# Compliance Posture Information Output

The compliance posture information output XML is returned from an API request for compliance posture information. The DTD for the compliance posture info output XML is described below.

DTD:

[https://<basurl>/api/2.0/fo/compliance/posture/info/posture\\_info\\_list\\_output.dtd](https://<basurl>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd)

## DTD for Compliance Posture Information Output

A recent DTD for the compliance posture information output is shown below.

```
<!-- QUALYS POSTURE_INFO_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT POSTURE_INFO_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, ((INFO_LIST?, SUMMARY?, WARNING_LIST?,
GLOSSARY?) | POLICY+))>

<!ELEMENT POLICY (ID, DATETIME, INFO_LIST?, SUMMARY?, WARNING_LIST?,
GLOSSARY?)>

<!ELEMENT INFO_LIST (INFO+)>
<!ELEMENT INFO (ID, HOST_ID, CONTROL_ID, TECHNOLOGY_ID, INSTANCE?, STATUS,
REMEDIATION?, POSTURE_MODIFIED_DATE?, EXCEPTION?,
EVIDENCE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT CONTROL_ID (#PCDATA)>
<!ELEMENT TECHNOLOGY_ID (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT POSTURE_MODIFIED_DATE (#PCDATA)>
```



```

<!ELEMENT EXCEPTION (ASSIGNEE, STATUS, END_DATETIME?, CREATED?,
                      LAST_MODIFIED?, COMMENT_LIST?)>
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT END_DATETIME (#PCDATA)>
<!ELEMENT CREATED (BY, DATETIME)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (BY, DATETIME)>
<!ELEMENT COMMENT_LIST (COMMENT+)>
<!ELEMENT COMMENT (DATETIME, BY, TEXT)>
<!ELEMENT TEXT (#PCDATA)>

<!ELEMENT EVIDENCE (BOOLEAN_EXPR, DPV_LIST?)>
<!ELEMENT BOOLEAN_EXPR (#PCDATA)>
<!ELEMENT DPV_LIST (DPV+)>
<!ELEMENT DPV (LABEL, (ERROR|V)+, TM_REF?)>
<!ATTLIST DPV lastUpdated CDATA #IMPLIED>

<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT ERROR (#PCDATA)>
<!ELEMENT V (#PCDATA)>
<!ELEMENT TM_REF (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?, HOST_LIST, CONTROL_LIST?,
                    TECHNOLOGY_LIST?, DPD_LIST?, TP_LIST?, FV_LIST?,
                    TM_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, IP, TRACKING_METHOD, DNS?, NETBIOS?, OS?, OS_CPE?,
                LAST_VULN_SCAN_DATETIME?, LAST_COMPLIANCE_SCAN_DATETIME?,
                PERCENTAGE?)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT LAST_VULN_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)>
<!ELEMENT PERCENTAGE (#PCDATA)>

<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, STATEMENT, CRITICALITY?, DEPRECATED?,
                  RATIONALE_LIST?)>
<!ELEMENT STATEMENT (#PCDATA)>

```

```
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT DEPRECATED (#PCDATA)>
<!ELEMENT RATIONALE_LIST (RATIONALE*)>
<!ELEMENT RATIONALE (TECHNOLOGY_ID, TEXT)>

<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT NAME (#PCDATA)>

<!ELEMENT DPD_LIST (DPD+)>
<!ELEMENT DPD (LABEL, ID?, NAME?, DESC)>
<!ELEMENT DESC (#PCDATA)>

<!ELEMENT TP_LIST (TP+)>
<!ELEMENT TP (LABEL, V+)>

<!ELEMENT FV_LIST (FV+)>
<!ELEMENT FV (LABEL, V*)>

<!ELEMENT TM_LIST (TM+)>
<!ELEMENT TM (LABEL, PAIR+)>
<!ELEMENT PAIR (K, V)>
<!ELEMENT K (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT SUMMARY (TOTAL_ASSETS, TOTAL_CONTROLS, CONTROL_INSTANCES)>
<!ELEMENT TOTAL_ASSETS (#PCDATA)>
<!ELEMENT TOTAL_CONTROLS (#PCDATA)>
<!ELEMENT CONTROL_INSTANCES (TOTAL, TOTAL_PASSED, TOTAL_FAILED,
                              TOTAL_ERROR, TOTAL_EXCEPTIONS)>
<!ELEMENT TOTAL (#PCDATA)>
<!ELEMENT TOTAL_PASSED (#PCDATA)>
<!ELEMENT TOTAL_FAILED (#PCDATA)>
<!ELEMENT TOTAL_ERROR (#PCDATA)>
<!ELEMENT TOTAL_EXCEPTIONS (#PCDATA)>
<!-- EOF -->
```

## XPaths for Compliance Posture Information Output

This section describes the XPaths for the compliance posture information output.

### Compliance Posture Information Output: Request

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT	(REQUEST?, RESPONSE)
/POSTURE_INFO_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/POSTURE_INFO_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/POSTURE_INFO_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/POSTURE_INFO_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/POSTURE_INFO_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/POSTURE_INFO_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/POSTURE_INFO_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/POSTURE_INFO_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/POSTURE_INFO_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.

### Compliance Posture Information Output: Response

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT	(REQUEST?, RESPONSE)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE	(DATETIME, ((INFO_LIST?, SUMMARY?, WARNING_LIST?, GLOSSARY?)   POLICY+))
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY	(ID, DATETIME, INFO_LIST?, SUMMARY?, WARNING_LIST?, GLOSSARY?)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/ID	(#PCDATA) The ID of a policy when “policy_ids” was specified.

<b>XPath</b>	<b>element specifications / notes</b>
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/DATETIME (#PCDATA)	The date and time when the policy's posture info was collected from the API user's account.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST (INFO+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO	(ID, HOST_ID, CONTROL_ID, TECHNOLOGY_ID, INSTANCE?, STATUS, REMEDIATION?, EXCEPTION?, EVIDENCE?)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/ID (#PCDATA)	A compliance posture info record ID.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/HOST_ID (#PCDATA)	A host ID for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CONTROL_ID (#PCDATA)	A control ID for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/INSTANCE (#PCDATA)	An instance value for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/STATUS (#PCDATA)	A compliance status for a compliance posture info record: Passed, Failed or Error. Error is returned only for a custom control in the case where an error occurred during control evaluation (and the ignore errors configuration option was not selected for the control).
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/REMEDiation (#PCDATA)	Remediation information for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION	(ASSIGNEE, STATUS, END_DATETIME?, CREATED?, LAST_MODIFIED?, COMMENT_LIST?)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/ASSIGNEE (#PCDATA)	An assignee for an exception for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/STATUS (#PCDATA)	The status of an exception for a compliance posture info record: Pending (approval), Accepted, Rejected or Expired.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/END_DATETIME (#PCDATA)	The date/time when an exception for a compliance posture info record expires (ends).
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/CREATED (BY, DATETIME)	The date/time when an exception for a compliance posture info record was created, and the user login ID of the user who created it.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/LAST_MODIFIED (BY, DATETIME)	The date/time when an exception for a compliance posture info record was last modified, and the user login ID of the user who modified it.

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/COMMENT_LIST (COMMENT+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EXCEPTION/COMMENT_LIST/COMMENT	(DATETIME, BY, TEXT)
	The date/time when comments were entered for an exception for a compliance posture info record, the user login ID of the user who entered these comments, and the text of the comments entered.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE (BOOLEAN_EXPR, DPV_LIST?)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/BOOLEAN_EXPR (#PCDATA)	A Boolean expression string representing a data point rule for a control, which is used by the service to evaluate data point information gathered by the most recent compliance scan of the host. A data point rule is derived from a policy in the user's account. To understand why a posture info record has a Passed or Failed compliance status, take this boolean expression and plug in the data point "actual" values gathered from the most recent compliance scan in <DPV_LIST> and "expected" values as defined in the policy in <FV_LIST> or <TP_LIST>.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST (DPV+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV	(LABEL, (ERROR   V)+, TM_REF?)
attribute: <b>lastUpdated</b>	<b>lastUpdated</b> is the most recent date/time the datapoint was scanned.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/LABEL (#PCDATA)	A label for a data point in the data point rule. This is a service-generated value in the format :dp_x such as :dp_1, :dp_2, :dp_3... These labels are not persistent and change each time an API call is made.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/ERROR (#PCDATA)	An error for a data point. The value NOT_FOUND is returned when a data point which is needed to evaluate a Boolean expression (in <BOOLEAN_EXPR>) was not detected on the host. When returned, no data point values are returned in <V> elements under <DPV_LIST>.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/V (#PCDATA)	A data point "actual" value, as returned from the most recent compliance scan.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/TM_REF (#PCDATA)	A translation context reference. This is a service-generated value in the format @tm_x such as @tm_1, @tm_2, @tm_3... These labels are not persistent and change each time an API call is made.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY	(TOTAL_ASSETS, TOTAL_CONTROLS, CONTROL_INSTANCES)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/TOTAL_ASSETS (#PCDATA)	Total number of hosts evaluated.

<b>XPath</b>	<b>element specifications / notes</b>
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/TOTAL_CONTROLS (#PCDATA)	Total number of controls evaluated.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES (TOTAL, TOTAL_PASSED, TOTAL_FAILED, TOTAL_ERROR, TOTAL_EXCEPTIONS)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES/ TOTAL (#PCDATA)	Total number of control instances evaluated.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES/ TOTAL_PASSED (#PCDATA)	Total number of control instances with passed status.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES/ TOTAL_FAILED (#PCDATA)	Total number of control instances with failed status
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES/ TOTAL_ERROR (#PCDATA)	Total number of control instances with error status.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/SUMMARY/CONTROL_INSTANCES/ TOTAL_EXCEPTIONS (#PCDATA)	Total number of control instances with exceptions.

## Compliance Posture Information Output: Glossary

<b>XPath</b>	<b>element specifications / notes</b>
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY	(USER_LIST?, HOST_LIST, CONTROL_LIST?, TECHNOLOGY_LIST?, DPD_LIST?, TP_LIST?, FV_LIST?, TM_LIST?)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST (USER+)	A list of users who created, modified, or added comments to exceptions associated with compliance posture info records which are included in the posture information output.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER (USER_LOGIN, FIRST_NAME, LAST_NAME)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER (#PCDATA)	A user login ID associated with an exception in a posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/FIRST_NAME (#PCDATA)	The first name of an account user associated with an exception in a posture info record.

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/LAST_NAME (#PCDATA)	The last name of an account user associated with an exception in a posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST (HOST+)	A list of hosts in compliance posture info records which are included in the posture list output.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST (ID, IP, TRACKING_METHOD, DNS?, NETBIOS?, OS?, OS_CPE?, LAST_VULN_SCAN_DATETIME?, LAST_COMPLIANCE_SCAN_DATETIME?, PERCENTAGE?)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/ID (#PCDATA)	A host ID for a host in a posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/IP (#PCDATA)	An IP address for a host in a posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The tracking method for a host in a posture info record: IP, DNS NETBIOS, or AGENT.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/DNS (#PCDATA)	The DNS user name for a host in a posture info record, when available.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/NETBIOS (#PCDATA)	The NetBIOS user name for a host in a posture info record, when available.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/OS (#PCDATA)	The operating system detected on a host in a posture info record, when available.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/OS_CPE (#PCDATA)	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/ LAST_VULN_SCAN_DATETIME (#PCDATA)	The date/time when a vulnerability scan was most recently launched on a host in a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/ LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)	The date/time when a compliance scan was most recently launched on a host in a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/PERCENTAGE (#PCDATA)	The percentage of controls that passed for the host. For example “85.71% (84 of 98)” mean 85.71% of the controls passed, 84 controls passed and 98 controls were evaluated).

<b>XPath</b>	<b>element specifications / notes</b>
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST (CONTROL+)	A list of compliance controls in compliance posture info records which are included in the posture information output.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL (ID, STATEMENT, CRITICALITY?, DEPRECATED?, RATIONALE_LIST?)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/ID (#PCDATA)	A control ID.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	A control statement.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/CRITICALITY/LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/DEPRECATED (#PCDATA)	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/RATIONALE_LIST (RATIONALE*)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/RATIONALE_LIST/RATIONALE (TECHNOLOGY_ID, TEXT)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/RATIONALE_LIST/RATIONALE/TECHNOLOGY_ID (#PCDATA)	An ID for a technology associated with a control's rationale..
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/CONTROL_LIST/CONTROL/RATIONALE_LIST/RATIONALE/TEXT (#PCDATA)	A text description associated with a control's rationale.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TECHNOLOGY_LIST (TECHNOLOGY+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TECHNOLOGY_LIST/TECHNOLOGY (ID, NAME)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TECHNOLOGY_LIST/TECHNOLOGY/ID (#PCDATA)	An ID for a technology in a posture info record.



XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TECHNOLOGY_LIST/TECHNOLOGY/NAME (#PCDATA)	A name for a technology in a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST (DPD+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST/DPD (LABEL, ID?, NAME?, DESC)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST/DPD/LABEL (#PCDATA)	A service-defined, internal label for a data point.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST/DPD/ID? (#PCDATA)	A service-defined, ID for a data point.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST/DPD/NAME? (#PCDATA)	A service-defined, name for a data point.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/DPD_LIST/DPD/DESC (#PCDATA)	A description for a data point, which corresponds to a data point label in a <LABEL> element.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TP_LIST (TP+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TP_LIST/TP (LABEL, V+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TP_LIST/TP/LABEL (#PCDATA)	A label for a data point text pattern as defined in a policy. This is a service-generated value \$tp_x such as \$tp_1, \$tp_2, \$tp_3... The data point text pattern labels are not persistent and change each time an API call is made.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TP_LIST/TP/V (#PCDATA)	A data point text pattern value in a policy.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/FV_LIST (FV+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/FV_LIST/FV (LABEL, V*)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/FV_LIST/FV/LABEL (#PCDATA)	A label for a fixed value selection in a policy. This is a service-generated value #fv_x such as #fv_1, #fv_2, #fv_3... The data point fixed value labels are not persistent and change each time an API call is made.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/FV_LIST/FV/V (#PCDATA)	A data point fixed value selection in a policy.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST (TM+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST/TM (LABEL, PAIR+)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST/TM/LABEL (#PCDATA)	A translation context reference. This is a service-generated value in the format @tm_x such as @tm_1, @tm_2, @tm_3... These labels are not persistent and change each time an API call is made.

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST/TM/PAIR	(K, V)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST/TM/PAIR/K	(#PCDATA)
	A translation context key in a mapping pair. This represents a raw, untranslated value returned by the scanning engine.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TM_LIST/PAIR/V	(#PCDATA)
	A translation context value in a mapping pair. This represents the meaning associated with the raw value in the mapping pair.

**Compliance Posture Information Output: Warning**

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/WARNING_LIST	(WARNING+)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/WARNING	(CODE?, TEXT, URL?)
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/WARNING/CODE	(#PCDATA)
	A warning code. A warning code appears when the API request identifies more than 5,000 records (compliance posture info records).
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/WARNING/TEXT	(#PCDATA)
	A warning message. A warning message appears when the API request identifies more than 5,000 records (compliance posture info records).
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/WARNING/URL	(#PCDATA)
	A URL for making another API request for the next batch of records (compliance posture info records).

## Compliance Evidence

This sections provides details about the compliance evidence information in the compliance posture information output (posture\_info\_output.dtd).

### Boolean Expression

To understand why a control has a certain compliance status, take the boolean expression for a posture info record in this element:

```
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/BOOLEAN_EXPR
```

and plug in the data point “actual” values (such as :dp\_1, :dp\_2, :dp3, etc.) found in this element:

```
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST
```

and text pattern “expected” values (such as \$tp\_1, \$tp2, \$tp3, etc.) found in this element:

```
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/TP_LIST
```

or fixed value selection “expected” values (such as #fv\_1, #fv\_2, #fv\_3, etc.) found in this element:

```
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/FV_LIST
```

### Boolean Expression: Data Type Operators

The following operators may be used to construct a Boolean expression string. The operators are specific to the data type of the data point value.

For all operator descriptions: X is the “actual” data point value (in the most recent scan results) compared to Y which is the “expected” value (in a policy).

Operator	Description	Data Type	Example
>	X is greater than Y	Integer	:dp_1 > 3
<	X is less than Y	Integer	:dp_1 < 5
>=	X is greater than or equal to Y	Integer	:dp_2 >= 4
<=	X is less than or equal to Y	Integer	:dp_2 <= 2
==	X is equal to Y	Integer	:dp_1 == 2
!(X)	X not equal to Y	Integer	!(:dp_1 > 5)
matches	X matches Y	Regular Expression	:dp_4 matches \$tp_1

**Boolean Expression: Cardinality Operators**

The following cardinality operators may be used to construct a Boolean expression string.

A cardinality operator is used to:

- Compare multiple “actual” values to a single “expected” value for a control
- Compare multiple “actual” values to multiple “expected” values for a control

For all cardinality operator descriptions: X is the “actual” data point value (in the most recent scan results) compared to Y which is the “expected” value (in a policy).

Cardinality Operator	Description	Data Type in List	Example
match_any	Match any X in Y	Integer Regular Expression	:dp_1 match_any \$tp_5
match_all	Match all X in Y	Integer Regular Expression	:dp_1 match_all \$tp_5
empty	X is empty	Integer Regular Expression	:dp_8 empty
not_empty	X is not empty	Integer Regular Expression	:dp_8 not_empty
contains	X contains all of Y	Integer Regular Expression	:dp_2 contains \$tp_2
does_not_contain	X does not contain any of Y	Integer Regular Expression	:dp_2 does_not_contain \$tp_1
intersect	Any value in X matches any value in Y	Integer Regular Expression	:dp_3 intersect \$tp_5
matches	All values in X match all values in Y	Integer Regular Expression	:dp_3 matches \$tp_2
is_contained_in	All values in X are contained in Y	Integer Regular Expression	:dp_9 is_contained_in \$tp_3

## Boolean Expression: Logical Grouping Operators

The following logical grouping operators may be used to construct a Boolean expression string.

For all operator descriptions: X is the “actual” data point value (in the most recent scan results) compared to Y which is the “expected” value (in a policy).

Operator	Description	Example
(X)	Evaluates subexpression X before evaluating anything outside of the parentheses	(:dp_1 > 5)
and	Combines two logical subexpressions (ANDed)	(:dp_1 < 4) and (:dp_1 > 8)
or	Combines two logical subexpressions (ORed)	(:dp_1 < 4) or (:dp_1 > 8)

## Control Values

Certain values appear in data point control values, for example registry permissions and file/directory permissions. For information on control values, log into your Qualys account and search for “control values” in the help.

# Compliance Policy Report

The policy report XML is returned when you download a saved policy report using the Report Share API. The DTD for the compliance policy report XML is described below and sample XML output for the three evaluation types is also provided.

DTD: [https://<baseurl>/compliance\\_policy\\_report.dtd](https://<baseurl>/compliance_policy_report.dtd)

## DTD for Compliance Policy Report

A recent DTD for the compliance policy report output (compliance\_policy\_report.dtd) is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE POLICY REPORT DTD -->

<!ELEMENT COMPLIANCE_POLICY_REPORT (ERROR | (HEADER, (SUMMARY),
(RERESULTS)))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO,
FILTERS)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT FILTERS (POLICY, POLICY_LOCKING?, ASSET_GROUPS?, IPS?,
HOST_INSTANCE?, ASSET_TAGS?, PC_AGENT_IPS?, POLICY_LAST_EVALUATED)>
<!ELEMENT POLICY (#PCDATA)>
<!ELEMENT POLICY_LOCKING (#PCDATA)>

<!ELEMENT ASSET_GROUPS (ASSET_GROUP?)>
<!ELEMENT ASSET_GROUP (ID, NAME)>

<!ELEMENT IPS (IP_LIST?, NETWORK?)>
```

```

<!ELEMENT IP_LIST (IP)>
<!ELEMENT NETWORK (#PCDATA)>

<!ELEMENT INCLUDED_TAGS (SCOPE, TAGS)>
<!ELEMENT EXCLUDED_TAGS (SCOPE, TAGS)>
<!ELEMENT TAGS (NAME*)>
<!ELEMENT SCOPE (#PCDATA)>

<!ELEMENT HOST_INSTANCE (IP?, INSTANCE?)>

<!ELEMENT PC_AGENT_IPS (#PCDATA)>

<!ELEMENT POLICY_LAST_EVALUATED (#PCDATA)>
<!ELEMENT SUMMARY (TOTAL_ASSETS, TOTAL_CONTROLS, CONTROL_INSTANCES,
CONTROLS_SUMMARY?, HOST_STATISTICS?)>
<!ELEMENT CONTROL_INSTANCES (TOTAL, TOTAL_PASSED, TOTAL_FAILED,
TOTAL_ERROR, TOTAL_EXCEPTIONS)>
<!ELEMENT TOTAL (#PCDATA)>
<!ELEMENT TOTAL_ASSETS (#PCDATA)>
<!ELEMENT TOTAL_CONTROLS (#PCDATA)>
<!ELEMENT TOTAL_PASSED (#PCDATA)>
<!ELEMENT TOTAL_FAILED (#PCDATA)>
<!ELEMENT TOTAL_ERROR (#PCDATA)>
<!ELEMENT TOTAL_EXCEPTIONS (#PCDATA)>

<!ELEMENT CONTROLS_SUMMARY (CONTROL_INFO*)>
<!ELEMENT CONTROL_INFO (ORDER, CONTROL_ID, STATEMENT, CRITICALITY?,
PERCENTAGE, DEPRECATED?)>
<!ELEMENT CONTROL_ID (#PCDATA)>
<!ELEMENT ORDER (#PCDATA)>
<!ELEMENT PERCENTAGE (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT DEPRECATED (#PCDATA)>

<!ELEMENT RESULTS ( HOST_LIST, CHECKS?, DP_DESCRIPTIONS?) >
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, OPERATING_SYSTEM?,
OS_CPE?, LAST_SCAN_DATE?, TOTAL_PASSED, TOTAL_FAILED, TOTAL_ERROR,
TOTAL_EXCEPTIONS, ASSET_TAGS?, CONTROL_LIST, NETWORK?)>

<!ELEMENT CHECKS (CHECK*)>
<!ELEMENT CHECK (NAME, DP_NAME, EXPECTED, ACTUAL, ADDED_DIRECTORIES?,
REMOVED_DIRECTORIES?, PERMISSON_CHANGED_DIRECTORIES?,
CONTENT_CHANGED_DIRECTORIES?, PERMISSION_TRANSLATION?,
EXTENDED_EVIDENCE?, STATISTICS?)>
<!ELEMENT DP_NAME (#PCDATA)>
<!ELEMENT EXTENDED_EVIDENCE (#PCDATA)>
<!ELEMENT STATISTICS (STATS*, SEARCH_DURATION?, ERRORS?)>
<!ELEMENT EVALUATION (#PCDATA)>

```

```
<!ELEMENT EXPECTED (V*, CRITERIA?)>
<!ATTLIST EXPECTED logic CDATA #FIXED "OR">
<!ELEMENT CRITERIA (EVALUATION, V*)>
<!ELEMENT ACTUAL (V*)>
<!ELEMENT V (#PCDATA)>
<!ATTLIST ACTUAL lastUpdated CDATA #IMPLIED>

<!ELEMENT ADDED_DIRECTORIES (V*)>
<!ELEMENT REMOVED_DIRECTORIES (V*)>
<!ELEMENT PERMISSON_CHANGED_DIRECTORIES (V*)>
<!ELEMENT CONTENT_CHANGED_DIRECTORIES (V*)>

<!ELEMENT PERMISSION_TRANSLATION (PAIR+)>
<!ELEMENT PAIR (K, V)>
<!ELEMENT K (#PCDATA)>

<!ELEMENT DP_DESCRIPTIONS (DP*)>
<!ELEMENT DP (DP_NAME, DESCRIPTION, SCAN_PARAMETERS?)>
<!ELEMENT DESCRIPTION (#PCDATA) >

<!ELEMENT SCAN_PARAMETERS (PARAM*)>
<!ELEMENT PARAM (LABEL, VALUE)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>

<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>
<!ELEMENT ASSET_TAGS (ASSET_TAG*|(INCLUDED_TAGS?, EXCLUDED_TAGS?))>
<!ELEMENT ASSET_TAG (#PCDATA)>

<!ELEMENT CONTROL_LIST (CONTROL*)>
<!ELEMENT CONTROL (CID, STATEMENT, CRITICALITY?, CONTROL_REFERENCES?,
DEPRECATED?, RATIONALE?, INSTANCE?, STATUS, REMEDIATION?, TECHNOLOGY,
EVALUATION_DATE?, EVIDENCE?, EXCEPTION?)>
<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CONTROL_REFERENCES (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT EVALUATION_DATE (#PCDATA)>
```



```
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT EVIDENCE (#PCDATA)>
<!ELEMENT EXCEPTION (ASSIGNEE, STATUS, END_DATE, CREATED_BY, CREATED_DATE,
MODIFIED_BY, MODIFIED_DATE, COMMENT_LIST?)>
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT END_DATE (#PCDATA)>
<!ELEMENT CREATED_BY (#PCDATA)>
<!ELEMENT CREATED_DATE (#PCDATA)>
<!ELEMENT MODIFIED_BY (#PCDATA)>
<!ELEMENT MODIFIED_DATE (#PCDATA)>

<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT COMMENT_LIST (COMMENT+)>
<!ELEMENT COMMENT (DATETIME, BY, TEXT)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT BY (#PCDATA)>

<!ELEMENT HOST_STATISTICS (HOST_INFO*)>
<!ELEMENT HOST_INFO (IP, TRACKING_METHOD, DNS, NETBIOS, OPERATING_SYSTEM,
LAST_SCAN_DATE, PERCENTAGE, NETWORK?)>

<!ELEMENT STATS (#PCDATA)>
<!ELEMENT SEARCH_DURATION (#PCDATA)>
<!ELEMENT ERRORS (#PCDATA)>
```

XPaths for Compliance Policy Report

The XPaths for the compliance policy report are described below.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT	(ERROR   (HEADER, (SUMMARY), (RESULTS)))
/COMPLIANCE_POLICY_REPORT/ERROR	(#PCDATA)
	An error message.
attribute: number	An error code, when available
/COMPLIANCE_POLICY_REPORT/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO, FILTERS)
/COMPLIANCE_POLICY_REPORT/HEADER/NAME	(#PCDATA)
	The report title as provided by the user at the time the report was generated. If a report title was not provided, then the report template title appears.
/COMPLIANCE_POLICY_REPORT/HEADER/GENERATION_DATETIME	(#PCDATA)
	The date and time when the report was generated.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_REPORT/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user's company name and address, as defined in the user's account.
/COMPLIANCE_POLICY_REPORT/HEADER/USER_INFO	(NAME, USERNAME, ROLE)
/COMPLIANCE_POLICY_REPORT/HEADER/USER_INFO/NAME	(#PCDATA)
	The name of the user who generated the report.
/COMPLIANCE_POLICY_REPORT/HEADER/USER_INFO/USERNAME	(#PCDATA)
	The user login ID of the user who generated the report.
/COMPLIANCE_POLICY_REPORT/HEADER/USER_INFO/ROLE	(#PCDATA)
	The user role assigned to the user who generated the report: Manager, Unit Manager, Auditor, Scanner, or Reader.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS	(POLICY, POLICY_LOCKING?, ASSET_GROUPS?, IPS?, HOST_INSTANCE?, ASSET_TAGS?, PC_AGENT_IPS?, POLICY_LAST_EVALUATED)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/POLICY	(#PCDATA)
	The title of the policy included in the report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/POLICY_LOCKING	(#PCDATA)
	The locking status for the policy included in the report: Locked or Unlocked.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_GROUPS	(ASSET_GROUP?)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_GROUP	(ID, NAME)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_GROUP/ID	(#PCDATA)
	IP of the asset group in the report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_GROUPS/ASSET_GROUP/NAME	(#PCDATA)
	Name of the asset group in the report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/IPS	(IP_LIST?, NETWORK?)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/IPS/IP_LIST	(IP)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/IPS/IP_LIST/IP	(#PCDATA)
	IP in the report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/IPS/NETWORK	(#PCDATA)
	Network of the IPs in the report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/HOST_INSTANCE	(IP?, INSTANCE?)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/HOST_INSTANCE/IP	(#PCDATA)
	IP of host instance in report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/HOST_INSTANCE/INSTANCE	(#PCDATA)
	ID of host instance in report.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS	(INCLUDED_TAGS?)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/INCLUDED_TAGS	(SCOPE, TAGS)
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/INCLUDED_TAGS/SCOPE	(#PCDATA)
	Tag selection scope for included tags i.e. any, all etc.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/INCLUDED_TAGS/TAGS (NAME*)	
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/INCLUDED_TAGS/TAGS/ NAME (#PCDATA)	Tag name of included tag.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS (EXCLUDED_TAGS?)	
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/EXCLUDED_TAGS (SCOPE, TAGS)	
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/EXCLUDED_TAGS/SCOPE (#PCDATA)	Tag selection scope for excluded tags i.e. any, all etc.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/EXCLUDED_TAGS/TAGS (NAME*)	
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/ASSET_TAGS/EXCLUDED_TAGS/TAGS/ NAME (#PCDATA)	Tag name of excluded tag.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/PC_AGENT_IPS (#PCDATA)	
	Flag indicating whether IPs have agents installed with PC enabled.
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/POLICY_LAST_EVALUATED (#PCDATA)	
	The date and time the policy included in the report was last evaluated.
/COMPLIANCE_POLICY_REPORT/SUMMARY	(TOTAL_ASSETS, TOTAL_CONTROLS, CONTROL_INSTANCES, CONTROLS_SUMMARY?, HOST_STATISTICS?)
/COMPLIANCE_POLICY_REPORT/SUMMARY/TOTAL_ASSETS (#PCDATA)	
	The number of hosts in the policy.
/COMPLIANCE_POLICY_REPORT/SUMMARY/TOTAL_CONTROLS (#PCDATA)	
	The number of controls in the policy.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES	(TOTAL, TOTAL_PASSED, TOTAL_FAILED, TOTAL_ERROR, TOTAL_EXCEPTIONS)
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL (#PCDATA)	
	The number of control instances in the report (sum of passed and failed instances).
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_PASSED (#PCDATA)	
	The number of control instances with a Passed status in the report.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_FAILED (#PCDATA)	
	The number of control instances with a Failed status in the report.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_ERROR (#PCDATA)	
	The number of control instances with an Error status in the report. An error status is returned for a custom control only in the case where an error occurred during control evaluation (and the ignore errors configuration option was not selected for the control).
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_EXCEPTIONS (#PCDATA)	
	The number of approved and pending exceptions in the policy report.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY (CONTROL_INFO*)	
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO	(ORDER, CONTROL_ID, STATEMENT, CRITICALITY?, PERCENTAGE, DEPRECATED?)
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/ORDER	(#PCDATA)
	The order number of the control in the policy. Controls in section 1 are numbered 1.1, 1.2, 1.3, and so on. Controls in section 2 are numbered 2.1, 2.2, 2.3, and so on.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/CONTROL_ID	(#PCDATA)
	The control ID number assigned to the control.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/STATEMENT	(#PCDATA)
	The control statement that describes how a technology specific item should be implemented in the environment.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/CRITICALITY	(LABEL, VALUE)
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/CRITICALITY/LABEL (#PCDATA)	
	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/CRITICALITY/VALUE (#PCDATA)	
	A criticality value (0-5) assigned to the control.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/PERCENTAGE	(#PCDATA)
	The percentage of hosts that passed for the control. For example, a value of "50% (3 of 6)" indicates that the control passed on 3 of the 6 hosts included in the report.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROLS_SUMMARY/CONTROL_INFO/DEPRECATED	(#PCDATA)
	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/COMPLIANCE_POLICY_REPORT/RESULTS (HOST_LIST, CHECKS?, DP_DESCRIPTIONS?)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST (HOST*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST	(TRACKING_METHOD, IP, DNS?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?, LAST_SCAN_DATE?, TOTAL_PASSED, TOTAL_FAILED, TOTAL_ERROR, TOTAL_EXCEPTIONS, ASSET_TAGS?, CONTROL_LIST, NETWORK?)
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	
	The tracking method for the host: IP, DNS, NetBIOS, or AGENT.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/IP (#PCDATA)	The IP address for the host.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/DNS (#PCDATA)	The DNS hostname for the host, when available.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/NETBIOS (#PCDATA)	The NetBIOS hostname for the host, when available
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/OPERATING_SYSTEM (#PCDATA)	The operating system detected on the host.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/OS_CPE (#PCDATA)	The OS CPE name assigned to the operating system detected on the host. (The OS CPE name appears only when the OS CPE feature is enabled for the subscription, and an authenticated scan was run on this host after enabling this feature.)
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/LAST_SCAN_DATE (#PCDATA)	The date and time the host was last scanned for compliance.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/ASSET_TAGS (ASSET_TAG*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/ASSET_TAGS/ASSET_TAG (#PCDATA)	An asset tag assigned to the host when the Asset Tagging feature is enabled in the user's account.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/TOTAL_PASSED (#PCDATA)	The number of control in the policy that Passed on the host.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/TOTAL_FAILED (#PCDATA)	The number of controls in the policy that Failed on the host.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/TOTAL_ERROR (#PCDATA)	The number of custom controls in the policy that were assigned the Error status on the host, because an error during control evaluation.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/TOTAL_EXCEPTIONS (#PCDATA)	The number of approved and pending exceptions on the host. This includes control instances with the Failed and Error status.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST (CONTROL*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL	(CID, STATEMENT, CRITICALITY?, CONTROL_REFERENCES?, DEPRECATED?, RATIONALE?, INSTANCE?, STATUS, REMEDIATION?, TECHNOLOGY, EVALUATION_DATE?, EVIDENCE?, EXCEPTION?)
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CID (#PCDATA)	The control ID number assigned to the control.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	The control statement that describes how a technology specific item should be implemented in the environment.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CRITICALITY/LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CONTROL_REFERENCES (#PCDATA)	User-defined references, added to the control using the Qualys user interface.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/DEPRECATED (#PCDATA)	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/RATIONALE (#PCDATA)	A rationale statement that describes how the control should be implemented for the technology.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/INSTANCE (#PCDATA)	Instance information for an Oracle host in this format: Oracle technology version:SID:port. For example: Oracle10:ora102030p:1521.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/STATUS (#PCDATA)	The status for the control on the host: Passed, Failed or Error.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/REMEDIATION (#PCDATA)	Remediation information for the control.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/TECHNOLOGY (ID, NAME))	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/TECHNOLOGY/ID (#PCDATA)	Technology ID for the control.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/TECHNOLOGY/NAME (#PCDATA)	Technology name for the control.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EVIDENCE (#PCDATA)	One or more data point checks that returned results for the control on the host during the scan. The data point checks appear as CHECK1, CHECK2, and so on, which correspond to the <NAME> element for each check.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/NETWORK (#PCDATA)	The network the host belongs to.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION (ASSIGNEE, STATUS, END_DATE, CREATED_BY, CREATED_DATE, MODIFIED_BY, MODIFIED_DATE, COMMENT_LIST?)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/ASSIGNEE (#PCDATA)	The name of the user who is assigned the exception.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/STATUS (#PCDATA)	The exception status: Pending, Accepted, Rejected and Expired.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/END_DATE (#PCDATA)	The date the exception is set to expire. Note that end dates are only relevant to Accepted exceptions.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/CREATED_BY (#PCDATA)	The user who requested the exception.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/CREATED_DATE (#PCDATA)	The date and time the exception was created.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/MODIFIED_BY (#PCDATA)	The user who last modified the exception.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/MODIFIED_DATE (#PCDATA)	The date and time the exception was modified.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/COMMENT_LIST (COMMENT+)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/COMMENT_LIST/COMMENT (DATETIME, BY, TEXT)	
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/COMMENT_LIST/COMMENT/DATETIME (#PCDATA)	The date and time when an action on the exception took place.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/COMMENT_LIST/COMMENT/BY (#PCDATA)	The user who performed the action on the exception.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/EXCEPTION/COMMENT_LIST/COMMENT/TEXT (#PCDATA)	Comments entered by the user who performed the action on the exception.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS (CHECK*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK	(NAME, DP_NAME, EXPECTED, ACTUAL, ADDED_DIRECTORIES?, REMOVED_DIRECTORIES?, PERMISSON_CHANGED_DIRECTORIES?, CONTENT_CHANGED_DIRECTORIES?, PERMISSION_TRANSLATION?, EXTENDED_EVIDENCE?, STATISTICS?)
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/NAME (#PCDATA)	A service-defined tag assigned to each data point.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/DP_NAME (#PCDATA)	A service-defined, unique name for a data point. The data point name identifies whether the data point is custom, the type of check performed, and the data point ID number. For example: custom.reg_key_exist.1001660.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXPECTED (V*, CRITERIA?)	A data point “expected” value, as defined in the compliance policy. The “expected” value may include fixed value selections, user-customized evaluation criteria, or a combination of both.
attribute: <b>logic</b>	<b>logic</b> is a fixed value equal to “OR”. When present, the control will pass if the “actual” value matches any of the “expected” values defined for the data point in the policy. This includes fixed value selections and user-customized evaluation criteria.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXPECTED/V (#PCDATA)	A fixed value selected for the data point in the compliance policy.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXPECTED/CRITERIA (EVALUATION, V*)	User-customized evaluation criteria for the data point, as defined in the compliance policy.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXPECTED/CRITERIA/EVALUATION (#PCDATA)	A data point rule used by the service to evaluate data point information gathered by the most recent compliance scan of the host. The data point rule includes the operator and cardinality options set in the compliance policy for the data point, if applicable.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXPECTED/CRITERIA/V (#PCDATA)	The user-provided “expected” value for the data point, as defined in the compliance policy.



XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/ACTUAL (V*)	A data point “actual” value, as found by the service during the most recent scan.
attribute: <b>lastUpdated</b>	<b>lastUpdated</b> is the most recent date/time the datapoint was scanned.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/ADDED_DIRECTORIES (V*)	Added directories returned from integrity content check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/REMOVED_DIRECTORIES (V*)	Removed directories returned from integrity content check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/PERMISSION_CHANGED_DIRECTORIES (V*)	Directories with permissions changed, returned from integrity content check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/CONTENT_CHANGED_DIRECTORIES (V*)	Directories with content changed, returned from integrity content check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/PERMISSION_TRANSLATION (PAIR+)	
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/PERMISSION_TRANSLATION/PAIR (K, V)	
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/PERMISSION_TRANSLATION/PAIR/K (#PCDATA)	A translation context key in a mapping pair. This represents a raw, untranslated value returned by the scanning engine. Each key maps to a registry or file/directory permission returned in the “actual” value.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/PERMISSION_TRANSLATION/PAIR/V (#PCDATA)	A translation context value in a mapping pair. This represents the meaning associated with the raw value in the mapping pair.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/EXTENDED_EVIDENCE (#PCDATA)	Extended evidence includes additional findings/information collected during the evaluation of the control on the host. This may include results returned from queries made by the scanning engine when checking the control value.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/STATISTICS (STATS*, SEARCH_DURATION, ERRORS?)	
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/STATISTICS/STATS (#PCDATA)	Reports the statistics information for UDCs, for this check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/STATISTICS/SEARCH_DURATION (#PCDATA)	The duration of the directory search for this check.
/COMPLIANCE_POLICY_REPORT/RESULTS/CHECKS/CHECK/STATISTICS/ERRORS (#PCDATA)	Any errors reported by this directory search check.
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS (DP*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP (DP_NAME, DESCRIPTION, SCAN_PARAMETERS?)	

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/DP_NAME (#PCDATA)	A service-defined, unique name for a data point. The data point name identifies whether the data point is custom, the type of check performed, and the data point ID number. For example: custom.reg_key_exist.1001660.
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/DESCRIPTION (#PCDATA)	A user-provided description for the data point. (Applies to a custom control.)
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/SCAN_PARAMETERS (PARAM*)	
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/SCAN_PARAMETERS/PARAM (LABEL, VALUE)	
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/SCAN_PARAMETERS/PARAM/LABEL (#PCDATA)	A service-defined label for a scan parameter: Registry Hive, Registry Key, NAME, File path, and Hash Type. (Only applies to a user-defined custom control.)
/COMPLIANCE_POLICY_REPORT/RESULTS/DP_DESCRIPTIONS/DP/SCAN_PARAMETERS/PARAM/VALUE (#PCDATA)	A value for a scan parameter, which corresponds to a scan parameter label in the <LABEL> element.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS (HOST_INFO+)	
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO (IP, TRACKING_METHOD, DNS, NETBIOS, OPERATING_SYSTEM, LAST_SCAN_DATE, PERCENTAGE, NETWORK?)	
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/IP (#PCDATA)	The host's IP address.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/TRACKING_METHOD (#PCDATA)	Tracking method used to discover the host.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/DNS (#PCDATA)	The host's DNS name.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/NETBIOS (#PCDATA)	The host's NetBIOS hostname.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/OPERATING_SYSTEM (#PCDATA)	The host's NetBIOS hostname.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/LAST_SCAN_DATE (#PCDATA)	The most recent date the host was scanned.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/PERCENTAGE (#PCDATA)	The percentage of controls that passed on the host.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/NETWORK (#PCDATA)	The network the host belongs to.

## Sample Compliance Policy Report XML Output

The compliance policy report XML includes three data point evaluation types: 1) user-customized evaluation criteria, 2) fixed value selection, and 3) a combination of user-customized evaluation criteria and fixed values. Sample XML output is provided below.

### Sample 1: Only User-Customized Criteria (No Fixed Values)

A control that does not have any fixed values looks like this:

```
<CHECK>
  <NAME>CHECK14</NAME>
  <DP_NAME>auth.passwords.expirywarning</DP_NAME>
  <EXPECTED logic="OR">
    <CRITERIA>
      <EVALUATION><![CDATA[less than]]></EVALUATION>
      <V><![CDATA[ 14 ]]></V>
    </CRITERIA>
  </EXPECTED>
  <ACTUAL lastUpdated="2012-04-01T15:21:36Z">
    <V><![CDATA[14]]></V>
  </ACTUAL>
</CHECK>
```

### Sample 2: Only Fixed Values (No User-Customized Criteria)

For controls that only allow fixed value selection (user must select/clear checkboxes in the policy editor), the evaluation looks like this:

```
<CHECK>
  <NAME>CHECK14</NAME>
  <DP_NAME>auth.passwords.expirywarning</DP_NAME>
  <EXPECTED logic="OR">
    <V><![CDATA[ Enabled]]></V>
    <V><![CDATA[ RegKey not found]]></V>
    <V><![CDATA[ RegSubKey not found]]></V>
  </EXPECTED>
  <ACTUAL lastUpdated="2012-04-01T15:21:36Z">
    <V><![CDATA[14]]></V>
  </ACTUAL>
</CHECK>
```

In this example, each fixed value checkbox selected in the policy is displayed in a separate <V> element under <EXPECTED>. Note that there is no <CRITERIA> element under <EXPECTED> because there is no user-customized evaluation criteria.

### Sample 3: Fixed Values and User-Customized Criteria

For controls using the fixed values in addition to user-customized evaluation criteria, the evaluation looks like this:

```
<CHECK>
  <NAME>CHECK14</NAME>
  <DP_NAME>auth.passwords.expirywarning</DP_NAME>
  <EXPECTED logic="OR">
    <CRITERIA>
      <EVALUATION><![CDATA[less than]]></EVALUATION>
      <V><![CDATA[14]]></V>
    </CRITERIA>
    <V><![CDATA[ RegSubKey not found]]></V>
  </EXPECTED>
  <ACTUAL lastUpdated="2012-04-01T15:21:36Z">
    <V><![CDATA[14]]></V>
  </ACTUAL>
</CHECK>
```

In this example, the <EXPECTED> element is used to display both the fixed value checkbox selections and the user-provided evaluation criteria (less than operator + value 14).

# Compliance Authentication Report

The authentication report XML is returned when you download a saved authentication report using the Qualys user interface.

DTD: [https://<baseurl>/compliance\\_authentication\\_report.dtd](https://<baseurl>/compliance_authentication_report.dtd)

## DTD for Compliance Authentication Report

A recent DTD (compliance\_authentication\_report.dtd) is shown below.

```
<!-- QUALYS COMPLIANCE AUTHENTICATION REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT COMPLIANCE_AUTHENTICATION_REPORT (ERROR | (HEADER,
(BUSINESS_UNIT_LIST | ASSET_GROUP_LIST | ASSET_TAG_LIST | IPS_LIST)))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO,
FILTERS)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT FILTERS (BUSINESS_UNIT_LIST | ASSET_GROUP_LIST | ASSET_TAG_LIST
| (IPS_LIST, NETWORK?))>

<!ELEMENT BUSINESS_UNIT_LIST (BUSINESS_UNIT*)>
<!ELEMENT BUSINESS_UNIT
(NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED|AUTH_N
OT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE|NOT_ATTEMPTED
_PERCENTAGE|TECHNOLOGY_LIST)*>
<!ELEMENT AUTH_PASSED (#PCDATA)>
<!ELEMENT AUTH_INSUFFICIENT (#PCDATA)>
<!ELEMENT AUTH_TOTAL (#PCDATA)>
<!ELEMENT PASSED_PERCENTAGE (#PCDATA)>
```

```
<!ELEMENT ASSET_TAG_LIST ((INCLUDED_TAGS, EXCLUDED_TAGS?) | ASSET_TAG)>
<!ELEMENT ASSET_TAG
 (INCLUDED_TAGS|EXCLUDED_TAGS|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>
<!ELEMENT INCLUDED_TAGS (TAG_ITEM+)>
<!ATTLIST INCLUDED_TAGS scope (any|all) #REQUIRED>
<!ELEMENT EXCLUDED_TAGS (TAG_ITEM+)>
<!ATTLIST EXCLUDED_TAGS scope (any|all) #REQUIRED>
<!ELEMENT TAG_ITEM (#PCDATA)>

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP*)>
<!ELEMENT ASSET_GROUP
 (NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>

<!ELEMENT IPS_LIST (IPS+)>
<!ELEMENT IPS
 (NAME|AUTH_PASSED|AUTH_INSUFFICIENT|AUTH_FAILED|AUTH_NOT_ATTEMPTED|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_PERCENTAGE|NOT_ATTEMPTED_PERCENTAGE|TECHNOLOGY_LIST)*>

<!ELEMENT AUTH_FAILED (#PCDATA)>
<!ELEMENT AUTH_NOT_ATTEMPTED (#PCDATA)>
<!ELEMENT AUTH_NOT_INSTALLED (#PCDATA)>
<!ELEMENT FAILED_PERCENTAGE (#PCDATA)>
<!ELEMENT NOT_ATTEMPTED_PERCENTAGE (#PCDATA)>

<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY*)>
<!ELEMENT TECHNOLOGY (NAME, HOST_LIST)>
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, HOST_TECHNOLOGY?, INSTANCE?, STATUS, CAUSE?, NETWORK?, OS?, LAST_AUTH?, LAST_SUCCESS?)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT HOST_TECHNOLOGY (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT LAST_AUTH (#PCDATA)>
<!ELEMENT LAST_SUCCESS (#PCDATA)>
```

## XPaths for Compliance Authentication Report

The XPaths for the compliance authentication report are described below.

XPath	element specifications / notes
/COMPLIANCE_AUTHENTICATION_REPORT	(ERROR   (HEADER, (BUSINESS_UNIT_LIST   ASSET_GROUP_LIST   ASSET_TAG_LIST   IPS_LIST)))
/COMPLIANCE_AUTHENTICATION_REPORT/ERROR (#PCDATA)	An error message.
attribute: <b>number</b>	An error code, when available
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO, FILTERS)
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/NAME (#PCDATA)	The report title as provided by the user at the time the report was generated. If a report title was not provided, then "Authentication Report" appears.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user's company name and address, as defined in the user's account.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/USER_INFO (NAME, USERNAME, ROLE)	
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/USER_INFO/NAME (#PCDATA)	The name of the user who generated the report.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/USER_INFO/USERNAME (#PCDATA)	The user login ID of the user who generated the report.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/USER_INFO/ROLE (#PCDATA)	The user role assigned to the user who generated the report.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS	(BUSINESS_UNIT_LIST   ASSET_GROUP_LIST   ASSET_TAG_LIST   (IPS_LIST, NETWORK?))
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/BUSINESS_UNIT_LIST (BUSINESS_UNIT*)	The business units included in the report source.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/BUSINESS_UNIT_LIST/BUSINESS_UNIT	(NAME   AUTH_PASSED   AUTH_INSUFFICIENT   AUTH_FAILED   AUTH_NOT_ATTEMPTED   AUTH_NOT_INSTALLED   AUTH_TOTAL   PASSED_PERCENTAGE   FAILED_PERCENTAGE   NOT_ATTEMPTED_PERCENTAGE   TECHNOLOGY_LIST)
	Host information for a business unit.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST	((INCLUDED_TAGS, EXCLUDED_TAGS?)   ASSET_TAG)

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/INCLUDED_TAGS	(TAG_ITEM+)
	The list of asset tags included in the report source. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/INCLUDED_TAGS/TAG_ITEM	(#PCDATA)
	The asset tag name for a tag included.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/EXCLUDED_TAGS	(TAG_ITEM+)
	The list of asset tags excluded from the report source. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/EXCLUDED_TAGS/TAG_ITEM	(#PCDATA)
	The asset tag name for a tag excluded.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/ASSET_TAG	(INCLUDED_TAGS   EXCLUDED_TAGS   AUTH_PASSED   AUTH_INSUFFICIENT   AUTH_FAILED   AUTH_NOT_ATTEMPTED   AUTH_NOT_INSTALLED   AUTH_TOTAL   PASSED_PERCENTAGE   FAILED_PERCENTAGE   NOT_ATTEMPTED_PERCENTAGE   TECHNOLOGY_LIST)
	Host information for an asset tag.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_GROUP_LIST (ASSET_GROUP*)	
	The asset groups included in the report source.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_GROUP_LIST /ASSET_GROUP	(NAME   AUTH_PASSED   AUTH_INSUFFICIENT   AUTH_FAILED   AUTH_NOT_ATTEMPTED   AUTH_NOT_INSTALLED   AUTH_TOTAL   PASSED_PERCENTAGE   FAILED_PERCENTAGE   NOT_ATTEMPTED_PERCENTAGE   TECHNOLOGY_LIST)
	Host information for an asset group.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/IPS_LIST (IPS+)	
	The IPs included in the report source.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/IPS_LIST/IPS	(NAME   AUTH_PASSED   AUTH_INSUFFICIENT   AUTH_FAILED   AUTH_NOT_ATTEMPTED   AUTH_NOT_INSTALLED   AUTH_TOTAL   PASSED_PERCENTAGE   FAILED_PERCENTAGE   NOT_ATTEMPTED_PERCENTAGE   TECHNOLOGY_LIST)
	Host information for an IP.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/NETWORK (#PCDATA)	
	The network selected for the report.



XPath	element specifications / notes
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/NAME	(#PCDATA) The name of the business unit or asset group.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_PASSED	(#PCDATA) The number of hosts that passed authentication.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_INSUFFICIENT	(#PCDATA) The number of hosts that passed with insufficient privileges, meaning that the scanning engine was able to authenticate to the hosts but there were insufficient privileges to perform posture evaluation.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_FAILED	(#PCDATA) The number of hosts that failed authentication.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_NOT_ATTEMPTED	(#PCDATA) The number of hosts where authentication was not used.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_NOT_INSTALLED	(#PCDATA) The number of hosts where authentication resulted in ERROR.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/AUTH_TOTAL	(#PCDATA) The total number of scanned hosts.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/PASSED_PERCENTAGE	(#PCDATA) The percentage of scanned hosts that passed.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/FAILED_PERCENTAGE	(#PCDATA) The percentage of scanned hosts that failed.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/NOT_ATTEMPTED_PERCENTAGE	(#PCDATA) The percentage of scanned hosts where authentication was not used.

<b>XPath</b>	<b>element specifications / notes</b>
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST (TECHNOLOGY*)	
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY (NAME, HOST_LIST)	
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/NAME (#PCDATA)	The authentication type, such as Windows, SSH, Oracle, SNMP, etc.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST (HOST*)	
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST	(TRACKING_METHOD, IP, DNS?, NETBIOS?, HOST_TECHNOLOGY?, INSTANCE?, STATUS, CAUSE?, NETWORK?, OS?, LAST_AUTH?, LAST_SUCCESS?)
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The tracking method assigned to the host: IP, DNS, or NETBIOS.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/IP (#PCDATA)	The IP address for the host.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/DNS (#PCDATA)	The DNS hostname for the host, when available.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/NETBIOS (#PCDATA)	The NetBIOS hostname for the host, when available.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/HOST_TECHNOLOGY (#PCDATA)	The compliance technology the host's operating system is matched to.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/INSTANCE (#PCDATA)	If the compliance information applies to a technology version on the host, like an Oracle version, instance information appears in this format: Port <number>, SID <value>. For example: Port 1521, SID ora010203p.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/STATUS (#PCDATA)	The host's authentication status: Passed, Failed, or Passed*. Passed* indicates that authentication to the host was successful but the login account had insufficient privileges.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/ TECHNOLOGY/HOST_LIST/HOST/CAUSE (#PCDATA)	Additional information for a host with a Failed or Passed* status. This may include the login ID used during the authentication attempt.

XPath	element specifications / notes
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/NETWORK (#PCDATA)	The network the host belongs to.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/OS (#PCDATA)	The host's operating system.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/LAST_AUTH (#PCDATA)	The last time the host was scanned using authentication. This is when the status was last updated to Passed or Failed.
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/{type_list}/{type}/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/LAST_SUCCESS (#PCDATA)	The last time authentication was successful for the host. N/A indicates that the host has been scanned with authentication enabled but it has not been successful.

# Compliance Scorecard Report

The compliance scorecard report XML is returned when you download a saved report using the Qualys user interface.

DTD: [https://<baseurl>/compliance\\_scorecard\\_report.dtd](https://<baseurl>/compliance_scorecard_report.dtd)

## DTD for Compliance Scorecard Report

A recent DTD for the compliance scorecard report output is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE SCORECARD REPORT DTD -->

<!ELEMENT COMPLIANCE_SCORECARD_REPORT (ERROR | (HEADER, (SUMMARY),
                                                    (DETAILS)))>
<!ELEMENT ERROR (#PCDATA|COUNT|PERCENT)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT HEADER (REPORT_TYPE, GENERATION_DATETIME)>
<!ELEMENT SUMMARY (ABOUT_REPORT, REPORT_SETTINGS, REPORT_DISCOVERIES)>
<!ELEMENT ABOUT_REPORT (REPORT_TYPE, CREATED, USER_NAME, LOGIN_NAME,
                        USER_ROLE, COMPANY_INFO)>
<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT REPORT_SETTINGS (TEMPLATE, NUMBER_OF_POLICIES,
                           REPORT_TIMEFRAME, ASSET_GROUPS*, ASSET_TAGS*,
                           CRITICALITY*)>
<!ELEMENT REPORT_DISCOVERIES (OVERALL_COMPLIANCE, BY_CONTROL, BY_HOSTS,
                              BY_TECHNOLOGY, BY_CRITICALITY*)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_NAME)+>
<!ELEMENT ASSET_TAGS ((INCLUDED_TAGS, EXCLUDED_TAGS?) | ASSET_TAG?)*>
<!ELEMENT OVERALL_COMPLIANCE (OVERALL_COMPLIANCE_PERCENT, UNIQUE_POLICES,
                              PASSED, FAILED, ERROR)>
<!ELEMENT BY_CONTROL (TOTAL_CONTROL_DETECTED, CHANGED_CONTROL, PASSED,
                      FAILED, ERROR)>
<!ELEMENT PASSED (COUNT, PERCENT)>
<!ELEMENT FAILED (COUNT, PERCENT)>
<!ELEMENT BY_HOSTS (TOTAL_HOSTS_IN_POLICIES, SCANNED_HOSTS, CHANGED)>
<!ELEMENT BY_TECHNOLOGY ((TOTAL_TECHNOLOGY, CHANGED_TECHNOLOGY,
                          TECHNOLOGY*) | (TECHNOLOGY+))>
<!ELEMENT TECHNOLOGY
  (#PCDATA|NAME|CONTROL_INSTANCES|COUNT|PERCENT|PASSED_TOTAL|PASSED_CHANGED
  |FAILED_TOTAL|FAILED_CHANGED|ERROR_TOTAL|ERROR_CHANGED|COMPLIANCE)*>
<!ELEMENT DETAILS (COMPLIANCE_BY_POLICY*, COMPLIANCE_BY_ASSET_GROUP*,
                  COMPLIANCE_BY_ASSET_TAG*, COMPLIANCE_BY_TECHNOLOGY*,
                  COMPLIANCE_BY_CRITICALITY*, TOP_HOST_WITH_CHANGES*,
                  TOP_CONTROLS_WITH_CHANGES*,
                  FAILED_CONTROLS_BY_CRITICALITY*)>
```

```

<!ELEMENT COMPLIANCE_BY_POLICY (DETAIL_DATE, BY_POLICY*,
                                BY_POLICY_ASSET_GROUP*,
                                BY_POLICY_ASSET_TAG*,
                                BY_POLICY_TECHNOLOGY*)>
<!ELEMENT COMPLIANCE_BY_ASSET_GROUP (DETAIL_DATE, BY_ASSET_GROUP*,
                                     BY_ASSET_GROUP_POLICY*,
                                     BY_ASSET_GROUP_TECHNOLOGY*)>
<!ELEMENT COMPLIANCE_BY_ASSET_TAG (DETAIL_DATE, BY_ASSET_TAG*,
                                    BY_ASSET_TAG_POLICY*,
                                    BY_ASSET_TAG_TECHNOLOGY*)>
<!ELEMENT COMPLIANCE_BY_TECHNOLOGY (DETAIL_DATE, BY_TECHNOLOGY)>
<!ELEMENT COMPLIANCE_BY_CRITICALITY (DETAIL_DATE, BY_CRITICALITY*,
                                     BY_CRITICALITY_POLICY*,
                                     BY_CRITICALITY_ASSET_GROUP*,
                                     BY_CRITICALITY_ASSET_TAG*,
                                     BY_CRITICALITY_TECHNOLOGY*)>
<!ELEMENT TOP_HOST_WITH_CHANGES (TOP, CHANGED_TO_PASS, CHANGED_TO_FAIL,
                                   CHANGED_TO_ERROR)>
<!ELEMENT TOP_CONTROLS_WITH_CHANGES (TOP, CHANGED_TO_PASS,
                                       CHANGED_TO_FAIL, CHANGED_TO_ERROR)>
<!ELEMENT FAILED_CONTROLS_BY_CRITICALITY (FAILED_CONTROLS*)>

<!ELEMENT BY_POLICY (POLICY+)>
<!ELEMENT BY_POLICY_ASSET_GROUP (POLICY+)>
<!ELEMENT BY_POLICY_ASSET_TAG (POLICY+)>
<!ELEMENT BY_POLICY_TECHNOLOGY (POLICY+)>
<!ELEMENT BY_ASSET_GROUP (ASSET_GROUP+)>
<!ELEMENT BY_ASSET_TAG (ASSET_TAG+)>
<!ELEMENT BY_ASSET_GROUP_POLICY (ASSET_GROUP+)>
<!ELEMENT BY_ASSET_TAG_POLICY (ASSET_TAG+)>
<!ELEMENT BY_ASSET_GROUP_TECHNOLOGY (ASSET_GROUP+)>
<!ELEMENT BY_ASSET_TAG_TECHNOLOGY (ASSET_TAG+)>
<!ELEMENT BY_CRITICALITY (TOTAL_FAILED_CONTROLS*,
                          TOTAL_FAILED_CONTROLS_CHANGED*, CRITICALITY*)>
<!ELEMENT BY_CRITICALITY_POLICY (CRITICALITY*)>
<!ELEMENT BY_CRITICALITY_ASSET_GROUP (CRITICALITY*)>
<!ELEMENT BY_CRITICALITY_ASSET_TAG (CRITICALITY*)>
<!ELEMENT BY_CRITICALITY_TECHNOLOGY (CRITICALITY*)>
<!ELEMENT FAILED_CONTROLS (CRITICALITY*)>

<!ELEMENT POLICY (POLICY_TITLE, ASSET_GROUP?, ASSET_TAG?, TECHNOLOGY?,
                  CONTROL_INSTANCES, HOSTS_TOTAL, HOSTS_SCANNED,
                  HOSTS_CHANGED, PASSED_TOTAL, PASSED_CHANGED,
                  FAILED_TOTAL, FAILED_CHANGED, ERROR_TOTAL,
                  ERROR_CHANGED, COMPLIANCE)>
<!ELEMENT ASSET_GROUP
  (#PCDATA|ASSET_GROUP_NAME|POLICY_TITLE|TECHNOLOGY|CONTROL_INSTANCES|HOSTS
   _TOTAL|HOSTS_SCANNED|HOSTS_CHANGED|PASSED_TOTAL|PASSED_CHANGED|FAILED_TOT
   AL|FAILED_CHANGED|ERROR_TOTAL|ERROR_CHANGED|COMPLIANCE)*>

```

```
<!ELEMENT ASSET_TAG (ASSET_TAG_NAME, POLICY_TITLE?, TECHNOLOGY?,  
                      CONTROL_INSTANCES, HOSTS_TOTAL, HOSTS_SCANNED,  
                      HOSTS_CHANGED, PASSED_TOTAL, PASSED_CHANGED,  
                      FAILED_TOTAL, FAILED_CHANGED, ERROR_TOTAL,  
                      ERROR_CHANGED, COMPLIANCE)>  
<!ELEMENT CHANGED_TO_PASS (HOST*|CONTROL*|CRITICALITY*)>  
<!ELEMENT CHANGED_TO_FAIL (HOST*|CONTROL*|CRITICALITY*)>  
<!ELEMENT CHANGED_TO_ERROR (HOST*|CONTROL*|CRITICALITY*)>  
<!ELEMENT HOST (IP_ADDRESS, TRACKING_METHOD, NETBIOS, DNS, NETWORK?,  
                ASSET_GROUP_NAME?, ASSET_TAG_NAME?, TECHNOLOGY,  
                NUMBER_OF_POLICIES, PASSED_TOTAL?, PASSED_CHANGED?,  
                FAILED_TOTAL?, FAILED_CHANGED?, ERROR_TOTAL?,  
                ERROR_CHANGED?, COMPLIANCE, NETWORK?)>  
<!ELEMENT CONTROL (ID, STATEMENT, COUNT)>  
<!ELEMENT CRITICALITY  
  (#PCDATA|CRITICALITY_NAME|COUNT|PERCENT|ASSET_GROUP|ASSET_TAG|POLICY_TITL  
  E|TECHNOLOGY|CONTROL_INSTANCES|HOSTS_TOTAL|HOSTS_SCANNED|HOSTS_CHANGED|PA  
  SSED_TOTAL|PASSED_CHANGED|FAILED_TOTAL|FAILED_CHANGED|ERROR_TOTAL|ERROR_C  
  HANGED|COMPLIANCE|CONTROL_ID|STATEMENT)*>  
  
<!ELEMENT OVERALL_COMPLIANCE_PERCENT (#PCDATA)>  
<!ELEMENT UNIQUE_POLICES (#PCDATA)>  
<!ELEMENT COUNT (#PCDATA)>  
<!ELEMENT PERCENT (#PCDATA)>  
<!ELEMENT TOTAL_CONTROL_DETECTED (#PCDATA)>  
<!ELEMENT CHANGED_CONTROL (#PCDATA)>  
<!ELEMENT TOTAL_HOSTS_IN_POLICIES (#PCDATA)>  
<!ELEMENT SCANNED_HOSTS (#PCDATA)>  
<!ELEMENT CHANGED (COUNT, PERCENT)>  
<!ELEMENT TOTAL_TECHNOLOGY (#PCDATA)>  
<!ELEMENT CHANGED_TECHNOLOGY (#PCDATA)>  
<!ELEMENT NETWORK (#PCDATA)>  
  
<!ELEMENT REPORT_TYPE (#PCDATA)>  
<!ELEMENT GENERATION_DATETIME (#PCDATA)>  
  
<!ELEMENT CREATED (#PCDATA)>  
<!ELEMENT USER_NAME (#PCDATA)>  
<!ELEMENT LOGIN_NAME (#PCDATA)>  
<!ELEMENT USER_ROLE (#PCDATA)>  
  
<!ELEMENT NAME (#PCDATA)>  
<!ELEMENT ADDRESS (#PCDATA)>  
<!ELEMENT CITY (#PCDATA)>  
<!ELEMENT STATE (#PCDATA)>  
<!ELEMENT COUNTRY (#PCDATA)>  
<!ELEMENT ZIP_CODE (#PCDATA)>
```

```
<!ELEMENT TEMPLATE (#PCDATA)>
<!ELEMENT NUMBER_OF_POLICIES (#PCDATA)>
<!ELEMENT REPORT_TIMEFRAME (#PCDATA)>

<!ELEMENT INCLUDED_TAGS (#PCDATA)>
<!ELEMENT EXCLUDED_TAGS (#PCDATA)>

<!ELEMENT DETAIL_DATE (#PCDATA)>
<!ELEMENT POLICY_TITLE (#PCDATA)>
<!ELEMENT CONTROL_INSTANCES (#PCDATA)>
<!ELEMENT HOSTS_TOTAL (#PCDATA)>
<!ELEMENT HOSTS_SCANNED (#PCDATA)>
<!ELEMENT HOSTS_CHANGED (#PCDATA)>
<!ELEMENT PASSED_TOTAL (#PCDATA)>
<!ELEMENT PASSED_CHANGED (#PCDATA)>
<!ELEMENT FAILED_TOTAL (#PCDATA)>
<!ELEMENT FAILED_CHANGED (#PCDATA)>
<!ELEMENT ERROR_TOTAL (#PCDATA)>
<!ELEMENT ERROR_CHANGED (#PCDATA)>
<!ELEMENT COMPLIANCE (#PCDATA)>

<!ELEMENT POSTURE (#PCDATA)>
<!ELEMENT ASSET_GROUP_NAME (#PCDATA)>
<!ELEMENT ASSET_TAG_NAME (#PCDATA)>
<!ELEMENT IP_ADDRESS (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT TOP (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT CRITICALITY_NAME (#PCDATA)>
<!ELEMENT TOTAL_FAILED_CONTROLS (#PCDATA)>
<!ELEMENT TOTAL_FAILED_CONTROLS_CHANGED (#PCDATA)>
<!ELEMENT CONTROL_ID (#PCDATA)>
```

# XPaths for Compliance Scorecard Report

The XPaths for the compliance scorecard report are described below.

XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT	(ERROR   (HEADER, (SUMMARY) (DETAILS)))
/COMPLIANCE_SCORECARD_REPORT/ERROR (#PCDATA   COUNT   PERCENT)	An error message.
attribute: <b>number</b>	An error code, when available
/COMPLIANCE_SCORECARD_REPORT/HEADER (REPORT_TYPE, GENERATION_DATETIME)	
/COMPLIANCE_SCORECARD_REPORT/HEADER/REPORT_TYPE (#PCDATA)	The user defined report title.
/COMPLIANCE_SCORECARD_REPORT/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was created.
COMPLIANCE_SCORECARD_REPORT/SUMMARY	(ABOUT_REPORT, REPORT_SETTINGS, REPORT_DISCOVERIES)
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT	(REPORT_TYPE, CREATED, USER_NAME, LOGIN_NAME, USER_ROLE, COMPANY INFO)
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/REPORT_TYPE (#PCDATA)	Compliance scorecard report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/CREATED (#PCDATA)	The date and time the report was created.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/USER_NAME (#PCDATA)	The name of the user who created the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/LOGIN_NAME (#PCDATA)	The login ID of the user who created the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/USER_ROLE (#PCDATA)	The user role assigned to the user who created the report: Manager, Unit Manager, Auditor, Scanner, or Reader.
./COMPLIANCE_SCORECARD_REPORT/SUMMARY/ABOUT_REPORT/COMPANY INFO)	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user's company name and address, as defined in the user's account.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS	(TEMPLATE, NUMBER_OF_POLICIES, REPORT_TIMEFRAME, ASSET_GROUPS*, ASSET_TAGS*, CRITICALITY*)
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/TEMPLATE (#PCDATA)	The name of the template used to generate the report.



XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/NUMBER_OF_POLICIES (#PCDATA)	The number of policies selected for the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/REPORT_TIMEFRAME (#PCDATA)	The date range reported on.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/ASSET_GROUPS	
ASSET_GROUP_NAME (#PCDATA)	An asset group name.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/ASSET_TAGS	((INCLUDED_TAGS, EXCLUDED_TAGS?)   ASSET_TAG?)
	The asset tags selected for the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/HOST	(IP_ADDRESS, TRACKING_METHOD, NETBIOS, DNS, NETWORK?, ASSET_GROUP_NAME?, ASSET_TAG_NAME?, TECHNOLOGY, NUMBER_OF_POLICIES, PASSED_TOTAL?, PASSED_CHANGED?, FAILED_TOTAL?, FAILED_CHANGED?, ERROR_TOTAL?, ERROR_CHANGED?, COMPLIANCE, NETWORK?)
	Host settings. For tracking method a valid value is: IP, DNS NETBIOS, or AGENT.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_SETTINGS/CRITICALITY (#PCDATA)	The criticality levels included in the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES	(OVERALL_COMPLIANCE, BY_CONTROL, BY_HOSTS, BY_TECHNOLOGY, BY_CRITICALITY*)
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE	(OVERALL_COMPLIANCE_PERCENT, UNIQUE_POLICES, PASSED, FAILED, ERROR)
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE/OVERALL_COMPLIANCE_PERCENT (#PCDATA)	The percent of compliance across all policies included in the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE/UNIQUE_POLICES (#PCDATA)	The number of unique policies included in the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE/PASSED (COUNT, PERCENT)	The number and percent of controls that passed.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE/FAILED (COUNT, PERCENT)	The number and percent of controls that failed.

XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/OVERALL_COMPLIANCE/ERROR (COUNT, PERCENT)	The number and percent of controls with an Error status in the report. An error status is returned for a custom control if an error occurred during control evaluation (and the ignore errors configuration option was not selected).
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL (TOTAL_CONTROL_DETECTED, CHANGED_CONTROL, PASSED, FAILED, ERROR)	
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL/TOTAL_CONTROL_DETECTED (#PCDATA)	The number of controls detected.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL/CHANGED_CONTROL (#PCDATA)	The number of changed controls detected.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL/PASSED (COUNT, PERCENT)	The number and percent of controls passed.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL/FAILED (COUNT, PERCENT) (#PCDATA)	The number and percent of controls failed.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CONTROL/ERROR (COUNT, PERCENT) (#PCDATA)	The number and percent of controls in error.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_HOSTS (TOTAL_HOSTS_IN_POLICIES, SCANNED_HOSTS, CHANGED)	
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_HOSTS/TOTAL_HOSTS_IN_POLICIES (#PCDATA)	The number of hosts in the selected policies.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_HOSTS/SCANNED_HOSTS (#PCDATA)	The number of scanned hosts included in the selected policies.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_HOSTS/CHANGED (COUNT, PERCENT)	The number and percent changed hosts
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_TECHNOLOGY ((TOTAL_TECHNOLOGY, CHANGED_TECHNOLOGY, TECHNOLOGY*) (TECHNOLOGY+))	
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_TECHNOLOGY/TOTAL_TECHNOLOGY (#PCDATA)	The number of technologies included in the report.

XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_TECHNOLOGY/CHANGED_TECHNOLOGY (#PCDATA)	The number of changed technologies in the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_TECHNOLOGY/TECHNOLOGY* (NAME, COUNT, PERCENT)	The technology name, count and percent.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CRITICALITY(TOTAL_FAILED_CONTROLS*,TOTAL_FAILED_CONTROLS_CHANGED*,CRITICALITY*)	
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CRITICALITY/TOTAL_FAILED_CONTROLS* (#PCDATA)	The number of failed controls in the report.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CRITICALITY/TOTAL_FAILED_CONTROLS_CHANGED* (#PCDATA)	The number of controls that changed to fail in the report time frame.
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_CRITICALITY/CRITICALITY* (NAME, COUNT, PERCENT)	The number and percentage of controls that changed to fail for each criticality.
/COMPLIANCE_SCORECARD_REPORT/DETAILS	(COMPLIANCE_BY_POLICY*, COMPLIANCE_BY_ASSET_GROUP*, COMPLIANCE_BY_ASSET_TAG*, COMPLIANCE_BY_TECHNOLOGY*, COMPLIANCE_BY_CRITICALITY*, TOP_HOST_WITH_CHANGES*, TOP_CONTROLS_WITH_CHANGES*, FAILED_CONTROLS_BY_CRITICALITY*)

# Exception List Output

The exception list output XML is returned when you request an exception list using the Exception API.

DTD: [https://<baseurl>/api/2.0/fo/compliance/exception/exception\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/compliance/exception/exception_list_output.dtd)

## DTD for Exception List Output

A recent DTD for the exception list output is shown below.

```
<!-- QUALYS EXCEPTION_LIST_OUTPUT DTD -->
<!ELEMENT EXCEPTION_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, (EXCEPTION_LIST|NUMBER_SET)?, WARNING?)>
<!ELEMENT EXCEPTION_LIST (EXCEPTION+)>
<!ELEMENT EXCEPTION (EXCEPTION_NUMBER, HOST?, TECHNOLOGY?, POLICY?,
                     CONTROL?, ASSIGNEE, STATUS, ACTIVE, EXPIRATION_DATE,
                     MODIFIED_DATE, HISTORY_LIST?)>
<!ELEMENT EXCEPTION_NUMBER (#PCDATA)>

<!ELEMENT HOST (IP_ADDRESS, TRACKING_METHOD, NETWORK?)>
<!ELEMENT IP_ADDRESS (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>

<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT POLICY (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>

<!ELEMENT CONTROL (CID, STATEMENT, CRITICALITY)>
<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (VALUE, LABEL)>
<!ELEMENT LABEL (#PCDATA)>
```

```
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>
<!ELEMENT REOPEN_ON_EVIDENCE_CHANGE (#PCDATA)>
<!ELEMENT EXPIRATION_DATE (#PCDATA)>
<!ELEMENT MODIFIED_DATE (#PCDATA)>
<!ELEMENT HISTORY_LIST (HISTORY+)>
<!ELEMENT HISTORY (USER, COMMENT, INSERTION_DATE)>
<!ELEMENT USER (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT INSERTION_DATE (#PCDATA)>

<!ELEMENT NUMBER_SET (NUMBER|NUMBER_RANGE)+>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT NUMBER_RANGE (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```

XPaths for Exception List Output

The XPaths for the exception list output are described below.

Exception List Output: Request

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT	(REQUEST?, RESPONSE)
/EXCEPTION_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/EXCEPTION_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/EXCEPTION_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The login ID of the user who made the request.
/EXCEPTION_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/EXCEPTION_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/EXCEPTION_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/EXCEPTION_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/EXCEPTION_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.

## Exception List Output: Response

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT (REQUEST?, RESPONSE)	
/EXCEPTION_LIST_OUTPUT/RESPONSE	(DATETIME, (EXCEPTION_LIST   NUMBER_SET)?, WARNING?)
/EXCEPTION_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST (EXCEPTION+)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION	(EXCEPTION_NUMBER, HOST?, TECHNOLOGY?, POLICY?, CONTROL?, ASSIGNEE, STATUS, ACTIVE, EXPIRATION_DATE, MODIFIED_DATE, HISTORY_LIST?)
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/EXCEPTION_NUMBER (#PCDATA)	The exception number of the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HOST (IP_ADDRESS, TRACKING_METHOD, NETWORK?)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HOST/IP_ADDRESS (#PCDATA)	IP address of the host associated with the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HOST/TRACKING_METHOD (#PCDATA)	The tracking method for the host: IP, DNS NETBIOS, or AGENT.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HOST/NETWORK (#PCDATA)	The network name to which the host, associated with the exception, belongs to.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/TECHNOLOGY (ID, NAME)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/POLICY (ID, NAME)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/POLICY/ ID (#PCDATA)	Policy ID of the policy that contains the control in the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/POLICY/ NAME (#PCDATA)	Name of the policy that contains the control in the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL	(CID, STATEMENT, CRITICALITY)

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL/CID (#PCDATA)	The control ID number assigned to the control in the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL/STATEMENT(#PCDATA)	A control statement.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL/CRITICALITY (VALUE, LABEL)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL/CRITICALITY VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/CONTROL/CRITICALITY LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/ASSIGNEE (#PCDATA)	An assignee of the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/STATUS (#PCDATA)	Status of the exception: pending, approved, rejected or expired.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/ACTIVE (#PCDATA)	1 for an active exception or 0 for a inactive exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/ REOPEN_ON_EVIDENCE_CHANGE (#PCDATA)	1 for an reopened exception; 0 otherwise.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/EXPIRATION_DATE (#PCDATA)	The exception expiration date.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/MODIFIED_DATE (#PCDATA)	The date when the exception was last modified.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/HISTORY_LIST (HISTORY+)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/HISTORY_LIST (USER, COMMENT, INSERTION_DATE)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HISTORY_LIST/USER (#PCDATA)	The login ID of the users who requested and updated the exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HISTORY_LIST/ COMMENT (#PCDATA)	User-defined comments.
/EXCEPTION_LIST_OUTPUT/RESPONSE/EXCEPTION_LIST/EXCEPTION/HISTORY_LIST/ INSERTION_DATE (#PCDATA)	The comments insertion date.

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT/RESPONSE/NUMBER_SET (NUMBER NUMBER_RANGE)+	
/EXCEPTION_LIST_OUTPUT/RESPONSE/NUMBER_SET/NUMBER (#PCDATA)	
	The exception number of the updated or deleted exception.
/EXCEPTION_LIST_OUTPUT/RESPONSE/NUMBER_SET/NUMBER_RANGE (#PCDATA)	
	The exception number range of the exceptions that were updated or deleted.

### Exception List Output: Warning

XPath	element specifications / notes
/EXCEPTION_LIST_OUTPUT/RESPONSE/WARNING_LIST (WARNING+)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/WARNING (CODE?, TEXT, URL?)	
/EXCEPTION_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	
	A warning code. A warning code appears when the API request identifies more than 5,000 exception records.
/EXCEPTION_LIST_OUTPUT/RESPONSE/WARNING/TEXT (#PCDATA)	
	A warning message. A warning message appears when the API request identifies more than 5,000 exception records.
/EXCEPTION_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	
	A URL for making another API request for the next batch of exception records.



# Exception Batch Return Output

The exception batch return is XML output returned when you update or delete an exception using the Exception API.

DTD: [https://<baseurl>/api/2.0/fo/compliance/exception/exception\\_batch\\_return.dtd](https://<baseurl>/api/2.0/fo/compliance/exception/exception_batch_return.dtd)

## DTD for Exception Batch Return

```
<!-- QUALYS EXCEPTION_BATCH_RETURN DTD -->
<!ELEMENT BATCH_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, BATCH_LIST?)>
<!ELEMENT BATCH_LIST (BATCH+)>
<!ELEMENT BATCH (CODE?, TEXT?, NUMBER_SET?)>

<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT NUMBER_SET (NUMBER|NUMBER_RANGE)+>
<!ELEMENT NUMBER_RANGE (#PCDATA)>
<!ELEMENT NUMBER (#PCDATA)>
<!-- EOF -->
```

## XPaths for Exception Batch Return Output

The XPaths for the exception batch return output are described below.

### Exception Batch Return Output: Request

XPath	element specifications / notes
/BATCH_RETURN	(REQUEST?, RESPONSE)
/BATCH_RETURN/REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)	
/BATCH_RETURN/REQUEST/DATETIME (#PCDATA)	
	The date and time of the request.
/BATCH_RETURN/REQUEST/USER_LOGIN (#PCDATA)	
	The user login ID of the user who made the request.
/BATCH_RETURN/REQUEST/RESOURCE (#PCDATA)	
	The resource specified for the request.
/BATCH_RETURN/REQUEST/PARAM_LIST (PARAM+)	
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	
	The input parameter name.
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	
	The input parameter value.
/BATCH_RETURN/REQUEST/POST_DATA (#PCDATA)	
	The POST data.

### Exception Batch Return Output: Response

XPath	element specifications / notes
/BATCH_RETURN/RESPONSE (DATETIME, BATCH_LIST?)	
/BATCH_RETURN/RESPONSE/DATETIME (#PCDATA)	
	The date and time of the response.
/BATCH_RETURN/RESPONSE/BATCH_LIST (BATCH+)	
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH (CODE?, TEXT?, NUMBER_SET?)	
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/CODE (#PCDATA)	
	A batch code.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/TEXT (#PCDATA)	
	A batch text description.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/NUMBER_SET(NUMBER NUMBER_RANGE)	
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/NUMBER_SET/NUMBER (#PCDATA)	
	The exception number of the updated or deleted exception.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/NUMBER_SET/NUMBER_RANGE (#PCDATA)	
	The exception number range of the exceptions that were updated or deleted.

# SCAP Policy List Output

The SCAP policy list XML is returned from an API request for an SCAP policy list.

DTD:

[https://<baseurl>/api/2.0/fo/compliance/fdcc\\_policy/fdcc\\_policy\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/compliance/fdcc_policy/fdcc_policy_list_output.dtd)

## DTD for SCAP Policy List Output

A recent DTD for the SCAP policy list is shown below.

```
<!-- QUALYS FDCC_POLICY_LIST_OUTPUT DTD -->
<!ELEMENT FDCC_POLICY_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, (FDCC_POLICY_LIST|ID_SET)?, WARNING_LIST?)>
<!ELEMENT FDCC_POLICY_LIST (FDCC_POLICY+)>
<!ELEMENT FDCC_POLICY (ID, TITLE, DESCRIPTION, BENCHMARK,
                       BENCHMARK_PROFILE, BENCHMARK_STATUS_DATE, VERSION,
                       TECHNOLOGY, NIST_PROVIDED, CREATED, LAST_MODIFIED,
                       ASSET_GROUP_LIST?, FDCC_FILE_LIST?)>

<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT BENCHMARK (#PCDATA)>
<!ELEMENT BENCHMARK_PROFILE (#PCDATA)>
<!ELEMENT BENCHMARK_STATUS_DATE (#PCDATA)>
<!ELEMENT VERSION (#PCDATA)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT NIST_PROVIDED (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME, BY)>

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
```

```
<!ELEMENT ASSET_GROUP (ID, TITLE)>

<!ELEMENT FDCC_FILE_LIST (FDCC_FILE+)>
<!ELEMENT FDCC_FILE (FILE_NAME, FILE_HASH)>
<!ELEMENT FILE_NAME (#PCDATA)>
<!ELEMENT FILE_HASH (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!-- EOF -->
```

**XPaths for SCAP Policy List Output**

This section describes the XPaths for the SCAP policy list output.

**SCAP Policy List Output: Request**

XPath	element specifications / notes
/FDCC_POLICY_LIST_OUTPUT	(REQUEST?, RESPONSE)
/FDCC_POLICY_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/FDCC_POLICY_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/FDCC_POLICY_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/FDCC_POLICY_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/FDCC_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/FDCC_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/FDCC_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/FDCC_POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/FDCC_POLICY_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.

## SCAP Policy List Output: Response

XPath	element specifications / notes
/FDCC_POLICY_LIST_OUTPUT	(REQUEST?, RESPONSE)
/FDCC_POLICY_LIST_OUTPUT/RESPONSE	(DATETIME, (FDCC_POLICY_LIST   ID_SET)?, WARNING_LIST?)
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST (FDCC_POLICY+)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/FDCC_POLICY	(ID, TITLE, DESCRIPTION, BENCHMARK, BENCHMARK_PROFILE, BENCHMARK_STATUS_DATE, VERSION, TECHNOLOGY, NIST_PROVIDED, CREATED, LAST_MODIFIED, ASSET_GROUP_LIST?, FDCC_FILE_LIST?)
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/ID (#PCDATA)	A SCAP policy ID.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/TITLE (#PCDATA)	A SCAP policy title.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/DESCRIPTION (#PCDATA)	A description of the SCAP policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/BENCHMARK (#PCDATA)	The SCAP benchmark defined for the FDCC policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/BENCHMARK_PROFILE (#PCDATA)	The SCAP profile that is defined for the FDCC policy in the FDCC Content.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/BENCHMARK_STATUS_DATE (#PCDATA)	The SCAP status date, as defined for the FDCC policy in the SCAP XCCDF file.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/VERSION (#PCDATA)	The base version of the SCAP policy as defined by NIST, when the policy is a NIST provided policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/TECHNOLOGY (#PCDATA)	The technology defined for the SCAP policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/NIST_PROVIDED (#PCDATA)	Yes indicates the SCAP policy was provided by NIST. No indicates the SCAP policy is a user-defined custom policy.

<b>XPath</b>	<b>element specifications / notes</b>
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/CREATED (DATETIME, BY)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/CREATED/DATETIME (#PCDATA)	
	The date/time when the SCAP policy was first created.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/CREATED/BY (#PCDATA)	
	The user login ID of the user who first created the SCAP policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/LAST_MODIFIED (DATETIME, BY)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/LAST_MODIFIED/DATETIME (#PCDATA)	
	The date/time when the policy was last updated.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/LAST_MODIFIED/BY (#PCDATA)	
	The user login ID of the user who last modified the policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/ASSET_GROUP_LIST (ASSET_GROUP+)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/ASSET_GROUP_LIST/ASSET_GROUP (ID, TITLE)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/ASSET_GROUP_LIST/ASSET_GROUP/ID (#PCDATA)	
	The ID of an asset group assigned to the SCAP policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/ASSET_GROUP_LIST/ASSET_GROUP/TITLE (#PCDATA)	
	The title of an asset group assigned to the SCAP policy.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/FDCC_FILE_LIST (FDCC_FILE+)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/FDCC_FILE_LIST/FDCC_FILE (FILE_NAME, FILE_HASH	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/FDCC_FILE_LIST/FDCC_FILE/FILE_NAME (#PCDATA)	
	A SCAP file name.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/FDCC_POLICY_LIST/FDCC_POLICY/FDCC_FILE_LIST/FDCC_FILE/FILE_HASH (#PCDATA)	
	The MD5 hash of a SCAP file name.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/ID_SET (ID ID_RANGE)	
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	
	A SCAP policy ID.
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	
	A range SCAP policy IDs.

## SCAP Policy List Output: Warning

XPath	element specifications / notes
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST	(WARNING+)
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING	(CODE?, TEXT, URL?)
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/WARNING/CODE	(#PCDATA)
	A warning code. A warning code appears when the API request identifies more than 1,000 records (policies).
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/WARNING/TEXT	(#PCDATA)
	A warning message. A warning message appears when the API request identifies more than 1,000 records (policies).
/FDCC_POLICY_LIST_OUTPUT/RESPONSE/WARNING/URL	(#PCDATA)
	The URL for making another API request for the next batch of SCAP policy records.

## Scan Authentication XML

This appendix describes the XML output returned from API V2 requests using the Scan Authentication API functions.

- Authentication Record List Output
- Authentication Record List by Type Output
- Authentication Record Return
- Authentication Vault List Output
- Authentication Vault View Output



# Authentication Record List Output

The authentication record list XML lists all record types returned from an authentication record list (/auth) API call.

DTD: [https://<base\\_url>/api/2.0/fo/auth/auth\\_records.dtd](https://<base_url>/api/2.0/fo/auth/auth_records.dtd)

## DTD for Authentication Record List Output

A recent DTD for the authentication record list is shown below.

```
<!-- 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_WEBSPPHERE_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?)>

<!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_WEBSPPHERE_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 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 -->
```

**XPaths for Authentication Record List Output**  
**Authentication Record List Output: Request**

XPath	element specifications / notes
/AUTH_RECORDS_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_RECORDS_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/AUTH_RECORDS_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/AUTH_RECORDS_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/AUTH_RECORDS_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/AUTH_RECORDS_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/AUTH_RECORDS_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/AUTH_RECORDS_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/AUTH_RECORDS_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.

XPath	element specifications / notes
-------	--------------------------------

/AUTH_RECORDS_OUTPUT/REQUEST/POST_DATA	(#PCDATA)
--	-----------

The POST data, if any.

## Authentication Record List Output: Response

XPath	element specifications / notes
-------	--------------------------------

/AUTH_RECORDS_OUTPUT	(REQUEST?, RESPONSE)
----------------------	----------------------

/AUTH_RECORDS_OUTPUT/RESPONSE	
-------------------------------	--

(DATETIME, AUTH\_RECORDS?, WARNING\_LIST?)

/AUTH_RECORDS_OUTPUT/RESPONSE/DATETIME	(#PCDATA)
--	-----------

The date and time of the response.

/AUTH_RECORDS_OUTPUT/RESPONSE/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\_WEBSPPHERE\_IDS?, AUTH\_HTTP\_IDS?, AUTH\_SYBASE\_IDS?, AUTH\_MYSQL\_IDS?, AUTH\_TOMCAT\_IDS?, AUTH\_ORACLE\_WEBLOGIC\_IDS?, AUTH\_DOCKER\_IDS?, AUTH\_POSTGRES\_IDS?, AUTH\_MONGODB\_IDS?, AUTH\_PALO\_ALTO\_FIREWALL\_IDS?, AUTH\_VCENTER\_IDS?)

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_UNIX_IDS	(ID_SET)
--	----------

A set of Unix and Cisco authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_WINDOWS_IDS	(ID_SET)
---	----------

A set of Windows authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_ORACLE_IDS	(ID_SET)
--	----------

A set of Oracle authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_ORACLE_LISTENER_IDS	(ID_SET)
---	----------

A set of Oracle Listener authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_SNMP_IDS	(ID_SET)
--	----------

A set of SNMP authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MS_SQL_IDS	(ID_SET)
--	----------

A set of MS SQL authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_IBM_DB2_IDS	(ID_SET)
---	----------

A set of IBM DB2 authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_VMWARE_IDS	(ID_SET)
--	----------

A set of VMware authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_AUTH_MS_IIS_IDS	(ID_SET)
---	----------

A set of Microsoft IIS Web Server authentication record IDs.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_APACHE_IDS?	(ID_SET)
---	----------

A set of Apache Web Server authentication record IDs.

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_IBM_WEBSHERE_IDS (ID_SET)	A set of IBM WebSphere Application Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_HTTP_IDS (ID_SET)	A set of HTTP authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_SYBASE_IDS (ID_SET)	A set of Sybase authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MYSQL_IDS (ID_SET)	A set of MySQL authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_TOMCAT_IDS (ID_SET)	A set of Tomcat Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)	A set of Oracle WebLogic Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_DOCKER_IDS (ID_SET)	A set of Docker authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_POSTGRESSQL_IDS (ID_SET)	A set of PostgreSQL authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MONGODB_IDS (ID_SET)	A set of MongoDB authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)	A set of Palo Alto Firewall authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_VCENTER_IDS (ID_SET)	This element will not appear in XML output at this time. This is pre-release functionality scheduled for a future release related to VMware vCenter authentication support.

## Authentication Record List Output: Warning List

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST (WARNING+)	
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING (CODE?, TEXT, URL?, ID_SET?)	
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/CODE (#PCDATA)	A warning code. A warning code appears when the API request identifies more than 1,000 records.
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/TEXT (#PCDATA)	A warning message. A warning message appears when the API request identifies more than 1,000 records.
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/URL (#PCDATA)	The URL for making another API request for the next batch of authentication records.

XPath	element specifications / notes
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET	(ID ID_RANGE)
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET/ID	(#PCDATA)
	An authentication record ID.
/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET/ID_RANGE	(#PCDATA)
	A range of authentication record IDs.

## Authentication Record List by Type Output

The authentication record list by type XML is returned from an API request (`/auth/<type>`) for an authentication record list by type.

DTD: `https://<base_url>/api/2.0/fo/auth/<type>/auth_<type>_list_output.dtd`

where `<type>` is an authentication type such as: `unix`, `windows`, `oracle`, `oracle_listener`, `snmp`, `ms_sql`, `mysql`, etc.

### DTD for Authentication Record List by Type Output

A recent DTD for the authentication record by type list is shown below. The following example is for the Windows authentication type. The response output will be different for different authentication types.

```
<!-- QUALYS AUTH_WINDOWS_LIST_OUTPUT DTD -->

<!ELEMENT AUTH_WINDOWS_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_WINDOWS_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_WINDOWS_LIST (AUTH_WINDOWS+)>

<!-- If WINDOWS_DOMAIN is set, then IP_SET is optional (not specified
means service selects IPs) -->

<!ELEMENT AUTH_WINDOWS (ID, TITLE, USERNAME, NTLM?, NTLM_v2?, KERBEROS?,
WINDOWS_DOMAIN?, WINDOWS_AD_DOMAIN?, WINDOWS_AD_TRUST?, IP_SET?,
LOGIN_TYPE, DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED,
COMMENTS?, USE_AGENTLESS_TRACKING?, MINIMUM_SMB_VERSION?,
REQUIRE_SMB_SIGNING?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT NTLM (#PCDATA)>
```

```

<!ELEMENT NTLM_V2 (#PCDATA)>
<!ELEMENT KERBEROS (#PCDATA)>
<!ELEMENT WINDOWS_DOMAIN (#PCDATA)>
<!ELEMENT WINDOWS_AD_DOMAIN (#PCDATA)>
<!ELEMENT WINDOWS_AD_TRUST (#PCDATA)>

<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>

<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT USE_AGENTLESS_TRACKING (#PCDATA)>
<!ELEMENT MINIMUM_SMB_VERSION (#PCDATA)>
<!ELEMENT REQUIRE_SMB_SIGNING (#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 -->
```

## XPaths for Authentication Record List by Type Output

This section describes the XPaths for the authentication record list by type output.

### All Record Types - common sections

Note that <TYPE> is the authentication type, such as unix, windows, oracle, snmp, ms\_sql, ibm\_db2.

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/AUTH_<TYPE>_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any. POST data is urlencoded.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE	(DATETIME, (AUTH_<TYPE>_LIST   ID_SET)?, WARNING_LIST? GLOSSARY?)
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST	(AUTH_<TYPE>+)
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>	(ID, TITLE, <type-specific elements>, IP_SET?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)



XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/ID (#PCDATA)	The authentication record ID.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TITLE (#PCDATA)	The authentication record title.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/IP_SET (IP IP_RANGE)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/IP_SET/IP (#PCDATA)	An IP address saved in the authentication record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/IP_SET/IP_RANGE (#PCDATA)	A range of IP addresses saved in the authentication record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/NETWORK_ID (#PCDATA)	The network ID for the record. Applies when the networks feature is enabled.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/CREATED (DATETIME BY)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/CREATED/DATETIME (#PCDATA)	The date and time the authentication record was created.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/CREATED/BY (#PCDATA)	The user login ID of the user who created the authentication record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/LAST_MODIFIED (DATETIME)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/LAST_MODIFIED/DATETIME (#PCDATA)	The date and time the authentication record was last modified.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/COMMENTS (#PCDATA)	User-provided notes (comments) saved in the record.

## Unix Response

Elements (in bold) for Unix, Cisco, and Checkpoint Firewall records are below.

XPath	element specifications / notes
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX	(ID, TITLE, <b>USERNAME</b> , <b>SKIP_PASSWORD?</b> , <b>CLEARTEXT_PASSWORD?</b> , ( <b>ROOT_TOOL?</b>   <b>ROOT_TOOL_INFO_LIST?</b> ), (( <b>RSA_PRIVATE_KEY?</b> , <b>DSA_PRIVATE_KEY?</b> )  <b>PRIVATE_KEY_CERTIFICATE_LIST?</b> ), <b>PORT?</b> , <b>IP_SET</b> , <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , <b>NETWORK_ID?</b> , <b>CREATED</b> , <b>LAST_MODIFIED</b> , <b>COMMENTS?</b> , <b>USE_AGENTLESS_TRACKING?</b> , <b>AGENTLESS_TRACKING_PATH?</b> , <b>QUALYS_SHELL?</b> )
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/SKIP_PASSWORD (#PCDATA)	

**XPath**

**element specifications / notes**

Set to 1 if skip password option enabled.

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
CLEARTEXT\_PASSWORD (#PCDATA)

A flag indicating whether the Cleartext Password option is enabled in the authentication record. The value 1 indicates that the option is enabled. The value 0 indicates that the option is disabled.

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/ROOT\_TOOL (#PCDATA)

Name of root delegation tool configured for the record or None (no root delegation tool configured).

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
ROOT\_TOOL\_INFO\_LIST (ROOT\_TOOL\_INFO)\*

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
ROOT\_TOOL\_INFO\_LIST/ROOT\_TOOL\_INFO (ID, ROOT\_TOOL, PASSWORD\_INFO?)

For Unix type record, a root delegation tool configured for the record.

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
ROOT\_TOOL\_INFO\_LIST/ROOT\_TOOL\_INFO/PASSWORD\_INFO (DIGITAL\_VAULT?)

attribute: type (basic | vault) "basic"

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/RSA\_PRIVATE\_KEY

Element no longer used.

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/DSA\_PRIVATE\_KEY

Element no longer used.

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST (PRIVATE\_KEY\_CERTIFICATE)\*

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST/PRIVATE\_KEY\_CERTIFICATE/  
(ID, PRIVATE\_KEY\_INFO, PASSPHRASE\_INFO, CERTIFICATE?)+

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST/PRIVATE\_KEY\_CERTIFICATE/PRIVATE\_KEY\_INFO  
(PRIVATE\_KEY | DIGITAL\_VAULT)

attribute: type (basic | vault) "basic"

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST/PRIVATE\_KEY\_CERTIFICATE/PRIVATE\_KEY\_INFO/PRIVATE\_KEY

attribute: type (rsa | dsa | ecdsa | ed25519)

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST/PRIVATE\_KEY\_CERTIFICATE/PASSPHRASE\_INFO  
(PRIVATE\_KEY | DIGITAL\_VAULT)

attribute: type (basic | vault) "basic"

/AUTH\_UNIX\_LIST\_OUTPUT/RESPONSE/AUTH\_UNIX\_LIST/AUTH\_UNIX/  
PRIVATE\_KEY\_CERTIFICATE\_LIST/PRIVATE\_KEY\_CERTIFICATE/CERTIFICATE

attribute: type (x.509 | openssh)

XPath	element specifications / notes
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/PORT (#PCDATA)	A list of custom ports defined for compliance scanning (authentication and compliance assessment).
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/LOGIN_TYPE (#PCDATA)	(Unix record only) Login type is "vault" when a vault is defined for the record. Note a vault can't be defined for these records - Cisco and Checkpoint Firewall.
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/DIGITAL_VAULT  (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?)	For a Unix record, vault information configured for the record. See <a href="#">Vault Information</a> . Note a vault can't be defined for these records - Cisco and Checkpoint Firewall.
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/USE_AGENTLESS_TRACKING (#PCDATA)	1 means that Agentless Tracking option is enabled in the record, and 0 means that it's disabled.
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/AGENTLESS_TRACKING_PATH (#PCDATA)	The pathname where the host ID file will be stored on each host. (Applies only when Agentless Tracking is enabled in the record.)
/AUTH_UNIX_LIST_OUTPUT/RESPONSE/AUTH_UNIX_LIST/AUTH_UNIX/QUALYS_SHELL (ENABLED, LOG_FACILITY?)	Information on Qualys Shell and log facility, when Qualys Shell is enabled for the subscription.

## Windows Response

Windows-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS	(ID, TITLE, <b>USERNAME</b> , <b>NTLM?</b> , <b>NTLM_V2?</b> , <b>KERBEROS?</b> , <b>WINDOWS_DOMAIN?</b> , <b>WINDOWS_AD_DOMAIN?</b> , <b>WINDOWS_AD_TRUST?</b> , IP_SET?, LOGIN_TYPE, <b>DIGITAL_VAULT</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?, <b>USE_AGENTLESS_TRACKING?</b> , <b>MINIMUM_SMB_VERSION?</b> , <b>REQUIRE_SMB_SIGNING?</b> )
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/NTLM (#PCDATA)	A flag indicating whether the NTLM protocol is enabled in the record. 1 means NTLM is enabled, 0 means it's not enabled.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/NTLM_V2 (#PCDATA)	A flag indicating whether the NTLM v2 protocol is enabled in the record. 1 means NTLM v2 is enabled, 0 means it's not enabled.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/KERBEROS (#PCDATA)	A flag indicating whether the Kerberos protocol is enabled in the record. 1 means Kerberos is enabled, 0 means it's not enabled.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/WINDOWS_DOMAIN (#PCDATA)	A Windows domain name appears when a NetBIOS domain type is selected.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/WINDOWS_AD_DOMAIN (#PCDATA)	An Active Directory domain name, specified as an FQDN name, appears when the Active Directory domain type is selected.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/WINDOWS_AD_TRUST (#PCDATA)	A flag indicating whether the "Follow trust relationships" option is selected for an Active Directory domain. The value 1 indicates the "Follow trust relationships" option is enabled. The value 0 indicates the "Follow trust relationships" option is not enabled.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/DIGITAL_VAULT	Vault information, when a vault is defined for the record. See <a href="#">Vault Information</a> .
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/MINIMUM_SMB_SIGNING (#PCDATA)	The minimum SMB version required or authentication. Valid value is: 1, 2.0.2, 2.1, 3.0, 3.0.2, 3.1.1, or "" (empty string means no version set).
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/REQUIRE_SMB_SIGNING (#PCDATA)	A flag indicating whether SMB signing is required for Windows authentication. 1 means SMB signing is required, and 0 means it's not required.

## Oracle Response

Oracle-specific elements (in bold>

XPath	element specifications / notes
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE	(ID,TITLE,USERNAME, (SID SERVICENAME), PORT, IP_SET, PC_ONLY?, WINDOWS_OS_CHECKS, WINDOWS_OS_OPTIONS?, UNIX_OPATCH_CHECKS, UNIX_OS_CHECKS, UNIX_OS_OPTIONS?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ SID (#PCDATA)	The Oracle System ID (SID) for the database instance to be authenticated to. This element appears only when a SID is defined for the Oracle record.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ SERVICENAME (#PCDATA)	The Oracle service name for the database instance to be authenticated to. This element appears only when a service name is defined for the Oracle record.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/PORT (#PCDATA)	The port number that the database instance is running on, if specified.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/PC_ONLY (#PCDATA)	The value 1 indicates the <b>pc_only=1</b> parameter is specified for this record and this record is used for compliance scans only.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ WINDOWS_OS_CHECKS (#PCDATA)	The value 1 indicates the option to perform Windows OS-level compliance checks is enabled for the record.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ WINDOWS_OS_OPTIONS	(WIN_ORA_HOME, WIN_ORA_HOME_PATH, WIN_INIT_ORA_PATH, WIN_SPFILE_ORA_PATH, WIN_LISTENER_ORA_PATH, WIN_SQLNET_ORA_PATH, WIN_TNSNAMES_ORA_PATH)  Values for Windows parameters used to perform OS-level compliance checks.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ UNIX_OPATCH_CHECKS (#PCDATA)	The value 1 indicates the option to perform Unix OPatch compliance checks is enabled for the record.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/ UNIX_OS_CHECKS (#PCDATA)	The value 1 indicates the option to perform Unix OS-level compliance checks is enabled for the record.

XPath	element specifications / notes
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/UNIX_OS_OPTIONS	(UNIX_ORA_HOME_PATH, UNIX_INIT_ORA_PATH, UNIX_SPFILE_ORA_PATH, UNIX_LISTENER_ORA_PATH, UNIX_SQLNET_ORA_PATH, UNIX_TNSNAMES_ORA_PATH, UNIX_INVPTRLOC_PATH)
	Values for Unix parameters used to perform OS-level compliance checks.

**SNMP Response**

SNMP-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP	(ID, TITLE, <b>USERNAME?</b> , <b>AUTH_ALG?</b> , <b>PRIV_ALG?</b> , <b>SEC_ENG?</b> , <b>CONTEXT_ENG?</b> , <b>CONTEXT?</b> , <b>COMMUNITY_STRINGS?</b> , <b>VERSION</b> , IP_SET, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/USERNAME (#PCDATA)	(SNMPv3 only) The user account to be used for authentication to target hosts.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/AUTH_ALG (#PCDATA)	(SNMPv3 only) The authentication algorithm to be used: SHA1 or MD5.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/PRIV_ALG (#PCDATA)	(SNMPv3 only) The algorithm to be used for privacy: DES or AES.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/SEC_ENG (#PCDATA)	(SNMPv3 only) The security engine ID.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/CONTEXT_ENG (#PCDATA)	(SNMPv3 only) The context engine ID.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/CONTEXT (#PCDATA)	(SNMPv3 only) The context name.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/COMMUNITY_STRINGS (#PCDATA)	(SNMPv1 or SNMPv2c only) User-provided SNMP community strings to be used for authentication to target hosts.
/AUTH_SNMP_LIST_OUTPUT/RESPONSE/AUTH_SNMP_LIST/AUTH_SNMP/VERSION (#PCDATA)	The SNMP protocol version: v1 (for SNMPv1), v2 (fSNMPv2c) or v3 (SNMPv3).

## MS SQL Response

MS SQL-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL	(ID, TITLE, <b>USERNAME</b> , NTLM_v1?, NTLM_V2?, <b>KERBEROS?</b> , (INSTANCE   AUTO_DISCOVER_INSTANCES), (DATABASE   AUTO_DISCOVER_DATABASES), (PORT   AUTO_DISCOVER_PORTS), DB_LOCAL, WINDOWS_DOMAIN?, (IP_SET   MEMBER_DOMAIN), NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/USERNAME (#PCDATA)	The user account to be used for authentication to target hosts.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/NTLM_v1 (#PCDATA)	A flag indicating whether the NTLM protocol is enabled in the record. 1 means NTLM is enabled, 0 means it's not enabled.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/NTLM_V2 (#PCDATA)	A flag indicating whether the NTLM v2 protocol is enabled in the record. 1 means NTLM v2 is enabled, 0 means it's not enabled.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/KERBEROS (#PCDATA)	A flag indicating whether the Kerberos protocol is enabled in the record. 1 means Kerberos is enabled, 0 means it's not enabled.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/INSTANCE   AUTO_DISCOVER_INSTANCES (#PCDATA)	A database instance or AUTO_DISCOVER_INSTANCES=1 if instances are auto-discovered.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/DATABASE   AUTO_DISCOVER_DATABASES (#PCDATA)	A database name or AUTO_DISCOVER_DATABASES=1 if database names are auto-discovered.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/PORT   AUTO_DISCOVER_PORTS (#PCDATA)	Port numbers or AUTO_DISCOVER_PORTS=1 if ports are auto-discovered.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/DB_LOCAL (#PCDATA)	A flag indicating the authentication type. 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.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/WINDOWS_DOMAIN (#PCDATA)	The domain name where the login credentials are stored, when the login credentials are for a Microsoft Windows operating system account.

XPath	element specifications / notes
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/MEMBER_DOMAIN (#PCDATA)	The domain name to auto discover all MS SQL servers for the authentication record.

## IBM DB2 Response

IBM DB2-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_IBM_DB2_LIST_OUTPUT/RESPONSE/AUTH_IBM_DB2_LIST/AUTH_IBM_DB2	(ID, TITLE, <b>USERNAME</b> , <b>DATABASE</b> , <b>PORT</b> , IP_SET, <b>PC_ONLY?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_IBM_DB2_LIST_OUTPUT/RESPONSE/AUTH_IBM_DB2_LIST/AUTH_IBM_DB2/USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.
/AUTH_IBM_DB2_LIST_OUTPUT/RESPONSE/AUTH_IBM_DB2_LIST/AUTH_IBM_DB2/DATABASE (#PCDATA)	The database name of the database to be scanned.
/AUTH_IBM_DB2_LIST_OUTPUT/RESPONSE/AUTH_IBM_DB2_LIST/AUTH_IBM_DB2/PORT (#PCDATA)	The port number that the database is running on.
/AUTH_IBM_DB2_LIST_OUTPUT/RESPONSE/AUTH_IBM_DB2_LIST/AUTH_IBM_DB2/PC_ONLY (#PCDATA)	The value 1 indicates the record is defined for compliance scans only.

## VMware Response

VMware-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE	(ID, TITLE, <b>USERNAME?</b> , <b>PORT</b> , <b>SSL_VERIFY?</b> , <b>HOSTS?</b> , IP_SET, <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/USERNAME (#PCDATA)	The user account to be used for authentication on target hosts. This is an ESXi account or a Windows domain account, in which case the format is domain\user.
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/PORT (#PCDATA)	The port where the ESXi web services are running.



XPath	element specifications / notes
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/SSL_VERIFY (#PCDATA)	A flag indicating the SSL validation setting: "all" means complete SSL validation is selected, "skip" means the "Skip Verify" option is selected (host SSL certificate is self-signed or uses an SSL certificate signed by a custom root CA), "none" means no SSL validation is selected.
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/HOSTS (#PCDATA)	The list of FQDNs for hosts that correspond to all ESXi host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record or "basic" when a vault is not defined.
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/DIGITAL_VAULT (#PCDATA)	Vault information, when a vault is defined for the record. See <a href="#">Vault Information</a> .

## Apache Response

Apache-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/	(ID, TITLE, IP_SET, <b>UNIX_CONFIGURATION_FILE</b> , <b>UNIX_CONTROL_COMMAND</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/UNIX_CONFIGURATION_FILE (#PCDATA)	The path to the Apache configuration file (valid for Apache Web Server record only).
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/UNIX_CONTROL_COMMAND (#PCDATA)	The path to the Apache control command (valid for Apache Web Server record only).

## IBM WebSphere Response

IBM WebSphere-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/	(ID, TITLE, IP_SET, <b>UNIX_INSTALLATION_DIRECTORY</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)

XPath	element specifications / notes
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPPHERE_LIST/AUTH_IBM_WEBSPPHERE/UNIX_INSTLLATION_DIRECTORY (#PCDATA)	The directory where the WebSphere application is installed.

**Tomcat Server Response**

Tomcat Server-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT	(ID, TITLE, IP_SET, <b>INSTALLATION_PATH</b> , <b>INSTANCE_PATH?</b> , <b>AUTO_DISCOVER_INSTANCES?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_APACHELIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTALLATION_PATH (#PCDATA)	The directory where the tomcat server is installed.
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTANCE_PATH (#PCDATA)	The directory where the tomcat server instance(s) are installed, if specified.
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/AUTO_DISCOVER_INSTANCES (#PCDATA)	The value 1 indicates that the “Auto Discover Instances” option is enabled for the record. The value 0 indicates that the option is disabled.

**HTTP Response**

HTTP-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_HTTP_LIST/AUTH_HTTP	(ID, TITLE, <b>USERNAME</b> , <b>SSL</b> , ( <b>REALM VHOST</b> ), IP_SET?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_HTTP_LIST/AUTH_HTTP/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_HTTP_LIST/AUTH_HTTP/SSL (#PCDATA)	A flag indicating the SSL setting. 1 means we’ll attempt authentication over SSL only; 0 means we’ll attempt authentication without this restriction.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_HTTP_LIST/AUTH_HTTP/REALM (#PCDATA)	The realm to authenticate against.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_HTTP_LIST/AUTH_HTTP/VHOST (#PCDATA)	The virtual host to authenticate against.

## Sybase

Sybase-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE	(ID, TITLE, <b>USERNAME</b> , <b>DATABASE</b> , <b>PORT</b> , <b>INSTALLATION_DIR?</b> , IP_SET?, <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/DATABASE (#PCDATA)	The name of the Sybase database to authenticate to.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/PORT (#PCDATA)	The port the Sybase database is on.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/INSTALLATION_DIR (#PCDATA)	The Sybase database installation directory.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/DIGITAL_VAULT/	Vault information, when a vault is defined for the record. See <a href="#">Vault Information</a> .

## MySQL Response

MySQL-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL	(ID, TITLE, <b>USERNAME</b> , <b>DATABASE</b> , <b>PORT</b> , <b>HOSTS?</b> , <b>IP_SET?</b> , <b>SSL_VERIFY</b> , <b>WINDOWS_CONF_FILE</b> , <b>UNIX_CONF_FILE</b> , <b>CLIENT_CERT?</b> , <b>CLIENT_KEY?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/DATABASE (#PCDATA)	The database that will be authenticated to.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/PORT (#PCDATA)	The port the database is running on.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/HOSTS (#PCDATA)	A list of FQDNs for the hosts that correspond to all host API addresses on which a custom SSL certificate signed by a trusted root CA is installed.

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/IP_SET (IP IP_RANGE)	The IP address(es) the server will log into using the record's credentials.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/SSL_VERIFY (#PCDATA)	A flag indicating whether complete SSL certificate validation is enabled. The value 1 (enabled) means we'll 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. The value 0 (disabled) means we'll attempt authentication with MySQL Servers that do and do not use SSL; in the case of SSL the server SSL certificate verification will be skipped.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/WINDOWS_CONF_FILE (#PCDATA)	The path to the Windows MySQL conf file.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/UNIX_CONF_FILE (#PCDATA)	The path to the Unix MySQL conf file.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/CLIENT_CERT (#PCDATA)	PEM-encoded X.509 certificate.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MYSQL_LIST/AUTH_MYSQL/CLIENT_KEY (#PCDATA)	PEM-encoded RSA private key.

## WebLogic Server Response

WebLogic Server-specific elements (in bold) are described below.

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_ORACLE_WEBLOGIC_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_WEBLOGIC_LIST/AUTH_ORACLE_WEBLOGIC	(ID, TITLE, IP_SET, <b>INSTALLATION_PATH</b> , <b>AUTO_DISCOVER</b> , <b>DOMAIN?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_ORACLE_WEBLOGIC_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_WEBLOGIC_LIST/AUTH_ORACLE_WEBLOGIC/INSTALLATION_PATH (#PCDATA)	The directory where the Oracle WebLogic Server is installed.
/AUTH_ORACLE_WEBLOGIC_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_WEBLOGIC_LIST/AUTH_ORACLE_WEBLOGIC/AUTO_DISCOVER (#PCDATA)	A flag indicating whether auto-discovery of domains is enabled. 1 means auto-discovery is enabled, and 0 means it's not enabled and a single domain is defined for the record.
/AUTH_ORACLE_WEBLOGIC_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_WEBLOGIC_LIST/AUTH_ORACLE_WEBLOGIC/DOMAIN (#PCDATA)	A single Oracle WebLogic Server domain name.

## Docker

Docker-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_DOCKER_LIST/AUTH_DOCKER	(ID, TITLE, <b>DAEMON_CONFIGURATION_FILE?</b> , <b>DOCKER_COMMAND?</b> , IP_SET, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_DOCKER_LIST/AUTH_DOCKER/DAEMON_CONFIGURATION_FILE (#PCDATA)	Location of the configuration file for the docker daemon.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_DOCKER_LIST/AUTH_DOCKER/DOCKER_COMMAND (#PCDATA)	The docker command to connect to a local docker daemon.

## PostgreSQL Response

PostgreSQL-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL	(ID, TITLE, <b>USERNAME</b> , <b>DATABASE</b> , <b>PORT</b> , <b>SSL_VERIFY</b> , <b>HOSTS?</b> , IP_SET?, <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , <b>UNIX_CONF_FILE</b> , <b>PRIVATE_KEY_CERTIFICATE_LIST?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/DATABASE (#PCDATA)	The database instance you want to authenticate to.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/PORT (#PCDATA)	The port where the PostgreSQL database is running.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/SSL_VERIFY (#PCDATA)	1 means SSL verification is enabled; 0 means it is not enabled.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/HOSTS (#PCDATA)	A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?)  Vault information, when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ UNIX_CONF_FILE (#PCDATA)	The full path to the PostgreSQL configuration file on your Unix assets (IP addresses).
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*	
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE	(ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO, CERTIFICATE?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/ID	The private certificate ID.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PRIVATE_KEY_INFO	(PRIVATE_KEY   DIGITAL_VAULT)  attribute: type (basic   vault) "basic"
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/ PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PASSPHRASE_INFO (DIGITAL_VAULT?)	attribute: type (basic   vault) "basic"

## MongoDB Response

MongoDB-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB	(ID, TITLE, <b>USERNAME?</b> , <b>DATABASE</b> , <b>PORT</b> , <b>UNIX_CONFIGURATION_FILE</b> , <b>SSL_VERIFY?</b> , <b>HOSTS?</b> , <b>IP_SET?</b> , <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , <b>PRIVATE_KEY_CERTIFICATE_LIST?</b> , <b>NETWORK_ID?</b> , <b>CREATED</b> , <b>LAST_MODIFIED</b> , <b>COMMENTS?</b> )
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/ USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/ DATABASE (#PCDATA)	The database instance you want to authenticate to.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PORT (#PCDATA)	The port where the MongoDB instance is running.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/SSL_VERIFY (#PCDATA)	1 means SSL verification is enabled; 0 means it is not enabled.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/HOSTS (#PCDATA)	A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_ACCOUNT_NAME?)  Vault information, when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/UNIX_CONF_FILE (#PCDATA)	The full path to the MongoDB configuration file on your Unix assets (IP addresses).
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*	
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE	(ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO, CERTIFICATE?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/ID	The private certificate ID.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PRIVATE_KEY_INFO	(PRIVATE_KEY   DIGITAL_VAULT)  attribute: type (basic   vault) "basic"
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PASSPHRASE_INFO (DIGITAL_VAULT?)	attribute: type (basic   vault) "basic"

**Palo Alto Firewall Response**

Palo Alto Firewall-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_PALO_ALTO_FIREWALL_LIST/AUTH_PALO_ALTO_FIREWALL	(ID, TITLE, <b>USERNAME?</b> , <b>SSL_VERIFY</b> , IP_SET?, <b>LOGIN_TYPE?</b> , <b>DIGITAL_VAULT?</b> , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_PALO_ALTO_FIREWALL_LIST/AUTH_PALO_ALTO_FIREWALL/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_PALO_ALTO_FIREWALL_LIST/AUTH_PALO_ALTO_FIREWALL/SSL_VERIFY (#PCDATA)	1 means SSL verification is enabled; 0 means it is not enabled.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_PALO_ALTO_FIREWALL_LIST/AUTH_PALO_ALTO_FIREWALL/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_PALO_ALTO_FIREWALL_LIST/AUTH_PALO_ALTO_FIREWALL/DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_ACCOUNT_NAME?)
	Vault information, when a vault is defined for the record.

**Vault Information**

A vault may be defined for certain record types. Note that <TYPE> is the authentication type (i.e. windows, unix).

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)
	The sub-elements under <DIGITAL_VAULT> differ per record type (technology).
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/DIGITAL_VAULT_ID (#PCDATA)	The vault ID.



XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/DIGITAL_VAULT_TYPE (#PCDATA)	The vault type.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/DIGITAL_VAULT_TITLE (#PCDATA)	The vault title.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_USERNAME (#PCDATA)	The user name of vault account.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_FOLDER (#PCDATA)	The name of the folder in the secure digital safe where the password to be used for authentication should be stored.q
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_FILE (#PCDATA)	The name of the file in the secure digital safe where the password to be used for authentication should be stored.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_SECRET_NAME (#PCDATA)	The secret name that contains the password to be used for authentication.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_SYSTEM_NAME (#PCDATA)	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.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_EP_NAME (#PCDATA)	The End-Point name identifies a managed system, either a target for local accounts or a domain controller for domain accounts.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_EP_TYPE (#PCDATA)	The End-Point type represents the method of access to the End-Point system.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_EP_CONT (#PCDATA)	The End-Point container.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_NS_TYPE (#PCDATA)	If vault type is Lieberman ERPM, the system type: auto, windows, unix, oracle, mssql, ldap, cisco, custom.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_NS_NAME (#PCDATA)	The custom system type name (valid only when VAULT_NS_TYPE=custom).

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_ACCOUNT_NAME (#PCDATA)	
	The account name for vault type BeyondTrust PBPS.

**Warning List**

Note that <TYPE> is the authentication type.

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST (WARNING+)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING (CODE?, TEXT, URL?, ID_SET?)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/CODE (#PCDATA)	
	A warning code. A warning code appears when the API request identifies more than 1,000 records.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/TEXT (#PCDATA)	
	A warning message. A warning message appears when the API request identifies more than 1,000 records.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/URL (#PCDATA)	
	The URL for making another API request for the next batch of authentication records.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET (ID ID_RANGE)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET/ID (#PCDATA)	
	An authentication record ID.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING/ID_SET/ID_RANGE (#PCDATA)	
	A range of authentication record IDs.

## Glossary

Note that <TYPE> is the authentication type, such as: unix, windows, oracle, snmp, etc.

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY (USER_LIST?)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST (USER+)	A list of users who created authentication records in the authentication record list by type output.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER (USER_LOGIN, FIRST_NAME, LAST_NAME)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER (#PCDATA)	A user login ID.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /FIRST_NAME (#PCDATA)	The first name of the account user.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /LAST_NAME (#PCDATA)	The last name of the account user.

## Authentication Record Return

The generic return output XML is returned from an API request for an authentication record management request (create, edit or delete).

The DTD can be found at the following URL (where `qualysapi.qualys.com` is the API server URL where your account is located):

`https://qualysapi.qualys.com/api/2.0/batch_return.dtd`

### DTD for Authentication Record Return Output

A recent DTD for the authentication record return output is shown below.

```
<!-- QUALYS BATCH_RETURN DTD -->
<!ELEMENT BATCH_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, BATCH_LIST?)>
<!ELEMENT BATCH_LIST (BATCH+)>
<!ELEMENT BATCH (CODE?, TEXT?, ID_SET?)>

<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!-- EOF -->
```

## XPaths for Authentication Record Return Output

This section describes the XPaths for the authentication record return output.

XPath	element specifications / notes
/BATCH_RETURN	(REQUEST?, RESPONSE)
/BATCH_RETURN/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/BATCH_RETURN/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/BATCH_RETURN/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/BATCH_RETURN/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/BATCH_RETURN/REQUEST/PARAM_LIST	(PARAM+)
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/BATCH_RETURN/REQUEST/POST_DATA	(#PCDATA) The POST data, if any. POST data is urlencoded.
/BATCH_RETURN/RESPONSE	(DATETIME, BATCH_LIST?)
/BATCH_RETURN/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/BATCH_RETURN/RESPONSE/BATCH_LIST	(BATCH+)
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH	(CODE?, TEXT?, ID_SET?)
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/CODE	(#PCDATA) An HTTP status code indicating whether the operation succeeded or failed.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/TEXT	(#PCDATA) An HTTP status message.
/BATCH_RETURN/RESPONSE/BATCH_LIST/BATCH/ID_SET	(ID   ID_RANGE) Record IDs or a range of IDs.

## Authentication Vault List Output

The authentication vault list XML is returned from an authentication vault list API call (/api/2.0/fo/vault/ with action=list) API.

The DTD can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

[https://<qualysapi.qualys.com>/api/2.0/fo/vault/vault\\_output.dtd](https://<qualysapi.qualys.com>/api/2.0/fo/vault/vault_output.dtd)

### DTD for Authentication Vault List Output

A recent DTD for the authentication vault list is shown below.

```
<!-- QUALYS VAULT_OUTPUT DTD -->

<!ELEMENT AUTH_VAULT_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, STATUS, COUNT, AUTH_VAULTS)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT COUNT (#PCDATA)>

<!ELEMENT AUTH_VAULTS (AUTH_VAULT*)>
<!ELEMENT AUTH_VAULT (UUID?, TITLE, VAULT_TYPE, LAST_MODIFIED?,
                     LAST_MODIFIED_DATE?, SERVER_ADDRESS?, ID?)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT VAULT_TYPE (#PCDATA)>
<!ELEMENT SERVER_ADDRESS (#PCDATA)>
<!ELEMENT LAST_MODIFIED_DATE (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!-- EOF -->
```

## XPaths for Authentication Vault List Output

This section describes the XPaths for the authentication vault list output.

XPath	element specifications / notes
/AUTH_VAULT_LIST_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_VAULT_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/AUTH_VAULT_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/AUTH_VAULT_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/AUTH_VAULT_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/AUTH_VAULT_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/AUTH_VAULT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/AUTH_VAULT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/AUTH_VAULT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/AUTH_VAULT_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/AUTH_VAULT_LIST_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_VAULT_LIST_OUTPUT/RESPONSE	(DATETIME, STATUS, COUNT, AUTH_VAULTS)
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/STATUS	(#PCDATA) Status of the API request if it is successful or not.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/COUNT	(#PCDATA) Number of authentication records in the response.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS	(AUTH_VAULT*) (UUID?, TITLE, VAULT_TYPE, LAST_MODIFIED?, LAST_MODIFIED_DATE?, SERVER_ADDRESS?, ID?)
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/UUID	(#PCDATA) The UUID of the vault if available.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/TITLE	(#PCDATA) The vault title.

<b>XPath</b>	<b>element specifications / notes</b>
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/VAULT_TYPE (#PCDATA)	The vault type, one of: Cyber-Ark PIM Suite, Cyber-Ark AIM, Thycotic Secret Server, Quest Vault, CA Access Control, Hitachi ID PAM, Lieberman ERPM, BeyondTrust PBPS
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/LAST_MODIFIED (DATETIME, BY?)	The date/time the vault was last modified, and the username of the user who made the change.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/SERVER_ADDRESS (#PCDATA)	The IP address of the vault server. Valid for vault types: Cyber-Ark PIM Suite, Quest Vault.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/ID (#PCDATA)	The vault ID.



# Authentication Vault View Output

The authentication vault list XML is returned from an authentication vault list API call (/api/2.0/fo/vault/ with action=view) API.

The DTD can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

[https://<qualysapi.qualys.com>/api/2.0/fo/vault/vault\\_view.dtd](https://<qualysapi.qualys.com>/api/2.0/fo/vault/vault_view.dtd)

## DTD for Authentication Vault View Output

A recent DTD for the authentication vault view is shown below.

```
<!-- QUALYS VAULT_OUTPUT DTD -->

<!ELEMENT VAULT_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, VAULT_QUEST)>

<!ELEMENT VAULT_QUEST (TITLE, COMMENTS, VAULT_TYPE, CREATED_ON?, OWNER?,
                       LAST_MODIFIED?, APPID?, APPKEY?, USERNAME?, URL?,
                       SSL_VERIFY?, DOMAIN?, API_USERNAME?,
                       WEB_USERNAME?, SERVER_ADDRESS?, PORT?, SAFE?,
                       (UUID|ID))>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT VAULT_TYPE (#PCDATA)>
<!ELEMENT CREATED_ON (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT APPID (#PCDATA)>
<!ELEMENT APPKEY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
```

```
<!ELEMENT URL (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT API_USERNAME (#PCDATA)>
<!ELEMENT WEB_USERNAME (#PCDATA)>
<!ELEMENT SERVER_ADDRESS (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SAFE (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME, BY?)>
<!ELEMENT BY (#PCDATA)>
<!-- EOF -->
```

**XPaths for Authentication Vault View Output**

This section describes the XPaths for the authentication vault view output.

XPath	element specifications / notes
/AUTH_VAULT_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_VAULT_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/AUTH_VAULT_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request.
/AUTH_VAULT_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/AUTH_VAULT_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/AUTH_VAULT_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/AUTH_VAULT_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/AUTH_VAULT_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name.
/AUTH_VAULT_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/AUTH_VAULT_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/AUTH_VAULT_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_VAULT_OUTPUT/RESPONSE	(DATETIME, VAULT_QEST)
/AUTH_VAULT_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.

XPath	element specifications / notes
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST	(TITLE, COMMENTS, VAULT_TYPE, CREATED_ON?, OWNER?, LAST_MODIFIED?, APPID?, APPKEY?, USERNAME?, URL?, SSL_VERIFY?, DOMAIN?, API_USERNAME?, WEB_USERNAME?, SERVER_ADDRESS?, PORT?, SAFE?, (UUID ID))
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/TITLE (#PCDATA)	The vault title.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/COMMENTS (#PCDATA)	User-defined comments for the vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/VAULT_TYPE (#PCDATA)	The vault type, one of: Cyber-Ark PIM Suite, Cyber-Ark AIM, Thycotic Secret Server, Quest Vault, CA Access Control, Hitachi ID PAM, Lieberman ERPM, BeyondTrust PBPS
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/CREATED_ON (#PCDATA)	The date/time when the vault was first created.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/OWNER (#PCDATA)	The vault owner.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/APPID (#PCDATA)	Application ID string defined by the customer. The application ID acts as an authenticator for our scanner to call CCP web services API.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/APPKEY (#PCDATA)	The application key (alpha-numeric string) provided by the customer for the BeyondTrust PBPS web services API.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/LAST_MODIFIED (DATETIME, BY?)	The date/time when the vault was last modified and the username of the user who made the change.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/URL (#PCDATA)	The URL of the vault web services. Valid for vault types: CA Access Control, Lieberman ERPM, Thycotic Secret Server.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/SSL_VERIFY (#PCDATA)	A flag indicating whether our service will verify the SSL certificate of the web services URL to make sure the certificate is valid and trusted. Valid for vault types: CA Access Control, Lieberman ERPM, Thycotic Secret Server.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/DOMAIN (#PCDATA)	The domain name if your vault server is part of a domain. Valid vault types: Lieberman ERPM, Thycotic Secret Server.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/API_USERNAME (#PCDATA)	The username to be used for authentication to the vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_REQUEST/WEB_USERNAME (#PCDATA)	The web username to be used to access Basic authentication of the CA Access Control web server. Not valid for other vault types.

XPath	element specifications / notes
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTIONNAIRE/SERVER_ADDRESS (#PCDATA)	The IP address of the vault server. Valid for vault types: Cyber-Ark PIM Suite, Quest Vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTIONNAIRE/PORT (#PCDATA)	The port the vault server is running on. Valid for vault types: Cyber-Ark PIM Suite, Quest Vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTIONNAIRE/SAFE (#PCDATA)	The name of the digital password safe for Cyber-Ark PIM Suite vault. Not valid for other vault types.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTIONNAIRE/(UUID ID) (#PCDATA)	The vault ID and UUID if available.

## Scorecard Report XML

This appendix describes the XML output returned from API V2 requests using the Scorecard Report API functions.

- Asset Group Vulnerability Report
- Ignored Vulnerabilities Report
- Most Prevalent Vulnerabilities Report
- Most Vulnerable Hosts Report
- Patch Report

# Asset Group Vulnerability Report

The asset group vulnerability report XML is returned from a scorecard report (**/report/scorecard**) API call.

The DTD can be found at the following URL:

`https://<qualysapi.qualys.com>/asset_group_scorecard.dtd`

where `<qualysapi.qualys.com>` is the API server URL where your account is located.

## DTD for Asset Group Vulnerability Report

A recent DTD for the asset group vulnerability report is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT ASSET_GROUP_SCORECARD (ERROR | (HEADER, SUMMARY, RESULTS))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT SCORECARD_TYPE (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- TARGETING, FILTERING, SORTING CRITERIA -->
<!ELEMENT SUMMARY (PARAM_LIST, DETAILS?)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>

<!-- RESULTS -->
<!ELEMENT RESULTS (ASSET_GROUP_LIST, NON_RUNNING_KERNELS?)>
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
```

```

<!ELEMENT ASSET_GROUP (TITLE, STATS)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT STATS (HOSTS, NUM_SEV_5?, NUM_SEV_5_VULNERABLE_HOSTS?,
    NUM_SEV_4?, NUM_SEV_4_VULNERABLE_HOSTS?, NUM_SEV_3?,
    NUM_SEV_3_VULNERABLE_HOSTS?, VULNERABLE_HOSTS?,
    VULNERABLE_HOSTS_PCT?, VULNERABLE_HOSTS_GOAL?,
    CONFIRMED_COUNT?, POTENTIAL_COUNT?, NEW_COUNT?,
    ACTIVE_COUNT?, FIXED_COUNT?, REOPENED_COUNT?,
    IGNORED_COUNT?, DAY_0_TO_30_COUNT?, DAY_31_TO_60_COUNT?,
    DAY_61_TO_90_COUNT?, DAY_91_TO_180_COUNT?,
    DAY_181_TO_270_COUNT?, DAY_271_TO_365_COUNT?)>
<!ELEMENT HOSTS (#PCDATA)>
<!ELEMENT NUM_SEV_5 (#PCDATA)>
<!ELEMENT NUM_SEV_5_VULNERABLE_HOSTS (#PCDATA)>
<!ELEMENT NUM_SEV_4 (#PCDATA)>
<!ELEMENT NUM_SEV_4_VULNERABLE_HOSTS (#PCDATA)>
<!ELEMENT NUM_SEV_3 (#PCDATA)>
<!ELEMENT NUM_SEV_3_VULNERABLE_HOSTS (#PCDATA)>
<!ELEMENT VULNERABLE_HOSTS (#PCDATA)>
<!ELEMENT VULNERABLE_HOSTS_PCT (#PCDATA)>
<!ELEMENT VULNERABLE_HOSTS_GOAL (#PCDATA)>
<!ELEMENT CONFIRMED_COUNT (#PCDATA)>
<!ELEMENT POTENTIAL_COUNT (#PCDATA)>
<!ELEMENT NEW_COUNT (#PCDATA)>
<!ELEMENT ACTIVE_COUNT (#PCDATA)>
<!ELEMENT FIXED_COUNT (#PCDATA)>
<!ELEMENT REOPENED_COUNT (#PCDATA)>
<!ELEMENT IGNORED_COUNT (#PCDATA)>
<!ELEMENT DAY_0_TO_30_COUNT (#PCDATA)>
<!ELEMENT DAY_31_TO_60_COUNT (#PCDATA)>
<!ELEMENT DAY_61_TO_90_COUNT (#PCDATA)>
<!ELEMENT DAY_91_TO_180_COUNT (#PCDATA)>
<!ELEMENT DAY_181_TO_270_COUNT (#PCDATA)>
<!ELEMENT DAY_271_TO_365_COUNT (#PCDATA)>
<!ELEMENT NON_RUNNING_KERNELS (NON_RUNNING_KERNEL*)>
<!ELEMENT NON_RUNNING_KERNEL (NRK_QID*, IP*, SEVERITY*)>
<!ELEMENT NRK_QID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>

```

**XPaths for Asset Group Vulnerability Report**

The XPaths for the asset group vulnerability report are described below.

XPath	element specifications / notes
/ASSET_GROUP_SCORECARD	(ERROR   (HEADER, SUMMARY, RESULTS))
/ASSET_GROUP_SCORECARD/ERROR	(#PCDATA)
	An error message.
attribute: <b>number</b>	An error code, when available
/ASSET_GROUP_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/ASSET_GROUP_SCORECARD/HEADER/NAME	(#PCDATA)
	The report header name is “Asset Group Vulnerability Report”.
/ASSET_GROUP_SCORECARD/HEADER/GENERATION_DATETIME	(#PCDATA)
	The date and time when the report was generated.
/ASSET_GROUP_SCORECARD/SCORECARD_TYPE	(#PCDATA)
	The scorecard type.
/ASSET_GROUP_SCORECARD/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user’s company name and address, as defined in the user’s account.
/ASSET_GROUP_SCORECARD/HEADER/USER_INFO	(NAME, USERNAME, ROLE)
/ASSET_GROUP_SCORECARD/HEADER/USER_INFO/NAME	(#PCDATA)
	The name of the user who generated the scorecard.
/ASSET_GROUP_SCORECARD/HEADER/USER_INFO/USERNAME	(#PCDATA)
	The user login ID of the user who generated the scorecard.
/ASSET_GROUP_SCORECARD/HEADER/USER_INFO/ROLE	(#PCDATA)
	The user role assigned to the user who generated the scorecard: Manager, Unit Manager, Scanner or Reader.
/ASSET_GROUP_SCORECARD/SUMMARY	(PARAM_LIST, DETAILS?)
/ASSET_GROUP_SCORECARD/SUMMARY/PARAM_LIST	(PARAM+)
/ASSET_GROUP_SCORECARD/SUMMARY/PARAM_LIST/PARAM	(KEY, VALUE)
/ASSET_GROUP_SCORECARD/SUMMARY/PARAM_LIST/PARAM/KEY	(#PCDATA)
	A scorecard parameter name in the report source settings.
/ASSET_GROUP_SCORECARD/SUMMARY/PARAM_LIST/PARAM/VALUE	(#PCDATA)
	A scorecard parameter value in the report source settings.
/ASSET_GROUP_SCORECARD/RESULTS	(ASSET_GROUP_LIST, NON_RUNNING_KERNELS?)
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP_LIST	(ASSET_GROUP+)
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP	(TITLE, STATS)
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/TITLE	(#PCDATA)
	An asset group title.



XPath	element specifications / notes
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS	(HOSTS, NUM_SEV_5?, NUM_SEV_5_VULNERABLE_HOSTS?, NUM_SEV_4?, NUM_SEV_4_VULNERABLE_HOSTS?, NUM_SEV_3?, NUM_SEV_3_VULNERABLE_HOSTS?, VULNERABLE_HOSTS?, VULNERABLE_HOSTS_PCT?, VULNERABLE_HOSTS_GOAL?, CONFIRMED_COUNT?, POTENTIAL_COUNT?, NEW_COUNT?, ACTIVE_COUNT?, FIXED_COUNT?, REOPENED_COUNT?, IGNORED_COUNT?, DAY_0_TO_30_COUNT?, DAY_31_TO_60_COUNT?, DAY_61_TO_90_COUNT?, DAY_91_TO_180_COUNT?, DAY_181_TO_270_COUNT?, DAY_271_TO_365_COUNT?)
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/HOSTS (#PCDATA)	The number of live hosts in the asset group that were scanned.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_5 (#PCDATA)	The number of severity 5 vulnerabilities across all hosts in the asset group.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_5_VULNERABLE_HOSTS (#PCDATA)	The number of hosts in the asset group with severity 5 vulnerabilities.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_4 (#PCDATA)	The number of severity 4 vulnerabilities across all hosts in the asset group.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_4_VULNERABLE_HOSTS (#PCDATA)	The number of hosts in the asset group with severity 4 vulnerabilities.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_3 (#PCDATA)	The number of severity 3 vulnerabilities across all hosts in the asset group.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NUM_SEV_3_VULNERABLE_HOSTS (#PCDATA)	The number of hosts in the asset group with severity 3 vulnerabilities.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/VULNERABLE_HOSTS	The number of hosts in the asset group that are vulnerable to the QID selection for the report.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/VULNERABLE_HOSTS_PCT	The percentage of hosts in the asset group that are vulnerable to the QID selection for the report.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/VULNERABLE_HOSTS_GOAL	(Appears only when Business Risk Goal is selected in the scorecard report template.) Indicates whether the asset group meets the level of acceptable risk. A value of 1 means that the group passes (the percentage of vulnerable hosts was equal to or less than the business risk goal set in the template), and a value of 0 means the group fails (the percentage of vulnerable hosts was greater than the business risk goal set in the template).
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/CONFIRMED_COUNT	The number of Confirmed vulnerabilities.

<b>XPath</b>	<b>element specifications / notes</b>
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/POTENTIAL_COUNT	The number of Potential vulnerabilities.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/NEW_COUNT	The number of vulnerabilities with status New.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/ACTIVE_COUNT	The number of vulnerabilities with status Active.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/FIXED_COUNT	The number of vulnerabilities with status Fixed.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/REOPENED_COUNT	The number of vulnerabilities with status Re-Opened.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/IGNORED_COUNT	The number of vulnerabilities with status Ignored.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_0_TO_30_COUNT	The number of vulnerabilities detected in the last 30 days.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_31_TO_60_COUNT	The number of vulnerabilities detected 31 to 60 days ago.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_61_TO_90_COUNT	The number of vulnerabilities detected 61 to 90 days ago.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_91_TO_180_COUNT	The number of vulnerabilities detected 91 to 180 days ago.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_181_TO_270_COUNT	The number of vulnerabilities detected 181 to 270 days ago.
/ASSET_GROUP_SCORECARD/RESULTS/ASSET_GROUP/STATS/DAY_271_TO_365_COUNT	The number of vulnerabilities detected 271 to 365 days ago.
/ASSET_GROUP_SCORECARD/RESULTS/NON_RUNNING_KERNELS (NON_RUNNING_KERNEL*)	
/ASSET_GROUP_SCORECARD/RESULTS/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL (NRK_QID*, IP*, SEVERITY*)>	
/ASSET_GROUP_SCORECARD/RESULTS/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/NRK_QID (#PCDATA)	The QID assigned to a vulnerability detected on a non-running kernel.
/ASSET_GROUP_SCORECARD/RESULTS/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/IP (#PCDATA)	The IP address of the host with the non-running kernel vulnerability.
/ASSET_GROUP_SCORECARD/RESULTS/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/SEVERITY (#PCDATA)	The severity of the vulnerability detected on a non-running kernel.

# Ignored Vulnerabilities Report

The ignored vulnerabilities report XML is returned from a scorecard report (**/report/scorecard**) API call.

The DTD can be found at the following URL:

[https://<qualysapi.qualys.com>/ignored\\_vulns\\_scorecard.dtd](https://<qualysapi.qualys.com>/ignored_vulns_scorecard.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Ignored Vulnerabilities Report

A recent DTD for the ignored vulnerabilities report is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS IGNORED VULNS SCORECARD DTD -->

<!ELEMENT IGNORED_VULNS_SCORECARD (ERROR | (HEADER, SUMMARY, RESULTS))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT SCORECARD_TYPE (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- TARGETING, FILTERING, SORTING CRITERIA -->
<!ELEMENT SUMMARY (PARAM_LIST)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
```

```

<!-- RESULTS -->
<!ELEMENT RESULTS (ASSET_GROUP_LIST)>
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (TITLE, DETECTION_LIST)>

<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (HOST, VULN, TICKET)>

<!ELEMENT HOST (IP, DNS?, NETBIOS?, OS?)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>

<!ELEMENT VULN (QID, TITLE, FIRST_FOUND_DATE?, SEVERITY, TYPE,
                CVSS_BASE?, CVSS_TEMPORAL?)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>

<!ELEMENT TICKET (NUMBER, STATE_DAYS, LAST_MODIFIED_DATE, COMMENTS?,
                  ASSIGNEE_NAME?, ASSIGNEE_EMAIL?)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT STATE_DAYS (#PCDATA)>
<!ELEMENT LAST_MODIFIED_DATE (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT ASSIGNEE_NAME (#PCDATA)>
<!ELEMENT ASSIGNEE_EMAIL (#PCDATA)>

```

**XPaths for Ignored Vulnerabilities Report**

The XPaths for the ignored vulnerabilities report are described below.

XPath	element specifications / notes
/IGNORED_VULNS_SCORECARD	(ERROR   (HEADER, SUMMARY, RESULTS))
/IGNORED_VULNS_SCORECARD/ERROR	(#PCDATA)
	An error message.
attribute: <b>number</b>	An error code, when available
/IGNORED_VULNS_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)

XPath	element specifications / notes
/IGNORED_VULNS_SCORECARD/HEADER/NAME (#PCDATA)	The report header name is “Ignored Vulnerabilities Report”.
/IGNORED_VULNS_SCORECARD/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated.
/IGNORED_VULNS_SCORECARD/HEADER/SCORECARD_TYPE (#PCDATA)	The scorecard type.
/IGNORED_VULNS_SCORECARD/HEADER/COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)	The user’s company name and address, as defined in the user’s account.
/IGNORED_VULNS_SCORECARD/HEADER/USER_INFO (NAME, USERNAME, ROLE)	
/IGNORED_VULNS_SCORECARD/HEADER/USER_INFO/NAME (#PCDATA)	The name of the user who generated the scorecard.
/IGNORED_VULNS_SCORECARD/HEADER/USER_INFO/USERNAME (#PCDATA)	The user login ID of the user who generated the scorecard.
/IGNORED_VULNS_SCORECARD/HEADER/USER_INFO/ROLE (#PCDATA)	The user role assigned to the user who generated the scorecard: Manager, Unit Manager, Scanner or Reader..
/IGNORED_VULNS_SCORECARD/SUMMARY (PARAM_LIST)	
/IGNORED_VULNS_SCORECARD/SUMMARY/PARAM_LIST (PARAM+)	
/IGNORED_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM (KEY, VALUE)	
/IGNORED_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/KEY (#PCDATA)	A scorecard parameter name in the report source settings.
/IGNORED_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/VALUE (#PCDATA)	A scorecard parameter value in the report source settings.
/IGNORED_VULNS_SCORECARD/RESULTS (ASSET_GROUP_LIST)	
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST (ASSET_GROUP+)	
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP (TITLE, DETECTION_LIST)	
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/TITLE	An asset group title.
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST (DETECTION+)	
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/ DETECTION (HOST, VULN, TICKET)	
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/ DETECTION/HOST (IP, DNS?, NETBIOS?, OS?)	Information about the host, including its IP address and this additional information when available: DNS hostname, NetBIOS hostname, and operating system.

XPath	element specifications / notes
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/DETECTION/VULN	<p>(QID, TITLE, FIRST_FOUND_DATE?, SEVERITY, TYPE, CVSS_BASE?, CVSS_TEMPORAL?)</p> <p>Information about the vulnerability detected. CVSS Base and Temporal scores are included when the CVSS Scoring feature is enabled for the subscription.</p>
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/DETECTION/TICKET	<p>(NUMBER, STATE_DAYS, LAST_MODIFIED_DATE, COMMENTS?, ASSIGNEE_NAME?, ASSIGNEE_EMAIL?)</p> <p>Information about a related ticket if one exists. Information includes the ticket number, the number of days the ticket has been in the Closed/Ignored state, and the date the ticket was created or last modified, any user-defined comments, and the ticket assignee’s name and email address.</p>

# Most Prevalent Vulnerabilities Report

The most prevalent vulnerabilities report XML is returned from a scorecard report (**/report/scorecard**) API call.

The DTD can be found at the following URL:

[https://<qualysapi.qualys.com>/most\\_prevalent\\_vulns\\_scorecard.dtd](https://<qualysapi.qualys.com>/most_prevalent_vulns_scorecard.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Most Prevalent Vulnerabilities Report

A recent DTD for the most prevalent vulnerabilities report is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS MOST PREVALENT VULNS SCORECARD DTD -->

<!ELEMENT MOST_PREVALENT_VULNS_SCORECARD (ERROR | (HEADER, SUMMARY,
                                                    RESULTS))>

<!ELEMENT ERROR (#PCDATA)>
<ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT SCORECARD_TYPE (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- TARGETING, FILTERING, SORTING CRITERIA -->
<!ELEMENT SUMMARY (PARAM_LIST, DETAILS?)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
```

```

<!-- RESULTS -->
<!ELEMENT RESULTS (VULN_LIST)>
<!ELEMENT VULN_LIST (VULN+)>
<!ELEMENT VULN (RANK, QID, TITLE, SEVERITY, TYPE, FIRST_FOUND_DATE?,
                DETECTIONS?, CVSS_BASE?, CVSS_TEMPORAL?,
                TOTAL_HOSTS_AFFECTED?, PERCENT_HOSTS_AFFECTED?)>
<!ELEMENT RANK (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT DETECTIONS (#PCDATA)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT TOTAL_HOSTS_AFFECTED (#PCDATA)>
<!ELEMENT PERCENT_HOSTS_AFFECTED (#PCDATA)>

```

**XPaths for Most Prevalent Vulnerabilities Report**

The XPaths for the most prevalent vulnerabilities report are described below.

XPath	element specifications / notes
/MOST_PREVALENT_VULNS_SCORECARD	(ERROR   (HEADER, SUMMARY, RESULTS))
/MOST_PREVALENT_VULNS_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: <b>number</b>	An error code, when available
/MOST_PREVALENT_VULNS_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/NAME (#PCDATA)	The report header name is “Most Prevalent Vulnerabilities Report”.
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated.
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/SCORECARD_TYPE (#PCDATA)	The scorecard type.
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user’s company name and address, as defined in the user’s account.
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/USER_INFO (NAME, USERNAME, ROLE)	
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/USER_INFO/NAME (#PCDATA)	The name of the user who generated the scorecard.



XPath	element specifications / notes
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/USER_INFO/USERNAME (#PCDATA)	The user login ID of the user who generated the scorecard.
/MOST_PREVALENT_VULNS_SCORECARD/HEADER/USER_INFO/ROLE (#PCDATA)	The user role assigned to the user who generated the scorecard: Manager, Unit Manager, Scanner or Reader.
/MOST_PREVALENT_VULNS_SCORECARD/SUMMARY (PARAM_LIST)	
/MOST_PREVALENT_VULNS_SCORECARD/SUMMARY/PARAM_LIST (PARAM+)	
/MOST_PREVALENT_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM (KEY, VALUE)	
/MOST_PREVALENT_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/KEY (#PCDATA)	A scorecard parameter name in the report source settings.
/MOST_PREVALENT_VULNS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/VALUE (#PCDATA)	A scorecard parameter value in the report source settings.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS (VULN_LIST)	
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN_LIST (VULN+)	
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN	(RANK, QID, TITLE, SEVERITY, TYPE, FIRST_FOUND_DATE?, DETECTIONS?, CVSS_BASE?, CVSS_TEMPORAL?, TOTAL_HOSTS_AFFECTED?, PERCENT_HOSTS_AFFECTED?)
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/RANK (#PCDATA)	The rank of the vulnerability. The vulnerability that was detected on the largest number of hosts is listed as #1.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/QID (#PCDATA)	The QID assigned to the vulnerability.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/TITLE (#PCDATA)	The vulnerability title.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/SEVERITY (#PCDATA)	The severity level assigned to the vulnerability.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/TYPE (#PCDATA)	The vulnerability type.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/FIRST_FOUND_DATE (#PCDATA)	The date and time the vulnerability was first detected.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/DETECTIONS (#PCDATA)	The total number of times the vulnerability was detected.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/CVSS_BASE (#PCDATA)	The CVSS base score for the vulnerability. This is displayed only when the CVSS Scoring feature is enabled for the subscription.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/CVSS_TEMPORAL (#PCDATA)	The CVSS temporal score for the vulnerability. This is displayed only when the CVSS Scoring feature is enabled for the subscription.

XPath	element specifications / notes
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/TOTAL_HOSTS_AFFECTED (#PCDATA)	The number of hosts that are currently affected by the vulnerability.
/MOST_PREVALENT_VULNS_SCORECARD/RESULTS/VULN/PERCENT_HOSTS_AFFECTED (#PCDATA)	The percentage of hosts that are currently affected by the vulnerability.

# Most Vulnerable Hosts Report

The most vulnerable hosts report XML is returned from a scorecard report (**/report/scorecard**) API call.

The DTD can be found at the following URL:

[https://<qualysapi.qualys.com>/most\\_vulnerable\\_hosts\\_scorecard.dtd](https://<qualysapi.qualys.com>/most_vulnerable_hosts_scorecard.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Most Vulnerable Hosts Report

A recent DTD for the most vulnerable hosts report is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS MOST VULNERABLE HOSTS SCORECARD DTD -->

<!ELEMENT MOST_VULNERABLE_HOSTS_SCORECARD (ERROR | (HEADER, SUMMARY,
                                                    RESULTS))>

<!ELEMENT ERROR (#PCDATA)>
<ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT SCORECARD_TYPE (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- TARGETING, FILTERING, SORTING CRITERIA -->
<!ELEMENT SUMMARY (PARAM_LIST, DETAILS?)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
```

```

<!-- RESULTS -->
<!ELEMENT RESULTS (HOST_LIST)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (RANK, IP, DNS?, NETBIOS?, LAST_SCAN_DATE?,
                NUM_SEV_5, NUM_SEV_4, BUSINESS_RISK, SECURITY_RISK,
                ASSET_GROUPS?)>
<!ELEMENT RANK (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>
<!ELEMENT NUM_SEV_5 (#PCDATA)>
<!ELEMENT NUM_SEV_4 (#PCDATA)>
<!ELEMENT BUSINESS_RISK (#PCDATA)>
<!ELEMENT SECURITY_RISK (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>

```

**XPaths for Most Vulnerable Hosts Report**

The XPaths for the most vulnerable hosts report are described below.

XPath	element specifications / notes
/MOST_VULNERABLE_HOSTS_SCORECARD	(ERROR   (HEADER, SUMMARY, RESULTS))
/MOST_VULNERABLE_HOSTS_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: <b>number</b>	An error code, when available
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/NAME (#PCDATA)	The report header name is “Most Vulnerable Hosts Report”.
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated.
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/SCORECARD_TYPE (#PCDATA)	The scorecard type.
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user’s company name and address, as defined in the user’s account.
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/USER_INFO (NAME, USERNAME, ROLE)	
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/USER_INFO/NAME (#PCDATA)	The name of the user who generated the scorecard.

XPath	element specifications / notes
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/USER_INFO/USERNAME (#PCDATA)	The user login ID of the user who generated the scorecard.
/MOST_VULNERABLE_HOSTS_SCORECARD/HEADER/USER_INFO/ROLE (#PCDATA)	The user role assigned to the user who generated the scorecard: Manager, Unit Manager, Scanner or Reader.
/MOST_VULNERABLE_HOSTS_SCORECARD/SUMMARY (PARAM_LIST)	
/MOST_VULNERABLE_HOSTS_SCORECARD/SUMMARY/PARAM_LIST (PARAM+)	
/MOST_VULNERABLE_HOSTS_SCORECARD/SUMMARY/PARAM_LIST/PARAM (KEY, VALUE)	
/MOST_VULNERABLE_HOSTS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/KEY (#PCDATA)	A scorecard parameter name in the report source settings.
/MOST_VULNERABLE_HOSTS_SCORECARD/SUMMARY/PARAM_LIST/PARAM/VALUE (#PCDATA)	A scorecard parameter value in the report source settings.
/MOST_VULNERABLE_HOSTS_SCORECARD/RESULTS (HOST_LIST)	
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST_LIST (HOST+)	
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST	(RANK, IP, DNS?, NETBIOS?, LAST_SCAN_DATE?, NUM_SEV_5, NUM_SEV_4, BUSINESS_RISK, SECURITY_RISK, ASSET_GROUPS?)
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/RANK (#PCDATA)	The rank for the host. The host with the highest number of vulnerabilities with severity levels 4 and 5 is listed as #1.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/IP (#PCDATA)	The IP address for the host.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/DNS (#PCDATA)	The DNS hostname.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/NETBIOS (#PCDATA)	The NetBIOS hostname.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/LAST_SCAN_DATE (#PCDATA)	The date and time the host was last scanned for vulnerabilities.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/NUM_SEV_5 (#PCDATA)	The current number of severity 5 vulnerabilities detected on the host.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/NUM_SEV_4 (#PCDATA)	The current number of severity 4 vulnerabilities detected on the host.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/BUSINESS_RISK (#PCDATA)	The business risk value. See “Business Risk” in the online help for information.  If the host belongs to one asset group in the report, the business risk value for that asset group is displayed. If the host belongs to multiple asset groups in the report, the highest business risk value across the asset groups is displayed.

XPath	element specifications / notes
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/SECURITY_RISK (#PCDATA)	The highest severity level across the vulnerabilities and potential vulnerabilities detected on the host.
/MOST_VULNERABLE_HOSTS_SCORECARD/HOST/ASSET_GROUPS (#PCDATA)	A list of asset groups that the host belongs to.

# Patch Report

The patch report XML is returned from a scorecard report (**/report/scorecard**) API call.

The DTD can be found at the following URL:

[https://<qualysapi.qualys.com>/patch\\_scorecard.dtd](https://<qualysapi.qualys.com>/patch_scorecard.dtd)

where <qualysapi.qualys.com> is the API server URL where your account is located.

## DTD for Patch Report

A recent DTD for the patch report is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS PATCH REPORT SCORECARD DTD -->

<!ELEMENT PATCH_REPORT_SCORECARD (ERROR | (HEADER, SUMMARY, RESULTS))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- TARGETING, FILTERING, SORTING CRITERIA -->
<!ELEMENT SUMMARY (PARAM_LIST, DETAILS?)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>

<!-- SUMMARY DETAILS -->
<!ELEMENT DETAILS (ASSET_GROUP_LIST)>
```

```

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP*)>
<!ELEMENT ASSET_GROUP (TITLE, (STATS | DETECTION_LIST))>
<!ELEMENT STATS (NUM_HOSTS?, SCANNED_HOSTS?, MISSING?)>
<!ELEMENT NUM_HOSTS (#PCDATA)>
<!ELEMENT SCANNED_HOSTS (#PCDATA)>
<!ELEMENT MISSING (ONE_OR_MORE_PATCHES?, SOFTWARE_1?, SOFTWARE_2?)>
<!ELEMENT ONE_OR_MORE_PATCHES (PERCENT, TOTAL_HOSTS)>
<!ELEMENT SOFTWARE_1 (PERCENT, TOTAL_HOSTS, QID?)>
<!ELEMENT SOFTWARE_2 (PERCENT, TOTAL_HOSTS, QID?)>
<!ELEMENT PERCENT (#PCDATA)>
<!ELEMENT TOTAL_HOSTS (#PCDATA)>
<!ELEMENT QID (#PCDATA)>

<!-- RESULTS -->
<!ELEMENT RESULTS (ASSET_GROUP_LIST)>

<!ELEMENT DETECTION_LIST (DETECTION*)>
<!ELEMENT DETECTION (HOST, VULN)>

<!ELEMENT HOST (IP, DNS?, NETBIOS?, OS?, OWNER?)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>

<!ELEMENT VULN (QID, VENDOR_REF?, TITLE)>
<!ELEMENT VENDOR_REF (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>

```

**XPaths for Patch Report**

The XPaths for the patch report are described below.

XPath	element specifications / notes
/PATCH_REPORT_SCORECARD	(ERROR   (HEADER, SUMMARY, RESULTS))
/PATCH_REPORT_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: <b>number</b>	An error code, when available
/PATCH_REPORT_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/PATCH_REPORT_SCORECARD/HEADER/NAME (#PCDATA)	The report header name is “Patch Report”.
/PATCH_REPORT_SCORECARD/HEADER/GENERATION_DATETIME (#PCDATA)	The date and time when the report was generated.



XPath	element specifications / notes
/PATCH_REPORT_SCORECARD/HEADER/COMPANY_INFO	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)
	The user's company name and address, as defined in the user's account.
/PATCH_REPORT_SCORECARD/HEADER/USER_INFO	(NAME, USERNAME, ROLE)
/PATCH_REPORT_SCORECARD/HEADER/USER_INFO/NAME (#PCDATA)	
	The name of the user who generated the scorecard.
/PATCH_REPORT_SCORECARD/HEADER/USER_INFO/USERNAME (#PCDATA)	
	The user login ID of the user who generated the scorecard.
/PATCH_REPORT_SCORECARD/HEADER/USER_INFO/ROLE (#PCDATA)	
	The user role for the user who generated the scorecard: Manager, Unit Manager, Scanner or Reader.
/PATCH_REPORT_SCORECARD/SUMMARY (PARAM_LIST, DETAILS?)	
/PATCH_REPORT_SCORECARD/SUMMARY/PARAM_LIST (PARAM+)	
/PATCH_REPORT_SCORECARD/SUMMARY/PARAM_LIST/PARAM (KEY, VALUE)	
/PATCH_REPORT_SCORECARD/SUMMARY/PARAM_LIST/PARAM/KEY (#PCDATA)	
	A scorecard parameter name in the report source settings.
/PATCH_REPORT_SCORECARD/SUMMARY/PARAM_LIST/PARAM/VALUE (#PCDATA)	
	A scorecard parameter value in the report source settings.
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS (ASSET_GROUP_LIST)	
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST (ASSET_GROUP*)	
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST/ASSET_GROUP )	
	(TITLE, (STATS   DETECTION_LIST)
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST/ASSET_GROUP/TITLE (#PCDATA)	
	An asset group title.
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST/ASSET_GROUP/STATS	
	(NUM_HOSTS?, SCANNED_HOSTS?, MISSING?)
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST/ASSET_GROUP/STATS/NUM_HOSTS (#PCDATA)	
	The number of hosts in the asset group for which there is vulnerability scan data, followed in parentheses by the total number of IP addresses in the asset group.
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/ASSET_GROUP_LIST/ASSET_GROUP/STATS/SCANNED_HOSTS (#PCDATA)	
	The number of hosts in the asset group for which there is vulnerability scan data.
/PATCH_REPORT_SCORECARD/SUMMARY/DETAILS/MISSING	
	(ONE_OR_MORE_PATCHES?, SOFTWARE_1?, SOFTWARE_2?)
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/ONE_OR_MORE_PATCHES (PERCENT, TOTAL_HOSTS)	

XPath	element specifications / notes
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/ONE_OR_MORE_PATCHES/ PERCENT (#PCDATA)	The percentage of scanned hosts in the asset group that are missing at least one of the user-specified patches.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/ONE_OR_MORE_PATCHES/TOTAL_HOSTS (#PCDATA)	The number of scanned hosts in the asset group that are missing at least one of the user-specified patches.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_1/ (PERCENT, TOTAL_HOSTS, QID?)	
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_1 /PERCENT (#PCDATA)	The percentage of scanned hosts in the asset group that are missing the first user-specified software QID.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_1/TOTAL_HOSTS (#PCDATA)	The number of scanned hosts in the asset group that are missing the first user-specified software QID.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_1/QID (#PCDATA)	The first user-specified software QID.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_2 (PERCENT, TOTAL_HOSTS, QID?)	
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_2/ PERCENT (#PCDATA)	The percentage of scanned hosts in the asset group that are missing the second user-specified software QID.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_2/TOTAL_HOSTS (#PCDATA)	The number of scanned hosts in the asset group that are missing the second user-specified software QID.
/PATCH_REPORT_SCORECARD/SUMMARY/ASSET_GROUP_LIST/ASSET_GROUP/STATS/DETAILS/MISSING/SOFTWARE_2/QID (#PCDATA)	The second user-specified software QID.
/PATCH_REPORT_SCORECARD/RESULTS (ASSET_GROUP_LIST)	
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP_LIST (ASSET_GROUP*)	
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP (TITLE, (STATS   DETECTION_LIST))	
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/TITLE (#PCDATA)	An asset group title.
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/STATS (NUM_HOSTS?, SCANNED_HOSTS?, MISSING?)	

XPath	element specifications / notes
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/STATS/NUM_HOSTS (#PCDATA)	The number of hosts in the asset group for which there is vulnerability scan data, followed in parentheses by the total number of IP addresses in the asset group.
/PATCH_REPORT_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/SCANNED_HOSTS (#PCDATA)	The number of hosts in the asset group for which there is vulnerability scan data.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST (DETECTION*)	
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION (HOST, VULN)	
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST	(IP, DNS?, NETBIOS?, OS?, OWNER?)
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST/IP (#PCDATA)	The IP address for a host missing required patches or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST/DNS (#PCDATA)	The registered DNS hostname for a host missing required patches or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST/NETBIOS (#PCDATA)	The NetBIOS hostname for a host missing required patches or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST/OS (#PCDATA)	The operating system detected on a host missing required patches or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/HOST/OWNER (#PCDATA)	The owner of the host missing required patches or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/VULN	(QID, VENDOR_REF?, TITLE)
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/VULN/QID	A vulnerability QID for a missing patch or software.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/VULN/VENDOR_REF (#PCDATA)	A vendor reference for the vulnerability, such as a security bulletin.
/PATCH_REPORT_SCORECARD/RESULTS/DETECTION_LIST/DETECTION/VULN/TITLE (#PCDATA)	The title for the vulnerability for a missing patch or software.

## Scan Configuration XML

This section covers XML data related to scan configurations.

- Scanner Appliance List Output
- Scanner Appliance Create Output
- Static Search List Output
- Dynamic Search List Output

# Scanner Appliance List Output

The Scanner Appliance List API v2 (/api/2.0/fo/appliance/ with action=list) returns a list of scanner appliances using the “appliance\_list\_output.dtd”. This DTD can be found DTD: [https://<baseurl>/api/2.0/fo/appliance/appliance\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/appliance/appliance_list_output.dtd)

## DTD for Scanner Appliance List Output

A recent DTD for the scanner appliance list output (appliance\_list\_output.dtd) is shown below.

```
<!-- QUALYS APPLIANCE_LIST_OUTPUT DTD -->

<!ELEMENT APPLIANCE_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, APPLIANCE_LIST?, LICENSE_INFO?)>
        <!ELEMENT APPLIANCE_LIST (APPLIANCE+)>
            <!ELEMENT APPLIANCE (ID, UUID, NAME, NETWORK_ID?,
SOFTWARE_VERSION, RUNNING_SLICES_COUNT, RUNNING_SCAN_COUNT, STATUS,
CMD_ONLY_START?, MODEL_NUMBER?, TYPE?, SERIAL_NUMBER?, ACTIVATION_CODE?,
INTERFACE_SETTINGS*, PROXY_SETTINGS?, IS_CLOUD_DEPLOYED?, CLOUD_INFO?,
VLANS?, STATIC_ROUTES?, ML_LATEST?, ML_VERSION?, VULNSIGS_LATEST?,
VULNSIGS_VERSION?, ASSET_GROUP_COUNT?, ASSET_GROUP_LIST?,
ASSET_TAGS_LIST?, LAST_UPDATED_DATE?, POLLING_INTERVAL?, USER_LOGIN?,
HEARTBEATS_MISSED?, SS_CONNECTION?, SS_LAST_CONNECTED?, FDCC_ENABLED?,
USER_LIST?, UPDATED?, COMMENTS?, RUNNING_SCANS?, MAX_CAPACITY_UNITS?)>
                <!ELEMENT ID (#PCDATA)>
                <!ELEMENT UUID (#PCDATA)>
                <!ELEMENT NAME (#PCDATA)>
                <!ELEMENT NETWORK_ID (#PCDATA)>
                <!ELEMENT SOFTWARE_VERSION (#PCDATA)>
                <!ELEMENT RUNNING_SLICES_COUNT (#PCDATA)>
                <!ELEMENT RUNNING_SCAN_COUNT (#PCDATA)>
                <!ELEMENT STATUS (#PCDATA)>
                <!ELEMENT CMD_ONLY_START (#PCDATA)>
```

```
<!--ELEMENT MODEL_NUMBER (#PCDATA)>
<!--ELEMENT TYPE (#PCDATA)>
<!--ELEMENT SERIAL_NUMBER (#PCDATA)>
<!--ELEMENT ACTIVATION_CODE (#PCDATA)>
<!--ELEMENT INTERFACE_SETTINGS (SETTING?, INTERFACE,
IP_ADDRESS, NETMASK, GATEWAY, LEASE, IPV6_ADDRESS?, SPEED, DUPLEX, DNS)>
    <!--ELEMENT SETTING (#PCDATA)>
    <!--ELEMENT INTERFACE (#PCDATA)>
    <!--ELEMENT IP_ADDRESS (#PCDATA)>
    <!--ELEMENT NETMASK (#PCDATA)>
    <!--ELEMENT GATEWAY (#PCDATA)>
    <!--ELEMENT LEASE (#PCDATA)>
    <!--ELEMENT IPV6_ADDRESS (#PCDATA)>
    <!--ELEMENT SPEED (#PCDATA)>
    <!--ELEMENT DUPLEX (#PCDATA)>
    <!--ELEMENT DNS (DOMAIN?, PRIMARY, SECONDARY)>
        <!--ELEMENT DOMAIN (#PCDATA)>
        <!--ELEMENT PRIMARY (#PCDATA)>
        <!--ELEMENT SECONDARY (#PCDATA)>
<!--ELEMENT PROXY_SETTINGS (SETTING, PROXY*)>
    <!--ELEMENT PROXY (PROTOCOL?, IP_ADDRESS?, HOSTNAME?,
        PORT, USER)>
        <!--ELEMENT PROTOCOL (#PCDATA)>
        <!--ELEMENT HOSTNAME (#PCDATA)>
        <!--ELEMENT PORT (#PCDATA)>
        <!--ELEMENT USER (#PCDATA)>

<!--ELEMENT IS_CLOUD_DEPLOYED (#PCDATA)>
<!--ELEMENT CLOUD_INFO (PLATFORM_PROVIDER, EC2_INFO?,
GCE_INFO?, AZURE_INFO?)>
    <!--ELEMENT PLATFORM_PROVIDER (#PCDATA)>
    <!--ELEMENT EC2_INFO (INSTANCE_ID, INSTANCE_TYPE,
KERNEL_ID?, AMI_ID, ACCOUNT_ID,
        INSTANCE_REGION, INSTANCE_AVAILABILITY_ZONE,
INSTANCE_ZONE_TYPE,
        INSTANCE_VPC_ID?, INSTANCE_SUBNET_ID?,
IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?,
        SECURITY_GROUPS?,
        API_PROXY_SETTINGS)>
        <!--ELEMENT INSTANCE_ID (#PCDATA)>
        <!--ELEMENT INSTANCE_TYPE (#PCDATA)>
        <!--ELEMENT KERNEL_ID (#PCDATA)>
        <!--ELEMENT AMI_ID (#PCDATA)>
        <!--ELEMENT ACCOUNT_ID (#PCDATA)>
        <!--ELEMENT INSTANCE_REGION (#PCDATA)>
        <!--ELEMENT INSTANCE_AVAILABILITY_ZONE (#PCDATA)>
        <!--ELEMENT INSTANCE_ZONE_TYPE (#PCDATA)>
        <!--ELEMENT INSTANCE_VPC_ID (#PCDATA)>
        <!--ELEMENT INSTANCE_SUBNET_ID (#PCDATA)>
```

```

<!ELEMENT IP_ADDRESS_PRIVATE (#PCDATA)>
<!ELEMENT HOSTNAME_PRIVATE (#PCDATA)>
<!ELEMENT SECURITY_GROUPS (SECURITY_GROUP_IDS?,
SECURITY_GROUP_NAMES?)>
    <!ELEMENT SECURITY_GROUP_IDS (#PCDATA)>
    <!ELEMENT SECURITY_GROUP_NAMES (#PCDATA)>
    <!ELEMENT API_PROXY_SETTINGS (SETTING, PROXY*)>

<!ELEMENT GCE_INFO (INSTANCE_ID, MACHINE_TYPE,
    PROJECT_ID, PROJECT_NAME,
    PREEMPTIBLE,
    INSTANCE_ZONE,
    IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?,
IP_ADDRESS_PUBLIC?,
    INSTANCE_NETWORK,
    GCE_INSTANCE_TAGS
)>
    <!ELEMENT MACHINE_TYPE (#PCDATA)>
    <!ELEMENT PROJECT_ID (#PCDATA)>
    <!ELEMENT PROJECT_NAME (#PCDATA)>
    <!ELEMENT PREEMPTIBLE (#PCDATA)>
    <!ELEMENT INSTANCE_ZONE (#PCDATA)>
    <!ELEMENT GCE_INSTANCE_TAGS (GCE_INSTANCE_TAG*)>
        <!ELEMENT GCE_INSTANCE_TAG (TAG_ID)>
            <!ELEMENT TAG_ID (#PCDATA)>
    <!ELEMENT IP_ADDRESS_PUBLIC (#PCDATA)>
    <!ELEMENT INSTANCE_NETWORK (#PCDATA)>

<!ELEMENT AZURE_INFO (INSTANCE_ID, USER_NAME,
    INSTANCE_LOCATION, DEPLOYMENT_MODE,
    IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?)>
    <!ELEMENT USER_NAME (#PCDATA)>
    <!ELEMENT INSTANCE_LOCATION (#PCDATA)>
    <!ELEMENT DEPLOYMENT_MODE (#PCDATA)>

<!ELEMENT VLANS (SETTING, VLAN*)>
    <!ELEMENT VLAN (ID, NAME, IP_ADDRESS, NETMASK)>
<!ELEMENT STATIC_ROUTES (ROUTE*)>
    <!ELEMENT ROUTE (NAME, IP_ADDRESS, NETMASK, GATEWAY)>
<!ELEMENT ML_LATEST (#PCDATA)>
<!ELEMENT ML_VERSION (#PCDATA)>
    <!ATTLIST ML_VERSION updated CDATA #IMPLIED>
<!ELEMENT VULNSIGS_LATEST (#PCDATA)>
<!ELEMENT VULNSIGS_VERSION (#PCDATA)>
    <!ATTLIST VULNSIGS_VERSION updated CDATA #IMPLIED>
<!ELEMENT ASSET_GROUP_COUNT (#PCDATA)>
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP*)>
    <!ELEMENT ASSET_GROUP (ID, NAME)>
<!ELEMENT ASSET_TAGS_LIST (ASSET_TAG*)>

```

```

        <!-- ELEMENT ASSET_TAG (UUID, NAME) -->
        <!-- ELEMENT LAST_UPDATED_DATE (#PCDATA) -->
        <!-- ELEMENT POLLING_INTERVAL (#PCDATA) -->
        <!-- ELEMENT HEARTBEATS_MISSED (#PCDATA) -->
        <!-- ELEMENT SS_CONNECTION (#PCDATA) -->
        <!-- ELEMENT SS_LAST_CONNECTED (#PCDATA) -->
        <!-- ELEMENT FDCC_ENABLED (#PCDATA) -->
        <!-- ELEMENT USER_LIST (USER_ACCOUNT*) -->
            <!-- ELEMENT USER_ACCOUNT (ID, NAME) -->
        <!-- ELEMENT UPDATED (#PCDATA) -->
        <!-- ELEMENT COMMENTS (#PCDATA) -->
        <!-- ELEMENT RUNNING_SCANS (SCAN+) -->
            <!-- ELEMENT SCAN (ID, TITLE, REF, TYPE, SCAN_DATE) -->
                <!-- ELEMENT TITLE (#PCDATA) -->
                <!-- ELEMENT REF (#PCDATA) -->
                <!-- ELEMENT TYPE (#PCDATA) -->
                <!-- ELEMENT SCAN_DATE (#PCDATA) -->
            <!-- ELEMENT MAX_CAPACITY_UNITS (#PCDATA) -->

        <!-- ELEMENT LICENSE_INFO (QVSA_LICENSES_COUNT, QVSA_LICENSES_USED) -->
            <!-- ELEMENT QVSA_LICENSES_COUNT (#PCDATA) -->
            <!-- ELEMENT QVSA_LICENSES_USED (#PCDATA) -->

<!-- EOF -->

```

**XPaths for Scanner Appliance List Output**

This section describes the XPaths for the scanner appliance list output.

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT	(REQUEST?,RESPONSE)
/APPLIANCE_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/APPLIANCE_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/APPLIANCE_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/APPLIANCE_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA)



## XPath

### element specifications / notes

An input parameter name. (This element appears only when the API request includes the parameter **echo\_request=1**.)

/APPLIANCE\_LIST\_OUTPUT/REQUEST/PARAM\_LIST/PARAM/VALUE (#PCDATA)

An input parameter value. This element appears only when the API request includes the parameter **echo\_request=1**.

/APPLIANCE\_LIST\_OUTPUT/REQUEST/POST\_DATA (#PCDATA)

The POST data, if any. (This element appears only when the API request includes the parameter **echo\_request=1**.)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE

(DATETIME, (APPLIANCE\_LIST?, LICENSE\_INFO?))

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/DATETIME (#PCDATA)

The date and time of the Qualys response.

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST (APPLIANCE+)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE

(ID, NAME, SOFTWARE\_VERSION, RUNNING\_SLICES\_COUNT, RUNNING\_SCAN\_COUNT, STATUS, CMD\_ONLY\_START?, MODEL\_NUMBER?, TYPE?, SERIAL\_NUMBER?, ACTIVATION\_CODE?, INTERFACE\_SETTINGS\*, PROXY\_SETTINGS?, IS\_CLOUD\_DEPLOYED?, CLOUD\_INFO?, VLANS?, STATIC\_ROUTES?, ML\_LATEST?, ML\_VERSION?, VULNSIGS\_LATEST?, VULNSIGS\_VERSION?, ASSET\_GROUP\_COUNT?, ASSET\_GROUP\_LIST?, ASSET\_TAGS\_LIST?, LAST\_UPDATED\_DATE?, POLLING\_INTERVAL?, USER\_LOGIN?, HEARTBEATS\_MISSED?, SS\_CONNECTION?, SS\_LAST\_CONNECTED?, FDCC\_ENABLED?, USER\_LIST?, UPDATED?, COMMENTS?, RUNNING\_SCANS?, MAX\_CAPACITY\_UNITS?)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/ID (#PCDATA)

The scanner appliance ID.

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/NAME (#PCDATA)

The friendly name of the scanner appliance.

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/SOFTWARE\_VERSION (#PCDATA)

The scanner appliance system software, which is installed on the appliance itself.

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/RUNNING\_SLICES\_COUNT

(#PCDATA)

The number of slices running on the appliance. A slice represents a portion of work being performed for a scan. A value of "0" indicates that the appliance is not busy because it is not working on a slice (it's available for a new scan). Any other value indicates that the appliance is busy.

Keep this in mind - When you distribute a scan to multiple appliances, then one or more appliances may finish their portion of the scan job while other appliances are still working on the scan. This means the scan status is Running but appliances may be available.

<b>XPath</b>	<b>element specifications / notes</b>
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCAN_COUNT (#PCDATA)	The number of scans currently running on the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATUS (#PCDATA)	The scanner appliance heartbeat check status. “Online” indicates the appliance did not miss the most recent heartbeat check. “Offline” indicates the appliance missed one or more heartbeat checks because it did not contact the Security Operations Center. (Heartbeat checks occur every 4 hours.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CMD_ONLY_START (#PCDATA)	The date/time an appliance enters into CMD Only (command only) mode. This mode may be entered for various reasons, such as when a session expires.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/MODEL_NUMBER (#PCDATA)	The model number of the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/TYPE (#PCDATA)	The type of the scanner appliance: physical or virtual or offline. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/SERIAL_NUMBER (#PCDATA)	The serial number (ID) of the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ACTIVATION_CODE (#PCDATA)	The activation code provisioned for the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS (SETTING?, INTERFACE, IP_ADDRESS, NETMASK, GATEWAY, LEASE, IPV6_ADDRESS?, SPEED, DUPLEX, DNS)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/SETTING (#PCDATA)	A flag indicating whether the WAN interface is disabled. When the WAN interface is disabled, the value Disabled appears. When enabled, this element is not displayed. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/INTERFACE (#PCDATA)	The network interface: “lan” or “wan”. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/IP_ADDRESS (#PCDATA)	The LAN or WAN IP address. (Appears when <b>output_mode=full</b> . is specified in API request.)

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/NETMASK (#PCDATA)	The netmask value for the LAN or WAN interface.(Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/GATEWAY (#PCDATA)	The gateway IP address for the LAN or WAN interface. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/LEASE (#PCDATA)	The lease for the LAN or WAN interface: Static for a static IP address or Dynamic for DHCP. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/IPV6_ADDRESS (#PCDATA)	The LAN Pv6 address, if any. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/SPEED (#PCDATA)	The speed of the LAN or WAN interface. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/DUPLEX (#PCDATA)	The duplex setting for the LAN or WAN port links: Full Duplex, Half Duplex, or Unknown. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/DNS (DOMAIN?, PRIMARY, SECONDARY)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/DNS/DOMAIN (#PCDATA)	The domain name of the DNS server. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/DNS/PRIMARY (#PCDATA)	The IP address of the primary DNS server. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/DNS/SECONDARY (#PCDATA)	The IP address of the secondary DNS server. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/PROXY_SETTINGS (SETTING, PROXY*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/PROXY_SETTINGS/PROXY (PROTOCOL?, IP_ADDRESS?, HOSTNAME?, PORT, USER)	

**XPath**

**element specifications / notes**

These elements appear as applicable only when the API request includes the parameter **output\_mode=full**.

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/IS\_CLOUD\_DEPLOYED (#PCDATA)

Set to 1 when virtual appliance is deployed on cloud platform. (Appears when **output\_mode=full** is specified in API request.)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO

(PLATFORM\_PROVIDER, EC2\_INFO?, GCE\_INFO?, AZURE\_INFO?)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/  
PLATFORM\_PROVIDER (#PCDATA)

Platform provider, one of: ec2, azure, gce. (Appears when **output\_mode=full** is specified in API request.)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO

(INSTANCE\_ID, INSTANCE\_TYPE, KERNEL\_ID?, AMI\_ID, ACCOUNT\_ID, INSTANCE\_REGION, INSTANCE\_AVAILABILITY\_ZONE, INSTANCE\_ZONE\_TYPE, INSTANCE\_VPC\_ID?, INSTANCE\_SUBNET\_ID?, IP\_ADDRESS\_PRIVATE?, HOSTNAME\_PRIVATE?, SECURITY\_GROUPS?, API\_PROXY\_SETTINGS)

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
INSTANCE\_ID (#PCDATA)

EC2 instance ID. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
INSTANCE\_TYPE (#PCDATA)

EC2 instance type. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
KERNEL\_ID (#PCDATA)

EC2 kernel ID. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
AMI\_ID (#PCDATA)

EC2 AMI ID. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
ACCOUNT\_ID (#PCDATA)

EC2 account ID. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
INSTANCE\_REGION (#PCDATA)

EC2 instance region. (Appears when **output\_mode=full** is specified in API request).

/APPLIANCE\_LIST\_OUTPUT/RESPONSE/APPLIANCE\_LIST/APPLIANCE/CLOUD\_INFO/EC2\_INFO/  
INSTANCE\_AVAILABILITY\_ZONE (#PCDATA)

EC2 instance availability zone. (Appears when **output\_mode=full** is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/INSTANCE_ZONE_TYPE (#PCDATA)	EC2 instance zone type. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/INSTANCE_VPC_ID (#PCDATA)	EC2 instance VPC ID. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/INSTANCE_SUBNET_ID (#PCDATA)	EC2 instance subnet ID. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/IP_ADDRESS_PRIVATE (#PCDATA)	EC2 instance private IP address. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/HOSTNAME_PRIVATE (#PCDATA)	EC2 instance private hostname. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/SECURITY_GROUPS (SECURITY_GROUP_IDS?, SECURITY_GROUP_NAMES?)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/SECURITY_GROUPS /SECURITY_GROUP_IDS (#PCDATA)	EC2 instance security group IDs. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/SECURITY_GROUPS /SECURITY_GROUP_NAMES (#PCDATA)	EC2 instance security group names. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/API_PROXY_SETTINGS (SETTING, PROXY*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/API_PROXY_SETTINGS/SETTING (#PCDATA)	“Enabled” when proxy settings are enabled for EC2 instance. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/API_PROXY_SETTINGS/PROXY	(PROTOCOL?, IP_ADDRESS?, HOSTNAME?, PORT, USER)  Elements appear as applicable only when <b>output_mode=full</b> is specified in API request.

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO	(INSTANCE_ID, MACHINE_TYPE, PROJECT_ID, PROJECT_NAME, PREEMPTIBLE, INSTANCE_ZONE, IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?, IP_ADDRESS_PUBLIC?, INSTANCE_NETWORK, GCE_INSTANCE_TAGS)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/INSTANCE_ID (#PCDATA)	GCE instance ID. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/MACHINE_TYPE (#PCDATA)	GCE instance machine type. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/PROJECT_ID (#PCDATA)	GCE instance project ID. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/PROJECT_NAME (#PCDATA)	GCE instance project name. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/PREEMPTIBLE (#PCDATA)	GCE instance preemptible flag, set to TRUE or FALSE. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/INSTANCE_ZONE (#PCDATA)	GCE instance zone (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/IP_ADDRESS_PRIVATE (#PCDATA)	GCE instance private IP address. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/HOSTNAME_PRIVATE (#PCDATA)	GCE instance private hostname. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/IP_ADDRESS_PUBLIC (#PCDATA)	GCE instance public IP address. (Appears when <b>output_mode=full</b> is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/INSTANCE_NETWORK (#PCDATA)	GCE instance network, set to default or a network name. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/GCE_INSTANCE_TAGS (GCE_INSTANCE_TAG*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/GCE_INSTANCE_TAGS/GCE_INSTANCE_TAG (TAG_ID)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/GCE_INSTANCE_TAGS/GCE_INSTANCE_TAG/TAG_ID (#PCDATA)	GCE instance tag. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO (INSTANCE_ID, USER_NAME, INSTANCE_LOCATION, DEPLOYMENT_MODE, IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/INSTANCE_ID (#PCDATA)	Azure instance ID. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/USER_NAME, (#PCDATA)	Azure user name. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/INSTANCE_LOCATION (#PCDATA)	Azure instance location. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/DEPLOYMENT_MODE (#PCDATA)	Azure instance deployment mode. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/IP_ADDRESS_PRIVATE (#PCDATA)	Azure instance private IP address. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/HOSTNAME_PRIVATE (#PCDATA)	Azure instance private hostname. (Appears when <b>output_mode=full</b> is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS (SETTING, VLAN*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/SETTING (#PCDATA)	A flag indicating whether VLANS are enabled: "enabled" or "disabled". (Appears when <b>output_mode=full</b> is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN (ID, NAME, IP_ADDRESS, NETMASK)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/ ID (#PCDATA)	A VLAN ID. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/ NAME	A VLAN name. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/ IP_ADDRESS (#PCDATA)	A valid IP address for a VLAN. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/ NETMASK (#PCDATA)	A valid netmask for a VLAN. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES (ROUTE*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE (NAME, IP_ADDRESS, NETMASK, GATEWAY)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/ NAME (#PCDATA)	A static route name. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/ IP_ADRESS (#PCDATA)	A target network for a static route. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/ NETMASK (#PCDATA)	A netmask for a static route. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/ GATEWAY (#PCDATA)	A gateway IP address for a static route. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ML_LATEST (#PCDATA)	The latest scanning engine version available. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ML_VERSION (#PCDATA)	The scanning engine version currently installed on the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
attribute: updated	“yes” indicates the appliance is updated with the latest version.



XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VULNSIGS_LATEST (#PCDATA)	The latest vulnerability signatures version available. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VULNSIGS_VERSION (#PCDATA)	The vulnerability signatures version currently installed on the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
attribute: updated	“yes” indicates the appliance is updated with the latest version.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_GROUP_COUNT (#PCDATA)	The number of asset groups that the scanner appliance belongs to. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_GROUP_LIST (ASSET_GROUP*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_GROUP_LIST/ASSET_GROUP (ID, NAME)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_GROUP_LIST/ASSET_GROUP/ID (#PCDATA)	The ID of an asset group that the appliance belongs to. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_GROUP_LIST/ASSET_GROUP/NAME (#PCDATA)	The name of an asset group that the appliance belongs to. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_TAGS_LIST (ASSET_TAG*)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_TAGS_LIST/ASSET_TAG (UUID, NAME)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_TAGS_LIST/ASSET_TAG/UUID (#PCDATA)	The asset tag UUID. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ASSET_TAGS_LIST/ASSET_TAG/NAME (#PCDATA)	The asset tag name. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/LAST_UPDATED_DATE (#PCDATA)	The last date and time when the scanner appliance received a software update. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/POLLING_INTERVAL (#PCDATA)	The polling interval defined for the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/USER_LOGIN (#PCDATA)	The user login. (Appears when <b>output_mode=full</b> . is specified in API request.)

<b>XPath</b>	<b>element specifications / notes</b>
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/HEARTBEATS_MISSED (#PCDATA)	The number of heartbeat checks missed. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/SS_CONNECTION (#PCDATA)	The new scanner services status: connected or not connected. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/SS_LAST_CONNECTED (#PCDATA)	The last date/time when new scanner services connected. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/FDCC_ENABLED (#PCDATA)	A flag indicating whether the FDCC module is enabled on the appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/UPDATED (#PCDATA)	A flag indicating whether the appliance is updated with the latest scanning engine software and vulnerability signatures software: “yes” or “no”. (Appears when <b>output_mode=full</b> . is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS (SCAN+)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN (ID, TITLE, REF, TYPE, SCAN_DATE)	
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN/ID (#PCDATA)	The scan ID of a currently scan running on the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN/TITLE (#PCDATA)	The title of a currently scan running on the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN/REF (#PCDATA)	The scan reference ID for a currently scan running on the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN/TYPE (#PCDATA)	The scan type of a scan currently running on the scanner appliance. The scan type will be one of: Vulnerability Scan, Compliance Scan, Web Application Scan, FDCC Scan, or Map.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/RUNNING_SCANS/SCAN/SCAN_DATE (#PCDATA)	The date and time when the currently running scan was launched.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/MAX_CAPACITY_UNITS (#PCDATA)	The percentage of capacity available for the scanner appliance. (Appears when <b>output_mode=full</b> . is specified in API request.)

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/LICENSE_INFO	(QVSA_LICENSES_COUNT, QVSA_LICENSES_USED)
/APPLIANCE_LIST_OUTPUT/RESPONSE/LICENSE_INFO /QVSA_LICENSES_COUNT (#PCDATA)	The number of virtual scanner licenses available in your account.
/APPLIANCE_LIST_OUTPUT/RESPONSE/LICENSE_INFO /QVSA_LICENSES_USED (#PCDATA)	The number of virtual scanner licenses that have been used.

# Scanner Appliance Create Output

The Scanner Appliance List API v2 (/api/2.0/fo/appliance/ with action=create) returns XML output using the “appliance\_create\_output.dtd”.

DTD: https://<basurl>/api/2.0/fo/appliance/appliance\_create\_output.dtd

## DTD for Scanner Appliance Create Output

A recent DTD for the scanner appliance create output (appliance\_create\_output.dtd) is shown below.

```

<!-- QUALYS APPLIANCE_CREATE_OUTPUT DTD -->
<!ELEMENT APPLIANCE_CREATE_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, APPLIANCE)>

<!ELEMENT APPLIANCE (ID, FRIENDLY_NAME, ACTIVATION_CODE,
                    REMAINING_QVSA_LICENSES)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT FRIENDLY_NAME (#PCDATA)>
<!ELEMENT ACTIVATION_CODE (#PCDATA)>
<!ELEMENT REMAINING_QVSA_LICENSES (#PCDATA)>

```

## XPaths for Scanner Appliance Create Output

This section describes the XPathS for the scanner appliance create output.

XPath	element specifications / notes
/APPLIANCE_CREATE_OUTPUT (REQUEST?,RESPONSE)	
/APPLIANCE_CREATE_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/APPLIANCE_CREATE_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the API request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )

XPath	element specifications / notes
/APPLIANCE_CREATE_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_CREATE_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_CREATE_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/APPLIANCE_CREATE_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/APPLIANCE_CREATE_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_CREATE_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value. This element appears only when the API request includes the parameter <b>echo_request=1.</b>
/APPLIANCE_CREATE_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. (This element appears only when the API request includes the parameter <b>echo_request=1.</b> )
/APPLIANCE_CREATE_OUTPUT/RESPONSE (DATETIME, APPLIANCE)	
/APPLIANCE_CREATE_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/APPLIANCE_CREATE_OUTPUT/RESPONSE/APPLIANCE	(ID, FRIENDLY_NAME, ACTIVATION_CODE, REMAINING_QVSA_LICENSES)
/APPLIANCE_CREATE_OUTPUT/RESPONSE/APPLIANCE/ID (#PCDATA)	The scanner appliance ID.
/APPLIANCE_CREATE_OUTPUT/RESPONSE/APPLIANCE/FRIENDLY_NAME (#PCDATA)	The friendly name of the scanner appliance.
/APPLIANCE_CREATE_OUTPUT/RESPONSE/APPLIANCE/ACTIVATION_CODE (#PCDATA)	The activation code for the scanner appliance.
/APPLIANCE_CREATE_OUTPUT/RESPONSE/APPLIANCE/REMAINING_QVSA_LICENSES (#PCDATA)	The number of remaining virtual scanner license in your account.

## Static Search List Output

The static search list XML output is returned from a static search list API v2 request.

DTD: [https://<basurl>/api/2.0/fo/qid/search\\_list/static/static\\_list\\_output.dtd](https://<basurl>/api/2.0/fo/qid/search_list/static/static_list_output.dtd)

### DTD for Static Search List Output

A recent DTD for is below.

```
<!-- QUALYS STATIC_SEARCH_LIST_OUTPUT DTD -->

<!ELEMENT STATIC_SEARCH_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, STATIC_LISTS?)>
<!ELEMENT STATIC_LISTS (STATIC_LIST+)>
<!ELEMENT STATIC_LIST (ID, TITLE, GLOBAL, OWNER, CREATED?, MODIFIED_BY?,
    MODIFIED?, QIDS?, OPTION_PROFILES?,
    REPORT_TEMPLATES?, REMEDIATION_POLICIES?,
    DISTRIBUTION_GROUPS?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT GLOBAL (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT CREATED (#PCDATA)>
<!ELEMENT MODIFIED_BY (#PCDATA)>
<!ELEMENT MODIFIED (#PCDATA)>
<!ELEMENT QIDS (QID+)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE+)>
<!ELEMENT OPTION_PROFILE (ID, TITLE)>
<!ELEMENT REPORT_TEMPLATES (REPORT_TEMPLATE+)>
<!ELEMENT REPORT_TEMPLATE (ID, TITLE)>
<!ELEMENT REMEDIATION_POLICIES (REMEDIATION_POLICY+)>
<!ELEMENT REMEDIATION_POLICY (ID, TITLE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (NAME)>
```

```
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!-- EOF -->
```

## XPaths for Static Search List Output

This section describes the XPaths for static search list output.

XPath	element specifications / notes
/STATIC_SEARCH_LIST_OUTPUT (REQUEST?, RESPONSE)	
/STATIC_SEARCH_LIST_OUTPUT/REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)	
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/STATIC_SEARCH_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE (DATETIME, STATIC_LISTS?)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS (STATIC_LIST+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST (ID, TITLE, GLOBAL, OWNER, CREATED?, MODIFIED_BY?, MODIFIED?, QIDS?, OPTION_PROFILES?, REPORT_TEMPLATES?, REMEDIATION_POLICIES?, DISTRIBUTION_GROUPS?, COMMENTS?)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/ID (#PCDATA)	Search list ID.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/TITLE (#PCDATA)	Search list title.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/OWNER (#PCDATA)	Owner of the search list.

<b>XPath</b>	<b>element specifications / notes</b>
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/GLOBAL (#PCDATA)	Set to Yes for a global search list, or No.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/CREATED (#PCDATA)	Search list creation date.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/MODIFIED_BY (#PCDATA)	User who modified the search list.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/MODIFIED (#PCDATA)	Date the search list was modified.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/QIDS (QID+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/QID (QID)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/QIDS/QID (#PCDATA)	QID included in the search list.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/OPTION_PROFILES (OPTION_PROFILE+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/OPTION_PROFILES/OPTION_PROFILE (ID, TITLE)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/OPTION_PROFILES/OPTION_PROFILE/ID (#PCDATA)	ID of the option profile where the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/OPTION_PROFILES/OPTION_PROFILE/TITLE (#PCDATA)	Title of an option profile title where the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REPORT_TEMPLATES (REPORT_TEMPLATE+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REPORT_TEMPLATES/REPORT_TEMPLATE (ID, TITLE)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REPORT_TEMPLATES/REPORT_TEMPLATE/ID (#PCDATA)	ID of a report template where the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REPORT_TEMPLATES/REPORT_TEMPLATE/TITLE (#PCDATA)	Title of a report template where of the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REMEDIATION_POLICIES (REMEDIATION_POLICY+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REMEDIATION_POLICIES/REMEDIATION_POLICY (ID, TITLE)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REMEDIATION_POLICIES/REMEDIATION_POLICY/ID (#PCDATA)	ID of a remediation policy where the search list is defined.



XPath	element specifications / notes
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/REMEDIATION_POLICIES/REMEDIATION_POLICY/TITLE (#PCDATA)	Title of a remediation policy where the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/DISTRIBUTION_GROUPS/DISTRIBUTION_GROUP (NAME)	
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/DISTRIBUTION_GROUPS/DISTRIBUTION_GROUP/NAME (#PCDATA)	Name of a distribution group where the search list is defined.
/STATIC_SEARCH_LIST_OUTPUT/RESPONSE/STATIC_LISTS/STATIC_LIST/COMMENTS (#PCDATA)	User defined comments.

## Dynamic Search List Output

The dynamic search list XML output is returned from a dynamic search list API v2 request.

DTD:

[https://<baseurl>/api/2.0/fo/qid/search\\_list/dynamic/dynamic\\_list\\_output.dtd](https://<baseurl>/api/2.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd)

### DTD for Dynamic Search List Output

A recent DTD for is below.

```
<!-- QUALYS DYNAMIC_SEARCH_LIST_OUTPUT DTD -->

<!ELEMENT DYNAMIC_SEARCH_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, DYNAMIC_LISTS?)>
<!ELEMENT DYNAMIC_LISTS (DYNAMIC_LIST+)>
<!ELEMENT DYNAMIC_LIST (ID, TITLE, GLOBAL, OWNER, CREATED?, MODIFIED_BY?,
                        MODIFIED?, QIDS?, CRITERIA, OPTION_PROFILES?,
                        REPORT_TEMPLATES?, REMEDIATION_POLICIES?,
                        DISTRIBUTION_GROUPS?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT GLOBAL (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT CREATED (#PCDATA)>
<!ELEMENT MODIFIED_BY (#PCDATA)>
<!ELEMENT MODIFIED (#PCDATA)>
<!ELEMENT QIDS (QID+)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT CRITERIA (VULNERABILITY_TITLE?, DISCOVERY_METHOD?,
                    AUTHENTICATION_TYPE?, USER_CONFIGURATION?, CATEGORY?,
                    CONFIRMED_SEVERITY?, POTENTIAL_SEVERITY?,
                    INFORMATION_SEVERITY?, VENDOR?, PRODUCT?, CVSS_BASE_SCORE?,
                    CVSS_TEMPORAL_SCORE?, CVSS3_BASE_SCORE?, CVSS3_TEMPORAL_SCORE?,
```

```

CVSS_ACCESS_VECTOR?, PATCH_AVAILABLE?, VIRTUAL_PATCH_AVAILABLE?,
CVE_ID?, EXPLOITABILITY?, ASSOCIATED_MALWARE?, VENDOR_REFERENCE?,
BUGTRAQ_ID?, VULNERABILITY_DETAILS?, SUPPORTED_MODULES?,
COMPLIANCE_DETAILS?, COMPLIANCE_TYPE?, QUALYS_TOP_20?, OTHER?,
NETWORK_ACCESS?, PROVIDER?, CVSS_BASE_SCORE_OPERAND?,
CVSS_TEMPORAL_SCORE_OPERAND?, CVSS3_BASE_SCORE_OPERAND?,
CVSS3_TEMPORAL_SCORE_OPERAND?, USER_MODIFIED?, PUBLISHED?,
SERVICE_MODIFIED?, CPE?)>
<!ELEMENT VULNERABILITY_TITLE (#PCDATA)>
<!ELEMENT DISCOVERY_METHOD (#PCDATA)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT USER_CONFIGURATION (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT CONFIRMED_SEVERITY (#PCDATA)>
<!ELEMENT POTENTIAL_SEVERITY (#PCDATA)>
<!ELEMENT INFORMATION_SEVERITY (#PCDATA)>
<!ELEMENT VENDOR (#PCDATA)>
<!ELEMENT PRODUCT (#PCDATA)>
<!ELEMENT CVSS_BASE_SCORE (#PCDATA)>
<!ELEMENT CVSS_TEMPORAL_SCORE (#PCDATA)>
<!ELEMENT CVSS_ACCESS_VECTOR (#PCDATA)>
<!ELEMENT PATCH_AVAILABLE (#PCDATA)>
<!ELEMENT VIRTUAL_PATCH_AVAILABLE (#PCDATA)>
<!ELEMENT CVE_ID (#PCDATA)>
<!ELEMENT EXPLOITABILITY (#PCDATA)>
<!ELEMENT ASSOCIATED_MALWARE (#PCDATA)>
<!ELEMENT VENDOR_REFERENCE (#PCDATA)>
<!ELEMENT BUGTRAQ_ID (#PCDATA)>
<!ELEMENT VULNERABILITY_DETAILS (#PCDATA)>
<!ELEMENT SUPPORTED_MODULES (#PCDATA)>
<!ELEMENT COMPLIANCE_DETAILS (#PCDATA)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT QUALYS_TOP_20 (#PCDATA)>
<!ELEMENT OTHER (#PCDATA)>
<!ELEMENT NETWORK_ACCESS (#PCDATA)>
<!ELEMENT PROVIDER (#PCDATA)>
<!ELEMENT CVSS_BASE_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS_TEMPORAL_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS3_BASE_SCORE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL_SCORE (#PCDATA)>
<!ELEMENT CVSS3_BASE_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL_SCORE_OPERAND (#PCDATA)>
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE+)>
<!ELEMENT OPTION_PROFILE (ID, TITLE)>
<!ELEMENT REPORT_TEMPLATES (REPORT_TEMPLATE+)>
<!ELEMENT REPORT_TEMPLATE (ID, TITLE)>
<!ELEMENT REMEDIATION_POLICIES (REMEDIATION_POLICY+)>
<!ELEMENT REMEDIATION_POLICY (ID, TITLE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>

```

```
<!ELEMENT DISTRIBUTION_GROUP (NAME)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT USER_MODIFIED (#PCDATA)>
<!ELEMENT PUBLISHED (#PCDATA)>
<!ELEMENT SERVICE_MODIFIED (#PCDATA)>
<!ELEMENT CPE (#PCDATA)>
<!-- EOF -->
```

**XPaths for Dynamic Search List Output**

This section describes the XPaths for dynamic search list output.

XPath	element specifications / notes
/DYNAMIC_SEARCH_LIST_OUTPUT (REQUEST?, RESPONSE)	
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/DYNAMIC_SEARCH_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE (DATETIME, DYNAMIC_LISTS?)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS (DYNAMIC_LIST+)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST	(ID, TITLE, GLOBAL, OWNER, CREATED?, MODIFIED_BY?, MODIFIED?, QIDS?, CRITERIA, OPTION_PROFILES?, REPORT_TEMPLATES?, REMEDIATION_POLICIES?, DISTRIBUTION_GROUPS?, COMMENTS?)
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/ID (#PCDATA)	Search list ID.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/TITLE (#PCDATA)

Search list title.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/GLOBAL (#PCDATA)

Set to Yes for a global search list, or No.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/OWNER (#PCDATA)

Owner of the search list.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CREATED (#PCDATA)

Search list creation date.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/MODIFIED\_BY  
(#PCDATA)

User who modified the search list.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/MODIFIED (#PCDATA)

Date the search list was modified.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/QIDS (QID+)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/QID (QID)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/QIDS/QID (#PCDATA)

QID included in the search list.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA

(VULNERABILITY\_TITLE?, DISCOVERY\_METHOD?,  
AUTHENTICATION\_TYPE?, USER\_CONFIGURATION?, CATEGORY?,  
CONFIRMED\_SEVERITY?, POTENTIAL\_SEVERITY?,  
INFORMATION\_SEVERITY?, VENDOR?, PRODUCT?, CVSS\_BASE\_SCORE?,  
CVSS\_TEMPORAL\_SCORE?, CVSS3\_BASE\_SCORE?,  
CVSS3\_TEMPORAL\_SCORE?, CVSS\_ACCESS\_VECTOR?,  
PATCH\_AVAILABLE?, VIRTUAL\_PATCH\_AVAILABLE?, CVE\_ID?,  
EXPLOITABILITY?, ASSOCIATED\_MALWARE?, VENDOR\_REFERENCE?,  
BUGTRAQ\_ID?, VULNERABILITY\_DETAILS?, SUPPORTED\_MODULES?,  
COMPLIANCE\_DETAILS?, COMPLIANCE\_TYPE?, QUALYS\_TOP\_20?,  
OTHER?, NETWORK\_ACCESS?, PROVIDER?,  
CVSS\_BASE\_SCORE\_OPERAND?, CVSS\_TEMPORAL\_SCORE\_OPERAND?,  
CVSS3\_BASE\_SCORE\_OPERAND?, CVSS3\_TEMPORAL\_SCORE\_OPERAND?,  
USER\_MODIFIED?, PUBLISHED?, SERVICE\_MODIFIED?, CPE?)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
VULNERABILITY\_TITLE (#PCDATA)

Vulnerability title.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
DISCOVERY\_METHOD (#PCDATA)

Discovery method.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
AUTHENTICATION\_TYPE (#PCDATA)

Authentication type.

## Appendix F — Scan Configuration XML

### Dynamic Search List Output

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
USER\_CONFIGURATION (#PCDATA)

User configuration.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/CATEGORY  
(#PCDATA)

Vulnerability category.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CONFIRMED\_SEVERITY (#PCDATA)

One or more severities of confirmed vulnerabilities.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
POTENTIAL\_SEVERITY (#PCDATA)

One or more severities of potential vulnerabilities.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
INFORMATION\_SEVERITY (#PCDATA)

One or more severities of information gathered.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/VENDOR  
(#PCDATA)

One or more vendor IDs.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/PRODUCT  
(#PCDATA)

One or more vendor product names.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CVSS\_BASE\_SCORE (#PCDATA)

CVSS2 base score value.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CVSS\_TEMPORAL\_SCORE (#PCDATA)

CVSS2 temporal score value.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CVSS3\_BASE\_SCORE (#PCDATA)

CVSS3 base score value.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CVSS3\_TEMPORAL\_SCORE (#PCDATA)

CVSS3 temporal score value.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
CVSS\_ACCESS\_VECTOR (#PCDATA)

Value of CVSS access vector.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
PATCH\_AVAILABLE (#PCDATA)

Set to Yes when vulnerabilities with patches are included in criteria.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
VIRTUAL\_PATCH\_AVAILABLE (#PCDATA)

Set to Yes when vulnerabilities with Trend Micro virtual patches are included in criteria.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/CVE\_ID  
(#PCDATA)

One or more CVE IDs.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
EXPLOITABILITY (#PCDATA)

One or more vendors with exploitability info.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
ASSOCIATED\_MALWARE (#PCDATA)

One or more vendors with malware info.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
VENDOR\_REFERENCE (#PCDATA)

One or more vendor references.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
BUGTRAQ\_ID (#PCDATA)

Bugtraq ID number assigned to vulnerabilities.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
VULNERABILITY\_DETAILS (#PCDATA)

A string matching vulnerability details.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
SUPPORTED\_MODULES (#PCDATA)

One or more Qualys modules that can be used to detect the vulnerability.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
COMPLIANCE\_DETAILS (#PCDATA)

A string matching compliance details.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
COMPLIANCE\_TYPE (#PCDATA)

One or more compliance types.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
QUALYS\_TOP\_20 (#PCDATA)

One or more Qualys top lists: Internal\_10, External\_10.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/OTHER  
(#PCDATA)

Not exploitable due to configuration listed (i.e. vulnerabilities on non running services).

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/CRITERIA/  
NETWORK\_ACCESS (#PCDATA)

NAC/NAM vulnerabilities are set when this element is present.

/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ PROVIDER (#PCDATA)	Provider of the vulnerability if not Qualys.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ CVSS_BASE_SCORE_OPERAND (#PCDATA)	CVSS2 base score operand. 1 for the greater than equal operand, or 2 for the less than operand.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ CVSS_TEMPORAL_SCORE_OPERAND (#PCDATA)	CVSS2 temporal score operand. 1 for the greater than equal operand, or 2 for the less than operand.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ CVSS3_BASE_SCORE_OPERAND (#PCDATA)	CVSS3 base score operand. 1 for the greater than equal operand, or 2 for the less than operand.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ CVSS3_TEMPORAL_SCORE_OPERAND (#PCDATA)	CVSS3 temporal score operand. 1 for the greater than equal operand, or 2 for the less than operand.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ USER_MODIFIED (#PCDATA)	Date user modified the list.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ PUBLISHED (#PCDATA)	Date the list was published.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ SERVICE_MODIFIED (#PCDATA)	Date the service modified the list.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/CRITERIA/ CPE (#PCDATA)	One or more CPE values: Operating System, Application, Hardware.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/OPTION_PROFILES (OPTION_PROFILE+)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/OPTION_PROFILES/ OPTION_PROFILE (ID, TITLE)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/OPTION_PROFILES/ OPTION_PROFILE/ID (#PCDATA)	ID of the option profile where the search list. is defined.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/OPTION_PROFILES/ OPTION_PROFILE/TITLE (#PCDATA)	Title of the option profile title where the search list is defined.



/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/REPORT\_TEMPLATES  
(REPORT\_TEMPLATE+)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/REPORT\_TEMPLATES/  
REPORT\_TEMPLATE (ID, TITLE)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/REPORT\_TEMPLATES/  
REPORT\_TEMPLATE/ID (#PCDATA)

ID of the report template where the search list is defined.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/REPORT\_TEMPLATES/  
REPORT\_TEMPLATE/TITLE (#PCDATA)

Title of a report template where the search list is defined.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
REMEDIATION\_POLICIES (REMEDIATION\_POLICY+)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
REMEDIATION\_POLICIES/REMEDIATION\_POLICY (ID, TITLE)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
REMEDIATION\_POLICIES/REMEDIATION\_POLICY/ID (#PCDATA)

ID of a remediation policy where the search list is defined.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
REMEDIATION\_POLICIES/REMEDIATION\_POLICY/TITLE (#PCDATA)

Title of a remediation policy where the search list is defined.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
DISTRIBUTION\_GROUPS (DISTRIBUTION\_GROUP+)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
DISTRIBUTION\_GROUPS/ DISTRIBUTION\_GROUP (NAME)

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/  
DISTRIBUTION\_GROUPS/DISTRIBUTION\_GROUP/NAME (#PCDATA)

Name of distribution group where the search list is defined.

/DYNAMIC\_SEARCH\_LIST\_OUTPUT/RESPONSE/DYNAMIC\_LISTS/DYNAMIC\_LIST/COMMENTS  
(#PCDATA)

User defined comments.

## Option Profile XML

This appendix describes the XML output returned from API V2 requests for the Option Profile API functions.

### Option Profile Output

The option profile XML is returned from export option profile API call.

DTD:

[https://<baseurl>/api/2.0/fo/subscription/option\\_profile/option\\_profile\\_info.dtd](https://<baseurl>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd)

### DTD for Option Profile

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID,
SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?,
IS_OFFLINE_SYNCABLE?, UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_TYPE (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT UNIT_ID (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT IS_DEFAULT (#PCDATA)>
<!ELEMENT IS_GLOBAL (#PCDATA)>
<!ELEMENT IS_OFFLINE_SYNCABLE (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>

<!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?,
```

```
PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?,
PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?,
ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, LITE_OS_SCAN?,
CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?, SCAN_RESTRICTION?,
FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?)>

<!ELEMENT PORTS (TCP_PORTS?, UDP_PORTS?, AUTHORITATIVE_OPTION?,
(STANDARD_SCAN|TARGETED_SCAN)?)>
<!ELEMENT TCP_PORTS (TCP_PORTS_TYPE?, TCP_PORTS_STANDARD_SCAN?,
TCP_PORTS_ADDITIONAL?, THREE_WAY_HANDSHAKE?, STANDARD_SCAN?,
TCP_ADDITIONAL?)>
<!ELEMENT TCP_PORTS_TYPE (#PCDATA)>
<!ELEMENT TCP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT HAS_ADDITIONAL (#PCDATA)>
<!ELEMENT ADDITIONAL_PORTS (#PCDATA)>
<!ELEMENT THREE_WAY_HANDSHAKE (#PCDATA)>

<!ELEMENT UDP_PORTS (UDP_PORTS_TYPE?, UDP_PORTS_STANDARD_SCAN?,
UDP_PORTS_ADDITIONAL?, (STANDARD_SCAN|CUSTOM_PORT)?)>
<!ELEMENT UDP_PORTS_TYPE (#PCDATA)>
<!ELEMENT UDP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>

<!ELEMENT AUTHORITATIVE_OPTION (#PCDATA)>
<!ELEMENT STANDARD_SCAN (#PCDATA)>
<!ELEMENT TARGETED_SCAN (#PCDATA)>

<!ELEMENT SCAN_DEAD_HOSTS (#PCDATA)>

<!ELEMENT CLOSE_VULNERABILITIES (HAS_CLOSE_VULNERABILITIES?,
HOST_NOT_FOUND_ALIVE?)>
<!ELEMENT HAS_CLOSE_VULNERABILITIES (#PCDATA)>
<!ELEMENT HOST_NOT_FOUND_ALIVE (#PCDATA)>

<!ELEMENT PURGE_OLD_HOST_OS_CHANGED (#PCDATA)>

<!ELEMENT PERFORMANCE (PARALLEL_SCALING?, OVERALL_PERFORMANCE,
HOSTS_TO_SCAN, PROCESSES_TO_RUN, PACKET_DELAY,
PORT_SCANNING AND HOST_DISCOVERY, EXTERNAL_SCANNERS_TO_USE?)>
<!ELEMENT PARALLEL_SCALING (#PCDATA)>
<!ELEMENT OVERALL_PERFORMANCE (#PCDATA)>
<!ELEMENT HOSTS_TO_SCAN (EXTERNAL_SCANNERS, SCANNER_APPLIANCES)>
<!ELEMENT EXTERNAL_SCANNERS (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCES (#PCDATA)>
<!ELEMENT PROCESSES_TO_RUN (TOTAL_PROCESSES, HTTP_PROCESSES)>
<!ELEMENT TOTAL_PROCESSES (#PCDATA)>
<!ELEMENT HTTP_PROCESSES (#PCDATA)>
<!ELEMENT PACKET_DELAY (#PCDATA)>
<!ELEMENT PORT_SCANNING_AND_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT EXTERNAL_SCANNERS_TO_USE (#PCDATA)>
```

```
<!ELEMENT LOAD_BALANCER_DETECTION (#PCDATA)>

<!ELEMENT PASSWORD_BRUTE_FORCING (SYSTEM?, CUSTOM_LIST?)>
<!ELEMENT SYSTEM (HAS_SYSTEM?, SYSTEM_LEVEL?)>
<!ELEMENT HAS_SYSTEM (#PCDATA)>
<!ELEMENT SYSTEM_LEVEL (#PCDATA)>

<!ELEMENT CUSTOM_LIST (CUSTOM+)>
<!ELEMENT CUSTOM (ID, TITLE, TYPE?, LOGIN_PASSWORD?)+>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT LOGIN_PASSWORD (#PCDATA)>

<!ELEMENT VULNERABILITY_DETECTION ((COMPLETE|CUSTOM_LIST|RUNTIME),
DETECTION_INCLUDE?, DETECTION_EXCLUDE?)>
<!ELEMENT COMPLETE (#PCDATA)>
<!ELEMENT RUNTIME (#PCDATA)>

<!ELEMENT DETECTION_INCLUDE (BASIC_HOST_INFO_CHECKS, OVAL_CHECKS,
QRDI_CHECKS?)>
<!ELEMENT BASIC_HOST_INFO_CHECKS (#PCDATA)>
<!ELEMENT OVAL_CHECKS (#PCDATA)>
<!ELEMENT QRDI_CHECKS (#PCDATA)>
<!ELEMENT DETECTION_EXCLUDE (CUSTOM_LIST+)>

<!ELEMENT AUTHENTICATION (#PCDATA)>
<!ELEMENT ADDL_CERT_DETECTION (#PCDATA)>

<!ELEMENT DISSOLVABLE_AGENT (DISSOLVABLE_AGENT_ENABLE,
PASSWORD_AUDITING_ENABLE?, WINDOWS_SHARE_ENUMERATION_ENABLE,
WINDOWS_DIRECTORY_SEARCH_ENABLE?)>
<!ELEMENT DISSOLVABLE_AGENT_ENABLE (#PCDATA)>
<!ELEMENT PASSWORD_AUDITING_ENABLE (HAS_PASSWORD_AUDITING_ENABLE?,
CUSTOM_PASSWORD_DICTIONARY?)>
<!ELEMENT HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)>
<!ELEMENT CUSTOM_PASSWORD_DICTIONARY (#PCDATA)>
<!ELEMENT WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)>
<!ELEMENT WINDOWS_DIRECTORY_SEARCH_ENABLE (#PCDATA)>

<!ELEMENT LITE_OS_SCAN (#PCDATA)>
<!ELEMENT CUSTOM_HTTP_HEADER (VALUE?, DEFINITION_KEY?,
DEFINITION_VALUE?)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT DEFINITION_KEY (#PCDATA)>
<!ELEMENT DEFINITION_VALUE (#PCDATA)>

<!ELEMENT HOST_ALIVE_TESTING (#PCDATA)>
```

```

<!ELEMENT SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)>

<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
<!ELEMENT AUTO_UPDATE_EXPECTED_VALUE (#PCDATA)>

<!ELEMENT CONTROL_TYPES (FIM_CONTROLS_ENABLED?, CUSTOM_WMI_QUERY_CHECKS?,
DO_NOT_OVERWRITE_OS?)>
<!ELEMENT FIM_CONTROLS_ENABLED (#PCDATA)>
<!ELEMENT CUSTOM_WMI_QUERY_CHECKS (#PCDATA)>
<!ELEMENT DO_NOT_OVERWRITE_OS (#PCDATA)>

<!ELEMENT MAP (BASIC_INFO_GATHERING_ON, TCP_PORTS?, UDP_PORTS?,
MAP_OPTIONS?, MAP_PERFORMANCE?, MAP_AUTHENTICATION?)>

<!ELEMENT BASIC_INFO_GATHERING_ON (#PCDATA)>
<!ELEMENT TCP_PORTS_STANDARD_SCAN (#PCDATA)>

<!ELEMENT UDP_PORTS_STANDARD_SCAN (#PCDATA)>

<!ELEMENT MAP_OPTIONS (PERFORM_LIVE_HOST_SWEEP?, DISABLE_DNS_TRAFFIC?)>
<!ELEMENT PERFORM_LIVE_HOST_SWEEP (#PCDATA)>
<!ELEMENT DISABLE_DNS_TRAFFIC (#PCDATA)>

<!ELEMENT MAP_PERFORMANCE (OVERALL_PERFORMANCE, MAP_PARALLEL?,
PACKET_DELAY)>
<!ELEMENT MAP_PARALLEL (EXTERNAL_SCANNERS, SCANNER_APPLIANCES,
NETBLOCK_SIZE)>
<!ELEMENT NETBLOCK_SIZE (#PCDATA)>

<!ELEMENT MAP_AUTHENTICATION (#PCDATA)>

<!ELEMENT ADDITIONAL (HOST_DISCOVERY, BLOCK_RESOURCES?, PACKET_OPTIONS?)>
<!ELEMENT HOST_DISCOVERY (TCP_PORTS?, UDP_PORTS?, ICMP?)>

<!ELEMENT TCP_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>

<!ELEMENT CUSTOM_PORT (#PCDATA)>

<!ELEMENT ICMP (#PCDATA)>

<!ELEMENT BLOCK_RESOURCES
((WATCHGUARD_DEFAULT_BLOCKED_PORTS|CUSTOM_PORT_LIST),
(ALL_REGISTERED_IPS|CUSTOM_IP_LIST))>
<!ELEMENT WATCHGUARD_DEFAULT_BLOCKED_PORTS (#PCDATA)>
<!ELEMENT CUSTOM_PORT_LIST (#PCDATA)>
<!ELEMENT ALL_REGISTERED_IPS (#PCDATA)>
<!ELEMENT CUSTOM_IP_LIST (#PCDATA)>

```

```

<!ELEMENT PACKET_OPTIONS ( IGNORE_FIREWALL_GENERATED_TCP_RST?,
IGNORE_ALL_TCP_RST?,  IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK?,
NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY? )>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_ALL_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK (#PCDATA)>
<!ELEMENT NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY (#PCDATA)>

```

**XPath descriptions**

XPath descriptions for the Option Profile DTD (option\_profile\_info.dtd) are below.

XPath	element specifications / notes
/OPTION_PROFILES	(OPTION_PROFILE?)
/OPTION_PROFILES/OPTION_PROFILE	
	(BASIC_INFO, SCAN, MAP?, ADDITIONAL)
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO	
	(ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID, SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?, UPDATE_DATE?)
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/ID (#PCDATA)	
	Option profile ID.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/GROUP_NAME (#PCDATA)	
	Option profile title.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/GROUP_TYPE (#PCDATA)	
	Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile), rv10 (for Qualys Top 10 real time internal and external vulnerabilities, sans20 (for SANS Top 20 profile).
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/USER_ID (#PCDATA)	
	User ID of the option profile owner.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/UNIT_ID (#PCDATA)	
	ID of business unit where option profile is defined.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/SUBSCRIPTION_ID (#PCDATA)	
	ID of subscription where option profile is defined.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/IS_DEFAULT (#PCDATA)	
	1 means the option profile is the default for the subscription, 0 means the option profile is not the default.
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/IS_GLOBAL (#PCDATA)	
	1 means the option profile is a global profile, 0 means the option profile is not global.

XPath	element specifications / notes
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/IS_OFFLINE_SYNCABLE (#PCDATA)	(VM only) “0” means the option profile will be downloaded to your offline scanners during the next sync with the platform; “1” means the profile will not be downloaded to offline scanners during the next sync. (Only applies to Offline Scanner Appliance)
/OPTION_PROFILES/OPTION_PROFILE/BASIC_INFO/UPDATE_DATE (#PCDATA)	Date when option profile was last updated. N/A appears if the profile has not been updated after creation.
/OPTION_PROFILES/OPTION_PROFILE/SCAN	PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?, PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?, PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?, ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, LITE_OS_SCAN?, CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?, SCAN_RESTRICTION?, FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS	(TCP_PORTS?, UDP_PORTS?, AUTHORITATIVE_OPTION?, (STANDARD_SCAN TARGETED_SCAN)?)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS	TCP_PORTS_TYPE?, TCP_PORTS_STANDARD_SCAN?, TCP_PORTS_ADDITIONAL?, THREE_WAY_HANDSHAKE?, STANDARD_SCAN?, TCP_ADDITIONAL?
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS/TCP_PORTS_TYPE (#PCDATA)	TCP ports type, one of: standard (for standard scan, about 1900 TCP ports), light (for light scan, about 160 TCP ports), none (for no TCP ports), full (for all TCP ports).
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS/TCP_PORTS_ADDITIONAL	HAS_ADDITIONAL?, ADDITIONAL_PORTS?
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS/TCP_PORTS_ADDITIONAL/HAS_ADDITIONAL (#PCDATA)	1 means additional TCP ports defined; 0 means additional TCP ports not defined.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS/TCP_PORTS_ADDITIONAL/ADDITIONAL_PORTS (#PCDATA)	List of additional TCP ports.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TCP_PORTS/THREE_WAY_HANDSHAKE (#PCDATA)	1 means scans will perform 3-way handshake with target hosts (performed only when you have a configuration that does not allow SYN packet to be followed by RST packet); 0 means scans will not perform 3-way handshake.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/UDP_PORTS	(UDP_PORTS_TYPE?, UDP_PORTS_STANDARD_SCAN?, UDP_PORTS_ADDITIONAL?, (STANDARD_SCAN CUSTOM_PORT)?)

<b>XPath</b>	<b>element specifications / notes</b>
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/UDP_PORTS/UDP_PORTS_TYPE (#PCDATA)	UDP ports type, one of: standard (for standard scan, about 180 UDP ports), light (for light scan, about 30 UDP ports), none (for no UDP ports), full (for all UDP ports).
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/UDP_PORTS/UDP_PORTS_ADDITIONAL HAS_ADDITIONAL?, ADDITIONAL_PORTS?	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/UDP_PORTS/UDP_PORTS_ADDITIONAL/ HAS_ADDITIONAL (#PCDATA)	1 means additional UDP ports defined; 0 means additional UDP ports not defined.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/UDP_PORTS/UDP_PORTS_ADDITIONAL/ ADDITIONAL_PORTS (#PCDATA)	List of additional UDP ports.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/AUTHORITATIVE_OPTION (#PCDATA)	(VM only) “0” means for partial port scans we’ll update the status for all vulnerabilities found regardless of which ports they are found on; “1” means for partial scans we’ll update the status of vulnerabilities detected by ports scanned.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/STANDARD_SCAN (#PCDATA)	(PC only) 1 means standard port scan is enabled for Windows and Unix scans; 0 means standard port scan is disabled. Standard scan includes well known ports: 22 (SSH), 23 (telnet) and 513 (rlogin). Note: STANDARD_SCAN or TARGETED_SCAN must be enabled, and these settings are mutually exclusive.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PORTS/TARGETED_SCAN (#PCDATA)	(PC only) A targeted port scan, defined by a custom list of ports, is enabled for Windows and Unix; 0 means targeted port scan is disabled. Note: STANDARD_SCAN or TARGETED_SCAN must be enabled, and these settings are mutually exclusive.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SCAN_DEAD_HOSTS (#PCDATA)	(VM only) “0” means we’ll scan dead hosts (this may increase scan time); “1” means we won’t scan dead hosts.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/CLOSE_VULNERABILITIES (HAS_CLOSE_VULNERABILITIES?, HOST_NOT_FOUND_ALIVE?)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/CLOSE_VULNERABILITIES/HAS_CLOSE_VULNERABILITIES (#PCDATA)	(VM only) “0” means we’ll close vulnerabilities on dead hosts during scan processing (vulnerability status will be set to Fixed, and existing tickets will be marked Closed/Fixed); “1” means we won’t close vulnerabilities on dead hosts. This option is valid only when the “Close vulnerabilities on dead hosts” feature is enabled for your subscription by Qualys Support or your Qualys Account Manager.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/CLOSE_VULNERABILITIES/HOST_NOT_FOUND_ALIVE (#PCDATA)	



## XPath

### element specifications / notes

(VM only) “0” means scans will perform host alive testing before vulnerability testing (only hosts found alive will be tested for vulnerabilities); “1” means scans won’t perform host alive testing.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PURGE\_OLD\_HOST\_OS\_CHANGED (#PCDATA)

(VM only) “0” means we’ll purge hosts when OS is changed during scan processing; “1” means we won’t purge hosts when OS is changed.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE

(PARALLEL\_SCALING?, OVERALL\_PERFORMANCE, HOSTS\_TO\_SCAN, PROCESSES\_TO\_RUN, PACKET\_DELAY, PORT\_SCANNING\_AND\_HOST\_DISCOVERY)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/  
PARALLEL\_SCALING (#PCDATA)

(VM only) 1 means parallel scaling for scanner appliances is enabled; 0 means parallel scaling for scanner appliances is disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/  
OVERALL\_PERFORMANCE (#PCDATA)

Overall scan performance level, one of:  
Normal - Recommended in most cases, well balanced between intensity and speed.  
High - Recommended only when scanning a single IP or 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.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/HOSTS\_TO\_SCAN  
(EXTERNAL\_SCANNERS, SCANNER\_APPLIANCES)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/HOSTS\_TO\_SCAN/  
EXTERNAL\_SCANNERS (#PCDATA)

Maximum number of hosts to scan in parallel using Qualys cloud (external) scanners.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/HOSTS\_TO\_SCAN/  
SCANNER\_APPLIANCES (#PCDATA)

Maximum number of hosts to scan in parallel using Qualys Scanner Appliances, installed on your internal network.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/PROCESSES\_TO\_RUN  
(TOTAL\_PROCESSES, HTTP\_PROCESSES)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/PROCESSES\_TO\_RUN/  
TOTAL\_PROCESSES (#PCDATA)

Maximum number of total processes to run at the same time per host.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/PROCESSES\_TO\_RUN/  
HTTP\_PROCESSES (#PCDATA)

Maximum number of HTTP processes to run at the same time per host.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PERFORMANCE/PACKET\_DELAY (#PCDATA)

**XPath**

**element specifications / notes**

The delay between groups of packets sent to each host during a scan.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PORT\_SCANNING\_AND\_HOST\_DISCOVERY (#PCDATA)

(VM only) The aggressiveness (parallelism) of port scanning and host discovery at the port level: Normal, Medium, Low or Minimum. Lowering the intensity level has the effect of serializing port scanning and host discovery.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/LOAD\_BALANCER\_DETECTION #PCDATA)

(VM only) "0" means scans will detect load balancers and report in QID 86189" "1" means scans will not detect load balancers.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING

(SYSTEM, CUSTOM\_LIST)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/SYSTEM

(HAS\_SYSTEM?, SYSTEM\_LEVEL?)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/SYSTEM/  
HAS\_SYSTEM (#PCDATA)

(VM only) 1 means system password brute forcing enabled; 0 means system password brute forcing is not enabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/SYSTEM/  
SYSTEM\_LEVEL (#PCDATA)

(VM only) System password brute forcing level, one of: 1 (for minimal, empty passwords), 2 (for Limited), 3 (for Standard, up to 60 per login ID), 4 (for Exhaustive).

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/CUSTOM\_LIST (CUSTOM+)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/CUSTOM\_LIST/CUSTOM

(ID, TITLE, TYPE, LOGIN\_PASSWORD+)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/CUSTOM\_LIST/CUSTOM/ID  
(#PCDATA)

(VM only) Custom password brute forcing list ID.

Note: An Import Option Profile API call does not import custom password brute forcing lists regardless of Option Profile XML file content. Please configure using Qualys portal UI.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/CUSTOM\_LIST/CUSTOM/TIT  
LE (#PCDATA)

(VM only) Custom password brute forcing list title.

Note: An Import Option Profile API call does not import custom password brute forcing lists regardless of Option Profile XML file content. Please configure using Qualys portal UI.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/PASSWORD\_BRUTE\_FORCING/CUSTOM\_LIST/CUSTOM/TY  
PE (#PCDATA)

(VM only) Type of custom password brute forcing list, one of: ftp, ssh, windows. Note: An Import Option Profile API call does not import custom password brute forcing lists regardless of Option Profile XML file content. Please configure using Qualys portal UI.

XPath	element specifications / notes
/OPTION_PROFILES/OPTION_PROFILE/SCAN/PASSWORD_BRUTE_FORCING/CUSTOM_LIST/CUSTOM/LOGIN_PASSWORD (#PCDATA)	(VM only) Login/password list (maximum 50) for custom password brute forcing list.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION	((COMPLETE   CUSTOM_LIST   RUNTIME), DETECTION_INCLUDE?, DETECTION_EXCLUDE?)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/COMPLETE (#PCDATA)	(VM only) 1 means complete detection is enabled (i.e. run all vulnerability tests in the KnowledgeBase); 0 means complete detection is disabled.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/CUSTOM_LIST (CUSTOM+)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/CUSTOM_LIST/CUSTOM (ID, TITLE)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/CUSTOM_LIST/CUSTOM/ID (#PCDATA)	(VM only) The ID of a search list when custom vulnerability detection is enabled and certain QIDs will be included in scans.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/CUSTOM_LIST/CUSTOM/TITLE (#PCDATA)	(VM only) The title of a search list when custom vulnerability detection is enabled and certain QIDs will be included in scans. The title must exactly match a title in the user's subscription otherwise complete detection is used.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/VULNERABILITY_DETECTION/RUNTIME (#PCDATA)	(VM only) 1 means vulnerability detection Select at runtime option is enabled; 0 means this option is disabled.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/	(BASIC_HOST_INFO_CHECKS, OVAL_CHECKS, QRDI_CHECKS)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/BASIC_HOST_INFO_CHECKS (#PCDATA)	(VM only) 1 means basic host information checks are included in scans; 0 means basic host information checks are not included.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/OVAL_CHECKS (#PCDATA)	(VM only) 1 means OVAL checks are included in scans; 0 means OVAL checks are not included in scans.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/QRDI_CHECKS (#PCDATA)	This flag is for Qualys Internal Use only.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/DETECTION_EXCLUDE (CUSTOM_LIST+)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/DETECTION_EXCLUDE/CUSTOM_LIST (ID, TITLE)	

<b>XPath</b>	<b>element specifications / notes</b>
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/DETECTION_EXCLUDE/CUSTOM_LIST/ID (#PCDATA)	(VM only) 1 means certain QIDs are always excluded from scans; 0 means this option is not enabled.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DETECTION_INCLUDE/DETECTION_EXCLUDE/CUSTOM_LIST/TITLE (#PCDATA)	(VM only) The title of a search list defining QIDS that are always excluded from scans. The title must exactly match a title in the user's subscription otherwise QIDs are not excluded.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/AUTHENTICATION (#PCDATA)	(VM only) Types of authentication enabled: Windows, Unix/Cisco etc. need valid values
/OPTION_PROFILES/OPTION_PROFILE/SCAN/ADDL_CERT_DETECTION (#PCDATA)	(VM only) 1 means scans will detect additional certificates beyond ports; 0 means scans won't detect these certificates.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/	(DISSOLVABLE_AGENT_ENABLE, PASSWORD_AUDITING_ENABLE?, WINDOWS_SHARE_ENUMERATION_ENABLE, WINDOWS_DIRECTORY_SEARCH_ENABLE?)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/DISSOLVABLE_AGENT_ENABLE (#PCDATA)	"0" means Qualys Dissolvable Agent is enabled for your subscription; "1" means the Qualys Dissolvable Agent is not enabled.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/PASSWORD_AUDITING_ENABLE	(HAS_PASSWORD_AUDITING_ENABLE?, CUSTOM_PASSWORD_DICTIONARY?)
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/PASSWORD_AUDITING_ENABLE/HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)	(PC only) "0" means Password Auditing is enabled using Qualys Dissolvable Agent, "1" means this feature is disabled. (Applies only when Dissolvable Agent is enabled using Qualys portal UI).
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/PASSWORD_AUDITING_ENABLE/CUSTOM_PASSWORD_DICTIONARY (#PCDATA)	(PC only) "0" means the Custom Password Dictionary for Password Auding is enabled using Qualys Dissolvable Agent, "1" means this feature is disabled. (Applies only when Dissolvable Agent is enabled using Qualys portal UI).
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)	"0" means Windows Share Enumeration is enabled using Qualys Dissolvable Agent; "1" means this option is not enabled. (Applies only when Dissolvable Agent is enabled using Qualys portal UI).
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DISSOLVABLE_AGENT/WINDOWS_DIRECORY_SEARCH_ENABLE (#PCDATA)	

## XPath

### element specifications / notes

(PC only) “0” means Windows Directory Search is enabled using Qualys Dissolvable Agent; “1” means this option is not enabled.  
(Applies only when Dissolvable Agent is enabled using Qualys portal UI).

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/LITE\_OS\_SCAN (#PCDATA)

(VM only) “0” means Lite OS detection is enabled; “1” means this feature is not enabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CUSTOM\_HTTP\_HEADER

(VALUE?, DEFINITION\_KEY?, DEFINITION\_VALUE?)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CUSTOM\_HTTP\_HEADER/VALUE (#PCDATA)

(VM only) “0” means a custom HTTP header key is defined (used for many CGI and Web application fingerprinting checks); “1” means this feature is not enabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CUSTOM\_HTTP\_HEADER/  
DEFINITION\_KEY? (#PCDATA)

(VM only) Key used in custom HTTP header.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CUSTOM\_HTTP\_HEADER/  
DEFINITION\_VALUE (#PCDATA)

(VM only) Key value used in custom HTTP header.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/SCAN\_RESTRICTION (SCAN\_BY\_POLICY?)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/SCAN\_RESTRICTION  
SCAN\_BY\_POLICY (POLICY+)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/SCAN\_RESTRICTION  
SCAN\_BY\_POLICY/POLICY (POLICY\_ID, POLICY\_TITLE)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/SCAN\_RESTRICTION  
SCAN\_BY\_POLICY/POLICY/ID (#PCDATA)

(PC only) For scan restriction, the ID of the policy to restrict the scan to.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/SCAN\_RESTRICTION  
SCAN\_BY\_POLICY/POLICY/TITLE (#PCDATA)

(PC only) For scan restriction, the title of the policy to restrict the scan to.  
Note: An Import Option Profile API call does not import policies for this feature.  
Please configure using Qualys portal UI.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/FILE\_INTEGRITY\_MONITORING  
(AUTO\_UPDATE\_EXPECTED\_VALUE?)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/FILE\_INTEGRITY\_MONITORING/AUTO\_UPDATE\_EXPECTED  
VALUE (#PCDATA)

(PC only) Specify 1 if you want to enable the option. When you export an option profile, the value of this element indicates if the auto update option is enabled or disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CONTROL\_TYPES

(FIM\_CONTROLS\_ENABLED?, CUSTOM\_WMI\_QUERY\_CHECKS?)

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CONTROL\_TYPES/  
FIM\_CONTROLS\_ENABLED (#PCDATA)

**XPath**

**element specifications / notes**

(PC only) “0” means File Integrity Monitoring controls are disabled; “1” means these controls are enabled.

Note: An Import Option Profile API call does not import policies for this feature. Please configure using Qualys portal UI.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CONTROL\_TYPES/  
CUSTOM\_WMI\_QUERY\_CHECKS (#PCDATA)

(PC only) “0” means Custom WMI Query Checks controls are disabled; “1” means these controls are enabled.

/OPTION\_PROFILES/OPTION\_PROFILE/SCAN/CONTROL\_TYPES/  
DO\_NOT\_OVERWRITE\_OS (#PCDATA)

(VM only) Specify 1 if you want to enable the option. When you export an option profile, the value of this element indicates if the do not overwrite os option is enabled or disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP

(BASIC\_INFO\_GATHERING\_ON, TCP\_PORTS?, UDP\_PORTS?,  
MAP\_OPTIONS?, MAP\_PERFORMANCE, MAP\_AUTHENTICATION?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/BASIC\_INFO\_GATHERING\_ON (#PCDATA)

(VM only) Perform basic information gathering on, one of: all (all hosts detected by the map), registered (hosts in your account), netblock (hosts added to a netblock in your account), none

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS

(TCP\_PORTS\_STANDARD\_SCAN?, TCP\_PORTS\_ADDITIONAL?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS/TCP\_PORTS\_STANDARD\_SCAN (#PCDATA)

(VM only) 1 means standard TCP port scan (about 13 ports) is enabled; 0 means standard TCP port scan is disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS/TCP\_PORTS\_ADDITIONAL  
(HAS\_ADDITIONAL?, ADDITIONAL\_PORTS?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS/TCP\_PORTS\_ADDITIONAL/  
HAS\_ADDITIONAL (#PCDATA)

(VM only) 1 means additional TCP ports defined; 0 means additional TCP ports not defined.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS/TCP\_PORTS\_ADDITIONAL/  
ADDITIONAL\_PORTS (#PCDATA)

(VM only) List of additional TCP ports.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/UDP\_PORTS

UDP\_PORTS\_STANDARD\_SCAN?, UDP\_PORTS\_ADDITIONAL?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/UDP\_PORTS/UDP\_PORTS\_STANDARD\_SCAN (#PCDATA)

(VM only) 1 means standard UDP port scan (about 6 ports) is enabled; 0 means standard UDP port scan is disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/UDP\_PORTS/UDP\_PORTS\_ADDITIONAL  
(HAS\_ADDITIONAL?, ADDITIONAL\_PORTS?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/UDP\_PORTS/UDP\_PORTS\_ADDITIONAL/  
HAS\_ADDITIONAL (#PCDATA)

## XPath

### element specifications / notes

(VM only) 1 means additional UDP ports defined; 0 means additional UDP ports not defined.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/TCP\_PORTS/TCP\_PORTS\_ADDITIONAL/  
ADDITIONAL\_PORTS (#PCDATA)

(VM only) List of additional UDP ports.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_OPTIONS

(PERFORM\_LIVE\_HOST\_SWEEP?, DISABLE\_DNS\_TRAFFIC?)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_OPTIONS/PERFORM\_LIVE\_HOST\_SWEEP (#PCDATA)

(VM only) "0" means Perform Live Host Sweep option is enabled; "1" means this option is disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_OPTIONS/DISABLE\_DNS\_TRAFFIC (#PCDATA)

(VM only) "0" means Disable DNS Traffic option is enabled; "1" means this option is disabled.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE

(OVERALL\_PERFORMANCE, MAP\_PARALLEL?, PACKET\_DELAY)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE/  
OVERALL\_PERFORMANCE (#PCDATA)

(VM only) Overall map performance level, one of:  
Normal - Recommended in most cases, 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.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE /MAP\_PARALLEL

(EXTERNAL\_SCANNERS, SCANNER\_APPLIANCES, NETBLOCK\_SIZE)

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE /MAP\_PARALLEL/  
EXTERNAL\_SCANNERS (#PCDATA)

(VM only) Maximum number of netblocks to map in parallel using Qualys cloud (external) scanners.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE /MAP\_PARALLEL/  
SCANNER\_APPLIANCES (#PCDATA)

(VM only) Maximum number of netblocks to map in parallel using Qualys Scanner Appliances, installed on your internal network.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE /MAP\_PARALLEL/  
NETBLOCK\_SIZE (#PCDATA)

(VM only) Maximum number of IPs per netblock to map in parallel per scanner.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_PERFORMANCE /PACKET\_DELAY (#PCDATA)

(VM only) Delay between groups of packets sent to the netblocks being mapped. With short delay packets are sent more frequently resulting in more bandwidth utilization and shorter mapping time. With long delay, packets are sent less frequently, resulting in less bandwidth utilization and longer mapping time.

/OPTION\_PROFILES/OPTION\_PROFILE/MAP/MAP\_AUTHENTICATION (#PCDATA)

XPath	element specifications / notes
	(VM only) 1 means VMware authentication is enabled for maps; 0 means this option is disabled.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL	
	(HOST_DISCOVERY, BLOCK_RESOURCES?, PACKET_OPTIONS?)
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY	
(TCP_PORTS?, UDP_PORTS?, ICMP?)	
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/TCP_PORTS	
(STANDARD_SCAN?, TCP_ADDITIONAL?)	
/OPTION_PROFILES/OPTION_PROFILE/HOST_DISCOVERY/TCP_PORTS/STANDARD_SCAN	
	1 means standard TCP ports (13 ports) are scanned during host discovery; 0 means standard TCP port scan option is not enabled.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/TCP_PORTS/TCP_ADDITIONAL	
(HAS_ADDITIONAL?, ADDITIONAL_PORTS?)	
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/TCP_PORTS/TCP_ADDITIONAL/ HAS_ADDITIONAL (#PCDATA)	
	1 means additional TCP ports are scanned during host discovery; 0 means no additional TCP ports are defined for host discovery.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/TCP_PORTS/TCP_ADDITIONAL/ ADDITIONAL_PORTS (#PCDATA)	
	List of additional TCP ports that are scanned during host discovery.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/UDP_PORTS	
(STANDARD_SCAN   CUSTOM)	
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/UDP_PORTS/ STANDARD_SCAN (#PCDATA)	
	1 means standard UDP ports (6 ports) are scanned during host discovery; 0 means standard UDP port scan option is not enabled.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/UDP_PORTS/ CUSTOM (#PCDATA)	
	Custom list of UDP ports that are scanned during host discovery.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/HOST_DISCOVERY/ICMP	
	“0” means ICMP ports are scanned during host discovery; “1” means these ports are not scanned during host discovery.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/BLOCK_RESOURCES	
	((WATCHGUARD_DEFAULT_BLOCKED_PORTS   CUSTOM_PORT_LIST), (ALL_REGISTERED_IPS   CUSTOM_IP_LIST))
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/BLOCK_RESOURCES/ WATCHGUARD_DEFAULT_BLOCKED_PORTS (#PCDATA)	
	1 means WatchGuard Firebox System series default ports are blocked and will not be scanned; 0 means these ports are not blocked.
/OPTION_PROFILES/OPTION_PROFILE/ADDITIONAL/BLOCK_RESOURCES/ CUSTOM_PORT_LIST (#PCDATA)	



## XPath

### element specifications / notes

1 means a custom list of blocked ports is defined and these ports will not be scanned; 0 means a custom list of blocked ports is not defined.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/BLOCK\_RESOURCES/  
ALL\_REGISTERED\_IPS (#PCDATA)

1 means all registered IP addresses protected by your firewall/IDS are blocked and will not be scanned; 0 means all registered IP addresses are not blocked.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/BLOCK\_RESOURCES/  
CUSTOM\_IP\_LIST (#PCDATA)

Custom list of registered IP addresses protected by your firewall/IDS that are blocked and will not be scanned.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/PACKET\_OPTIONS

(IGNORE\_FIREWALL\_GENERATED\_TCP\_RST?, IGNORE\_ALL\_TCP\_RST?,  
IGNORE\_FIREWALL\_GENERATED\_TCP\_SYN\_ACK?,  
NOT\_SEND\_TCP\_ACK\_OR\_SYN\_ACK\_DURING\_HOST\_DISCOVERY?)

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/PACKET\_OPTIONS/  
IGNORE\_FIREWALL\_GENERATED\_TCP\_RST (#PCDATA)

“0” means scans will try to identify firewall generated TCP RST packets and ignore them when found; “1” means scans will not try to identify and ignore TCP RST packets.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/PACKET\_OPTIONS/  
IGNORE\_ALL\_TCP\_RST (#PCDATA)

(Applies to maps only) “” means maps will ignore all TCP RST packets, both firewall generated and live hist generated; “false” means maps do not ignore these packets.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/PACKET\_OPTIONS/  
IGNORE\_FIREWALL\_GENERATED\_TCP\_SYN\_ACK (#PCDATA)

“0” means scans attempt to determine if TCP SYN-ACK packets are generated by a filtering device and ignore those packets that appear to originate from such devices; “1” means scans do not try to ignore packets that appear to originate from filtering devices.

/OPTION\_PROFILES/OPTION\_PROFILE/ADDITIONAL/PACKET\_OPTIONS/  
NOT\_SEND\_TCP\_ACK\_OR\_SYN\_ACK\_DURING\_HOST\_DISCOVERY (#PCDATA)

“0” means scans do not send TCP ACK or SYN-ACK packets during host discovery; “1” means scans send these packets. (Valid only when THREE\_WAY\_HANDSHAKE is disabled.)

## Report XML

This section covers report XML data.

- Report List
- Schedule Report List
- Scan Report Template Output
- PCI Scan Template Output
- Patch Template Output
- Map Template Output

# Report List

The report list output is an XML report returned from the report list API call.

The DTD “report\_list\_output.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

```
https://qualysapi.qualys.com/api/2.0/fo/report/
report_list_output.dtd
```

## DTD for Report List Output

A recent DTD for the report list output (report\_list\_output.dtd) is shown below.

```
<!-- QUALYS REPORT_LIST_OUTPUT DTD -->
<!ELEMENT REPORT_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, REPORT_LIST?)>
<!ELEMENT REPORT_LIST (REPORT+)>
<!ELEMENT REPORT (ID, TITLE, TYPE, USER_LOGIN, LAUNCH_DATETIME,
                  OUTPUT_FORMAT, SIZE, STATUS, EXPIRATION_DATETIME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>
<!ELEMENT OUTPUT_FORMAT (#PCDATA)>
<!ELEMENT SIZE (#PCDATA)>
<!ELEMENT STATUS (STATE, MESSAGE?, PERCENT?)>
<!ELEMENT EXPIRATION_DATETIME (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>
<!ELEMENT PERCENT (#PCDATA)>
<!ELEMENT EXPIRATION_DATETIME (#PCDATA)>
<!-- EOF -->
```

## XPaths for Report List Output

This section describes the XPaths for the report list output (report\_list\_output.dtd).

XPath	element specifications / notes
/REPORT_LIST_OUTPUT	(REQUEST?, RESPONSE)
/REPORT_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/REPORT_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/REPORT_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/REPORT_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/REPORT_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/REPORT_LIST_OUTPUT/RESPONSE	(DATETIME, REPORT_LIST?)
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST (REPORT+)	
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT	(ID, TITLE, TYPE, USER_LOGIN, LAUNCH_DATETIME, OUTPUT_FORMAT, SIZE, STATUS, EXPIRATION_DATETIME)
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/ID (#PCDATA)	The report ID of the report.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/TITLE (#PCDATA)	The report title.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/TYPE (#PCDATA)	The report type: Map, Scan, Compliance, Remediation, Scorecard, WAS, Web Application Scorecard, or Patch.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/USER_LOGIN (#PCDATA)	The user login ID of the user who launched the report.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/LAUNCH_DATETIME (#PCDATA)	The date and time when the report was launched.

<b>XPath</b>	<b>element specifications / notes</b>
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/OUTPUT_FORMAT (#PCDATA)	The report output format: HTML, XML, PDF, MHT, CSV, or Online (for Qualys Patch Report only).
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/SIZE (#PCDATA)	The report size.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/STATUS (STATE, MESSAGE?, PERCENT?)	
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/STATUS/STATE (#PCDATA)	The report state: Running, Finished, Canceled or Errors.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/STATUS/MESSAGE (#PCDATA)	The report status message.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/STATUS/PERCENT (#PCDATA)	For a report in progress, the percentage complete.
/REPORT_LIST_OUTPUT/RESPONSE/REPORT_LIST/REPORT/EXPIRATION_DATETIME (#PCDATA)	The report expiration date and time.

# Schedule Report List

The schedule report list output is an XML report returned from the schedule report list API call.

The DTD “schedule\_report\_list\_output.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

[https://qualysapi.qualys.com/api/2.0/fo/schedule/report/schedule\\_report\\_list\\_output.dtd](https://qualysapi.qualys.com/api/2.0/fo/schedule/report/schedule_report_list_output.dtd)

## DTD for Schedule Report List Output

A recent DTD for the schedule report list output (schedule\_report\_list\_output.dtd) is shown below.

```
<!-- QUALYS SCHEDULE_REPORT_LIST_OUTPUT DTD -->

<!ELEMENT SCHEDULE_REPORT_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, SCHEDULE_REPORT_LIST?)>
<!ELEMENT SCHEDULE_REPORT_LIST (REPORT+)>
<!ELEMENT REPORT (ID, TITLE?, OUTPUT_FORMAT, TEMPLATE_TITLE?,
                  ACTIVE, SCHEDULE)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT OUTPUT_FORMAT (#PCDATA)>
<!ELEMENT TEMPLATE_TITLE (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>

<!ELEMENT SCHEDULE ((DAILY|WEEKLY|MONTHLY), START_DATE_UTC,
                    START_HOUR, START_MINUTE, TIME_ZONE,
                    DST_SELECTED, MAX_OCCURRENCE?)>
<!ELEMENT DAILY EMPTY>
```

```

<!-- ATTLIST DAILY
      frequency_days  CDATA #REQUIRED>

<!-- weekdays is comma-separated list of weekdays e.g. 0,1,4,5 -->
<!-- ELEMENT WEEKLY EMPTY>
<!-- ATTLIST WEEKLY
      frequency_weeks  CDATA #REQUIRED
      weekdays         CDATA #REQUIRED>

<!-- either day of month, or (day of week and week of month) must be
provided -->
<!-- ELEMENT MONTHLY EMPTY>
<!-- ATTLIST MONTHLY
      frequency_months  CDATA #REQUIRED
      day_of_month      CDATA #IMPLIED
      day_of_week       (0|1|2|3|4|5|6) #IMPLIED
      week_of_month     (1|2|3|4|5) #IMPLIED>

<!-- start date of the task in UTC -->
<!-- ELEMENT START_DATE_UTC (#PCDATA)>
<!-- User Selected hour -->
<!-- ELEMENT START_HOUR (#PCDATA)>
<!-- User Selected Minute -->
<!-- ELEMENT START_MINUTE (#PCDATA)>
<!-- ELEMENT TIME_ZONE (TIME_ZONE_CODE, TIME_ZONE_DETAILS)>

<!-- timezone code like US-CA -->
<!-- ELEMENT TIME_ZONE_CODE (#PCDATA)>

<!-- timezone details like (GMT-0800) United States (California): Los
Angeles, Sacramento, San Diego, San Francisco-->
<!-- ELEMENT TIME_ZONE_DETAILS (#PCDATA)>

<!-- Did user select DST? 0-not selected 1-selected -->
<!-- ELEMENT DST_SELECTED (#PCDATA)>
<!-- ELEMENT MAX_OCCURRENCE (#PCDATA)>

<!-- EOF -->

```

# XPaths for Schedule Report List Output

This section describes the XPaths for the schedule report list output (schedule\_report\_list\_output.dtd).

XPath	element specifications / notes
/SCHEDULE_REPORT_LIST_OUTPUT	(REQUEST?, RESPONSE)
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/SCHEDULE_REPORT_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE	(DATETIME, SCHEDULE_REPORT_LIST?)
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST (REPORT+)	
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT	(ID, TITLE?, OUTPUT_FORMAT, TEMPLATE_TITLE?, ACTIVE, SCHEDULE)
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/ID (#PCDATA)	The report ID of the report.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/TITLE (#PCDATA)	The report title.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/OUTPUT_FORMAT (#PCDATA)	The report format.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/TEMPLATE_TITLE (#PCDATA)	



## XPath

## element specifications / notes

The report template title.

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/ACTIVE (#PCDATA)

1 for an active schedule, or 0 for a deactivated schedule.

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE

((DAILY|WEEKLY|MONTHLY), START\_DATE\_UTC, START\_HOUR, START\_MINUTE, TIME\_ZONE, DST\_SELECTED, MAX\_OCCURRENCE?)

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/DAILY

attribute: **frequency\_days** **frequency\_days** is *required* for a report that runs after some number of days (from 1 to 365)

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/WEEKLY

attribute: **frequency\_weeks** **frequency\_weeks** is *required* for a report that runs after some number of weeks (from 1 to 52)

attribute: **weekdays** **weekdays** is *required* for a report that runs after some number of weeks on a particular weekday (from 0 to 6), where 0 is Sunday and 6 is Saturday, multiple weekdays are comma separated

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/MONTHLY

attribute: **frequency\_months** **frequency\_months** is *required* for a report that runs after some number of months (from 1 to 12)

attribute: **day\_of\_month** **day\_of\_month** is *implied* and, if present, indicates the report runs on the Nth day of the month (from 1 to 31)

attribute: **day\_of\_week** **day\_of\_week** is *implied* and, if present, indicates the report runs on the Nth day of the month on a particular weekday (from 0 to 6), where 0 is Sunday and 6 is Saturday

attribute: **week\_of\_month** **week\_of\_month** is *implied* and, if present, indicates the report runs on the Nth day of the month on the Nth week of the month (from 1 to 5), where 1 is the first week of the month and 5 is the fifth week of the month

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/START\_DATE\_UTC (#PCDATA)

The start date (in UTC format) defined for the report schedule.

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/START\_HOUR (#PCDATA)

The start hour defined for the report schedule.

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/START\_MINUTE (#PCDATA)

The start minute defined for the report schedule.

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/TIME\_ZONE (TIME\_ZONE\_CODE, TIME\_ZONE\_DETAILS)

/SCHEDULE\_REPORT\_LIST\_OUTPUT/RESPONSE/SCHEDULE\_REPORT\_LIST/REPORT/SCHEDULE/TIME\_ZONE/TIME\_ZONE\_CODE (#PCDATA)

The time zone code defined for the report schedule. For example: US-CA.

XPath	element specifications / notes
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/SCHEDULE/TIME_ZONE/TIME_ZONE_DETAILS (#PCDATA)	The time zone details (description) for the local time zone, identified in the <TIME_ZONE_CODE> element. For example:, (GMT-0800) United States (California): Los Angeles, Sacramento, San Diego, San Francisco.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/SCHEDULE/DST_SELECTED (#PCDATA)	When set to 1, Daylight Saving Time (DST) is enabled for the report schedule.
/SCHEDULE_REPORT_LIST_OUTPUT/RESPONSE/SCHEDULE_REPORT_LIST/REPORT/SCHEDULE/MAX_OCCURRENCE (#PCDATA)	The number of times the report schedule will be run before it is deactivated (from 1 to 99).

# Scan Report Template Output

The Scan Report Template output is an XML report returned from the Scan Report Template Export API call.

/api/2.0/fo/report/template/scan/?action=export

The DTD “scanreporttemplate\_info.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/scanreporttemplate\_info.dtd

## DTD for Scan Report Template Output

A recent DTD for the scan report template output (scanreporttemplate\_info.dtd) is shown below.

```
<!-- QUALYS REPORT_SCAN_TEMPLATE_OUTPUT DTD -->
<!ELEMENT REPORTTEMPLATE (SCANTEMPLATE)*>
<!ELEMENT SCANTEMPLATE
(TITLE|TARGET|DISPLAY|FILTER|SERVICESPORTS|USERACCESS)*>
<!ELEMENT TITLE (INFO)*>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
    key CDATA #REQUIRED>
<!ELEMENT TARGET (INFO)*>
<!ELEMENT DISPLAY (INFO)*>
<!ELEMENT FILTER (INFO)*>
<!ELEMENT SERVICESPORTS (INFO)*>
<!ELEMENT USERACCESS (INFO)*>
<!-- EOF -->
```

## XPaths for Scan Report Template Output

This section describes the XPaths for the scan report template output (scanreporttemplate\_info.dtd).

XPath	element specifications / notes
/REPORT_SCAN_TEMPLATE_OUTPUT	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE	(TITLE TARGET DISPLAY FILTER SERVICESPORTS USERACCESS)
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/TITLE	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/TITLE/INFO (#PCDATA)	
The template title and owner.	

<b>XPath</b>	<b>element specifications / notes</b>
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/TARGET	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/TARGET/INFO (#PCDATA)	
	The target assets to include in the report.
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/DISPLAY	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/DISPLAY/INFO (#PCDATA)	
	Display options such as graphs amount of detail.
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/FILTER	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/FILTER/INFO (#PCDATA)	
	Filter options such as vulnerability status, categories, QIDs, and OS.
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/SERVICESPORTS	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/SERVICESPORTS/INFO (#PCDATA)	
	Services and ports to include in report.
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/USERACCESS	
/REPORT_SCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/SCANTEMPLATE/USERACCESS/INFO (#PCDATA)	
	Control user access to template and reports generated from the template.

# PCI Scan Template Output

The PCI Scan Template output is an XML report returned from the PCI Scan Template Export API call.

/api/2.0/fo/report/template/pciscan/?action=export

The DTD “pciscanreporttemplate\_info.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

https://qualysapi.qualys.com/api/2.0/fo/report/template/pciscan/pciscanreporttemplate\_info.dtd

## DTD for PCI Scan Template Output

A recent DTD for the pci scan template output (pciscanreporttemplate\_info.dtd) is shown below.

```
<!ELEMENT REPORTTEMPLATE (PCISCANTEMPLATE)*>
<!ELEMENT PCISCANTEMPLATE
(TITLE|TARGET|DISPLAY|FILTER|SERVICESPORTS|USERACCESS|PCIRISKRANKING)*>
<!ELEMENT TITLE (INFO)*>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
      key CDATA #REQUIRED>
<!ELEMENT TARGET (INFO)*>
<!ELEMENT DISPLAY (INFO)*>
<!ELEMENT FILTER (INFO)*>
<!ELEMENT SERVICESPORTS (INFO)*>
<!ELEMENT USERACCESS (INFO)*>
<!ELEMENT PCIRISKRANKING (INFO)*>
```

## XPaths for PCI Scan Template Output

This section describes the XPaths for the pci scan template output (pciscanreporttemplate\_info.dtd).

XPath	element specifications / notes
/REPORT_PCISCAN_TEMPLATE_OUTPUT	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE	(TITLE TARGET DISPLAY FILTER SERVICESPORTS USERACCESS PCIRISKRANKING)
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/TITLE	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/TITLE/INFO (#PCDATA)	

XPath	element specifications / notes
	The template title and owner.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/TARGET	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/TARGET/	
INFO (#PCDATA)	
	The target assets to include in the report.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/DISPLAY	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/DISPLAY/	
INFO (#PCDATA)	
	Display options such as graphs amount of detail.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/FILTER	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/FILTER/	
INFO (#PCDATA)	
	Filter options such as vulnerability status, categories, QIDs, and OS.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/SERVICESPORTS	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/SERVICESPORTS/	
INFO (#PCDATA)	
	Services and ports to include in report.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/USERACCESS	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/USERACCESS/	
INFO (#PCDATA)	
	Control user access to template and reports generated from the template.
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE/PCISCANTEMPLATE/PCIRISKRANKING	
/REPORT_PCISCAN_TEMPLATE_OUTPUT/REPORTTEMPLATE	
/PCISCANTEMPLATE/PCIRISKRANKING/INFO (#PCDATA)	
	Configure PCI Risk Ranking.

# Patch Template Output

The Patch Template output is an XML report returned from the Patch Template Export API call.

/api/2.0/fo/report/template/patch/?action=export

The DTD “patchreporttemplate\_info.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/patchreporttemplate\_info.dtd

## DTD for Patch Template Output

A recent DTD for the patch template output (patchreporttemplate\_info.dtd) is shown below.

```
<!ELEMENT REPORTTEMPLATE (PATCHTEMPLATE)*>
<!ELEMENT PATCHTEMPLATE (TITLE|TARGET|DISPLAY|FILTER|USERACCESS)*>
<!ELEMENT TITLE (INFO)*>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
    key CDATA #REQUIRED>
<!ELEMENT TARGET (INFO)*>
<!ELEMENT DISPLAY (INFO)*>
<!ELEMENT FILTER (INFO)*>
<!ELEMENT USERACCESS (INFO)*>
```

## XPaths for Patch Template Output

This section describes the XPaths for the patch template output (patchreporttemplate\_info.dtd).

XPath	element specifications / notes
/REPORT_PATCH_TEMPLATE_OUTPUT	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE	(TITLE TARGET DISPLAY FILTER USERACCESS)
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/TITLE	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/TITLE/INFO (#PCDATA)	The template title and owner.
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/TARGET	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/TARGET/INFO (#PCDATA)	The target assets to include in the report.

XPath	element specifications / notes
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/DISPLAY	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/DISPLAY/INFO (#PCDATA)	
	Display options to include in the report.
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/FILTER	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/FILTER/INFO (#PCDATA)	
	Filter options such as vulnerabilities, QIDs, patches.
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/USERACCESS	
/REPORT_PATCH_TEMPLATE_OUTPUT/REPORTTEMPLATE/PATCHTEMPLATE/USERACCESS/INFO (#PCDATA)	
	Control user access to template and reports generated from the template.



# Map Template Output

The Map Template output is an XML report returned from the Map Template Export API call.

/api/2.0/fo/report/template/map/?action=export

The DTD “mapreporttemplate\_info.dtd” can be found at the following URL (where <qualysapi.qualys.com> is the API server URL where your account is located):

https://qualysapi.qualys.com/api/2.0/fo/report/template/map/mapreporttemplate\_info.dtd

## DTD for Map Template Output

A recent DTD for the map template output (mapreporttemplate\_info.dtd) is shown below.

```
<!ELEMENT REPORTTEMPLATE (MAPTEMPLATE)*>
<!ELEMENT MAPTEMPLATE (TITLE|DISPLAY|FILTER|OPERATINGSYSTEM)*>
<!ELEMENT TITLE (INFO)*>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
    key CDATA #REQUIRED>
<!ELEMENT DISPLAY (INFO)*>
<!ELEMENT FILTER (INFO)*>
<!ELEMENT OPERATINGSYSTEM (INFO)*>
```

## XPaths for Map Template Output

This section describes the XPaths for the map template output (mapreporttemplate\_info.dtd).

XPath	element specifications / notes
/REPORT_MAP_TEMPLATE_OUTPUT	
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE	
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE	
	(TITLE   DISPLAY   FILTER   OPERATINGSYSTEM)
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/TITLE	
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/TITLE/INFO (#PCDATA)	
	The template title and owner.
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/DISPLAY	
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/DISPLAY/INFO (#PCDATA)	
	Display options to include in the report.
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/FILTER	

XPath	element specifications / notes
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/FILTER/INFO (#PCDATA)	Filter options such as vulnerabilities, QIDs, MAPes.
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/OPERATINGSYSTEM	
/REPORT_MAP_TEMPLATE_OUTPUT/REPORTTEMPLATE/MAPTEMPLATE/OPERATINGSYSTEM/INFO (#PCDATA)	Select the Operating System.

## Error Codes / Descriptions

Here's a list of Qualys API v2 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 Status	Error Code	Error Text	Meaning
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/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 Status	Error Code	Error Text	Meaning
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.

## A

- API limits 14
- Appliance functions
  - view scanner appliance list 77, 87
- Asset functions
  - purge hosts 218
  - view host list 170, 178
  - view IP list 167
- asset group list output
  - XPath elements 617, 623
- asset group vulnerability report 760
- assign scanner appliance to network 523
- authentication 10, 325
- authentication record list 327
- authentication record list by type 329
- authentication record list by type output
  - XPath elements 728
- authentication record list output
  - XPath elements 722
- authentication record return
  - XPath elements 749
- authentication using V2 APIs 20
- authentication vault list output
  - XPath elements 751
- authentication vault view output
  - XPath elements 754

## B

- batch return
  - XPath elements 529
- batch return DTD 221, 366, 379, 383, 403, 444

## C

- characters in URLs 12
- Cisco authentication record 410
- compliance authentication report
  - XPath elements 695

- compliance control list output
  - XPath elements 632
- Compliance functions
  - view compliance control list 271
  - view compliance policy list 277
  - view compliance posture information 298
  - view FDCC policy list 320
- compliance policy export output
  - XPath elements 651
- compliance policy list output
  - XPath elements 643, 716
- compliance policy report
  - XPath elements 681
- compliance posture output
  - XPath elements 667
- compliance scan result output
  - XPath elements 550
- compliance scorecard report
  - XPath elements 704
- control criticality 305
- Cyberscope report 315

## D

- date format 12
- Docker authentication record 336
- DTD for compliance authentication report 693
- DTD for compliance control list output 273, 629
- DTD for compliance scan result output 548
- DTD for compliance scorecard report 700
- DTD for exception batch return 713
- DTD for exception list output 708
- DTD for IPv6 mapping records list output 265
- DTD for KnowledgeBase output 566, 579
- DTD for map report output 560
- DTD for PCI scan share status output 558
- DTD for report list output 827
- DTD for scan list output 530, 534, 537
- DTD for scanner appliance create output 796
- DTD for scanner appliance list output 781

- DTD for schedule report list output 830
- DTD for VM Recrypt Results 555
- DTDs for assets
  - asset group list output 240, 615, 621
  - excluded hosts change history output 603
  - excluded hosts list output 601
  - host list detection output 592
  - host list output 176, 585
  - IP list output 168, 224, 583
  - IPv6 mapping records list output 608
  - restricted IPs list output 610
  - scanner appliance list output 82
  - virtual host list output 222, 606
- DTDs for compliance policies
  - compliance policy export output 648
  - compliance policy list output 280, 641, 715
  - compliance posture information output 304, 664
  - FDCC policy list output 322
- DTDs for reports
  - host list detection 193
  - report batch return 221
  - report list output 130
  - report simple return 40, 146, 154, 156, 163, 165
  - schedule report list output 164
- DTDs for scan authentication
  - authentication record list by type output 330, 726
  - authentication record list output 327, 721
  - authentication record return 366, 379, 383, 403, 444, 748
  - authentication vault list output 750
  - authentication vault view output 753
- DTDs for scorecard reports
  - asset group vulnerability report 758
  - ignored vulnerabilities report 763
  - most prevalent vulnerabilities report 767
  - most vulnerable hosts report 771
  - patch report 775
- DTDs, most recent 13
- dynamic search list
  - XPath elements 804

## E

- exception batch return
  - Xpath elements 713
- exception list output
  - XPath elements 709
- excluded hosts change history output
  - XPath elements 604
- excluded hosts list output
  - XPath elements 602
- Expires header 24

## G

- GET method 12
- gotolink vaultapi 446

## H

- header parameter 20
- host list detection
  - DTD 193
- host list detection DTD 193
- host list detection output
  - XPath elements 594
- host list output
  - XPath elements 587
- HTTP Expires header 24

## I

- ignored vulnerabilities report 764
- IP list output
  - XPath elements 584
- IPv4 to IPv6 asset mapping functions
  - remove IPv4 to IPv6 mapping records list 268
- IPv6 asset mapping functions
  - add IPv6 mapping records 266
  - view IPv6 mapping records list 264

## K

- KnowledgeBase output
  - XPath elements 569, 580

## M

- map report output
  - XPath elements 561
- most prevalent vulnerabilities report 768
- most vulnerable hosts report 772
- MS SQL authentication record 356

## N

- Network functions
  - assign scanner appliance to network 523
  - create a network 521
  - network list 520
  - update a network 522
- network list 520
  - XPath elements 564
- network security audits 30
- network support 519

## O

- Oracle authentication record 372
- Oracle Listener authentication record 380
- Oracle WebLogic authentication record 384

## P

- patch report 776
- PCI scan share status output
  - XPath elements 559
- POST method 12

## Q

- Qualys
  - API server 10
  - user account 10
  - vulnerability scans 30
- Qualys API server 10
- Qualys Support 8
- Qualys user account 10

## R

- report batch return
  - DTD 221
- report DTDs, most recent 13
- report list output
  - DTD 130
  - XPath elements 828
- Report Share functions
  - cancel report 155
  - delete report 162
  - download report 157
  - launch report 131
  - launch scorecard 147
  - report list 128
  - report template list 142
  - session login/logout 26, 28
- report simple return
  - DTD 40, 146, 154, 156, 163, 165
- reports
  - batch return 221
  - Cyberscope report 315
  - date format 12
  - decoding reports 13
  - host list detection 193
  - report list output 130
  - schedule report list 164
  - simple return 40, 146, 154, 156, 163, 165
- restricted IPs list output
  - XPath elements 611, 613



## S

- Scan Authentication functions
  - authentication record list 327
  - authentication record list by type 329
  - Cisco authentication record 410
  - Docker authentication record 336
  - MS SQL authentication record 356
  - Oracle authentication record 372
  - Oracle Listener authentication record 380
  - Oracle WebLogic authentication record 384
  - SNMP authentication record 397
  - Unix authentication record 410
  - Windows authentication record 439
- Scan functions
  - cancel running scan 31
  - KnowledgeBase 95
  - share PCI scan 73
  - VM scan statistics 70
- scan list output
  - XPath elements 531, 535, 540
- scanner appliance create output
  - XPath elements 796
- scanner appliance list output
  - XPath elements 784
- scans 30
- schedule report list output
  - DTD 164, 830
  - XPath elements 832
- session timeout 25
- simple return
  - XPath elements 527
- simple return DTD 40, 146, 154, 156, 163, 165
- SNMP authentication record 397
- special characters in URLs 12
- static search list
  - XPath elements 799

## U

- Unix authentication record 410
- URL elements 13
- URL encoded variables 12

- user account
  - login credentials 10
- UTF-8 encoding 12

## V

- virtual host list output
  - XPath elements 607, 609
- VM Recrypt Results
  - XPath elements 556

## W

- Windows authentication record 439

## X

- XML output
  - Asset 582
  - authentication records 720, 757
  - compliance data 628
  - scan and report share 525
  - scan authentication 720, 757