



Qualys API (VM, PC)

XML/DTD Reference
Version 10.25.1

January 11, 2024

Copyright 2018-2024 by Qualys, Inc. All Rights Reserved.

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

Qualys, Inc.
919 E Hillsdale Blvd

4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

Preface.....	6
Chapter 1 - Introduction	7
Helpful resources	7
URL to Qualys API Server	7
Chapter 2 - Scans XML	8
Scan List Output	9
Schedules Run History Output	15
Scheduled Scan List Output	18
Vulnerability Scan Results	28
Compliance Scan Results	29
VM Recrypt Results (Scan Statistics)	38
VM Scan Summary Output	40
Scan Summary Output	51
Scanner List Output	53
PCI Scan Share Status Output	55
KnowledgeBase Output	57
Customized Vulnerability List Output	72
Map Report - Version 2	75
Map Report - Single Domain	81
Map Report List Output	86
EC2 Instance ID Scan Launch Output	89
New API: Domain V2 API DTD Output	91
Chapter 3 - Scan Configuration XML	93
Scanner Appliance List Output	93
Scanner Appliance Create Output	107
Replace Scanner Appliance Output	108
Static Search List Output	111
Dynamic Search List Output	114
Option Profile Output	121
QID List Output	139
Chapter 4 - Scan Authentication XML	146
Authentication Record List Output	147
List SAP IQ Record Output	153
List Postgre SQL Record Output	155
List Greenplum Record Output	157
List Windows Record Output	159
List Unix Record Output	161

List Oracle Record Output	163
Authentication Record List by Type Output	164
Authentication Vault List Output	197
Authentication Vault View Output	199

Chapter 5 - Assets XML..... 203

IP List Output	203
Host List Output	205
Host Update Output	214
Host Purge Output	216
Host List VM Detection Output	218
Excluded Hosts List Output	228
Network List Output	255
Patch List Output	257

Chapter 6 - VM Reports XML..... 260

Report List Output	260
Schedule Report List Output	263
Scan Report Template Output	267
PCI Scan Template Output	269
Patch Template Output	271
Map Template Output	272
Map Report Output	273
Patch Report (XML) Output	276
VM Scan Report Output	281

Chapter 7 - VM Scorecard Reports XML..... 301

Asset Group Vulnerability Report	301
Ignored Vulnerabilities Report	306
Most Prevalent Vulnerabilities Report	309
Most Vulnerable Hosts Report	312
Patch Scorecard Report	315

Chapter 8 - VM Remediation Tickets XML..... 320

Ticket List Output	320
Ticket Edit Output	334
Ticket Delete Output	338
Deleted Ticket List Output	342
Get Ticket Information Report	344
Ignore Vulnerability Output	353

Chapter 9 - Compliance XML.....355

Compliance Control List Output	355
Compliance Policy List Output	368

Compliance Posture Info List Output	391
Compliance Policy Report	406
Compliance Authentication Report	423
Compliance Scorecard Report	429
Exception List Output	436
Exception Batch Return Output	440
SCAP Policy List Output	442

Chapter 10 - User XML 446

User Output	446
User List Output	447
User Action Log Report	452
Password Change Output	454

Appendix..... 457

Simple Return	457
Batch Return	459
.....	460

Preface

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

About Qualys

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

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

Contact Qualys Support

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

Chapter 1 - Introduction

The Qualys Cloud Platform API (VM, PC) allows third parties to integrate their own applications with Qualys Vulnerability Management and Policy Compliance solutions using an extensible XML interface. This document provides a reference to XML output and DTDs related to the Qualys API.

Helpful resources

Looking for API documentation?

Visit our Documentation page at

<https://www.qualys.com/documentation/>

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](#)

URL to Qualys API Server

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

[Click here to identify your Qualys platform and get the API URL](#)

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

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

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

Chapter 2 - Scans XML

This section describes the XML output returned from Scans API requests.

[Scan List Output](#)

[SCAP Scan List Output](#)

[Schedules Run History Output](#)

[Scheduled Scan List Output](#)

[Vulnerability Scan Results](#)

[Compliance Scan Results](#)

[VM Recrypt Results \(Scan Statistics\)](#)

[VM Scan Summary Output](#)

[Scan Summary Output](#)

[Scanner List Output](#)

[PCI Scan Share Status Output](#)

[KnowledgeBase Output](#)

[Customized Vulnerability List Output](#)

[Map Report - Version 2](#)

[Map Report - Single Domain](#)

[Map Report List Output](#)

[EC2 Instance ID Scan Launch Output](#)

Scan List Output

API used

[<platform API server>](#)/api/2.0/fo/scan/?action=list

DTD for Scan List Output

[<platform API server>](#)/api/2.0/fo/scan/scan_list_output.dtd

A recent 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 CLIENT (ID,NAME)>
<!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

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".
/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/CLIENT	(ID,NAME)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT/ID (#PCDATA)	Id assigned to the client. (only for Consultant type subscriptions)

XPath	element specifications / notes
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT /NAME (#PCDATA)	Name of the client. (only for Consultant type subscriptions)
/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.
/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

API used

[platform API server](#)/api/2.0/fo/scan/scap/?action=list

DTD for SCAP Scan List Output

[platform API server](#)/api/2.0/fo/scan/qscap_scan_list_output.dtd

A recent 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

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.
/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.

XPath	element specifications / notes
/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.

Schedules Run History Output

API used

<platform API server>/api/2.0/fo/scan/schedules/runhistory

DTD

<platform API server>/api/2.0/fo/scan/schedules/runhistory/output.dtd

A recent DTD is shown below:

```
<!ELEMENT SCHEDULES_RUN_HISTORY (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 url encoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, SCHEDULE_LIST?)>
<!ELEMENT SCHEDULE_LIST (SCHEDULE+)>
<!ELEMENT SCHEDULE (SCHEDULE_ID, SCHEDULE_RUN_HISTORY?)>
<!ATTLIST SCHEDULE id CDATA #IMPLIED>
<!ELEMENT SCHEDULE_ID (#PCDATA)>
<!ELEMENT SCHEDULE_RUN_HISTORY (SCHEDULE_RUN+)>
<!ELEMENT SCHEDULE_RUN ((SCHEDULE_RUN_INFO?, SCAN_LAUNCH_INFO?)+)>
<!ELEMENT SCHEDULE_RUN_INFO (ACTION_TEXT)>
<!ELEMENT ACTION_TEXT (#PCDATA)>
<!ELEMENT SCAN_LAUNCH_INFO (SCAN_ID, SCAN_REFERENCE, LAUNCH_DATETIME,
TITLE, TARGET, SCAN_TYPE?, STATUS, DURATION, NBHOST, SUBSCRIPTION_ID,
OPTION_PROFILE_TITLE, IS_PROCESSED, CONNECTOR_UUID?, ENDPOINT_UUID?)>
<!ELEMENT SCAN_ID (#PCDATA)>
<!ELEMENT SCAN_REFERENCE (#PCDATA)>
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TARGET (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT DURATION (#PCDATA)>
<!ELEMENT NBHOST (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ELEMENT IS_PROCESSED (#PCDATA)>
<!ELEMENT CONNECTOR_UUID (#PCDATA)>
<!ELEMENT ENDPOINT_UUID (#PCDATA)>
<!-- EOF -->
```

XPaths for Schedules Run History Output

XPath	element specifications / notes
/SCHEDULES_RUN_HISTORY (REQUEST?,RESPONSE)	
/SCHEDULES_RUN_HISTORY/REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)	
/SCHEDULES_RUN_HISTORY/REQUEST/DATETIME(#PCDATA)	The date and time of the request.
/SCHEDULES_RUN_HISTORY/REQUEST/USER_LOGIN(#PCDATA)	The user login ID for the user who owns the scan schedule.
/SCHEDULES_RUN_HISTORY/REQUEST/RESOURCE(#PCDATA)	The resource specified for the request.
/SCHEDULES_RUN_HISTORY/REQUEST/PARAM_LIST (PARAM+)	
/SCHEDULES_RUN_HISTORY/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCHEDULES_RUN_HISTORY/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCHEDULES_RUN_HISTORY/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/SCHEDULES_RUN_HISTORY/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/SCHEDULES_RUN_HISTORY/RESPONSE (DATETIME, SCHEDULE_LIST?)	
/SCHEDULES_RUN_HISTORY/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST (SCHEDULE+)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE (SCHEDULE_ID, SCHEDULE_RUN_HISTORY?)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_ID (#PCDATA)	The schedule ID.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY (SCHEDULE_RUN+)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN ((SCHEDULE_RUN_INFO?, SCAN_LAUNCH_INFO?)+)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCHEDULE_RUN_INFO (ACTION_TEXT)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCHEDULE_RUN_INFO/ACTION_TEXT (#PCDATA)	The run history info if scan launch fails.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO (SCAN_ID, SCAN_REFERENCE, LAUNCH_DATETIME, TITLE, TARGET, SCAN_TYPE?, STATUS, DURATION, NBHOST, SUBSCRIPTION_ID, OPTION_PROFILE_TITLE, IS_PROCESSED, CONNECTOR_UUID?, ENDPOINT_UUID?)	
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/SCAN_ID (#PCDATA)	The scan ID.

XPath	element specifications / notes
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/SCAN_REFERENCE (#PCDATA)	The scan reference code.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/LAUNCH_DATETIME (#PCDATA)	The date and time when the scan was launched.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/TITLE (#PCDATA)	The scan title.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/TARGET (#PCDATA)	The scan target hosts.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/SCAN_TYPE (#PCDATA)	For a CertView VM scan this is set to "CertView".
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/STATUS (#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).
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/DURATION (#PCDATA)	The scan duration.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/NBHOST (#PCDATA)	The number of total hosts alive for the scan.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/SUBSCRIPTION_ID (#PCDATA)	ID of subscription where schedule is defined.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/OPTION_PROFILE_TITLE (#PCDATA)	The title of the option profile used.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/IS_PROCESSED (#PCDATA)	The scan processed status.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/CONNECTOR_UUID (#PCDATA)	The connector uuid for the AWS integration used for the EC2 scan.
/SCHEDULES_RUN_HISTORY/RESPONSE/SCHEDULE_LIST/SCHEDULE/SCHEDULE_RUN_HISTORY/SCHEDULE_RUN/SCAN_LAUNCH_INFO/ENDPOINT_UUID (#PCDATA)	The endpoint uuid for the AWS integration used for the EC2 scan.

Scheduled Scan List Output

API used

[<platform API server>/api/2.0/fo/schedule/scan/?action=list](#)

DTD for Scheduled Scan List Output

[<platform API server>/api/2.0/fo/schedule/scan/schedule_scan_list_output.dtd](#)

A recent 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?, ELB_DNS, OPTION_PROFILE?, PROCESSING_PRIORITY?,
SCHEDULE, NOTIFICATIONS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT CLIENT (ID,NAME)>
<!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,
USE_IP_NT_RANGE_TAGS_INCLUDE, USE_IP_NT_RANGE_TAGS_EXCLUDE?)>
<!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 USE_IP_NT_RANGE_TAGS_INCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS_EXCLUDE (#PCDATA)>
<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ELEMENT USER_ENTERED_IPS (RANGE+)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
<!ELEMENT ELB_DNS (DNS+)>
<!ELEMENT DNS (#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? LAUNCH_DELAY?,
LAUNCH_SKIP?, DEACTIVATE_SCHEDULE?, DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT LAUNCH_DELAY (MESSAGE)>
<!ELEMENT LAUNCH_SKIP (MESSAGE)>
<!ELEMENT DEACTIVATE_SCHEDULE (MESSAGE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>

```

XPaths for Scheduled Scan List Output

XPath	element specifications / notes
/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)

XPath	element specifications / notes
/SCHEDULE_SCAN_LIST_OUTPUT/REQUEST/RESOURCE (#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?, ELB_DNS?, 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.
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT	(ID,NAME)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT/ID (#PCDATA)	Id assigned to the client. (only for Consultant type subscriptions)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT/NAME (#PCDATA)	Name of the client. (only for Consultant type subscriptions)
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/USER_LOGIN (#PCDATA)	The user login ID for the user who owns the scan schedule.
/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.

XPath	element specifications / notes
/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.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/CLOUD_DETAILS/ CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)	The element CLOUD_TARGET under CLOUD_DETAILS is optional as it only applies to AWS EC2 scans and does not apply to Azure scans.
/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.

XPath	element specifications / notes
/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, USE_IP_NT_RANGE_TAGS_INCLUDE, USE_IP_NT_RANGE_TAGS_EXCLUDE?)	
/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).
/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_INCLUDE (#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/ASSET_TAGS/USE_IP_NT_RANGE_TAGS_EXCLUDE (#PCDATA)	0 means select from all tags (tags with any tag rule). 1 means exclude all IP addresses defined in tags with the rule "IP address in Network Range(s)".

XPath	element specifications / notes
/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)". This parameter has been replaced by use_ip_nt_range_tags_include and use_ip_nt_range_tags_exclude parameters. The use_ip_nt_range_tag parameter is still supported.
/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/ELB_DNS (DNS+)	
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/ELB_DNS/ DNS (#PCDATA)	One or more load balancer DNS names to include in the scan job. Multiple values are comma separated.
/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: frequency_days frequency_days is required 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: frequency_weeks frequency_weeks is required for a scan that runs after some number of weeks (from 1 to 52)

XPath	element specifications / notes
attribute: weekdays	weekdays 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: frequency_months	frequency_months is <i>required</i> for a scan that runs after some number of months (from 1 to 12)
attribute: day_of_month	day_of_month is <i>implied</i> and, if present, indicates the scan runs on the Nth day of the month (from 1 to 31)
attribute: day_of_week	day_of_week 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: week_of_month	week_of_month 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.
/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)	

XPath	element specifications / notes
/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?, LAUNCH_DELAY?, LAUNCH_SKIP?, DEACTIVATE_SCHEDULE?, 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.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ LAUNCH_DELAY (MESSAGE)	A user-provided custom message added to the delay scan notification.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ LAUNCH_SKIP (MESSAGE)	A user-provided custom message added to the skip scan notification.
/SCHEDULE_SCAN_LIST_OUTPUT/RESPONSE/SCHEDULE_SCAN_LIST/SCAN/NOTIFICATIONS/ DEACTIVATE_SCHEDULE (MESSAGE)	A user-provided custom message added to the deactivate schedule 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

API used

<platform API server>/api/2.0/fo/scan/?action=fetch

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

API used

[<platform API server>/api/2.0/fo/scan/compliance/?action=fetch](#)

DTD for Compliance Scan Result Output

[<platform API server>/api/2.0/fo/scan/compliance/compliance_scan_result_output.dtd](#)

A recent 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?, FQDNS?, 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)*>
<!ELEMENT FQDNS (FQDN+)>
<!ELEMENT FQDN (#PCDATA)>
```

```

<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANER) -->
<!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, NETWORK)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>

<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?,
AUTHENTICATION?, OS_AUTH_BASED_TECHNOLOGY_LIST?,
AUTH_DISCOVERY_INSTANCE_LIST?, AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?,
AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED?)>
<!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 OS_AUTH_BASED_TECHNOLOGY_LIST (OS_AUTH_BASED_TECHNOLOGY*)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY (TECHNOLOGY_FAMILY,
TECHNOLOGY_INSTANCE_LIST*)>
<!ELEMENT TECHNOLOGY_FAMILY (#PCDATA)>
<!ELEMENT TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY_INSTANCE+)>
<!ELEMENT TECHNOLOGY_INSTANCE (TECHNOLOGY, INSTANCE_INFO_LIST*, IP)>
<!ELEMENT INSTANCE_INFO_LIST (INSTANCE_INFO*)>
<!ELEMENT TECHNOLOGY (#PCDATA)>

```

```

<!ELEMENT INSTANCE_INFO (#PCDATA)>
<!-- ATTLIST INSTANCE_INFO key CDATA #IMPLIED -->

<!-- ELEMENT AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*) -->
<!-- ELEMENT AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?, IP) -->

<!-- ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST
(AUTH_DISCOVERY_INSTANCE_NOT_FOUND*) -->
<!-- ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP) -->

<!-- ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED (AUTH_TYPE_LIST*) -->
<!-- ELEMENT AUTH_TYPE_LIST (AUTH_TYPE*) -->

<!-- ELEMENT AUTH_PARAM_LIST (AUTH_PARAM+) -->
<!-- ELEMENT AUTH_TYPE (#PCDATA) -->
<!-- ELEMENT AUTH_PARAM (#PCDATA) -->
<!-- ATTLIST AUTH_PARAM name CDATA #IMPLIED -->

<!-- ELEMENT FAILED (IP, INSTANCE?) -->
<!-- ELEMENT SUCCESS (IP, INSTANCE?) -->
<!-- ELEMENT INSUFFICIENT (IP, INSTANCE?) -->
<!-- EOF -->

```

XPaths for Compliance Scan Result 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.

XPath	element specifications / notes
/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?)
/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)

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/FQDNS (FQDN+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/HEADER/FQDNS/FQDN (#PCDATA)	The target FQDN for a compliance scan.
/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, NETWORK)	
/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_FAILED/HOST_INFO/NETWORK (#PCDATA)	Network information for a host that failed authentication. You will see this element in the API output when the Network Support feature is enabled.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT (HOST_INFO)	

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/AUTH_SCAN_ISSUES/AUTH_SCAN_INSUFFICIENT/HOST_INFO	(DNS, IP, NETBIOS, INSTANCE, CAUSE)
/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?, OS_AUTH_BASED_TECHNOLOGY_LIST?, AUTH_DISCOVERY_INSTANCE_LIST?, AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?, AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED?)
/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.

XPath	element specifications / notes
/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)	
/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.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION (AUTH+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION/AUTH (TYPE?, (FAILED SUCCESS INSUFFICIENT)+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION/AUTH/TYPE (#PCDATA)	The authentication type.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION/AUTH/FAILED (IP,INSTANCE?)	A list of IP addresses with failed authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION/AUTH/SUCCESS (IP,INSTANCE?)	A list of IP addresses with successful authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTHENTICATION/AUTH/INSUFFICIENT (IP,INSTANCE?)	A list of IP addresses with insufficient privileges for authentication.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST (OS_AUTH_BASED_TECHNOLOGY*)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST (TECHNOLOGY_FAMILY, TECHNOLOGY_INSTANCE_LIST*)	

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST /TECHNOLOGY_FAMILY (#PCDATA)	The technology family of the discovered instance.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST/TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY, INSTANCE_INFO_LIST*, IP)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST/TECHNOLOGY_INSTANCE_LIST/TECHNOLOGY (#PCDATA)	Technology of the instance.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST/TECHNOLOGY_INSTANCE_LIST/INSTANCE_INFO_LIST (INSTANCE_INFO, INSTANCE_INFO key CDATA)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST/TECHNOLOGY_INSTANCE_LIST/INSTANCE_INFO_LIST/INSTANCE_INFO (#PCDATA)	Information related to the instance.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/OS_AUTH_BASED_TECHNOLOGY_LIST/OS_AUTH_BASED_TECHNOLOGY_LIST/TECHNOLOGY_INSTANCE_LIST/INSTANCE_INFO_LIST/INSTANCE_INFO key CDATA (#IMPLIED)	
	Information related to the instance key.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST/AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?, IP)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST/AUTH_DISCOVERY_INSTANCE/AUTH_TYPE (#PCDATA)	The authentication types for instance discovery: Apache Web Server, IBM WebSphere App Server and Jboss Server.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST/AUTH_DISCOVERY_INSTANCE/AUTH_PARAM_LIST (AUTH_PARAM+)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST/AUTH_DISCOVERY_INSTANCE/AUTH_PARAM_LIST/AUTH_PARAM (#PCDATA)	The instance configuration parameters Apache: apache config file and apache control command. The instance configuration parameter IBM WebSphere: websphere Installation directory. The instance configuration parameters JBoss: jboss domain mode, jboss home path, jboss base path, jboss config directory path, jboss config file path, jboss config host file path. The instance configuration parameters Tomcat Server: apache tomcat home directory and apache tomcat base directory.
attribute: name	The parameter name (implied).
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/AUTH_DISCOVERY_INSTANCE_LIST/AUTH_DISCOVERY_INSTANCE/IP (#PCDATA)	The IP address with one or more discovered instances.

XPath	element specifications / notes
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_DISCOVERY_INSTANCE_NOT_FOUND*)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ AUTH_DISCOVERY_INSTANCE_NOT_FOUND/AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ AUTH_DISCOVERY_INSTANCE_NOT_FOUND/AUTH_DISCOVERY_INSTANCE_NOT_FOUND/ AUTH_TYPE (#PCDATA)	The authentication type for instance discovery: Apache Web Server, IBM WebSphere App Server, Jboss Server and Tomcat Server.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ AUTH_DISCOVERY_INSTANCE_NOT_FOUND/AUTH_DISCOVERY_INSTANCE_NOT_FOUND/IP (#PCDATA)	
	The IP address that was successfully scanned but no instances were found.
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED (AUTH_TYPE_LIST*)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED/ AUTH_TYPE_LIST (AUTH_TYPE*)	
/COMPLIANCE_SCAN_RESULT_OUTPUT/RESPONSE/COMPLIANCE_SCAN/APPENDIX/ ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED/ AUTH_TYPE_LIST/ AUTH_TYPE (#PCDATA)	The authentication types for which no instances are found on any scanned assets.

VM Recrypt Results (Scan Statistics)

API used

[platform API server](#)/api/2.0/fo/scan/stats/?action=list

DTD for VM Recrypt Results

[platform API server](#)/api/2.0/fo/scan/stats/vm_recrypt_results.dtd

A recent 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.

XPath	element specifications / notes
/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.
/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.

VM Scan Summary Output

API used

[<platform API server>](#)/api/2.0/fo/scan/vm/summary/?action=list

DTD for VM Scan Summary Output

[<platform API server>](#)/api/2.0/fo/scan/vm/summary/output.dtd

A recent DTD is shown below.

```
<!-- QUALYS VM SCAN_SUMMARY_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT SCAN_SUMMARY_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_SUMMARY_LIST?)>
<!ELEMENT SCAN_SUMMARY_LIST (SCAN_SUMMARY+)>
<!ELEMENT SCAN_SUMMARY (SCAN_REFERENCE,
SCAN_INPUT?,SCAN_DETAILS?,SCAN_RESULTS? )>
<!ELEMENT SCAN_REFERENCE (#PCDATA)>
<!ELEMENT SCAN_INPUT
(TITLE?,USER?,SCHEDULED?,SCAN_DATETIME?,SCAN_TYPE?,NETWORK?,OPTION_PROFIL
E?,TARGETS?)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USER (USERNAME)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SCHEDULED (#PCDATA)>
<!ELEMENT SCAN_DATETIME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT NETWORK (ID,NAME)>
<!ELEMENT OPTION_PROFILE (ID,NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT TARGETS (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?,
ASSET_GROUP_LIST?, ASSET_TAG_LIST?, EXCLUDED_IP_LIST?)>
<!ELEMENT IP_LIST (COUNT, IP_DATA?)>
<!ELEMENT EXCLUDED_IP_LIST (COUNT, IP_DATA?)>
<!ELEMENT IP_DATA (RANGES?, IP_CSV?)>
<!ELEMENT COUNT (#PCDATA)>
<!ELEMENT RANGES (RANGE+)>
<!ELEMENT RANGE (#PCDATA)>
```

```

<!ELEMENT IP_CSV (#PCDATA)>
<!ELEMENT DNS_LIST (COUNT, DNS_DATA)>
<!ELEMENT DNS_DATA (DNS_CSV)>
<!ELEMENT DNS_CSV (#PCDATA)>
<!ELEMENT NETBIOS_LIST (COUNT, NETBIOS_DATA)>
<!ELEMENT NETBIOS_DATA (NETBIOS_CSV)>
<!ELEMENT NETBIOS_CSV (#PCDATA)>
<!ELEMENT INSTANCE_ID_LIST (COUNT, INSTANCE_ID_DATA)>
<!ELEMENT INSTANCE_ID_DATA (INSTANCE_ID_CSV)>
<!ELEMENT INSTANCE_ID_CSV (#PCDATA)>
<!ELEMENT ASSET_GROUP_LIST (COUNT, ASSET_GROUP_DATA)>
<!ELEMENT ASSET_GROUP_DATA (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, NAME)>
<!ELEMENT ASSET_TAG_LIST (INCLUDE_TAG_LIST?, EXCLUDE_TAG_LIST?)>
<!ELEMENT INCLUDE_TAG_LIST (COUNT, INCLUDE_TAG_DATA)>
<!ELEMENT INCLUDE_TAG_DATA (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (ID, NAME)>
<!ELEMENT EXCLUDE_TAG_LIST (COUNT, EXCLUDE_TAG_DATA)>
<!ELEMENT EXCLUDE_TAG_DATA (ASSET_TAG+)>
<!ELEMENT SCAN_DETAILS (STATUS, LAUNCH_DATETIME, DURATION?)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>
<!ELEMENT DURATION (#PCDATA)>
<!ELEMENT SCAN_RESULTS (HOSTS?, DETECTIONS?)>
<!ELEMENT HOSTS (COUNT?, HOSTS_DATA)>
<!ELEMENT HOSTS_DATA
(SCANNED?, NOT_VULNERABLE?, CANCELLED?, DEAD?, EXCLUDED?, UNRESOLVED?, DUPLICAT
E?, BLOCKED?, ABORTED?, FAILED_SLICE_HOSTS?, EXCEEDED_SCAN_DURATION?)>
<!ELEMENT SCANNED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT NOT_VULNERABLE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT CANCELLED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT DEAD (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT EXCLUDED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT UNRESOLVED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT DUPLICATE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT BLOCKED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT ABORTED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT FAILED_SLICE_HOSTS (IPV4_LIST?, IPV6_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT EXCEEDED_SCAN_DURATION (IPV4_LIST?, IPV6_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT IPV4_LIST (COUNT, IPV4_DATA)>
<!ELEMENT IPV4_DATA (IPV4_CSV)>
<!ELEMENT IPV4_CSV (#PCDATA)>
<!ELEMENT IPV6_LIST (COUNT, IPV6_DATA)>
<!ELEMENT IPV6_DATA (IPV6_CSV)>
<!ELEMENT IPV6_CSV (#PCDATA)>
<!ELEMENT DETECTIONS (IG?, VULN?)>
<!ELEMENT IG (TOTAL_COUNT, COUNT_BY_SEVERITY)>

```

```
<!ELEMENT VULN (CONFIRMED,POTENTIAL)>
<!ELEMENT CONFIRMED (TOTAL_COUNT,COUNT_BY_SEVERITY)>
<!ELEMENT POTENTIAL (TOTAL_COUNT,COUNT_BY_SEVERITY)>
<!ELEMENT TOTAL_COUNT (#PCDATA)>
<!ELEMENT COUNT_BY_SEVERITY
(SEVERITY_1,SEVERITY_2,SEVERITY_3,SEVERITY_4,SEVERITY_5)>
<!ELEMENT SEVERITY_1 (#PCDATA)>
<!ELEMENT SEVERITY_2 (#PCDATA)>
<!ELEMENT SEVERITY_3 (#PCDATA)>
<!ELEMENT SEVERITY_4 (#PCDATA)>
<!ELEMENT SEVERITY_5 (#PCDATA)>
<!-- EOF -->
```

XPaths for VM Scan Summary Output

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT	(REQUEST?, RESPONSE)
/SCAN_SUMMARY_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCAN_SUMMARY_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/SCAN_SUMMARY_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/SCAN_SUMMARY_OUTPUT/RESPONSE	(DATETIME, SCAN_SUMMARY_LIST?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST	(SCAN_SUMMARY+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY	(SCAN_REFERENCE, SCAN_INPUT?, SCAN_DETAILS?, SCAN_RESULTS?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_REFERENCE	(#PCDATA) The scan reference ID.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT	(TITLE?,USER?,SCHEDULED?,SCAN_DATETIME?,SCAN_TYPE?,NETWORK?, OPTION_PROFILE?,TARGETS?)

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TITLE (#PCDATA)	The scan title.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/USER (USERNAME)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/USER/USER NAME (#PCDATA)	The user who launched the scan.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/SCHEDULED (#PCDATA)	Flag that indicates whether the scan was scheduled. 1 indicates the scan was scheduled. 0 indicates the scan was not scheduled.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/SCAN_DATE TIME (#PCDATA)	The date/time when the scan was launched.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/SCAN_TYPE (#PCDATA)	The type of scan.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/NETWORK (ID, NAME)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/NETWORK/ ID (#PCDATA)	The network ID.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/NETWORK/ NAME (#PCDATA)	The network name.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/OPTION_PR OFILE (ID, NAME)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/OPTION_PR OFILE/ID (#PCDATA)	The ID of the option profile used for the scan.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/OPTION_PR OFILE/NAME (#PCDATA)	The name of the option profile used for the scan.

Targets

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS	(IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?, ASSET_GROUP_LIST?, ASSET_TAG_LIST?, EXCLUDED_IP_LIST?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST	(COUNT, IP_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST/COUNT (#PCDATA)	The total number of IP addresses in the target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST/IP_DATA	(RANGES?, IP_CSV?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST/IP_DATA/RANGES	(RANGE+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST/IP_DATA/RANGES/RANGE (#PCDATA)	Target IP address ranges.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/IP_LIST/IP_DATA /IP_CSV (#PCDATA)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST	(COUNT, IP_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST/COUNT (#PCDATA)	The total number of excluded IP addresses in the target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST/IP_DATA	(RANGES?, IP_CSV?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST/IP_DATA/RANGES	(RANGE+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST/IP_DATA/RANGES/RANGE (#PCDATA)	Excluded IP address ranges.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/EXCLUDED_IP_LIST/IP_DATA /IP_CSV (#PCDATA)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/DNS_LIST	(COUNT, DNS_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/DNS_LIST/COUNT (#PCDATA)	

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/DNS_LIST/DNS_DATA	(DNS_CSV)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/DNS_LIST/DNS_DATA/DNS_CSV (#PCDATA)	The DNS names.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/NETBIOS_LIST	(COUNT, NETBIOS_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/NETBIOS_LIST/COUNT (#PCDATA)	The total number of NetBIOS assets included in the scan target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/NETBIOS_LIST/NETBIOS_DATA	(NETBIOS_CSV)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/NETBIOS_LIST/NETBIOS_DATA/NETBIOS_CSV (#PCDATA)	The NetBIOS names.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/INSTANCE_ID_LIST	(COUNT, INSTANCE_ID_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/INSTANCE_ID_LIST/COUNT (#PCDATA)	The total number of instance IDs included in the scan target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/INSTANCE_ID_LIST/INSTANCE_ID_DATA	(INSTANCE_ID_CSV)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/INSTANCE_ID_LIST/INSTANCE_ID_DATA/INSTANCE_ID_CSV (#PCDATA)	The list of instance IDs.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST	(COUNT, ASSET_GROUP_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST/COUNT (#PCDATA)	The total number of asset groups included in the scan target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST/ASSET_GROUP_DATA	(ASSET_GROUP+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST/ASSET_GROUP_DATA/ASSET_GROUP	(ID, NAME)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST/ASSET_GROUP_DATA/ASSET_GROUP/ID (#PCDATA)	

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_GROUP_LIST/ASSET_GROUP_DATA/ASSET_GROUP/NAME (#PCDATA)	The ID of the asset group.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST	The name of the asset group.
(INCLUDE_TAG_LIST?, EXCLUDE_TAG_LIST?)	
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST	(COUNT, INCLUDE_TAG_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST/COUNT (#PCDATA)	The total number of asset tags included in the scan target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST/INCLUDE_TAG_DATA	(ASSET_TAG+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST/INCLUDE_TAG_DATA/ASSET_TAG	(ID, NAME)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST/INCLUDE_TAG_DATA/ASSET_TAG/ID (#PCDATA)	The ID of the asset tag.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/INCLUDE_TAG_LIST/INCLUDE_TAG_DATA/ASSET_TAG/NAME (#PCDATA)	The name of the asset tag.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST	(COUNT, EXCLUDE_TAG_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST/COUNT (#PCDATA)	The total number of excluded asset tags in the scan target.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST/EXCLUDE_TAG_DATA	(ASSET_TAG+)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST/EXCLUDE_TAG_DATA/ASSET_TAG	(ID, NAME)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST/EXCLUDE_TAG_DATA/ASSET_TAG/ID (#PCDATA)	The ID of the excluded asset tag.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_INPUT/TARGETS/ASSET_TAG_LIST/EXCLUDE_TAG_LIST/EXCLUDE_TAG_DATA/ASSET_TAG/NAME (#PCDATA)	The name of the excluded asset tag.

Scan Details

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_DETAILS	(STATUS,LAUNCH_DATETIME,DURATION?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_DETAILS/STATUS (#PCDATA)	The scan status.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_DETAILS/LAUNCH_DATETIME (#PCDATA)	The date/time when the scan was launched.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_DETAILS/DURATION (#PCDATA)	The scan duration.

Scan Results

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS	(HOSTS?,DETECTIONS?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS	(COUNT?,HOSTS_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/COUNT (#PCDATA)	The total number of hosts included in the scan results.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA	(SCANNED?,NOT_VULNERABLE?,CANCELLED?,DEAD?,EXCLUDED?,UNRESOLVED?,DUPLICATE?,BLOCKED?,ABORTED?, FAILED_SLICE_HOSTS?, EXCEEDED_SCAN_DURATION?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/SCANNED	(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)
	Hosts that were successfully scanned.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/NOT_VULNERABLE	(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)
	Hosts that were found to be not vulnerable during host discovery without having to run a full scan.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/CANCELLED	(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)
	Hosts that were not scanned because the scan was cancelled.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/DEAD	(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

XPath

element specifications / notes

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/EXCLUDED

(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/UNRESOLVED

(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/DUPLICATE

(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/BLOCKED

(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/ABORTED

(IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)

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

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/FAILED_SLICE_HOSTS

(IPV4_LIST?, IPV6_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)

The scan failed for these hosts.

/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/EXCEEDED_SCAN_DURATION

(IPV4_LIST?, IPV6_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?)

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

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV4_LIST	(COUNT, IPV4_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV4_LIST/COUNT (#PCDATA)	The total number of IPv4 addresses in the scan results.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV4_LIST/IPV4_DATA	(IPV4_CSV)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV4_LIST/IPV4_DATA/IPV4_CSV (#PCDATA)	The list of IPv4 addresses.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV6_LIST	(COUNT, IPV6_DATA)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV6_LIST/COUNT (#PCDATA)	The total number of IPv6 addresses in the scan results
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV6_LIST/IPV6_DATA	(IPV6_CSV)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/HOSTS/HOSTS_DATA/.../IPV6_LIST/IPV6_DATA/IPV6_CSV (#PCDATA)	The list of IPv6 addresses
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS	(IG?,VULN?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG	(TOTAL_COUNT,COUNT_BY_SEVERITY)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG/TOTAL_COUNT (#PCDATA)	The total number of Information Gathered (IG) detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG/COUNT_BY_SEVERITY	(SEVERITY_1,SEVERITY_2,SEVERITY_3,SEVERITY_4,SEVERITY_5)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG/COUNT_BY_SEVERITY/SEVERITY_1 (#PCDATA)	The number of severity 1 Information Gathered detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG/COUNT_BY_SEVERITY/SEVERITY_2 (#PCDATA)	The number of severity 2 Information Gathered detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTIONS/IG/COUNT_BY_SEVERITY/SEVERITY_3 (#PCDATA)	The number of severity 3 Information Gathered detections.

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/IG/COUNT_BY_SEVERITY/SEVERITY_4 (#PCDATA)	The number of severity 4 Information Gathered detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/IG/COUNT_BY_SEVERITY/SEVERITY_5 (#PCDATA)	The number of severity 5 Information Gathered detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN	(CONFIRMED,POTENTIAL)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED	(TOTAL_COUNT,COUNT_BY_SEVERITY)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/TOTAL_COUNT (#PCDATA)	The total number of Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY	(SEVERITY_1,SEVERITY_2,SEVERITY_3,SEVERITY_4,SEVERITY_5)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY/SEVERITY_1 (#PCDATA)	The number of severity 1 Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY/SEVERITY_2 (#PCDATA)	The number of severity 2 Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY/SEVERITY_3 (#PCDATA)	The number of severity 3 Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY/SEVERITY_4 (#PCDATA)	The number of severity 4 Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/CONFIRMED/COUNT_BY_SEVERITY/SEVERITY_5 (#PCDATA)	The number of severity 5 Confirmed Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/POTENTIAL	(TOTAL_COUNT,COUNT_BY_SEVERITY)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/POTENTIAL/TOTAL_COUNT (#PCDATA)	The total number of Potential Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/POTENTIAL/COUNT_BY_SEVERITY	(SEVERITY_1,SEVERITY_2,SEVERITY_3,SEVERITY_4,SEVERITY_5)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTION/VULN/POTENTIAL/COUNT_BY_SEVERITY/SEVERITY_1 (#PCDATA)	The number of severity 1 Potential Vulnerability detections.

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTI NS/VULN/POTENTIAL/COUNT_BY_SEVERITY/SEVERITY_2 (#PCDATA)	The number of severity 2 Potential Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTI NS/VULN/POTENTIAL/COUNT_BY_SEVERITY/SEVERITY_3 (#PCDATA)	The number of severity 3 Potential Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTI NS/VULN/POTENTIAL/COUNT_BY_SEVERITY/SEVERITY_4 (#PCDATA)	The number of severity 4 Potential Vulnerability detections.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_RESULTS/DETECTI NS/VULN/POTENTIAL/COUNT_BY_SEVERITY/SEVERITY_5 (#PCDATA)	The number of severity 5 Potential Vulnerability detections.

Scan Summary Output

API used

[<platform API server>/api/2.0/fo/scan/summary/?action=list](#)

DTD for Scan Summary Output

[<platform API server>/api/2.0/fo/scan/summary/scan_summary_output.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS SCAN_SUMMARY_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT SCAN_SUMMARY_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_SUMMARY_LIST?)>
<!ELEMENT SCAN_SUMMARY_LIST (SCAN_SUMMARY*)>
<!ELEMENT SCAN_SUMMARY (SCAN_REF?, SCAN_DATE?, HOST_SUMMARY*)>
<!ELEMENT SCAN_REF (#PCDATA)>
<!ELEMENT SCAN_DATE (#PCDATA)>
<!ELEMENT HOST_SUMMARY (#PCDATA)>

<!ATTLIST HOST_SUMMARY category CDATA #IMPLIED>
<!ATTLIST HOST_SUMMARY tracking CDATA #IMPLIED>
```

<!-- EOF -->

XPaths for Scan Summary Output

XPath	element specifications / notes
/SCAN_SUMMARY_OUTPUT	(REQUEST?, RESPONSE)
/SCAN_SUMMARY_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCAN_SUMMARY_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/SCAN_SUMMARY_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/SCAN_SUMMARY_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.
/SCAN_SUMMARY_OUTPUT/RESPONSE	(DATETIME, SCAN_SUMMARY_LIST?)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST	(SCAN_SUMMARY*)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY	(SCAN_REF?, SCAN_DATE?, HOST_SUMMARY*)
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_REF	(#PCDATA) The scan reference ID.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/SCAN_DATE	(#PCDATA) The scan date.
/SCAN_SUMMARY_OUTPUT/RESPONSE/SCAN_SUMMARY_LIST/SCAN_SUMMARY/HOST_SUMMARY	(#PCDATA) The host(s) that were included in the target but not scanned for some reason.
attribute: category	The category/reason the host was not scanned (implied).
attribute: tracking	The host's tracking method (implied).

Scanner List Output

API used

[platform API server](#)/api/2.0/fo/scan/scanner/?action=list

DTD for Scanner List Output

[platform API server](#)/api/2.0/fo/scan/scanner/scanner_list_output.dtd

A recent DTD is shown below.

```
<!-- QUALYS SCANNER_LIST_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT IP_SCANNERS_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_SCANNERS_OUTPUT?)>
<!ELEMENT IP_SCANNERS_OUTPUT (IP_SCANNED*)>
<!ELEMENT IP_SCANNED (IP, SCAN_REF, SCAN_DATE, SCANNER_IDENTIFIER,
SCANNER_TYPE, ML_VERSION, VULNSIGS_VERSION)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT SCAN_REF (#PCDATA)>
<!ELEMENT SCAN_DATE (#PCDATA)>
<!ELEMENT SCANNER_IDENTIFIER (#PCDATA)>
<!ELEMENT SCANNER_TYPE (#PCDATA)>
<!ELEMENT ML_VERSION (#PCDATA)>
<!ELEMENT VULNSIGS_VERSION (#PCDATA)>

<!-- EOF -->
```

XPaths for Scanner List Output

XPath	element specifications / notes
/IP_SCANNERS_LIST_OUTPUT	(REQUEST?, RESPONSE)
/IP_SCANNERS_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/IP_SCANNERS_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.

XPath	element specifications / notes
/IP_SCANNERS_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/IP_SCANNERS_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/IP_SCANNERS_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/IP_SCANNERS_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/IP_SCANNERS_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/IP_SCANNERS_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/IP_SCANNERS_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/IP_SCANNERS_LIST_OUTPUT/RESPONSE (DATETIME, IP_SCANNERS_OUTPUT?)	
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT	(IP_SCANNED*)
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED	(IP, SCAN_REF, SCAN_DATE, SCANNER_IDENTIFIER, SCANNER_TYPE, ML_VERSION, VULNSIGS_VERSION)
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/IP (#PCDATA)	The scanned IP address.
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/SCAN_REF (#PCDATA)	The scan reference ID.
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/SCAN_DATE (#PCDATA)	The date of the scan.
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/SCANNER_IDENTIFIER (#PCDATA)	The scanner identifier (external scanner or scanner appliance name).
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/SCANNER_TYPE (#PCDATA)	The type of the scanner (extranet or appliance).
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/ML_VERSION (#PCDATA)	The scanning engine version currently installed on the scanner appliance.
/IP_SCANNERS_LIST_OUTPUT/RESPONSE/IP_SCANNERS_OUTPUT/IP_SCANNED/VULNSIGS_VERSION (#PCDATA)	The vulnerability signatures version currently installed on the scanner appliance.

PCI Scan Share Status Output

API used

<platform API server>/api/2.0/fo/scan/pci/?action=share

DTD for PCI Scan Share Status Output

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

A recent 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.

XPath	element specifications / notes
/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.

KnowledgeBase Output

API used

[<platform API server>](#)/api/2.0/fo/knowledge_base/vuln/?action=list

DTD for KnowledgeBase Output

[<platform API server>](#)/api/2.0/fo/knowledge_base/vuln/
knowledge_base_vuln_list_output.dtd

A recent DTD 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)>
        <!-- CATEGORY -->
        <!ELEMENT CATEGORY (#PCDATA)>
        <!-- DETECTION_INFO -->
        <!ELEMENT DETECTION_INFO (#PCDATA)>
        <!-- LAST_CUSTOMIZATION -->
        <!ELEMENT LAST_CUSTOMIZATION (DATETIME, USER_LOGIN?)>
        <!-- USER_LOGIN already defined (no USER_LOGIN for OVAL Vulns) -->
        <!-- LAST_SERVICE_MODIFICATION_DATETIME -->
        <!ELEMENT LAST_SERVICE_MODIFICATION_DATETIME (#PCDATA)>
        <!-- PUBLISHED_DATETIME -->
        <!ELEMENT PUBLISHED_DATETIME (#PCDATA)>
        <!-- BUGTRAQ_LIST -->
        <!ELEMENT BUGTRAQ_LIST (BUGTRAQ+)>
          <!-- 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?, VECTOR_STRING?, ACCESS?,
IMPACT?, AUTHENTICATION?,
EXPLOITABILITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?) -->
                    <!-- ELEMENT BASE (#PCDATA) -->
                        <!-- ATTLIST BASE source CDATA #IMPLIED -->
                    <!-- ELEMENT TEMPORAL (#PCDATA) -->
                    <!-- ELEMENT VECTOR_STRING (#PCDATA) -->
                    <!-- ELEMENT CVSS3_VERSION (#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?, VECTOR_STRING?,
CVSS3_VERSION?, ATTACK?, IMPACT?, PRIVILEGES_REQUIRED?,
USER_INTERACTION?, SCOPE?, EXPLOIT_CODE_MATURITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
        <!ELEMENT ATTACK (VECTOR?, COMPLEXITY?)>
        <!ELEMENT PRIVILEGES_REQUIRED (#PCDATA)>
        <!ELEMENT USER_INTERACTION (#PCDATA)>
        <!ELEMENT SCOPE (#PCDATA)>
        <!ELEMENT EXPLOIT_CODE_MATURITY (#PCDATA)>

        <!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

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 echo_request=1.)
/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 echo_request=1.)
/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 echo_request=1.)
/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 echo_request=1.)
/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 echo_request=1.
/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 echo_request=1.)
/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	(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?)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/QID (#PCDATA)	The vulnerability QID (Qualys ID), assigned by the service.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VULN_TYPE (#PCDATA)	

XPath

element specifications / notes

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).
/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.

XPath	element specifications / notes
/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 details=All.)
/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 details=All.)
/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.
/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.

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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?, VECTOR_STRING?, 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 details=All.)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_BASE (#PCDATA)	CVSS base score assigned to the vulnerability.
attribute: source	source 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/VECTOR_STRING (#PCDATA)	CVSS scores of individual metrics. See "CVSS Sub Metrics Mapping" below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/ACCESS (VECTOR?, COMPLEXITY?)	
/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)	

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/REMEDIATION_LEVEL (#PCDATA)	CVSS exploitability metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS/REPORT_CONFIDENCE (#PCDATA)	CVSS remediation level metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS_V3	CVSS report confidence metric. See “CVSS Sub Metrics Mapping” below.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS_V3	(BASE, TEMPORAL?, VECTOR_STRING?, CVSS3_VERSION?, ATTACK?, IMPACT?, PRIVILEGES_REQUIRED?, USER_INTERACTION?, SCOPE?, EXPLOIT_CODE_MATURITY?, 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 details=All.)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ CVSS_V3/CVSS3_VERSION (#PCDATA)	The CVSS3 version currently supported.
/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.
/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 show_pci_reasons=1.
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ THREAT_INTELLIGENCE (THREAT_INTEL+)	
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/ THREAT_INTELLIGENCE/THREAT_INTEL	Qualys Real-Time Threat Indicators (RTIs) associated with the vulnerability.
attribute: id	id is <i>required</i> and is a reference ID (CDATA) that corresponds to a Qualys Real-Time Threat Indicator (RTI).
/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 show_supported_modules_info=1.

XPath	element specifications / notes
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY	(REMOTE, AUTH_TYPE_LIST?, ADDITIONAL_INFO?)
/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/DISCOVERY/AUTH_TYPE_LIST	(ADDITIONAL_INFO+)
/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/AUTH_TYPE_LIST/ADDITIONAL_INFO	(#PCDATA)
	Provides additional information such as "Patch Available", "Exploit Available", "Malware Associated", "Not exploitable due to configuration", "Non-running services" for the requested data.
/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 v2 and v3.1 sub metric values, as returned in the KnowledgeBase output, and the CVSS v2 and v3.1 sub metric names, as defined by the CVSS standard, is provided below.

CVSS v2: Base Family

Metric Value	KnowledgeBase Output XML Element and Value
Access Vector (AV)	
Local (L)	<VECTOR>1</VECTOR>
Adjacent Network (A)	<VECTOR>2</VECTOR>
Network (N)	<VECTOR>3</VECTOR>
Access Complexity	
Low (L)	<COMPLEXITY>1</COMPLEXITY>
Medium (M)	<COMPLEXITY>2</COMPLEXITY>
High (H)	<COMPLEXITY>3</COMPLEXITY>
Authentication (Au)	
None (N)	<AUTHENTICATION>1</AUTHENTICATION>
Single (S)	<AUTHENTICATION>2</AUTHENTICATION>
Multiple (M)	<AUTHENTICATION>3</AUTHENTICATION>
Confidentiality Impact (C)	
None (N)	<CONFIDENTIALITY>1</CONFIDENTIALITY>
Partial (P)	<CONFIDENTIALITY>2</CONFIDENTIALITY>
Complete (C)	<CONFIDENTIALITY>3</CONFIDENTIALITY>
Integrity Impact (I)	
None (N)	<INTEGRITY>1</INTEGRITY>
Partial (P)	<INTEGRITY>2</INTEGRITY>
Complete (C)	<INTEGRITY>3</INTEGRITY>
Availability Impact (A)	
None (N)	<AVAILABILITY>1</AVAILABILITY>
Partial (P)	<AVAILABILITY>2</AVAILABILITY>
Complete (C)	<AVAILABILITY>3</AVAILABILITY>

CVSS v2: Temporal Metrics Family

Metric Value	KnowledgeBase Download XML Element and Value
Exploitability (E)	
Not Defined (ND)	<EXPLOITABILITY>0</EXPLOITABILITY>
Unproven (U)	<EXPLOITABILITY>1</EXPLOITABILITY>
Proof-of-Concept (POC)	<EXPLOITABILITY>2</EXPLOITABILITY>
Functional (F)	<EXPLOITABILITY>3</EXPLOITABILITY>
High (H)	<EXPLOITABILITY>4</EXPLOITABILITY>
Remediation Level (RL)	
Not Defined (ND)	<REMEDIATION_LEVEL>0</REMEDIATION_LEVEL>
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>
Report Confidence (RC)	
Not Defined (ND)	<REPORT_CONFIDENCE>0</REPORT_CONFIDENCE>
Unconfirmed (UC)	<REPORT_CONFIDENCE>1</REPORT_CONFIDENCE>
Uncorroborated (UR)	<REPORT_CONFIDENCE>2</REPORT_CONFIDENCE>
Confirmed (C)	<REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>

CVSS v3.1: Base Family

Metric Value	KnowledgeBase Output XML Element and Value
Attack Vector (AV)	
Network (N)	<VECTOR>1</VECTOR>
Adjacent Network (A)	<VECTOR>2</VECTOR>
Local (L)	<VECTOR>3</VECTOR>
Physical (P)	<VECTOR>4</VECTOR>
Attack Complexity (AC)	
Low (L)	<COMPLEXITY>1</COMPLEXITY>
High (H)	<COMPLEXITY>2</COMPLEXITY>
Privileges Required (PR)	
None (N)	<PRIVILEGES_REQUIRED>1</PRIVILEGES_REQUIRED>
Low (L)	<PRIVILEGES_REQUIRED>2</PRIVILEGES_REQUIRED>
High (H)	<PRIVILEGES_REQUIRED>3</PRIVILEGES_REQUIRED>
User Interaction (UI)	
None (N)	<USER_INTERACTION>1</USER_INTERACTION>
Required (R)	<USER_INTERACTION>2</USER_INTERACTION>
Scope	
Unchanged (U)	<SCOPE>1</SCOPE>
Changed (C)	<SCOPE>2</SCOPE>
Confidentiality Impact (C)	
None (N)	<CONFIDENTIALITY>1</CONFIDENTIALITY>
Low (L)	<CONFIDENTIALITY>2</CONFIDENTIALITY>
High (H)	<CONFIDENTIALITY>3</CONFIDENTIALITY>
Integrity Impact (I)	
None (N)	<INTEGRITY>1</INTEGRITY>
Low (L)	<INTEGRITY>2</INTEGRITY>
High (H)	<INTEGRITY>3</INTEGRITY>
Availability Impact (A)	
None (N)	<AVAILABILITY>1</AVAILABILITY>
Low (L)	<AVAILABILITY>2</AVAILABILITY>
High (H)	<AVAILABILITY>3</AVAILABILITY>

CVSS v3.1: Temporal Metrics Family

Metric Value	KnowledgeBase Download XML Element and Value
Exploit Code Maturity (E)	
Not Defined (X)	<EXPLOIT_CODE_MATURITY>0</EXPLOIT_CODE_MATURITY>
Unproven (U)	<EXPLOIT_CODE_MATURITY>1</EXPLOIT_CODE_MATURITY>
Proof-of-Concept (P)	<EXPLOIT_CODE_MATURITY>2</EXPLOIT_CODE_MATURITY>
Functional (F)	<EXPLOIT_CODE_MATURITY>3</EXPLOIT_CODE_MATURITY>
High (H)	<EXPLOIT_CODE_MATURITY>4</EXPLOIT_CODE_MATURITY>
Remediation Level (RL)	
Not Defined (X)	<REMEDIATION_LEVEL>0</REMEDIATION_LEVEL>
Official Fix (O)	<REMEDIATION_LEVEL>1</REMEDIATION_LEVEL>
Temporary Fix (T)	<REMEDIATION_LEVEL>2</REMEDIATION_LEVEL>
Workaround (W)	<REMEDIATION_LEVEL>3</REMEDIATION_LEVEL>
Unavailable (U)	<REMEDIATION_LEVEL>4</REMEDIATION_LEVEL>
Report Confidence (RC)	
Not Defined (X)	<REPORT_CONFIDENCE>0</REPORT_CONFIDENCE>
Unknown (U)	<REPORT_CONFIDENCE>1</REPORT_CONFIDENCE>
Reasonable (R)	<REPORT_CONFIDENCE>2</REPORT_CONFIDENCE>
Confirmed (C)	<REPORT_CONFIDENCE>3</REPORT_CONFIDENCE>

Customized Vulnerability List Output

API used

[platform API server](#)/api/2.0/fo/knowledge_base/vuln/?action=custom

DTD for Vulnerability List Output

[platform API server](#)/api/2.0/fo/knowledge_base/vuln/
kb_custom_vuln_list_output.dtd

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

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 echo_request=1.)
/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 echo_request=1..)
/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 echo_request=1..)
/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 echo_request=1..)
/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 echo_request=1..
/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 echo_request=1..)
/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).

Map Report - Version 2

API used

[platform API server](#)/msp/map-2.php

The map-2.php API returns live map results using the map-2.dtd. This is used for live map results only.

DTD for Map Report v2 Output

[platform API server](#)/map-2.dtd

A recent DTD is below.

```
<!-- QUALYS MAP-2 DTD -->

<!ELEMENT MAP_REQUEST (MAP*|ERROR*) >

<!-- value is the report ref -->
<!ELEMENT MAP (HEADER?, (IP+|ERROR)?)>

<!ATTLIST MAP
    value CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- INFORMATION ABOUT THE MAP -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?,
OPTION_PROFILE?)>

<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
    value CDATA #IMPLIED>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>
```

```

<!-- value is the IP -->
<!-- type is the kind of server : router, mail server ... -->
<!-- "port" is deprecated, replaced by "discovery" -->
<!ELEMENT IP ((PORT*,DISCOVERY*,LINK*)|LINK+)?>
<!-- ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    type CDATA #IMPLIED
    os CDATA #IMPLIED
    netbios CDATA #IMPLIED
    account CDATA #IMPLIED
    network CDATA #IMPLIED
    network_id CDATA #IMPLIED-->

<!-- value indicates an open port on a server (deprecated) -->
<!ELEMENT PORT (#PCDATA)*>
<!-- ATTLIST PORT
    value CDATA #REQUIRED-->

<!-- value indicates a method that discovered this machine -->
<!ELEMENT DISCOVERY (#PCDATA)*>
<!-- ATTLIST DISCOVERY
    method CDATA #REQUIRED-->

<!-- value of a link, indicates the need to go through a server to see -->
<!-- another (ie. gateway or router) -->
<!ELEMENT LINK EMPTY>
<!-- ATTLIST LINK
    value CDATA #REQUIRED-->

```

XPaths for Map Report v2 output

XPath	element specification / notes
/MAP	(HEADER?,(IP+ ERROR)?)
attribute: value	value is <i>implied</i> and, if present, is the reference number for the map
/MAP/ERROR	(#PCDATA)*
attribute: number	number is <i>implied</i> and, if present, is an error code
/MAP/HEADER	((KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?, OPTION_PROFILE?)

XPath	element specification / notes
/MAP/HEADER/KEY	(#PCDATA)*
attribute: value	value is <i>implied</i> and, if present, will be one of the following: - USERNAME..... The Qualys user login name for the user that initiated the map request. - COMPANY The company associated with the Qualys user. - DATE The date when the map was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" - TITLE A descriptive title. - TARGET The target domain. - NBHOST_TOTAL The total number of hosts included in the map. - DURATION The time it took to complete the map. - SCAN_HOST The IP address of the host that processed the map. - REPORT_TYPE..... The report type: "API" for an on-demand map request launched from the API, "On-demand" for an on-demand map request launched from the Qualys user interface, and "Scheduled" for a scheduled map. - OPTIONS..... The option profile applied to the map. Note that the options information provided may be incomplete. - DEFAULT_SCANNER. The value 1 indicates that the default scanner was enabled for the map. - ISCANNER_NAME The scanner appliance name or "external" (for external scanner) used for the map. - STATUS The job status of the map. - FINISHED - The scanner(s) have finished the map job, the map results were loaded onto the platform, and hosts were discovered. - NOHOSTALIVE - The scanner(s) have finished the map job, the map results were loaded onto the platform, and no devices were discovered. - LOADING - The scanner(s) have finished the map job, and the map results are being loaded onto the platform. - CANCELED - A user canceled the map, and the scanner(s) have stopped the map job. - ERROR - An error occurred during the map, and the map did not complete. - INTERRUPTED - The map was interrupted and did not complete.

XPath	element specification / notes
/MAP/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was specified as a map target.
/MAP/HEADER/USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)	
/MAP/HEADER/USER_ENTERED_DOMAINS/DOMAIN (#PCDATA)	
	A domain name entered as a target for the map.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK (RANGE+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE (START+, END+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/START (#PCDATA)	
	An IP address that represents the start of the netblock range.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/END (#PCDATA)	
	An IP address that represents the end of the netblock range.
/MAP/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/MAP/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that was applied to the map.
attribute: option_profile_default	option_profile_default is <i>implied</i> and, if present, is a code 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.
/MAP/IP	((PORT*,DISCOVERY*,LINK*) LINK+)?
attribute: value	value is <i>required</i> and is an IP address
attribute: name	name is <i>implied</i> and, if present, is the device's registered DNS host name
attribute: type	type is <i>implied</i> and, if present, will indicate a device type such as "router"
attribute: os	os is <i>implied</i> and, if present, is a string indicating the device's operating system
attribute: netbios	netbios is <i>implied</i> and, if present, is the device's Windows NetBIOS name
attribute: account	account is <i>implied</i> and, if present, will be the following: yes..... The user account allows the IP address to be scanned
attribute: network	network is <i>implied</i> and indicates network selected for the map
attribute: network_id	network_id is <i>implied</i> and identifies a network ID when the networks feature is enabled in the subscription

XPath	element specification / notes
/MAP/IP/DISCOVERY	(#PCDATA)
attribute: method	method is <i>required</i> and will be one of the following: DNS DNS lookup DNS Zone Transfer DNS zone transfer detected ICMP ICMP packets received from the host Reverse_DNS Reverse DNS lookup TCP Port [n] Open TCP port [number] TCP RST TCP reset packets received from the host TraceRoute Trace route UDP Port [n] Open UDP port [number] Other Protocol or ICMP IP packet received from the host whose protocol is not TCP, UDP, or ICMP Other TCP Ports TCP packet received containing source ports not in the list of probed ports
/MAP/IP/PORT	(#PCDATA)
attribute: value	value is <i>required</i> and will be one of the following: 21 FTP 22 SSH 23 Telnet 25 SMTP 53 DNS 80 HTTP 110 POP3 139 NetBios 443 HTTPS Note: The PORT element no longer appears in map reports, including new reports and existing reports saved on the Qualys platform. The PORT element may appear in existing reports that you have saved locally.
/MAP/IP/LINK	EMPTY
attribute: value	value is <i>required</i>. If /MAP/IP[@type="router"] then there will be one /MAP/IP/LINK per host found in the domain that is served by that router. In this case, value will be the IP address of the host that this router serves. Otherwise, value is the IP address of the router that serves this host; if value is empty in this case, it means that the router was protected by a firewall or otherwise shielded from discovery.

No Devices Detected

When a network discovery does not detect any devices, live map results are returned. Live map results include header information and an error message. Live map results are not saved on the Qualys server and cannot be retrieved. Sample live map results are shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE MAP_REQUEST SYSTEM "https://qualysapi.qualys.com/map-2.dtd">
<!-- Map is running on: mydomain.com -->
<!-- keep-alive -->
<MAP_REQUEST>
  <MAP value="map/1112217109.26598">
    <HEADER>
```

```

<KEY value="USERNAME">username</KEY>
<KEY value="COMPANY"><![CDATA[My Company]]></KEY>
<KEY value="DATE">2005-03-30T21:11:48Z</KEY>
<KEY value="TITLE"><![CDATA[My Map]]></KEY>
<KEY value="TARGET">mydomain.com</KEY>
<KEY value="NBHOST_TOTAL">0</KEY>
<KEY value="DURATION">00:00:31</KEY>
<KEY value="SCAN_HOST">hostname (SCANNER 2.9.39-1, WEB 4.0.102-1,
VULNSIGS 1.10.74-1)</KEY>
<KEY value="REPORT_TYPE">API (default option profile)</KEY>
<KEY value="STATUS">NOHOSTALIVE</KEY>
<KEY value="OPTIONS"><![CDATA[Information gathering: All Hosts,
Perform live host sweep, Standard TCP port list, ICMP Host
Discovery]]></KEY>
  <USER_ENTERED_DOMAINS>
    <DOMAIN><![CDATA[mydomain.com]]></DOMAIN>
  </USER_ENTERED_DOMAINS>
  <OPTION_PROFILE>
    <OPTION_PROFILE_TITLE option_profile_default="1"><![CDATA[Initial
Options]]></OPTION_PROFILE_TITLE>
  </OPTION_PROFILE>
</HEADER>
</ERROR number="4503">No host found</ERROR>
</MAP>
</ERROR number="4503">No host found</ERROR>
</MAP_REQUEST>

```

Map Report - Single Domain

API used

[<platform API server>/msp/map.php](#)

The map.php API returns a map report which identifies hosts found during the network discovery, and the discovery methods used to identify services on the hosts found. When no hosts are found, empty results are returned.

DTD for Map Report - Single Domain

[<platform API server>/map.dtd](#)

A recent DTD is below.

```
<!-- QUALYS MAP DTD -->

<!-- value is the report ref -->
<!ELEMENT MAP (HEADER?, (IP+|ERROR)?) >
<!ATTLIST MAP
    value CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- INFORMATION ABOUT THE MAP -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?,
OPTION_PROFILE?)>

<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
    value CDATA #IMPLIED>

<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
    option_profile_default CDATA #IMPLIED
>

<!-- value is the IP -->
<!-- type is the kind of server : router, mail server ... -->
<!-- "port" is deprecated, replaced by "discovery" -->
```

```

<!ELEMENT IP ((PORT*,DISCOVERY*,LINK*)|LINK+)?>
<!ATTLIST IP
    value CDATA #REQUIRED
    name CDATA #IMPLIED
    type CDATA #IMPLIED
    os CDATA #IMPLIED
    account CDATA #IMPLIED
    netbios CDATA #IMPLIED

<!-- value indicates an open port on a server (deprecated) -->
<!ELEMENT PORT (#PCDATA)*>
<!ATTLIST PORT
    value CDATA #REQUIRED>

<!-- value indicates a method that successfully discovered this machine -
-->
<!ELEMENT DISCOVERY (#PCDATA)*>
<!ATTLIST DISCOVERY
    method CDATA #REQUIRED>

<!-- value of a link, indicates the need to go through a server to see -->
<!-- another (ie. gateway or router) -->
<!ELEMENT LINK EMPTY>
<!ATTLIST LINK
    value CDATA #REQUIRED>

```

XPaths for Map Report - Single Domain

XPath	element specification / notes
/MAP	(HEADER?,(IP+ ERROR)?)
attribute: value	value is <i>implied</i> and, if present, is the reference number for the map
/MAP/ERROR	(#PCDATA)*
attribute: number	number is <i>implied</i> and, if present, is an error code
/MAP/HEADER	(KEY)+

XPath	element specification / notes
/MAP/HEADER/KEY	(PCDATA)*
attribute: value	value is <i>implied</i> and, if present, will be one of the following:
	USERNAME..... The Qualys user login name for the user that initiated the map request. COMPANY The company associated with the Qualys user. DATE The date when the map was started. The date appears in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z" TITLE A descriptive title. When the user specifies a title for the map request, the user-supplied title appears. When unspecified, a standard title is assigned. TARGET The target domain. NBHOST_TOTAL The total number of hosts included in the map. DURATION The time it took to complete the map. SCAN_HOST The IP address of the host that processed the map. REPORT_TYPE..... The report type: "API" for an on-demand map request launched from the API, "On-demand" for an on-demand map request launched from the Qualys user interface, and "Scheduled" for a scheduled map. OPTIONS..... The option profile applied to the map. Note that the options information provided may be incomplete. DEFAULT_SCANNER. The value 1 indicates that the default scanner was enabled for the map. ISCANNER_NAME The name of the scanner appliance applied to the map. STATUS The job status of the map. FINISHED The scanner(s) have finished the map job, the map results were loaded onto the platform, and hosts were discovered. NOHOSTALIVE The scanner(s) have finished the map job, the map results were loaded onto the platform, and no devices were discovered. LOADING The scanner(s) have finished the map job, and the map results are being loaded onto the platform. CANCELED A user canceled the map, and the scanner(s) have stopped the map job. ERROR An error occurred during the map, and the map did not complete. INTERRUPTED The map was interrupted and did not complete.

XPath	element specification / notes
/MAP/HEADER/ASSET_GROUPS (ASSET_GROUP+)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP (ASSET_GROUP_TITLE)	
/MAP/HEADER/ASSET_GROUPS/ASSET_GROUP/ASSET_GROUP_TITLE (#PCDATA)	
	The title of an asset group that was specified as a map target.
/MAP/HEADER/USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)	
/MAP/HEADER/USER_ENTERED_DOMAINS/DOMAIN (#PCDATA)	
	A domain name entered as a target for the map.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK (RANGE+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE (START+, END+)	
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/START (#PCDATA)	
	An IP address that represents the start of the netblock range.
/MAP/HEADER/USER_ENTERED_DOMAINS/NETBLOCK/RANGE/END (#PCDATA)	
	An IP address that represents the end of the netblock range.
/MAP/HEADER/OPTION_PROFILE (OPTION_PROFILE_TITLE)	
/MAP/HEADER/OPTION_PROFILE/OPTION_PROFILE_TITLE (#PCDATA)	
	The title of the option profile, as defined in the Qualys user interface, that was applied to the map.
attribute: option_profile_default	option_profile_default is <i>implied</i> and, if present, is a code 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.
/MAP/IP	(PORT*, DISCOVERY*, LINK*) LINK+) ?
attribute: value	value is <i>required</i> and is an IP address
attribute: name	name is <i>implied</i> and, if present, is an Internet host name
attribute: type	type is <i>implied</i> and, if present, will indicate a device type such as “router”
attribute: os	os is <i>implied</i> and, if present, is a string indicating the device’s operating system
attribute: account	account is <i>implied</i> and, if present, will be the following: yes..... The user account allows the IP address to be scanned
attribute: netbios	netbios is <i>implied</i> and, if present, is the device’s Windows NetBIOS name
/MAP/IP/DISCOVERY	(#PCDATA)
attribute: method	method is <i>required</i> and will be one of the following: DNS DNS lookup DNS Zone Transfer DNS zone transfer detected ICMP ICMP packets received from the host Reverse_DNS Reverse DNS lookup TCP Port [n] Open TCP port [number] TCP_RST TCP reset packets received from the host TraceRoute Trace route UDP Port [n] Open UDP port [number] Other Protocol or ICMP IP packet received from the host whose protocol is not TCP, UDP, or ICMP Other TCP Ports TCP packet received containing source ports not in the list of probed ports

XPath	element specification / notes
/MAP/IP/PORT	(#PCDATA)
attribute: value	value is <i>required</i> and will be one of the following: 21 FTP 22 SSH 23 Telnet 25 SMTP 53 DNS 80 HTTP 110 POP3 139 NetBios 443 HTTPS Note: The PORT element no longer appears in map reports, including new reports and existing reports saved on the Qualys platform. The PORT element may appear in existing reports that you have saved locally.
/MAP/IP/LINK	EMPTY
attribute: value	value is <i>required</i>. If /MAP/IP[@type="router"] then there will be one /MAP/IP/LINK per host found in the domain that is served by that router. In this case, value will be the IP address of the host that this router serves. Otherwise, value is the IP address of the router that serves this host; if value is empty in this case, it means that the router was protected by a firewall or otherwise shielded from discovery.

Map Report List Output

API used

[<platform API server>/msp/map_report_list.php](#)

DTD for Map Report List Output

[<platform API server>/map_report_lists.dtd](#)

A recent DTD is below.

```
<!-- QUALYS MAP_REPORT_LIST DTD -->

<!ELEMENT MAP_REPORT_LIST (ERROR | MAP_REPORT*)>
<!ATTLIST MAP_REPORT_LIST
    user CDATA #REQUIRED
    from CDATA #REQUIRED
    to CDATA #REQUIRED
    with_domain CDATA #IMPLIED>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT MAP_REPORT (TITLE, ASSET_GROUPS?, OPTION_PROFILE?)>
<!ATTLIST MAP_REPORT
    ref CDATA #REQUIRED
    date CDATA #REQUIRED
    domain CDATA #REQUIRED
    status CDATA #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!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
>
<!-- EOF -->
```

XPaths for Map Report List

XPath	element specification / notes
/MAP_REPORT_LIST	(ERROR MAP_REPORT*)
attribute: user	user is <i>required</i> and is the Qualys user name.
attribute: from	from is <i>required</i> and is the oldest date in the available map reports, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT) like this: "2002-06-08T16:30:15Z"
attribute: to	to is <i>required</i> and is the newest date in the available map reports, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT)
attribute: with_domain	with_domain is <i>implied</i> and, if present, is a domain found in each of the map reports in the list
/MAP_REPORT_LIST/ERROR	(#PCDATA)*
attribute: number	number is <i>implied</i> and, if present, is an error code
/MAP_REPORT_LIST/MAP_REPORT	(TITLE, ASSET_GROUPS?, OPTION_PROFILE?)
attribute: ref	ref is <i>required</i> and is the reference, or key, for the map
attribute: date	date is <i>required</i> and is the date when the network discovery was performed, in YYYY-MM-DDTHH:MM:SSZ format (in UTC/GMT)
attribute: domain	domain is <i>required</i> and is the domain for which the map was produced
attribute: status	status is <i>required</i> and is the job status reported for the map. QUEUED - A user launched the map or the service started a map based on a map schedule. The map job is waiting to be distributed to scanner(s). RUNNING - The scanner(s) are actively running the map job. LOADING - The scanner(s) finished the map job, and the map results are being loaded onto the platform. FINISHED - The scanner(s) have finished the map job, and the map results were loaded onto the platform. CANCELED - A user canceled the map, the scanner(s) have stopped the map job, and some results may be available. NOHOSTALIVE - The scanner(s) finished the map job, the map results were loaded onto the platform, and target hosts were down (not alive). ERROR - An error occurred during map, and the map did not complete. INTERRUPTED - The map was interrupted and did not complete.
/MAP_REPORT_LIST/MAP_REPORT/TITLE	(#PCDATA)*
	The map title.
/MAP_REPORT_LIST/MAP_REPORT/ASSET_GROUPS	(ASSET_GROUP+)

XPath	element specification / notes
/MAP_REPORT_LIST/MAP_REPORT/ASSET_GROUPS/ASSET_GROUP	(ASSET_GROUP_TITLE)
	(#PCDATA)
	The title of an asset group that was specified as a map target.
/MAP_REPORT_LIST/MAP_REPORT/OPTION_PROFILE	(OPTION_PROFILE_TITLE)
/MAP_REPORT_LIST/MAP_REPORT/OPTION_PROFILE/OPTION_PROFILE_TITLE	(#PCDATA)
	The title of the option profile that was applied to the map.
attribute:	
option_profile_default	option_profile_default is <i>implied</i> and, if present, specifies whether the option profile was defined as the default in the user account. A valid value is: 1 (option profile is the default), or 0 (option profile is not the default).

EC2 Instance ID Scan Launch Output

This is a DTD for the Scan Launch output. You can use it when launching the EC2 scan and specify EC2 instance IDs as part of the scan target, we can identify and skip any invalid instances and continue the scan on the valid instances.

DTD for EC2 Instance ID Scan Launch Output

<platform>/api/2.0/fo/scan/dtd/launch_output.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, NOTIFICATION?, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT NOTIFICATION (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
<!-- EOF -->
```

XPaths for EC2 Instance ID Scan Launch

XPath	element specifications / notes
/SCAN_LAUNCH_OUTPUT	(REQUEST?, RESPONSE)
/SCAN_LAUNCH_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCAN_LAUNCH_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/SCAN_LAUNCH_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/SCAN_LAUNCH_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/SCAN_LAUNCH_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/SCAN_LAUNCH_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/SCAN_LAUNCH_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/SCAN_LAUNCH_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	

XPath	element specifications / notes
/SCAN_LAUNCH_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The input parameter value.
/SCAN_LAUNCH_OUTPUT/RESPONSE	The POST data, if any.
(DATETIME, CODE?, TEXT, NOTIFICATION?, ITEM LIST?)	
/SCAN_LAUNCH_OUTPUT/CODE (#PCDATA)	
	The POST data, if any.
/SCAN_LAUNCH_OUTPUT/TEXT (#PCDATA)	
	The POST data, if any.
/SCAN_LAUNCH_OUTPUT/NOTIFICATION (#PCDATA)	
	The user will receive scan launch output notification message.
/SCAN_LAUNCH_OUTPUT/ITEM_LIST(ITEM+)	
/SCAN_LAUNCH_OUTPUT/ITEM (IKEY, VALUE*)	
	The scan launch output item key value.

New API: Domain V2 API DTD Output

API Used

[<platform API server>](#)/api/2.0/fo/asset/domain/with action=create, update, delete

DTD for Create/Update/Delete Domain Output

```
curl --location '<qualys_base_url>/api/2.0/simple_return.dtd'

<!-- QUALYS SIMPLE_RETURN DTD -->
<!-- $Revision$ -->
<!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*)>
<!-- EOF -->
```

API Used

[<platform API server>](#)/api/2.0/fo/asset/domain/with action=list

DTD for Domain List Output

```
curl --location
'<qualys_base_url>/api/2.0/fo/asset/domain/domain_list_output.dtd'

<!-- QUALYS DOMAIN LIST DTD -->
<!-- $Revision$ -->
<!ELEMENT DOMAIN (DOMAIN_NAME, DOMAIN_ID, NETWORK?, NETBLOCK?)*>
<!ELEMENT DOMAIN_LIST (DOMAIN*)>
<!ELEMENT DOMAIN_NAME (#PCDATA)>
<!ELEMENT DOMAIN_ID (#PCDATA)>
<!ELEMENT NETWORK (NETWORK_NAME, NETWORK_ID)>
<!ELEMENT NETWORK_NAME (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
```

<!ELEMENT NETBLOCK (RANGE+)>

<!ELEMENT RANGE (START, END)>

<!ELEMENT START (#PCDATA)>

<!ELEMENT END (#PCDATA)>

Chapter 3 - Scan Configuration XML

This section describes XML returned from Scan API requests for search lists, scanner appliances, option profiles.

[Scanner Appliance List Output](#)

[Scanner Appliance Create Output](#)

[Replace Scanner Appliance Output](#)

[Static Search List Output](#)

[Dynamic Search List Output](#)

[Option Profile Output](#)

[QID List Output](#)

Scanner Appliance List Output

API used

[platform API server](#)/api/2.0/fo/appliance/ with action=list

DTD for Scanner Appliance List Output

[platform API server](#)/api/2.0/fo/appliance/appliance_list_output.dtd

A recent 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 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?,
IPV6_ADDRESS?, IPV6_SLAAC?)-->
                        <!--ELEMENT IPV6_SLAAC EMPTY-->
        <!--ELEMENT STATIC_ROUTES (ROUTE*)-->
                <!--ELEMENT ROUTE (NAME, IP_ADDRESS?, NETMASK?, GATEWAY?,
IPV6_ADDRESS?, IPV6_NETWORK?, IPV6_GATEWAY?)-->
                        <!--ELEMENT IPV6_NETWORK (#PCDATA)-->
                        <!--ELEMENT IPV6_GATEWAY (#PCDATA)-->
        <!--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 CPU_INFO (#PCDATA) -->
<!-- ELEMENT MEMORY_INFO (#PCDATA) -->
<!-- ELEMENT REGION_INFO (#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

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 echo_request=1.)
/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 echo_request=1.)
/APPLIANCE_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA)

XPath

element specifications / notes

The resource specified for the request. (This element appears only when the API request includes the parameter echo_request=1.)

/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)	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.

XPath	element specifications / notes
/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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/INTERFACE (#PCDATA)	The network interface: "lan" or "wan". (Appears when output_mode=full. 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/NETMASK (#PCDATA)	The netmask value for the LAN or WAN interface. (Appears when output_mode=full. is specified in API request.)

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/INTERFACE_SETTINGS/ GATEWAY (#PCDATA)	The gateway IP address for the LAN or WAN interface. (Appears when output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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)	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?)	

XPath	element specifications / notes
/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).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/ INSTANCE_ZONE_TYPE (#PCDATA)	EC2 instance zone type. (Appears when output_mode=full 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 output_mode=full 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 output_mode=full is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/EC2_INFO/IP_ADDRESS_PRIVATE (#PCDATA)	EC2 instance private IP address. (Appears when output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full is specified in API request.
/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 output_mode=full 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 output_mode=full 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 output_mode=full is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/PROJECT_NAME (#PCDATA)	GCE instance project name. (Appears when output_mode=full 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 output_mode=full is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/GCE_INFO/INSTANCE_ZONE (#PCDATA)	GCE instance zone (Appears when output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full is specified in API request).
/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 output_mode=full 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 output_mode=full 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 output_mode=full is specified in API request).
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/USER_NAME, (#PCDATA)	Azure user name. (Appears when output_mode=full is specified in API request).

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/CLOUD_INFO/AZURE_INFO/INSTANCE_LOCATION (#PCDATA)	Azure instance location. (Appears when output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN	(ID, NAME, IP_ADDRESS?, NETMASK?, IPV6_ADDRESS?, IPV6_SLAAC?)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/ID (#PCDATA)	A VLAN ID. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/NAME	A VLAN name. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/IP_ADDRESS (#PCDATA)	A valid IPv4 address for a VLAN. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/NETMASK (#PCDATA)	A valid IPv4 netmask for a VLAN. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/IPV6_ADDRESS (#PCDATA)	A valid IPv6 address for a VLAN. (Appears when output_mode=full is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VLANS/VLAN/IPV6_SLAAC EMPTY	An empty value indicates that ipv6_auto was specified for auto-configuring IPv6 using SLAAC on the VLAN.
/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?, IPV6_ADDRESS?, IPV6_NETWORK?, IPV6_GATEWAY?)

XPath	element specifications / notes
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/NAME (#PCDATA)	A static route name. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/IP_ADDRESS (#PCDATA)	A target IPv4 network for a static route. (Appears when output_mode=full. 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/GATEWAY (#PCDATA)	A gateway IPv4 address for a static route. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/IPV6_ADDRESS (#PCDATA)	A valid IPv6 address for a static route. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/IPV6_NETWORK (#PCDATA)	A target IPv6 network for a static route. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/STATIC_ROUTES/ROUTE/IPV6_GATEWAY (#PCDATA)	A gateway IPv6 address for a static route. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ML_LATEST (#PCDATA)	The latest scanning engine version available. (Appears when output_mode=full. 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 output_mode=full. is specified in API request.)
attribute: updated	"yes" indicates the appliance is updated with the latest version.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/VULNSIGS_LATEST (#PCDATA)	The latest vulnerability signatures version available. (Appears when output_mode=full. 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 output_mode=full. 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 output_mode=full. is specified in API request.)

XPath	element specifications / notes
/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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/USER_LOGIN (#PCDATA)	The user login. (Appears when output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/HEARTBEATS_MISSED (#PCDATA)	The number of heartbeat checks missed. (Appears when output_mode=full. 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 output_mode=full. 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 output_mode=full. 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.

XPath	element specifications / notes
/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 output_mode=full. 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 output_mode=full. is specified in API request.)
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ELEMENT CPU_INFO (#PCDATA)	The processor details of the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ELEMENT MEMORY_INFO (#PCDATA)	The memory information of the scanner appliance.
/APPLIANCE_LIST_OUTPUT/RESPONSE/APPLIANCE_LIST/APPLIANCE/ELEMENT REGION_INFO (#PCDATA)	The region information of the scanner appliance.
/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

API used

<platform API server>/api/2.0/fo/appliance/ with action=create

DTD for Scanner Appliance Create Output

<platform API server>/api/2.0/fo/appliance/appliance_create_output.dtd

A recent DTD is 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

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 echo_request=1.)
/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 echo_request=1.)
/APPLIANCE_CREATE_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request. (This element appears only when the API request includes the parameter echo_request=1.)

XPath	element specifications / notes
/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 echo_request=1.)
/APPLIANCE_CREATE_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_CREATE_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_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.

Replace Scanner Appliance Output

API used

<platform API server>/api/2.0/fo/appliance/ with action=replace_iscanner

DTD for Replace Scanner Appliance Output

<platform API server>/api/2.0/fo/appliance/replace_iscanner/
replace_iscanner_output.dtd

A recent DTD is below.

```
<!-- QUALYS REPLACE_ISCANNER_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT SCANNER_REPLACE_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, NEW_SETTINGS?, SCHEDULED_SCANS?,
ASSET_GROUPS?, SUCCESS?)>

<!ELEMENT NEW_SETTINGS (#PCDATA)>
<!ELEMENT SCHEDULED_SCANS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT SUCCESS (#PCDATA)>

<!-- EOF -->

```

XPaths for Replace Scanner Appliance Output

XPath	element specifications / notes
/SCANNER_REPLACE_OUTPUT	(REQUEST?, RESPONSE)
/SCANNER_REPLACE_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/SCANNER_REPLACE_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/SCANNER_REPLACE_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/SCANNER_REPLACE_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/SCANNER_REPLACE_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/SCANNER_REPLACE_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/SCANNER_REPLACE_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) The input parameter name.
/SCANNER_REPLACE_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) The input parameter value.
/SCANNER_REPLACE_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data.
/SCANNER_REPLACE_OUTPUT/RESPONSE	(DATETIME, NEW_SETTINGS?, SCHEDULED_SCANS?, ASSET_GROUPS?, SUCCESS?)
/SCANNER_REPLACE_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the response.
/SCANNER_REPLACE_OUTPUT/RESPONSE/NEW_SETTINGS	(#PCDATA) The scanner appliance settings transferred from the old scanner appliance to the new scanner appliance.

XPath	element specifications / notes
/SCANNER_REPLACE_OUTPUT/RESPONSE/SCHEDULED_SCANS (#PCDATA)	The scheduled scans updated with the new scanner appliance.
/SCANNER_REPLACE_OUTPUT/RESPONSE/ASSET_GROUPS (#PCDATA)	The asset groups updated with the new scanner appliance.
/SCANNER_REPLACE_OUTPUT/RESPONSE/SUCCESS (#PCDATA)	The success message.

Static Search List Output

API used

[<platform API server>/api/2.0/fo/qid_search_list/static/?action=list](#)

DTD for Static Search List Output

[<platform API server>/api/2.0/fo/qid/search_list/static/static_list_output.dtd](#)

A recent DTD 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

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.
/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+)	

XPath	element specifications / notes
/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.
/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

API used

[<platform API server>](#)/api/2.0/fo/qid_search_list/dynamic/?action=list

DTD for Dynamic Search List Output

[<platform API server>](#)/api/2.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd

A recent DTD 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?, CVSS3_VERSION?, 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_IDS_FILTER (#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 CVSS3_VERSION (#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

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?, CVSS3_VERSION?, 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.
/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/CVSS3_VERSION (#PCDATA)	CVSS3 version that is currently supported.
/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/REPO RT_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/REPO RT_TEMPLATE/TITLE (#PCDATA)	Title of a report template where the search list is defined.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/ REMEDATION_POLICIES (REMEDATION_POLICY+)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/ REMEDATION_POLICIES/REMEDATION_POLICY (ID, TITLE)	
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/ REMEDATION_POLICIES/REMEDATION_POLICY/ID (#PCDATA)	ID of a remediation policy where the search list is defined.
/DYNAMIC_SEARCH_LIST_OUTPUT/RESPONSE/DYNAMIC_LISTS/DYNAMIC_LIST/ REMEDATION_POLICIES/REMEDATION_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 Output

API used

<platform API server>/api/2.0/fo/subscription/option_profile/?action=export

<platform API server>/api/2.0/fo/subscription/option_profile/?action=import

DTD for Option Profile Output

<platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

A recent DTD is shown below.

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?, OS_BASED_INSTANCE_DISC_COLLECTION?)>
<!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?,
AUTHENTICATION_LEAST_PRIVILEGE?, ADDL_CERT_DETECTION?,
DISSOLVABLE_AGENT?, SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?,
SYSTEM_AUTH_RECORD?, LITE_OS_SCAN?, CUSTOM_HTTP_HEADER?,
HOST_ALIVE_TESTING?, ETHERNET_IP_PROBING?, FILE_INTEGRITY_MONITORING?,
CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?,
MAX_SCAN_DURATION_PER_ASSET?)>

<!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?,
HOST_CGI_CHECKS?, MAX_CGI_CHECKS?, MAX_TARGETS_PER_SLICE?,
MAX_NUMBER_OF_TARGETS?, CONF_SCAN_LIMITED_CONNECTIVITY?,
SKIP_PRE_SCANNING?, SCAN_MULTIPLE_SLICES_PER_SCANNER?)>
<!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 HOST_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_TARGETS_PER_SLICE (#PCDATA)>
<!ELEMENT MAX_NUMBER_OF_TARGETS (#PCDATA)>
<!ELEMENT CONF_SCAN_LIMITED_CONNECTIVITY (#PCDATA)>
<!ELEMENT SKIP_PRE_SCANNING (#PCDATA)>
<!ELEMENT SCAN_MULTIPLE_SLICES_PER_SCANNER (#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 MAX_SCAN_DURATION_PER_ASSET (#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 AUTHENTICATION_LEAST_PRIVILEGE (#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 SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)>

<!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?,
SAPIQ?, DB2?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)>

<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
IBM_WAS_DISCOVERY_MODE?, ORACLE_AUTHENTICATION_TEMPLATE?,
MONGODB_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT AUTHENTICATION_TYPE_LIST (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT IBM_WAS_DISCOVERY_MODE (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE (ID, TITLE)>
<!ELEMENT MONGODB_AUTHENTICATION_TEMPLATE (ID, TITLE)>
<!ELEMENT INCLUDE_SYSTEM_AUTH

```

```
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#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 ETHERNET_IP_PROBING (#PCDATA)>

<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
<!ELEMENT AUTO_UPDATE_EXPECTED_VALUE (#PCDATA)>

<!ELEMENT CONTROL_TYPES (FIM_CONTROLS_ENABLED?,
CUSTOM_WMI_QUERY_CHECKS?)>
<!ELEMENT FIM_CONTROLS_ENABLED (#PCDATA)>
<!ELEMENT CUSTOM_WMI_QUERY_CHECKS (#PCDATA)>
<!ELEMENT DO_NOT_OVERWRITE_OS (#PCDATA)>
<!ELEMENT TEST_AUTHENTICATION (#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)>

<!ELEMENT INSTANCE_DATA_COLLECTION (DATABASES?)>
<!ELEMENT DATABASES (AUTHENTICATION_TYPES_LIST)>
<!ELEMENT AUTHENTICATION_TYPES_LIST (AUTHENTICATION_TYPE+)>

<!ELEMENT OS_BASED_INSTANCE_DISC_COLLECTION (TECHNOLOGIES?)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (#PCDATA)>

```

XPath descriptions

XPath	element specifications / notes
/OPTION_PROFILES	(OPTION_PROFILE?)
/OPTION_PROFILES/OPTION_PROFILE	(BASIC_INFO, SCAN, MAP?, ADDITIONAL, INSTANCE_DATA_COLLECTION?, OS_BASED_INSTANCE_DISC_COLLECTION?)
/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)	

XPath

element specifications / notes

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.
/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?, AUTHENTICATION_LEAST_PRIVILEGE?, ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?, SYSTEM_AUTH_RECORD?, LITE_OS_SCAN?, CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?, ETHERNET_IP_PROBING?, FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?, MAX_SCAN_DURATION_PER_ASSET?)
/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)	

XPath

element specifications / notes

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)?)
/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)	

XPath

element specifications / notes

(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)

(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.

XPath	element specifications / notes
/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)	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/TITLE (#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/TYPE (#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)	
/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.

XPath	element specifications / notes
/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 for the scan, which may include any of the following: Windows, Unix, Oracle, Oracle Listener, SNMP, VMware, DB2, HTTP, MySQL, Tomcat Server, MongoDB, Palo Alto Networks Firewall, Oracle WebLogic Server, Jboss Server, Sybase, etc.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/AUTHENTICATION_LEAST_PRIVILEGE (#PCDATA)	(VM only) Unix appears when the Authentication Least Privilege option is enabled for the Unix authentication type.
/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 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/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_DIRECTORY_SEARCH_ENABLE (#PCDATA)	(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).

XPath	element specifications / notes
/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/DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/MSSQL/DB_UDC_RESTRICTION (#PCDATA)	(PC only) (Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom MSSQL Database checks.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/MSSQL/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/ORACLE/DB_UDC_RESTRICTION (#PCDATA)	(PC only) (Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Oracle Database checks.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/ORACLE/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SYBASE/DB_UDC_RESTRICTION (#PCDATA)	(PC only) (Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom Sybase Database checks.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SYBASE/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.

XPath	element specifications / notes
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/POSTGRESQL/DB_UDC_RESTRICTION (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/POSTGRESQL/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SAPIQ/DB_UDC_RESTRICTION (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/SAPIQ/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/DB2/DB_UDC_RESTRICTION (#PCDATA)	(PC only) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks. The default value is 0.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/DATABASE_PREFERENCE_KEY/DB2/DB_UDC_LIMIT (#PCDATA)	(PC only) Provide a value to define the number of rows to be returned per scan. The default value is 256 and maximum allowed limit is 5000 rows.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION INCLUDE_SYSTEM_AUTH)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST, IBM_WAS_DISCOVERY_MODE, ORACLE_AUTHENTICATION_TEMPLATE)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/AUTHENTICATION_TYPE_LIST (AUTHENTICATION_TYPE+)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/AUTHENTICATION_TYPE_LIST/AUTHENTICATION_TYPE (#PCDATA)	(PC only) The option “Allow instance discovery and record creation” is enabled for Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle and MongoDB authentication types.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/IBM_WAS_DISCOVERY_MODE (#PCDATA)	(PC only) Specify ibm_was_discovery_mode with a value of “server_dir” to discover instances from the server directory or “installation_dir” to discover instances from the installation directory.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/ORACLE_AUTHENTICATION_TEMPLATE (ID, TITLE)	

XPath	element specifications / notes
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/ORACLE_AUTHENTICATION_TEMPLATE/ID (#PCDATA)	(PC only) The ID of the Oracle system record template selected when the option “Allow instance discovery and record creation” is enabled for Oracle authentication type.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/ORACLE_AUTHENTICATION_TEMPLATE/TITLE (#PCDATA)	(PC only) The title of the Oracle system record template selected when the option “Allow instance discovery and record creation” is enabled for Oracle authentication type.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION INCLUDE_SYSTEM_AUTH)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST, IBM_WAS_DISCOVERY_MODE, MONGODB_AUTHENTICATION_TEMPLATE)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/AUTHENTICATION_TYPE_LIST (AUTHENTICATION_TYPE+)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/AUTHENTICATION_TYPE_LIST/AUTHENTICATION_TYPE (#PCDATA)	(PC only) The option “Allow instance discovery and record creation” is enabled for Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server, Oracle and MongoDB authentication types.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/IBM_WAS_DISCOVERY_MODE (#PCDATA)	(PC only) Specify ibm_was_discovery_mode with a value of “server_dir” to discover instances from the server directory or “installation_dir” to discover instances from the installation directory.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/MONGODB_AUTHENTICATION_TEMPLATE (ID, TITLE)	
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/MONGODB_AUTHENTICATION_TEMPLATE/ID (#PCDATA)	(PC only) The ID of the MongoDB system record template selected when the option “Allow instance discovery and record creation” is enabled for MongoDB authentication type.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/ALLOW_AUTH_CREATION/MONGODB_AUTHENTICATION_TEMPLATE/TITLE (#PCDATA)	(PC only) The title of the MongoDB system record template selected when the option “Allow instance discovery and record creation” is enabled for MongoDB authentication type.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/INCLUDE_SYSTEM_AUTH (ON_DUPLICATE_USE_USER_AUTH ON_DUPLICATE_USE_SYSTEM_AUTH)	(PC only) A value of 0 for “Include system authentication” parameter indicates that user authentication record will be selected for authentication scan.
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/INCLUDE_SYSTEM_AUTH/ON_DUPLICATE_USE_USER_AUTH (#PCDATA)	(PC only) The option “Include system created authentication records in scans” is enabled, and a value of 1 indicates that the user created record will be used when there are 2 records for the same instance configuration.

XPath	element specifications / notes
/OPTION_PROFILES/OPTION_PROFILE/SCAN/SYSTEM_AUTH_RECORD/INCLUDE_SYSTEM_AUTH/ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)	(PC only) The option "Include system created authentication records in scans" is enabled, and a value of 1 indicates that the system created record will be used when there are 2 records for the same instance configuration.
/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/ETHERNET_IP_PROBING (#PCDATA)	This flag is for Qualys Internal Use only.
/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)	(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/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/SCAN/TEST_AUTHENTICATION (#PCDATA)	

XPath

element specifications / notes

(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 Test Authentication option is enabled or disabled.

/OPTION_PROFILES/OPTION_PROFILE/SCAN/MAX_SCAN_DURATION_PER_ASSET (#PCDATA)	(VM only) This specifies scan time limit configured in option profile. The minimum time is 30 minutes and maximum time is 48 hours.
(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)	(VM only) 1 means additional UDP ports defined; 0 means additional UDP ports not defined.
/OPTION_PROFILES/OPTION_PROFILE/MAP/UDP_PORTS/UDP_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)	

XPath

element specifications / notes

(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)	(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?)	

XPath	element specifications / notes
/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)	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.

XPath	element specifications / notes
/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.)
/OPTION_PROFILES/OPTION_PROFILE/INSTANCE_DATA_COLLECTION (DATABASES?)	
/OPTION_PROFILES/OPTION_PROFILE/INSTANCE_DATA_COLLECTION/DATABASES (AUTHENTICATION_TYPES_LIST)	
/OPTION_PROFILES/OPTION_PROFILE/INSTANCE_DATA_COLLECTION/DATABASES/AUTHENTICATION_TYPE S_LIST/AUTHENTICATION_TYPE (AUTHENTICATION_TYPE+)	
	Database instance type for which OS-auth-based data collection is enabled.
/OPTION_PROFILES/OPTION_PROFILE/OS_BASED_INSTANCE_DISC_COLLECTION (TECHNOLOGIES?)	
/OPTION_PROFILES/OPTION_PROFILE/OS_BASED_INSTANCE_DISC_COLLECTION/TECHNOLOGIES (TECHNOLOGY+)	
/OPTION_PROFILES/OPTION_PROFILE/OS_BASED_INSTANCE_DISC_COLLECTION/TECHNOLOGIES/TECHNOLOGY (#PCDATA)	
	OS-based instance discovery technologies for which OS-auth-based data collection is enabled.

QID List Output

API used

<platform API server>/api/2.0/fo/knowledge_base/vuln with action=list

DTD for SCA QID List Output

```
<!-- QUALYS KNOWLEDGE_BASE_VULN_LIST_OUTPUT DTD -->
<!ELEMENT KNOWLEDGE_BASE_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, (VULN_LIST|ID_SET)?, WARNING?)>
<!-- DATETIME already defined -->
<!ELEMENT VULN_LIST (VULN*)>
<!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE,
CATEGORY?, TECHNOLOGY?, 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? )>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT VULN_TYPE (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT DETECTION_INFO (#PCDATA)>
<!ELEMENT LAST_CUSTOMIZATION (DATETIME, USER_LOGIN?)> .....

<!-- EOF ---
```

DTD for Code Modified Date QID List Output

```
<!-- QUALYS KNOWLEDGE_BASE_VULN_LIST_OUTPUT DTD -->
<!ELEMENT KNOWLEDGE_BASE_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, (VULN_LIST|ID_SET)?, WARNING?)>
<!-- DATETIME already defined -->
<!ELEMENT VULN_LIST (VULN*)>
<!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE,
CATEGORY?, TECHNOLOGY?, DETECTION_INFO?,
LAST_CUSTOMIZATION?, LAST_SERVICE_MODIFICATION_DATETIME?,
PUBLISHED_DATETIME, CODE_MODIFIED_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? )>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT VULN_TYPE (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT TECHNOLOGY (#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 CODE_MODIFIED_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?, VECTOR_STRING?, ACCESS?, IMPACT?,
AUTHENTICATION?,
EXPLOITABILITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?)>
<!ELEMENT BASE (#PCDATA)>
<!ATTLIST BASE source CDATA #IMPLIED>
<!ELEMENT TEMPORAL (#PCDATA)>
<!ELEMENT VECTOR_STRING (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#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?, VECTOR_STRING?, CVSS3_VERSION?,
ATTACK?, IMPACT?, PRIVILEGES_REQUIRED?, USER_INTERACTION?, SCOPE?,
EXPLOIT_CODE_MATURITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
<!ELEMENT ATTACK (VECTOR?, COMPLEXITY?)>
<!ELEMENT PRIVILEGES_REQUIRED (#PCDATA)>
<!ELEMENT USER_INTERACTION (#PCDATA)>
<!ELEMENT SCOPE (#PCDATA)>
<!ELEMENT EXPLOIT_CODE_MATURITY (#PCDATA)>
<!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 -->
```

DTD for CVE Matching QID List Output

```
<!-- QUALYS KNOWLEDGE_BASE_VULN_LIST_OUTPUT DTD -->
<!ELEMENT KNOWLEDGE_BASE_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, (VULN_LIST|ID_SET)?, WARNING?)>
<!-- DATETIME already defined -->
<!ELEMENT VULN_LIST (VULN*)>
<!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE,
CATEGORY?,TECHNOLOGY?, DETECTION_INFO?,
LAST_CUSTOMIZATION?, LAST_SERVICE_MODIFICATION_DATETIME?,
PUBLISHED_DATETIME, CODE_MODIFIED_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? )>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT VULN_TYPE (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT TECHNOLOGY (#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 CODE_MODIFIED_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?, VECTOR_STRING?, ACCESS?, IMPACT?,
AUTHENTICATION?,
EXPLOITABILITY?, REMEDIATION_LEVEL?, REPORT_CONFIDENCE?)>
<!ELEMENT BASE (#PCDATA)>
<!ATTLIST BASE source CDATA #IMPLIED>
<!ELEMENT TEMPORAL (#PCDATA)>
<!ELEMENT VECTOR_STRING (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#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?, VECTOR_STRING?, CVSS3_VERSION?,
ATTACK?, IMPACT?, PRIVILEGES_REQUIRED?, USER_INTERACTION?, SCOPE?,
EXPLOIT_CODE_MATURITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
<!ELEMENT ATTACK (VECTOR?, COMPLEXITY?)>
<!ELEMENT PRIVILEGES_REQUIRED (#PCDATA)>
<!ELEMENT USER_INTERACTION (#PCDATA)>
<!ELEMENT SCOPE (#PCDATA)>
<!ELEMENT EXPLOIT_CODE_MATURITY (#PCDATA)>
<!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 -->

```

Chapter 4 - Scan Authentication XML

This section describes the XML output returned from Scan Authentication API requests.

[Authentication Record List Output](#)

[Authentication Record List by Type Output](#)

[Authentication Vault List Output](#)

[Authentication Vault View Output](#)

Authentication Record List Output

API used

[platform API server](#)/api/2.0/fo/auth/ with action=list

DTD for Auth Record List Output

[platform API server](#)/api/2.0/fo/auth/auth_records.dtd

A recent DTD is shown below.

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!-- $Revision$ -->
<!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_POSTGRES_SQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?,
AUTH_SAPIQ_IDS?, AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?,
AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?,
AUTH_INFOBLOX_IDS?, AUTH_DNS_BIND_IDS?, AUTH_CISCO_APIC_IDS?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
```

```
<!ELEMENT AUTH_IBM_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_POSTGRES_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAPIQ_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_HANA_IDS (ID_SET)>
<!ELEMENT AUTH_NEO4J_IDS (ID_SET)>
<!ELEMENT AUTH_AZURE_MS_SQL_IDS (ID_SET)>
<!ELEMENT AUTH_NETWORK_SSH_IDS (ID_SET)>
<!ELEMENT AUTH_NGINX_IDS (ID_SET)>
<!ELEMENT AUTH_INFOBLOX_IDS (ID_SET)>
<!ELEMENT AUTH_DNS_BIND_IDS (ID_SET)>
<!ELEMENT AUTH_CISCO_APIC_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>

<!-- EOF -->
```

XPaths for Authentication Record List Output

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.
/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_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIX_IDS?, AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?, AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?, AUTH_SAPIQ_IDS?, AUTH_SAP_HANA_IDS?, AUTH_NEO4J_IDS?, AUTH_AZURE_MS_SQL_IDS?, AUTH_NETWORK_SSH_IDS?, AUTH_NGINX_IDS?, AUTH_INFOBLOX_IDS?, AUTH_CISCO_APIC_IDS?, AUTH_DNS_BIND_IDS?)

XPath	element specifications / notes
/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.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_IBM_WEBSPHERE_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)	

XPath

element specifications / notes

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.

/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_JBOSS_IDS (ID_SET)	A set of JBoss Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MARIADB_IDS (ID_SET)	A set of MariaDB authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_INFORMIXDB_IDS (ID_SET)	A set of InformixDB Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MS_EXCHANGE_IDS (ID_SET)	A set of MS Exchange Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)	A set of Oracle HTTP Server authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_GREENPLUM_IDS (ID_SET)	A set of Pivotal Greenplum authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)	A set of Microsoft SharePoint authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_KUBERNETES_IDS (ID_SET)	A set of Kubernetes authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_SAPIQ_IDS (ID_SET)	A set of SAP IQ authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_SAP_HANA_IDS (ID_SET)	A set of SAP Hana authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_NEO4J_IDS (ID_SET)	A set of Ne04j authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_AZURE_MS_SQL_IDS (ID_SET)	A set of Azure MS SQL authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_NETWORK_SSH_IDS? (ID_SET)	A set of Network SSH authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_NGINX_IDS? (ID_SET)	A set of Nginx authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_INFOBLOX_IDS? (ID_SET)	A set of Infoblox authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_CISCO_APIC_IDS? (ID_SET)	A set of Cisco Apic authentication record IDs.
/AUTH_RECORDS_OUTPUT/RESPONSE/AUTH_RECORDS/AUTH_DNS_BIND_IDS? (ID_SET)	A set of DNS Bind authentication record IDs.

Authentication Record List Output: Warning List

XPath

element specifications / notes

/AUTH_RECORDS_OUTPUT/RESPONSE/WARNING_LIST (WARNING+)

XPath	element specifications / notes
/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.
/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.

List SAP IQ Record Output

API used

<platform API server>/api/2.0/fo/auth/sapiq with action=list

DTD for SAP IQ Record List Output

```
<!-- QUALYS AUTH_SAPIQ_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_SAPIQ_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_SAPIQ_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_SAPIQ_LIST (AUTH_SAP_IQ+)>

<!ELEMENT AUTH_SAP_IQ (ID, TITLE, USERNAME, IP_SET?, DATABASE, PORT,
INSTALLATION_DIR?, PASSWORD_ENCRYPTION?, LOGIN_TYPE?, DIGITAL_VAULT?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT INSTALLATION_DIR (#PCDATA)>
<!ELEMENT PASSWORD_ENCRYPTION (#PCDATA)>

<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_RESOURCE_ID?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
```

```
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_RESOURCE_ID (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

List Postgre SQL Record Output

API used

<platform API server>/api/2.0/fo/auth/postgresql with action=list

DTD for PostgreSQL Record List Output

```
<!-- QUALYS AUTH_POSTGRESQL_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_POSTGRESQL_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_POSTGRESQL_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_POSTGRESQL_LIST (AUTH_POSTGRESQL+)>
<!ELEMENT AUTH_POSTGRESQL (ID, TITLE, USERNAME, DATABASE, PORT,
SSL_VERIFY, HOSTS?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, WIN_CONF_FILE?,
UNIX_CONF_FILE?, PRIVATE_KEY_CERTIFICATE_LIST?, NETWORK_ID?, CREATED,
LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>

<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO,
CERTIFICATE?)+>
<!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">
<!-- Private key contents will never be rendered -->
<!ELEMENT PRIVATE_KEY EMPTY>
<!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
<!-- Certificate contents will never be rendered -->
<!ELEMENT CERTIFICATE EMPTY>

<!ELEMENT PORT (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT HOSTS (HOST+)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT WIN_CONF_FILE (#PCDATA)>
<!ELEMENT UNIX_CONF_FILE (#PCDATA)>
```

```

<!ELEMENT CLIENT_CERT (#PCDATA)>
<!ELEMENT CLIENT_KEY (#PCDATA)>
<!ELEMENT CERT_PASSPHASE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_RESOURCE_ID?,
VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_RESOURCE_ID (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>
<!-- EOF -->

```

List Greenplum Record Output

API used

<platform API server>/api/2.0/fo/auth/greenplum with action=list

DTD for Greenplum Record List Output

```
<!-- QUALYS AUTH_GREENPLUM_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_GREENPLUM_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_GREENPLUM_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_GREENPLUM_LIST (AUTH_GREENPLUM+)>
<!ELEMENT AUTH_GREENPLUM (ID, TITLE, USERNAME, DATABASE, PORT, SSL_VERIFY,
HOSTS?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, UNIX_CONF_FILE,
PRIVATE_KEY_CERTIFICATE_LIST?, NETWORK_ID?, CREATED, LAST_MODIFIED,
COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>

<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO,
CERTIFICATE?)+>
<!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">
<!-- Private key contents will never be rendered -->
<!ELEMENT PRIVATE_KEY EMPTY>
<!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
<!-- Certificate contents will never be rendered -->
<!ELEMENT CERTIFICATE EMPTY>

<!ELEMENT PORT (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT HOSTS (HOST+)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT UNIX_CONF_FILE (#PCDATA)>
<!ELEMENT CLIENT_CERT (#PCDATA)>
```

```
<!ELEMENT CLIENT_KEY (#PCDATA)>
<!ELEMENT CERT_PASSPHASE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_RESOURCE_ID?,
VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_RESOURCE_ID (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>
<!-- EOF -->
```

List Windows Record Output

API used

[platform API server](#)/api/2.0/fo/auth/windows with action=list

DTD for Windows Record List Output

```
<!-- QUALYS AUTH_WINDOWS_LIST_OUTPUT DTD -->
  <!-- $Revision$ -->
  <!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?, IPV6_SET?, TAGS?, 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 IPV6_SET (IPV6|IPV6_RANGE)+>
        <!ELEMENT IPV6 (#PCDATA)>
        <!ELEMENT IPV6_RANGE (#PCDATA)>

        <!ELEMENT TAGS (TAG_TYPE, TAGS_INCLUDE, TAGS_EXCLUDE?)>
```

```

<!ELEMENT TAG_TYPE (#PCDATA)>
<!ELEMENT TAGS_INCLUDE (SELECTOR, TAG+)>
<!ELEMENT SELECTOR (#PCDATA)>
<!ELEMENT TAG (ID, NAME)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT TAGS_EXCLUDE (SELECTOR, TAG?)>

<!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_RESOURCE_ID?, VAULT_EP_NAME?, VAULT_EP_TYPE?,
VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?,
VAULT_AUTHORIZATION_NAME?, VAULT_TARGET_NAME?, VAULT_SECRET_KV_PATH?,
VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_USE_AD_HASHICORP?,
VAULT_DEVICE_NAME?, VAULT_DEVICE_HOST?, VAULT_APP_NAME?,
VAULT_SERVICE_TYPE?)>
  <!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_RESOURCE_ID (#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 VAULT_AUTHORIZATION_NAME (#PCDATA)>
  <!ELEMENT VAULT_TARGET_NAME (#PCDATA)>
  <!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
  <!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
  <!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
  <!ELEMENT VAULT_USE_AD_HASHICORP (#PCDATA)>
  <!ELEMENT VAULT_DEVICE_NAME (#PCDATA)>
  <!ELEMENT VAULT_DEVICE_HOST (#PCDATA)>
  <!ELEMENT VAULT_APP_NAME (#PCDATA)>
  <!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT 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 -->
```

List Unix Record Output

API used

<platform API server>/api/2.0/fo/auth/unix with action=list

DTD for Unix Record List Output

```
<!-- QUALYS AUTH_UNIX_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_UNIX_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_UNIX_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_UNIX_LIST (AUTH_UNIX+)>
<!ELEMENT AUTH_UNIX (ID, TITLE, USERNAME, SKIP_PASSWORD?,
CLEARTEXT_PASSWORD?, TARGET_TYPE?, KERBEROS_AUTHENTICATION?,
REALM_DISCOVERY?, USER_REALM?, USER_KDC?, SERVICE_REALM?, SERVICE_KDC?,
KERBEROS_LOGIN_INFO?, (ROOT_TOOL?|ROOT_TOOL_INFO_LIST?),
((RSA_PRIVATE_KEY?, DSA_PRIVATE_KEY?)|PRIVATE_KEY_CERTIFICATE_LIST?),
PORT?, IP_SET?, IPV6_SET?, TAGS?, LOGIN_TYPE?, DIGITAL_VAULT?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?, USE_AGENTLESS_TRACKING?,
AGENTLESS_TRACKING_PATH?, QUALYS_SHELL?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SKIP_PASSWORD (#PCDATA)>
<!ELEMENT CLEARTEXT_PASSWORD (#PCDATA)>
<!ELEMENT TARGET_TYPE (#PCDATA)>
<!ELEMENT KERBEROS_AUTHENTICATION (#PCDATA)>
<!ELEMENT REALM_DISCOVERY (#PCDATA)>
<!ELEMENT USER_REALM (#PCDATA)>
<!ELEMENT USER_KDC (#PCDATA)>
<!ELEMENT SERVICE_REALM (#PCDATA)>
<!ELEMENT SERVICE_KDC (#PCDATA)>
<!ELEMENT KERBEROS_LOGIN_INFO (DIGITAL_VAULT?)>
<!ATTLIST KERBEROS_LOGIN_INFO type (basic|vault) "basic">
<!ELEMENT ROOT_TOOL (#PCDATA)>
<!ELEMENT ROOT_TOOL_INFO_LIST (ROOT_TOOL_INFO)*>
<!ELEMENT RSA_PRIVATE_KEY EMPTY>
<!ELEMENT DSA_PRIVATE_KEY EMPTY>
<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
```

```

<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT IPV6_SET (IPV6|IPV6_RANGE)+>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT IPV6_RANGE (#PCDATA)>
<!ELEMENT TAGS (TAG_TYPE, TAGS_INCLUDE, TAGS_EXCLUDE?)>
<!ELEMENT TAG_TYPE (#PCDATA)>
<!ELEMENT TAGS_INCLUDE (SELECTOR, TAG+)>
<!ELEMENT SELECTOR (#PCDATA)>
<!ELEMENT TAG (ID, NAME)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT TAGS_EXCLUDE (SELECTOR, TAG?)>
<!ELEMENT LOGIN_TYPE (#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 AGENTLESS_TRACKING_PATH (#PCDATA)>
<!ELEMENT QUALYS_SHELL (ENABLED, LOG_FACILITY?)>
<!ELEMENT ROOT_TOOL_INFO (ID, ROOT_TOOL, PASSWORD_INFO?)>
<!ELEMENT PASSWORD_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSWORD_INFO type (basic|vault) "basic">
<!-- Private key contents will never be rendered -->
<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO,
CERTIFICATE?)+>
<!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">
<!-- Private key/Certificate contents will never be rendered -->
<!ELEMENT PRIVATE_KEY EMPTY>
<!ATTLIST PRIVATE_KEY type (rsa|dsa|ecdsa|ed25519|pkcs8) #REQUIRED>
<!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
<!ELEMENT CERTIFICATE EMPTY>
<!ATTLIST CERTIFICATE type (x.509|openssh) #REQUIRED>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_RESOURCE_ID?,
VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?,
VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?, VAULT_AUTHORIZATION_NAME?,
VAULT_TARGET_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?, VAULT_DEVICE_NAME?, VAULT_DEVICE_HOST?,
VAULT_APP_NAME?, VAULT_SERVICE_TYPE?)>
...
<!-- EOF -->

```

List Oracle Record Output

API used

[platform API server](#)/api/2.0/fo/auth/oracle with action=list

DTD for Oracle Record List Output

```
<!-- QUALYS AUTH_ORACLE_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_ORACLE_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_ORACLE_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_ORACLE_LIST (AUTH_ORACLE+)>

<!ELEMENT AUTH_ORACLE (ID, TITLE, USERNAME, (SID|SERVICENAME)?, CWALLET?,
EWALLET?, EWALLET_PASSPHRASE?, PORT?, SSL_VERIFY?, HOSTS? , IP_SET?,
PC_ONLY?, IS_CDB?, WINDOWS_OS_CHECKS?, WINDOWS_OS_OPTIONS?,
UNIX_OPATCH_CHECKS?, UNIX_OS_CHECKS?, UNIX_OS_OPTIONS?, LOGIN_TYPE?,
DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED?,
IS_ACTIVE?, IS_TEMPLATE?, TEMPLATE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SID (#PCDATA)>
<!ELEMENT SERVICENAME (#PCDATA)>
<!ELEMENT CWALLET (#PCDATA)>
<!ELEMENT EWALLET (#PCDATA)>
<!ELEMENT EWALLET_PASSPHRASE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT HOSTS (HOST+)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT PC_ONLY (#PCDATA)>

<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY?)>
```

```
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT IS_SYSTEM_CREATED (#PCDATA)>
<!ELEMENT IS_ACTIVE (#PCDATA)>
<!ELEMENT IS_TEMPLATE (#PCDATA)>
<!ELEMENT TEMPLATE (ID, TITLE)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT IS_CDB (#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)>

<!ELEMENT WINDOWS_OS_CHECKS (#PCDATA)>
<!ELEMENT UNIX_OPATCH_CHECKS (#PCDATA)>
<!ELEMENT UNIX_OS_CHECKS (#PCDATA)>

<!ELEMENT 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)>
<!ELEMENT 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)>

<!ELEMENT WIN_ORA_HOME (#PCDATA)>
<!ELEMENT WIN_ORA_HOME_PATH (#PCDATA)>
<!ELEMENT WIN_INIT_ORA_PATH (#PCDATA)>
<!ELEMENT WIN_SPFILE_ORA_PATH (#PCDATA)>
<!ELEMENT WIN_LISTENER_ORA_PATH (#PCDATA)>
<!ELEMENT WIN_SQLNET_ORA_PATH (#PCDATA)>
<!ELEMENT WIN_TNSNAMES_ORA_PATH (#PCDATA)>

<!ELEMENT UNIX_ORA_HOME_PATH (#PCDATA)>
<!ELEMENT UNIX_INIT_ORA_PATH (#PCDATA)>
<!ELEMENT UNIX_SPFILE_ORA_PATH (#PCDATA)>
<!ELEMENT UNIX_LISTENER_ORA_PATH (#PCDATA)>
<!ELEMENT UNIX_SQLNET_ORA_PATH (#PCDATA)>
<!ELEMENT UNIX_TNSNAMES_ORA_PATH (#PCDATA)>
<!ELEMENT UNIX_INVPTRLOC_PATH (#PCDATA)>

<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?,
```

```
VAULT_EP_CONT?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,  
VAULT_SECRET_KV_KEY?, VAULT_USE_AD_HASHICORP?, VAULT_SERVICE_TYPE?,  
VAULT_ACCOUNT_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?)>  
<!--ELEMENT DIGITAL_VAULT_ID (#PCDATA)>  
<!--ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>  
<!--ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>  
<!--ELEMENT VAULT_USERNAME (#PCDATA)>  
<!--ELEMENT VAULT_FOLDER (#PCDATA)>  
<!--ELEMENT VAULT_FILE (#PCDATA)>  
<!--ELEMENT VAULT_SECRET_NAME (#PCDATA)>  
<!--ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>  
<!--ELEMENT VAULT_EP_NAME (#PCDATA)>  
<!--ELEMENT VAULT_EP_TYPE (#PCDATA)>  
<!--ELEMENT VAULT_EP_CONT (#PCDATA)>  
<!--ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>  
<!--ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>  
<!--ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>  
<!--ELEMENT VAULT_USE_AD_HASHICORP (#PCDATA)>  
<!--ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>  
<!--ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>  
<!--ELEMENT VAULT_NS_TYPE (#PCDATA)>  
<!--ELEMENT VAULT_NS_NAME (#PCDATA)>  
<!-- EOF -->
```

Authentication Record List by Type Output

API used

[<platform API server>](#)/api/2.0/fo/auth/<type>/ with action=list

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

[<platform API server>](#)/api/2.0/fo/auth/<type>/auth_<type>_list_output.dtd

Some authentication record lists follow this format for the DTD path:

[<platform API server>](#)/api/2.0/fo/auth/<type>/dtd/auth_list_output.dtd

A recent DTD for Windows is shown below.

```
<!-- 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?, TAGS?,
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 TAGS (TAG_TYPE, TAGS_INCLUDE, TAGS_EXCLUDE?)>
<!ELEMENT TAG_TYPE (#PCDATA)>
<!ELEMENT TAGS_INCLUDE (SELECTOR, TAG+)>
<!ELEMENT SELECTOR (#PCDATA)>
<!ELEMENT TAG (ID, NAME)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT TAGS_EXCLUDE (SELECTOR, TAG?)>

<!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?,
VAULT_AUTHORIZATION_NAME?, VAULT_TARGET_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 VAULT_AUTHORIZATION_NAME (#PCDATA)>
<!ELEMENT VAULT_TARGET_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

All Record Types - common sections

<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?)
/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.

XPath	element specifications / notes
/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.

Record Types with Tag Support

<TYPE> is the authentication type, such as unix and windows

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS (TAG_TYPE, TAGS_INCLUDE, TAGS_EXCLUDE)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAG_TYPE (#PCDATA)	The tag asset type selected in the record: asset_tags or ip_range_tag_rule.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_INCLUDE (SELECTOR, TAG+)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_INCLUDE/SELECTOR (#PCDATA)	The tag selector (any or all) for tags included in the record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_INCLUDE/TAG (ID, NAME)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_INCLUDE/TAG/ID (#PCDATA)	The ID of an asset tag in the included list.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_INCLUDE/TAG/NAME (#PCDATA)	The name of an asset tag in the included list.

XPath	element specifications / notes
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_EXCLUDE (SELECTOR, TAG+)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_EXCLUDE/ SELECTOR (#PCDATA)	The tag selector (any or all) for tags excluded in the record.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_EXCLUDE/TAG (ID, NAME)	
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_EXCLUDE/TAG/ ID (#PCDATA)	The ID of an asset tag in the excluded list.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/TAGS/TAGS_EXCLUDE/TAG/ NAME (#PCDATA)	The name of an asset tag in the excluded list.

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, USERNAME , SKIP_PASSWORD? , CLEARTEXT_PASSWORD? , TARGET_TYPE? , (ROOT_TOOL? ROOT_TOOL_INFO_LIST?), ((RSA_PRIVATE _KEY? , DSA_PRIVATE_KEY?) PRIVATE_KEY_CERTIFICATE_LIST?), PORT? , IP_SET, TAGS?, LOGIN_TYPE? , DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?, USE_AGENTLESS_TRACKING? , AGENTLESS_TRACKING_PATH? , QUALYS_SHELL?)	
/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)	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/TARGET_TYPE (#PCDATA)	Allows you to define the type of target for a Unix auth record.
/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?)	

XPath	element specifications / notes
	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)
/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	For a Unix record, vault information configured for the record. See Vault Information . 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.

Network SSH Response

Elements (in bold>

XPath	element specifications / notes
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH	(ID, TITLE, USERNAME , SKIP_PASSWORD? , CLEARTEXT_PASSWORD? , PASSWORD2_INFO , TARGET_TYPE? , ((RSA_PRIVATE_KEY? , DSA_PRIVATE_KEY?) PRIVATE_KEY_CERTIFICATE_LIST?), PORT? , IP_SET, LOGIN_TYPE? , DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/USER_NAME (#PCDATA)	The user account to be used for authentication on target hosts.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/SKIP_PASSWORD (#PCDATA)	Set to 1 if skip password option enabled.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/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_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/TARGET_TYPE (#PCDATA)	Allows you to define the type of target for a Network SSH auth record.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PASSWORD2_INFO (DIGITAL_VAULT?)	attribute: type (basic vault) "basic"
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/RSA_PRIVATE_KEY	RSA private key.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/DSA_PRIVATE_KEY	DSA private key.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*	
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/(ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO, CERTIFICATE?)+	
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PRIVATE_KEY_INFO (PRIVATE_KEY DIGITAL_VAULT)	attribute: type (basic vault) "basic"
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PRIVATE_KEY_INFO/PRIVATE_KEY	attribute: type (rsa dsa ecdsa ed25519)
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/PASSPHRASE_INFO (PRIVATE_KEY DIGITAL_VAULT)	attribute: type (basic vault) "basic"

XPath	element specifications / notes
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/PRIVATE_KEY_CERTIFICATE_LIST/PRIVATE_KEY_CERTIFICATE/CERTIFICATE	attribute: type (x.509 openssh)
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/POR T (#PCDATA)	A list of custom ports defined for compliance scanning (authentication and compliance assessment).
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/LOGI N_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_NETWORK_SSH_LIST_OUTPUT/RESPONSE/AUTH_NETWORK_SSH_LIST/AUTH_NETWORK_SSH/DIGI TAL_VAULT	Vault information configured for the record.

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, USERNAME , NTLM? , NTLM_V2? , KERBEROS? , WINDOWS_DOMAIN? , WINDOWS_AD_DOMAIN? , WINDOWS_AD_TRUST? , IP_SET?, TAGS?, LOGIN_TYPE , DIGITAL_VAULT , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?, USE_AGENTLESS_TRACKING? , MINIMUM_SMB_VERSION? , REQUIRE_SMB_SIGNING?)
/AUTH_WINDOWS_LIST_OUTPUT/RESPONSE/AUTH_WINDOWS_LIST/AUTH_WINDOWS/ USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.
/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.

XPath	element specifications / notes
/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 Vault Information .
/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> are described below.

XPath	element specifications / notes
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE	(ID, TITLE, USERNAME , (SID SERVICENAME)?, PORT? , IP_SET? , PC_ONLY? , IS_CDB? , WINDOWS_OS_CHECKS , WINDOWS_OS_OPTIONS? , UNIX_OPATCH_CHECKS , UNIX_OS_CHECKS , UNIX_OS_OPTIONS? , NETWORK_ID? , CREATED , LAST_MODIFIED , IS_SYSTEM_CREATED? , IS_ACTIVE? , IS_TEMPLATE? , TEMPLATE? , 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.

XPath	element specifications / notes
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/PC_ONLY (#PCDATA)	The value 1 indicates that the pc_only=1 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/IS_CDB (#PCDATA)	The value 1 indicates that the IS_CDB option is enabled for the record. This means the Oracle database is a Multitenant Container Database.
/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.
/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.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/IS_SYSTEM_CREATED (#PCDATA)	The value 1 indicates that this record was system created. A value of 0 indicates that it's user created.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/IS_ACTIVE (#PCDATA)	The value 1 indicates that this record is active. A value of 0 indicates that it is inactive.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/IS_TEMPLATE (#PCDATA)	The value 1 indicates that this record is an Oracle system record template. A value of 0 indicates that this is a regular Oracle record.
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/TEMPLATE (ID, TITLE)	
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/TEMPLATE/ID (#PCDATA)	The ID of the Oracle system record template associated with a system created Oracle record.

XPath	element specifications / notes
/AUTH_ORACLE_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_LIST/AUTH_ORACLE/TEMPLATE/TITLE (#PCDATA)	The title of the Oracle system record template associated with a system created Oracle record.

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, USERNAME? , AUTH_ALG? , PRIV_ALG? , SEC_ENG? , CONTEXT_ENG? , CONTEXT? , COMMUNITY_STRINGS? , VERSION , 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 (for SNMPv2c) 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, USERNAME , NTLM_v1? , NTLM_V2? , KERBEROS? , (INSTANCE AUTO_DISCOVER_INSTANCES), (DATABASE AUTO_DISCOVER_DATABASES), (PORT AUTO_DISCOVER_PORTS), DB_LOCAL , AUTH_OS_TYPE? , UNIX_CONF_PATH? , UNIX_INSTA_PATH? , WINDOWS_DOMAIN? , (IP_SET MEMBER_DOMAIN), NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)

XPath	element specifications / notes
/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/AUTH_OS_TYPE (#PCDATA)	The authentication OS type selected in the record: windows or unix.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/UNIX_CONF_PATH (#PCDATA)	The path to the MS SQL Server configuration file on Unix hosts, as defined in the record.
/AUTH_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_MS_SQL_LIST/AUTH_MS_SQL/UNIX_INSTA_PATH (#PCDATA)	The path to the MS SQL Server instance directory on Unix hosts, as defined in the record.
/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.
/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.

Azure MS SQL Response

Azure MS SQL-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL	(ID, TITLE, PROVIDER_NAME , USERNAME , INSTANCE , (DATABASE AUTO_DISCOVER_DATABASES), PORT , IP_SET, LOGIN_TYPE?, DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL/PROVIDER_NAME (#PCDATA)	Name of the cloud service provider. The only value supported is azure.
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL/USERNAME (#PCDATA)	The user account to be used for authentication to target hosts.
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL/Instance (#PCDATA)	.The name of the database instance to be scanned. This is the instance name assigned to the TCP/IP port.
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL/DATABASE AUTO_DISCOVER_DATABASES (#PCDATA)	A database name or AUTO_DISCOVER_DATABASES=1 if database names are auto-discovered.
/AUTH_AZURE_MS_SQL_LIST_OUTPUT/RESPONSE/AUTH_AZURE_MS_SQL_LIST/AUTH_AZURE_MS_SQL/PORT (#PCDATA)	The port number assigned to the database instance to be scanned.

Neo4j Response

Neo4j-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J	(ID, TITLE, USERNAME , DATABASE? , PORT , SSL_VERIFY?, HOSTS?,IP_SET?, UNIX_CONF_PATH? , UNIX_BASE_PATH? , VERSION? , AUTO_PATH? , LOGIN_TYPE?, DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/USERNAME (#PCDATA)	The user account to be used for authentication on target hosts.
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/DATABASE (#PCDATA)	The database name of the database to be scanned.
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/PORT (#PCDATA)	The port number that the database is running on.
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/UNIX_BASE_PATH (#PCDATA)	The base path for Neo4j on your Unix hosts.
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/UNIX_CONF_PATH (#PCDATA)	The path to the Neo4j configuration file on your Unix hosts.

XPath	element specifications / notes
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/VERSION (#PCDATA)	The Neo4j version. Only Neo4j 3.x version is supported at this time.
/AUTH_NEO4J_LIST_OUTPUT/RESPONSE/AUTH_NEO4J_LIST/AUTH_NEO4J/NEO4J_AUTO_PATH (#PCDATA)	The value 1 indicates that auto discovery is enabled in the record for auto discovering the base and configuration paths on Unix hosts. The value 0 indicates the option is disabled.

Nginx Response

Nginx-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_NGINX_LIST_OUTPUT/RESPONSE/AUTH_NGINX_LIST/AUTH_NGINX	(ID, TITLE, IP_SET?, UNIX_BIN_PATH? , UNIX_CONF_PATH? , UNIX_PREFIX_PATH? , COMMENTS?)
/AUTH_NGINX_LIST_OUTPUT/RESPONSE/AUTH_NGINX_LIST/AUTH_NGINX/UNIX_BIN_PATH (#PCDATA)	The absolute path of the Nginx binary file location your Unix hosts.
/AUTH_NGINX_LIST_OUTPUT/RESPONSE/AUTH_NGINX_LIST/AUTH_NGINX/UNIX_CONF_PATH (#PCDATA)	The path to the Nginx configuration file on your Unix hosts.
/AUTH_NGINX_LIST_OUTPUT/RESPONSE/AUTH_NGINX_LIST/AUTH_NGINX/UNIX_PREFIX_PATH (#PCDATA)	The path to the Nginx base directory on your Unix hosts.

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, USERNAME , DATABASE , PORT , IP_SET, PC_ONLY? , LOGIN_TYPE? , DIGITAL_VAULT? , 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	

XPath	element specifications / notes
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/USERNAME (#PCDATA)	(ID, TITLE, USERNAME? , PORT , SSL_VERIFY? , HOSTS? , IP_SET, LOGIN_TYPE? , DISCONNECTED_ESXI? , DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?) 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.
/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/DISCONNECTED_ESXI (#PCDATA)	 Specify 1 if the ESXi hosts are disconnected and you don't want to send any traffic to the ESXi hosts.
/AUTH_VMWARE_LIST_OUTPUT/RESPONSE/AUTH_VMWARE_LIST/AUTH_VMWARE/DIGITAL_VAULT (#PCDATA)	 Vault information, when a vault is defined for the record. See Vault Information .

Apache Response

Apache-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/UNIX_CONFIGURATION_FILE (#PCDATA)	(ID, TITLE, IP_SET, UNIX_CONFIGURATION_FILE , UNIX_CONTROL_COMMAND , WINDOWS_CONFIGURATION_FILE? , WINDOWS_CONTROL_COMMAND? , NETWORK_ID?, CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED? , IS_ACTIVE? , COMMENTS?) The path to the Apache configuration file (valid for Apache Web Server record only).

XPath	element specifications / notes
/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).
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/WINDOWS_CONFIGURATION_FILE (#PCDATA)	The Windows path to the Apache configuration file (valid for Apache Web Server record only).
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/WINDOWS_CONTROL_COMMAND (#PCDATA)	The Windows path to the Apache control command (valid for Apache Web Server record only).
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/IS_SYSTEM_CREATED (#PCDATA)	A value of 1 indicates that the record is system created. A value of 0 indicates that the record is user created. Valid for Apache Web Server record only.
/AUTH_APACHE_LIST_OUTPUT/RESPONSE/AUTH_APACHE_LIST/AUTH_APACHE/IS_ACTIVE (#PCDATA)	A value of 1 indicates that the record is active. A value of 0 indicates that the record is not active. Valid for Apache Web Server record only.

IBM WebSphere Response

IBM WebSphere-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE	(ID, TITLE, IP_SET, UNIX_INSTALLATION_DIRECTORY? , UNIX_DIR_MODE? , WINDOWS_INSTALLATION_DIRECTORY? , NETWORK_ID?, CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED? , IS_ACTIVE? , COMMENTS?)
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE/UNIX_INSTALLATION_DIRECTORY (#PCDATA)	The directory where the WebSphere application is installed.
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE/UNIX_DIR_MODE (#PCDATA)	The Unix directory mode setting in the record: installation_dir (for installation directory) or server_dir (for server directory).
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE/WINDOWS_INSTALLATION_DIRECTORY (#PCDATA)	The Windows directory where the WebSphere application is installed.
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE/IS_SYSTEM_CREATED (#PCDATA)	The value 1 indicates that this record was system created. A value of 0 indicates that it's user created.
/AUTH_IBM_WEBSPHERE_LIST_OUTPUT/RESPONSE/AUTH_IBM_WEBSPHERE_LIST/AUTH_IBM_WEBSPHERE/IS_ACTIVE (#PCDATA)	

XPath	element specifications / notes
	The value 1 indicates that this record is active. A value of 0 indicates that it is inactive.

Tomcat Server Response

Tomcat Server-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT	(ID, TITLE, IP_SET, INSTALLATION_PATH? , INSTANCE_PATH? , AUTO_DISCOVER_INSTANCES? , INSTALLATION_PATH_WINDOWS? , INSTANCE_PATH_WINDOWS? , SERVICE_NAME_WINDOWS? , IS_SYSTEM_CREATED? , IS_ACTIVE? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTALLATION_PATH (#PCDATA)	The Unix directory where the tomcat server is installed.
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTANCE_PATH (#PCDATA)	The Unix directory where the tomcat server instance(s) are installed, if specified.
/AUTH_TOMCAT_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.
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTALLATION_PATH_WINDOWS (#PCDATA)	The Windows directory where the tomcat server is installed.
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/INSTANCE_PATH_WINDOWS (#PCDATA)	The Windows directory where the tomcat server instance(s) are installed, if specified.
/AUTH_TOMCAT_LIST_OUTPUT/RESPONSE/AUTH_TOMCAT_LIST/AUTH_TOMCAT/SERVICE_NAME_WINDOWS (#PCDATA)	The Windows service name for the apache tomcat server running as a service, if specified.

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, USERNAME , SSL , (REALM VHOST), 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.

XPath	element specifications / notes
/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_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE	(ID, TITLE, USERNAME , (DATABASE AUTO_DISCOVER_DATABASES), PORT , PASSWORD_ENCRYPTION? , INSTALLATION_DIR? , IP_SET? , LOGIN_TYPE? , DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/DATABASE AUTO_DISCOVER_DATABASES (#PCDATA)	The name of the Sybase database to authenticate to or AUTO_DISCOVER_DATABASES=1 if databses are auto-discovered.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/PORT (#PCDATA)	The port the Sybase database is on.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/PASSWORD_ENCRYPTION (#PCDATA)	The flag for password encryption. Set to 1 when password encryption is enabled in the Sybase record. When set to 0 (the default), password encryption is not enabled.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/ INSTALLATION_DIR (#PCDATA)	The Sybase database installation directory.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/ LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_SYBASE_LIST_OUTPUT/RESPONSE/AUTH_SYBASE_LIST/AUTH_SYBASE/ DIGITAL_VAULT/	Vault information, when a vault is defined for the record. See Vault Information .

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, USERNAME , DATABASE , PORT , HOSTS? , IP_SET? , DIGITAL_VAULT? , SSL_VERIFY , WINDOWS_CONF_FILE , UNIX_CONF_FILE , CLIENT_CERT? , CLIENT_KEY? , 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.
/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/DIGITAL_VAULT	Vault information, when a vault is defined for the record.
/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.

MariaDB Response

MariaDB-specific elements (in bold> are described below.

XPath	element specifications / notes
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB	(ID, TITLE, USERNAME , DATABASE , PORT , HOSTS? , IP_SET? , LOGIN_TYPE? , DIGITAL_VAULT? , SSL_VERIFY , WINDOWS_CONF_FILE , UNIX_CONF_FILE , CLIENT_CERT? , CLIENT_KEY? , NETWORK_ID? , CREATED , LAST_MODIFIED , COMMENTS?)

XPath	element specifications / notes
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/DATABASE (#PCDATA)	The database that will be authenticated to.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/PORT (#PCDATA)	The port the database is running on.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/HOSTS (#PCDATA)	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.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/LOGIN_TYPE (#PCDATA)	Login type is "vault" when a vault is defined for the record.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/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?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?)
	Vault information, when a vault is defined for the record.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/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 MariaDB server uses SSL, the server SSL certificate is valid and matches the scanned host. The value 0 (disabled) means we'll attempt authentication with MariaDB servers that do and do not use SSL; in the case of SSL the server SSL certificate verification will be skipped.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/WINDOWS_CONF_FILE (#PCDATA)	The path to the Windows MariaDB conf file.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/UNIX_CONF_FILE (#PCDATA)	The path to the Unix MariaDB conf file.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/CLIENT_CERT (#PCDATA)	PEM-encoded X.509 certificate.
/AUTH_MARIADB_LIST_OUTPUT/RESPONSE/AUTH_MARIADB_LIST/AUTH_MARIADB/CLIENT_KEY (#PCDATA)	PEM-encoded RSA private key.

WebLogic Server Response

WebLogic Server-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_ORACLE_WEBLOGIC_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_WEBLOGIC_LIST/AUTH_ORACLE_WEBLOGIC	(ID, TITLE, IP_SET, INSTALLATION_PATH , AUTO_DISCOVER , DOMAIN? , 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, DAEMON_CONFIGURATION_FILE? , DOCKER_COMMAND? , 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, USERNAME , DATABASE , PORT , SSL_VERIFY , HOSTS? , IP_SET?, LOGIN_TYPE? , DIGITAL_VAULT? , WIN_CONF_FILE? , UNIX_CONF_FILE? , PRIVATE_KEY_CERTIFICATE_LIST? , 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.

XPath	element specifications / notes
/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.
/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_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?)
	Vault information, when a vault is defined for the record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_POSTGRESQL_LIST/AUTH_POSTGRESQL/WIN_CONF_FILE (#PCDATA)	The full path to the PostgreSQL configuration file on your Window assets (IP addresses).
/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, USERNAME? , CREDENTIAL_TYPE? , CLEARTEXT? , DATABASE , PORT , UNIX_CONFIGURATION_FILE , SSL_VERIFY? , HOSTS? , IP_SET? , LOGIN_TYPE? , DIGITAL_VAULT? , REQUIRE_CERT? , PRIVATE_KEY_CERTIFICATE_LIST? , NETWORK_ID? , CREATED , LAST_MODIFIED , IS_SYSTEM_CREATED? , IS_ACTIVE? , IS_TEMPLATE? , TEMPLATE? , COMMENTS?)
/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/CREDENTIAL_TYPE (#PCDATA)	The credential type used for authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/CLEARTEXT (#PCDATA)	The cleartext option used for external LDAP authentication.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/DATABASE (#PCDATA)	The database instance you want to authenticate to.
/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_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?) 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).

XPath	element specifications / notes
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/REQUIRE_CERT (#PCDATA)	The flag that indicates whether certificate/Private keys needs to be passed along with basic & Vault login.
/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"
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/IS_SYSTEM_CREATED (#PCDATA)	The value 1 indicates that this record was system created. A value of 0 indicates that it's user created.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/IS_ACTIVE (#PCDATA)	The value 1 indicates that this record is active. A value of 0 indicates that it is inactive.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/IS_TEMPLATE (#PCDATA)	The value 1 indicates that this record is an MongoDB system record template. A value of 0 indicates that this is a regular MongoDB record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/TEMPLATE (ID, TITLE)	
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/TEMPLATE/ID (#PCDATA)	The ID of the MongoDB system record template associated with a system created MongoDB record.
/AUTH_HTTP_LIST_OUTPUT/RESPONSE/AUTH_MONGODB_LIST/AUTH_MONGODB/TITLE (#PCDATA)	The title of the MongoDB system record template associated with a system created MongoDB record.

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	

XPath	element specifications / notes
	(ID, TITLE, USERNAME? , SSL_VERIFY , IP_SET?, LOGIN_TYPE? , DIGITAL_VAULT? , 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.

JBoss Server Response

JBoss Server-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_JBOSS_OUTPUT/RESPONSE	(DATETIME, (AUTH_JBOSS_LIST ID_SET)?, WARNING_LIST?, GLOSSARY?)>
/AUTH_JBOSS_OUTPUT/RESPONSE/AUTH_JBOSS_LIST ID_SET	
	One or more JBoss authentication record IDs.
/AUTH_JBOSS_OUTPUT/RESPONSE/AUTH_JBOSS_LIST/AUTH_JBOSS	
	(ID, TITLE, IP_SET, WINDOWS? , UNIX? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_JBOSS_OUTPUT/RESPONSE/AUTH_JBOSS_LIST/AUTH_JBOSS/WINDOWS (HOME_PATH?, DOMAIN_MODE?, BASE_PATH?, CONF_DIR_PATH?, CONF_FILE_PATH?, CONF_HOST_FILE_PATH?)	
	Windows platform configuration settings
/AUTH_JBOSS_OUTPUT/RESPONSE/AUTH_JBOSS_LIST/AUTH_JBOSS/UNIX (HOME_PATH?, DOMAIN_MODE?, BASE_PATH?, CONF_DIR_PATH?, CONF_FILE_PATH?, CONF_HOST_FILE_PATH?)	
	Unix platform configuration settings

InformixDB Response

InformixDB-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB	

XPath	element specifications / notes
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/USERNAME (#PCDATA)	(ID, TITLE, USERNAME , DATABASE , SERVER? , PORT , UNIX? , SSL_VERIFY? , HOSTS? , IP_SET?, LOGIN_TYPE? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?) The user name used for authentication.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/DATABASE (#PCDATA)	The database that will be authenticated to.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/SERVER (#PCDATA)	The unique name of the database server that will be authenticated to.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/PORT (#PCDATA)	The port the database is running on.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/UNIX (CONFIG_PATH?, ONCONFIG?, SQLHOSTS?)	Enter the full path to the InformixDB configuration files on your Unix hosts.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/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 InformixDB server uses SSL, the server SSL certificate is valid and matches the scanned host. The value 0 (disabled) means we'll attempt authentication with InformixDB servers that do and do not use SSL; in the case of SSL the server SSL certificate verification will be skipped.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/HOSTS (#PCDATA)	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.
/AUTH_INFORMIXDB_LIST_OUTPUT/RESPONSE/AUTH_INFORMIXDB_LIST/AUTH_INFORMIXDB/LOGIN_TYPE (#PCDATA)	Login type is basic by default.

Infoblox Response

Infoblox-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST/AUTH_INFOBLOX	(ID, TITLE, USERNAME , SSL_VERIFY? , IP_SET?, API_VERSION? , LOGIN_TYPE? , DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST/AUTH_INFOBLOX/USERNAME (#PCDATA)	The user name used for authentication.
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST/AUTH_INFOBLOX/SSL_VERIFY (#PCDATA)	

XPath	element specifications / notes
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST ID_SET/AUTH_INFOBLOX/API_VERSION? (#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 Infoblox server uses SSL, the server SSL certificate is valid and matches the scanned host. The value 0 (disabled) means we'll attempt authentication with Infoblox servers that do and do not use SSL; in the case of SSL the server SSL certificate verification will be skipped.
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST/AUTH_INFOBLOX/LOGIN_TYPE (#PCDATA)	The API version used for authentication
/AUTH_INFOBLOX_LIST_OUTPUT/RESPONSE/AUTH_INFOBLOX_LIST ID_SET/AUTH_INFOBLOX/DIGITAL_VAULT? (#PCDATA)	Login type is basic by default.
	Vault information, when a vault is defined for the record. See Vault Information .

Oracle HTTP Server Response

Oracle HTTP Server-specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT/RESPONSE/AUTH_ORACLE_HTTP_SERVER_LIST/AUTH_ORACLE_HTTP_SERVER	(ID, TITLE, IP_SET, WINDOWS? , UNIX? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_ORACLE_HTTP_SERVER_OUTPUT/RESPONSE/AUTH_ORACLE_HTTP_SERVER_LIST/AUTH_ORACLE_HTTP_SERVER/WINDOWS (HOME_PATH?, DOMAIN_PATH?, INST_PATH?, INST_NAME?)	Windows platform configuration settings
/AUTH_ORACLE_HTTP_SERVER_OUTPUT/RESPONSE/AUTH_ORACLE_HTTP_SERVER_LIST/AUTH_ORACLE_HTTP_SERVER/UNIX (HOME_PATH?, DOMAIN_PATH?, INST_PATH?, INST_NAME?)	Unix platform configuration settings

Pivotal Greenplum Response

Pivotal Greenplum specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM	(ID, TITLE, USERNAME , DATABASE , PORT , SSL_VERIFY , HOSTS? , IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT? , UNIX_CONF_FILE , PRIVATE_KEY_CERTIFICATE_LIST? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)

XPath	element specifications / notes
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/USERNAME? (#PCDATA)	The user name used for authentication.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/DATABASE (#PCDATA)	The database instance you want to authenticate to.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PORT (#PCDATA)	The port where the database instance is running. Default is 5432.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/SSL_VERIFY (#PCDATA)	SSL verification is skipped by default. Set to 1 if you want to verify the server's certificate is valid and trusted.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/HOSTS? (#PCDATA)	(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.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/DIGITAL_VAULT? (#PCDATA)	Vault information, when a vault is defined for the record. See Vault Information .
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/UNIX_CONF_FILE (#PCDATA)	The full path to the configuration file (postgresql.conf) on your Unix assets (IP addresses). The file must be in the same location on all assets for this record.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST? (PRIVATE_KEY_CERTIFICATE)*	
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST?/PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO, CERTIFICATE?)	
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST?/PRIVATE_KEY_CERTIFICATE/ID	The private key certificate ID.
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST?/PRIVATE_KEY_CERTIFICATE/PRIVATE_KEY_INFO (PRIVATE_KEY DIGITAL_VAULT)	attribute: type (basic vault) "basic"
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST?/PRIVATE_KEY_CERTIFICATE/PASSPHRASE_INFO(DIGITAL_VAULT?)	attribute: type (basic vault) "basic"
/AUTH_GREENPLUM_LIST_OUTPUT/RESPONSE/AUTH_GREENPLUM_LIST ID_SET/AUTH_GREENPLUM/PRIVATE_KEY_CERTIFICATE_LIST?/PRIVATE_KEY_CERTIFICATE/CERTIFICATE?	The private key certificate.

SAP IQ Response

SAP IQ specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ	(ID, TITLE, USERNAME , IP_SET?, DATABASE , PORT , INSTALLATION_DIR ?, PASSWORD_ENCRYPTION ?, LOGIN_TYPE ?, DIGITAL_VAULT ?, NETWORK_ID ?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/USERNAME? (#PCDATA)	The user name used for authentication.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/DATABASE (#PCDATA)	The database instance you want to authenticate to.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/PORT (#PCDATA)	The port where the database instance is running.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/INSTALLATION_DIR (#PCDATA)	The database installation directory for scanning Unix hosts.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/PASSWORD_ENCRYPTION (#PCDATA)	1 means password encryption is enabled in the record and 0 (the default) means password encryption is not enabled.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/LOGIN_TYPE (#PCDATA)	Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password.
/AUTH_SAPIQ_LIST_OUTPUT/RESPONSE/AUTH_SAPIQ_LIST/AUTH_SAP_IQ/DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)
	Vault information, when a vault is defined for the record. See Vault Information .

SAP Hana Response

SAP Hana specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA	(ID, TITLE, USERNAME , DATABASE , PORT , SSL_VERIFY ?, HOSTS ?, IP_SET?, UNIX_CONF_PATH ?, PASSWORD_ENCRYPTION ?, LOGIN_TYPE ?, DIGITAL_VAULT ?, NETWORK_ID ?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/USERNAME? (#PCDATA)	The user name used for authentication.
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/DATABASE (#PCDATA)	The database instance you want to authenticate to.

XPath	element specifications / notes
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/PORT (#PCDATA)	The port where the database instance is running.
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/SSL_VERIFY (#PCDATA)	1 means SSL verification is enabled; 0 means it is not enabled.
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/HOSTS (HOST+)	
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/HOSTS/HOST (#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_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/UNIX_CONF_PATH (#PCDATA)	The full path to the SAP HANA configuration file on your Unix assets (IP addresses).
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/PASSWORD_ENCRYPTION (#PCDATA)	1 means password encryption is enabled in the record and 0 (the default) means password encryption is not enabled.
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/LOGIN_TYPE (#PCDATA)	Login type can be basic (the default) or vault. Set to vault if a third party vault will be used to retrieve the password.
/AUTH_SAP_HANA_LIST_OUTPUT/RESPONSE/AUTH_SAP_HANA_LIST/AUTH_SAP_HANA/DIGITAL_VAULT	(DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)
	Vault information, when a vault is defined for the record. See Vault Information .

Microsoft SharePoint Response

Microsoft SharePoint specific elements (in bold) are described below.

XPath	element specifications / notes
/AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT/RESPONSE/AUTH_MICROSOFT_SHAREPOINT_LIST ID_SET /AUTH_MICROSOFT_SHAREPOINT	(ID, TITLE, USERNAME? , IP_SET?, MSSQL? , LOGIN_TYPE?, DIGITAL_VAULT? , NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)
/AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT/RESPONSE/AUTH_MICROSOFT_SHAREPOINT_LIST ID_SET /AUTH_MICROSOFT_SHAREPOINT/USERNAME? (#PCDATA)	The user name used for authentication.
/AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT/RESPONSE/AUTH_MICROSOFT_SHAREPOINT_LIST ID_SET /AUTH_MICROSOFT_SHAREPOINT/MSSQL? (#PCDATA)	(DB_LOCAL?, WINDOWS_DOMAIN?, KERBEROS?, NTLMV2?, NTLMV1?)

XPath	element specifications / notes
	Values for MS SQL parameters.
/AUTH_MICROSOFT_SHAREPOINT_LIST_OUTPUT/RESPONSE/AUTH_MICROSOFT_SHAREPOINT_LIST ID_SET/AUTH_MICROSOFT_SHAREPOINT/DIGITAL_VAULT? (#PCDATA)	
	Vault information, when a vault is defined for the record. See Vault Information .

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?, VAULT_AUTHORIZATION_NAME?, VAULT_TARGET_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.
/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.
/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.

XPath	element specifications / notes
/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).
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_ACCOUNT_NAME (#PCDATA)	The account name for vault type BeyondTrust PBPS.
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_AUTHORIZATION_NAME (#PCDATA)	The authorization name for vault type Wallix AdminBastion (WAB).
/AUTH_<TYPE>_LIST_OUTPUT/RESPONSE/AUTH_<TYPE>_LIST/AUTH_<TYPE>/DIGITAL_VAULT/VAULT_TARGET_NAME (#PCDATA)	The target name for vault type Wallix AdminBastion (WAB).

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)	

XPath

element specifications / notes

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

<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 Vault List Output

API used

<platform API server>/api/2.0/fo/vault/ with action=list

DTD for Authentication Vault List Output

<platform API server>/api/2.0/fo/vault/vault_output.dtd

A recent DTD 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

XPath	element specifications / notes
/AUTH_VAULT_LIST_OUTPUT	(REQUEST?, RESPONSE)
/AUTH_VAULT_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)

XPath	element specifications / notes
/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.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/VAULT_TYPE (#PCDATA)	The vault type, one of: CyberArk PIM Suite, CyberArk 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 vault server. Valid for: CyberArk PIM Suite, Quest Vault.
/AUTH_VAULT_LIST_OUTPUT/RESPONSE/AUTH_VAULTS/AUTH_VAULT/ID (#PCDATA)	The vault ID.

Authentication Vault View Output

API used

<platform API server>/api/2.0/fo/vault/ with action=view

DTD for Authentication Vault View Output

<platform API server>/api/2.0/fo/vault/vault_view.dtd

A recent DTD 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?,
                       API_VERSION?, AUTH_TYPE?, PATH?, ROLE_NAME?,
                       ROLE_ID?, SECRET_ID?, APP_ID?, (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 API_VERSION (#PCDATA)>
<!ELEMENT AUTH_TYPE (#PCDATA)>
<!ELEMENT PATH (#PCDATA)>
<!ELEMENT ROLE_NAME (#PCDATA)>
<!ELEMENT ROLE_ID (#PCDATA)>
<!ELEMENT SECRET_ID (#PCDATA)>
<!ELEMENT APP_ID (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME, BY?)>
<!ELEMENT BY (#PCDATA)>
<!-- EOF -->
```

XPaths for 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_QUEST)
/AUTH_VAULT_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/AUTH_VAULT_OUTPUT/RESPONSE/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?, API_VERSION?, AUTH_TYPE?, PATH?, ROLE_NAME?, ROLE_ID?, SECRET_ID?, APP_ID?, (UUID ID))
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/TITLE (#PCDATA)	The vault title.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/COMMENTS (#PCDATA)	

XPath	element specifications / notes
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/VAULT_TYPE (#PCDATA)	User-defined comments for the vault. The vault type, one of: CyberArk PIM Suite, CyberArk AIM, Thycotic Secret Server, Quest Vault, CA Access Control, Hitachi ID PAM, Lieberman ERPM, BeyondTrust PBPS
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/CREATED_ON (#PCDATA)	The date/time when the vault was first created.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/OWNER (#PCDATA)	The vault owner.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/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_QUESTION/APPKEY (#PCDATA)	The application key (alpha-numeric string) provided by the customer for the BeyondTrust PBPS web services API.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/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_QUESTION/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_QUESTION/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_QUESTION/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_QUESTION/API_USERNAME (#PCDATA)	The username to be used for authentication to the vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/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.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/SERVER_ADDRESS (#PCDATA)	The IP address of the vault server. Valid for vault types: CyberArk PIM Suite, Quest Vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/PORT (#PCDATA)	The port the vault server is running on. Valid for vault types: CyberArk PIM Suite, Quest Vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/SAFE (#PCDATA)	The name of the digital password safe for CyberArk PIM Suite vault. Not valid for other vault types.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUESTION/API_VERSION (#PCDATA)	The HTTP or HTTPS URL to access the Vault HTTP API. Valid for the HashiCorp vault.

XPath	element specifications / notes
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/AUTH_TYPE (#PCDATA)	The authentication types supported by vault API: userpass, cert and approle. Valid for the HashiCorp vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/PATH (#PCDATA)	The path for the Username/Password authentication method. Valid for the HashiCorp vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/ROLE_NAME (#PCDATA)	The role associated with the CA certificate. Valid for the HashiCorp vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/ROLE_ID (#PCDATA)	The role ID of the App Role you want to use for authentication. Valid for the HashiCorp vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/SECRET_ID (#PCDATA)	The secret ID of the App Role you want to use for authentication. Valid for the HashiCorp vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/APP_ID (#PCDATA)	The application ID associated with the vault application created in the Azure Key Vault.
/AUTH_VAULT_OUTPUT/RESPONSE/VAULT_QUEST/(UUID ID) (#PCDATA)	The vault ID and UUID if available.

Chapter 5 - Assets XML

This section describes the XML output returned from Assets API requests.

[IP List Output](#)

[Host List Output](#)

[Host Update Output](#)

[Host Purge Output](#)

[Host List VM Detection Output](#)

[Excluded Hosts List Output](#)

[Excluded Hosts Change History Output](#)

[Virtual Host List Output](#)

[IPv6 Mapping Records List Output](#)

[vCenter - ESXi Mapping Records List Output](#)

[Restricted IPs List Output](#)

[Duplicate Hosts Error Output](#)

[Asset Group List Output](#)

[Asset Search Report](#)

[Network List Output](#)

[Patch List Output](#)

IP List Output

API used

[<platform API server>/api/2.0/fo/asset/ip](#) with action=list

DTD for Auth Record List Output

[<platform API server>/api/2.0/fo/asset/ip/ip_list_output.dtd](#)

A recent DTD 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

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

API used

<platform API server>/api/2.0/fo/asset/host/ with action=list

DTD for Host List Output

<platform API server>/api/2.0/fo/asset/host/dtd/list/output.dtd

A recent DTD is shown below.

```
<!-- QUALYS HOST_OUTPUT DTD FOR LIST ACTION-->
<!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, ASSET_ID?, IP?, IPV6?, ASSET_RISK_SCORE?,
TRURISK_SCORE?, ASSET_CRITICALITY_SCORE?,
ARS_FACTORS?,TRURISK_SCORE_FACTORS?, TRACKING_METHOD?, NETWORK_ID?,
DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?,
LAST_BOOT?, SERIAL_NUMBER?, HARDWARE_UUID?, FIRST_FOUND_DATE?,
LAST_ACTIVITY?, AGENT_STATUS?, CLOUD_AGENT_RUNNING_ON?, TAGS?, METADATA?,
CLOUD_PROVIDER_TAGS?, 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?, LAST_SCAP_SCAN_DATETIME?,
OWNER?, COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT ASSET_RISK_SCORE (#PCDATA)>
<!ELEMENT TRURISK_SCORE (#PCDATA)>
<!ELEMENT ASSET_CRITICALITY_SCORE (#PCDATA)>
<!ELEMENT ARS_FACTORS (ARS_FORMULA, VULN_COUNT*)>
<!ELEMENT ARS_FORMULA (#PCDATA)>
<!ELEMENT TRURISK_SCORE_FACTORS (TRURISK_SCORE_FORMULA, VULN_COUNT*)>
<!ELEMENT TRURISK_SCORE_FORMULA (#PCDATA)>
<!ELEMENT VULN_COUNT (#PCDATA)>
<!ATTLIST VULN_COUNT qds_severity CDATA #REQUIRED>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
```

```

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)>
<!ELEMENT HOSTNAME (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_BOOT (#PCDATA)>
<!ELEMENT SERIAL_NUMBER (#PCDATA)>
<!ELEMENT HARDWARE_UUID (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATE (#PCDATA)>
<!ELEMENT LAST_ACTIVITY (#PCDATA)>
<!ELEMENT AGENT_STATUS (#PCDATA)>
<!ELEMENT CLOUD_AGENT_RUNNING_ON (#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 LAST_SCAP_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)>
<!--ATTLIST VALUE_1
ud_attr CDATA #REQUIRED-->
<!ELEMENT VALUE_2 (#PCDATA)>
<!--ATTLIST VALUE_2
ud_attr CDATA #REQUIRED-->
<!ELEMENT VALUE_3 (#PCDATA)>
<!--ATTLIST VALUE_3
ud_attr CDATA #REQUIRED-->

<!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 CLOUD_PROVIDER_TAGS (CLOUD_TAG+)>
<!ELEMENT CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)>

<!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

XPath	element specifications / notes
/HOST_LIST_OUTPUT	(REQUEST?,RESPONSE)
/HOST_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/HOST_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/HOST_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/HOST_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/HOST_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+))
/HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/HOST_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/HOST_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.

XPath	element specifications / notes
/HOST_LIST_OUTPUT/RESPONSE	(DATETIME, (HOST_LIST ID_SET)?, WARNING?, GLOSSARY?)
/HOST_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the Qualys response.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST	(HOST+)
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST	(ID, ASSET_ID?, IP?, IPV6?, ASSET_RISK_SCORE?, TRURISK_SCORE?, ASSET_CRITICALITY_SCORE?, ARS_FACTORS?, TRURISK_SCORE_FACTORS?, TRACKING_METHOD?, NETWORK_ID?, DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?, CLOUD_RESOURCE_ID?, 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?, CLOUD_PROVIDER_TAGS?) The HOST element is returned when the “details” input parameter is set to “basic” or “all” or if the parameter is unspecified.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ID	(#PCDATA) The host ID.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_ID	(#PCDATA) The asset ID of the host.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/IP	(#PCDATA) The asset's IP address.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/IPV6	(#PCDATA) The asset's IPv6 address.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_RISK_SCORE	(#PCDATA) The asset risk score (ARS). This is the overall risk score assigned to the asset based on multiple contributing factors. ARS has a range from 0 to 1000: - Severe (850-1000) - High (700-849) - Medium (500-699) - Low (0-499) Note: This element is now replaced with TRURISK_SCORE. The ASSET_RISK_SCORE element will be deprecated in an upcoming release.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRURISK_SCORE	(#PCDATA) The TruRisk score. This is the overall risk score assigned to the asset based on multiple contributing factors. TruRisk score has a range from 0 to 1000: - Severe (850-1000) - High (700-849) - Medium (500-699) - Low (0-499)
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_CRITICALITY_SCORE	(#PCDATA) The asset criticality score (ACS).

XPath	element specifications / notes
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ARS_FACTORS (ARS_FORMULA, VULN_COUNT*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ARS_FACTORS/ARS_FORMULA (#PCDATA)	
	The formula used to calculate the ARS.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ARS_FACTORS/VULN_COUNT (#PCDATA)	
	The vulnerability count at each QDS (Qualys Detection Score) severity level.
attribute: qds_severity	qds_severity is required for each vulnerability count
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRURISK_SCORE_FACTORS (ATRURISK_SCORE_FORMULA, VULN_COUNT*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRURISK_SCORE_FACTORS/TRURISK_SCORE_FORMULA (#PCDATA)	
	The formula used to calculate the TruRisk score.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRURISK_SCORE_FACTORS/VULN_COUNT (#PCDATA)	
	The vulnerability count at each QDS (Qualys Detection Score) severity level.
attribute: qds_severity	qds_severity is required for each vulnerability count
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	
	The tracking method assigned to the asset: IP, DNS, NETBIOS, EC2.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/NETWORK_ID (#PCDATA)	
	The network ID of the asset, if the Networks feature is enabled.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS (#PCDATA)	
	DNS name for the asset. For an EC2 asset this is the private DNS name.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/HOSTNAME (#PCDATA)	
	The DNS hostname for the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/DOMAIN (#PCDATA)	
	The domain name for the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/FQDN (#PCDATA)	
	The Fully Qualified Domain Name (FQDN) for the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_SERVICE (#PCDATA)	
	Cloud service of the asset. For example: (VM for Azure, EC2 for AWS).
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_RESOURCE_ID (#PCDATA)	
	Cloud resource ID of the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/EC2_INSTANCE_ID (#PCDATA)	
	EC2 instance ID for the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/NETBIOS (#PCDATA)	
	NetBIOS host name for the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/OS (#PCDATA)	
	Operating system detected on the asset.
/HOST_LIST_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_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_BOOT (#PCDATA)	
	The date and time when the host asset was last rebooted.

XPath	element specifications / notes
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/SERIAL_NUMBER (#PCDATA)	The BIOS serial number of the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/HARDWARE_UUID (#PCDATA)	The BIOS hardware UUID of the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/FIRST_FOUND_DATE (#PCDATA)	The date and time when the asset was first listed or detected on Qualys platform.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_ACTIVITY (#PCDATA)	(Agent Only) The date and time when the host asset was last active.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/AGENT_STATUS (#PCDATA)	(Agent Only) The status or activity of the agent on the asset.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_AGENT_RUNNING_ON (#PCDATA)	(Agent Only) The name of the cloud on which the agent is deployed.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS (TAG_ID?, NAME?)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG_ID (#PCDATA)	A tag ID associated with the asset when show_tags=1 is specified.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/NAME (#PCDATA)	A tag name associated with the asset when show_tags=1 is specified.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA	(EC2 GOOGLE AZURE)+
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 (ATTRIBUTE*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/GOOGLE (ATTRIBUTE*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/AZURE (ATTRIBUTE*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE	(NAME, LAST_STATUS, VALUE, LAST_SUCCESS_DATE?, LAST_ERROR_DATE?, LAST_ERROR?)
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/NAME (#PCDATA)	Attribute name, fetched from instance metadata.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_STATUS (#PCDATA)	Attribute last status, fetched from instance metadata.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/VALUE (#PCDATA)	Attribute value fetched, from instance metadata.
/HOST_LIST_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_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_ERROR_DATE (#PCDATA)	Attribute last error date/time, fetched from instance metadata.

XPath	element specifications / notes
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/METADATA/EC2 GOOGLE AZURE/ATTRIBUTE/LAST_ERROR (#PCDATA)	Attribute last error, fetched from instance metadata.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS (CLOUD_TAG*)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)	
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG/NAME (#PCDATA)	The name of the cloud tag.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG/VALUE (#PCDATA)	The value of the cloud tag.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG/LAST_SUCCESS_DATE (#PCDATA)	Tag last success date/time, fetched from instance.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VULN_SCAN_DATETIME (#PCDATA)	The date and time of the most recent vulnerability scan.
/HOST_LIST_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_LIST_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_LIST_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_LIST_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_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)	The date and time of the most recent compliance scan.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_SCAP_SCAN_DATETIME (#PCDATA)	The date and time of the most recent SCAP scan.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/OWNER (#PCDATA)	The asset owner.
/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/COMMENTS (#PCDATA)	The comments defined for the asset.
/HOST_LIST_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_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/USER_DEF/LABEL_n (#PCDATA)	Not returned inside the <HOST> element. Returned inside <GLOSSARY>.

XPath	element specifications / notes
/HOST_LIST_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_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_GROUP_IDS (#PCDATA)	The asset group IDs for the asset groups which the host belongs to.
/HOST_LIST_OUTPUT/RESPONSE/ID_SET ((ID ID_RANGE)+)	The ID_SET element is returned when the “details” input parameter is set to “none”.
/HOST_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	A host ID.
/HOST_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	A host ID range.
/HOST_LIST_OUTPUT/RESPONSE/WARNING (CODE?, TEXT, URL?)	
/HOST_LIST_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_LIST_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_LIST_OUTPUT/RESPONSE/WARNING/URL (#PCDATA)	The URL for making another request for the next batch of host records.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY (USER_DEF?, USER_LIST?, ASSET_GROUP_LIST?)	
/HOST_LIST_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_LIST_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_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_DEF/VALUE_n (#PCDATA)	Not returned inside the <GLOSSARY> element. Returned inside <HOST>.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST (USER+)	A list of users who are asset owners for the hosts in the host list output.
/HOST_LIST_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_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER_LOGIN (#PCDATA)	A user login ID.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER/FIRST_NAME (#PCDATA)	A user’s first name.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST/USER/LAST_NAME	A user’s last name.

XPath	element specifications / notes
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST (ASSET_GROUP+)	A list of asset groups which hosts in the host list output belong to.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP (ID, TITLE)	
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP/ID	An asset group ID.
/HOST_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP/TITLE	An asset group title.

Host Update Output

API used

<platform API server>/api/2.0/fo/asset/host/ with action=update

DTD for Host Update Output

<platform API server>/api/2.0/fo/asset/host/dtd/update/output.dtd

A recent DTD is shown below.

```
<!-- QUALYS HOST_UPDATE DTD FOR UPDATE ACTION-->
<!-- $Revision$ -->
<!ELEMENT HOST_UPDATE_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 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*)>
<!-- EOF -->
```

XPaths for Host Update Output

XPath	element specifications / notes
/HOST_UPDATE_OUTPUT	(REQUEST?,RESPONSE)
/HOST_UPDATE_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/HOST_UPDATE_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the API request.
/HOST_UPDATE_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/HOST_UPDATE_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/HOST_UPDATE_OUTPUT/REQUEST/PARAM_LIST	(PARAM+))
/HOST_UPDATE_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE))
/HOST_UPDATE_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.

XPath	element specifications / notes
/HOST_UPDATE_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/HOST_UPDATE_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.
/HOST_UPDATE_OUTPUT/RESPONSE (DATETIME, CODE?, TEXT, ITEM_LIST?)	
/HOST_UPDATE_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/HOST_UPDATE_OUTPUT/RESPONSE/CODE (#PCDATA)	The response error code.
/HOST_UPDATE_OUTPUT/RESPONSE/TEXT (#PCDATA)	The response error text.
/HOST_UPDATE_OUTPUT/RESPONSE/ITEM_LIST (ITEM+)	
/HOST_UPDATE_OUTPUT/RESPONSE/ITEM_LIST/ITEM (KEY, VALUE+)	
/HOST_UPDATE_OUTPUT/RESPONSE/ITEM_LIST/ITEM/KEY (#PCDATA)	The response item keyword.
/HOST_UPDATE_OUTPUT/RESPONSE/ITEM_LIST/ITEM/VALUE (#PCDATA)	The response item value.

Host Purge Output

API used

<platform API server>/api/2.0/fo/asset/host/ with action=purge

DTD for Host Purge Output

<platform API server>/api/2.0/fo/asset/host/dtd/purge/output.dtd

A recent DTD is shown below.

```
<!-- QUALYS HOST_OUTPUT DTD FOR PURGE ACTION-->
<!-- $Revision$ -->
<!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 Host Update 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)

XPath	element specifications / notes
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.	
/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.	

Host List VM Detection Output

API used

[platform API server](#)/api/2.0/fo/asset/host/vm/detection with action=list

DTD for Host List VM Detection Output

[platform API server](#)/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd

A recent DTD 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, ASSET_ID?, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?,
OS?, OS_CPE?, DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, 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?, CLOUD_PROVIDER_TAGS?,
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 DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)>
<!ELEMENT HOSTNAME (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#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 (UNIQUE_VULN_ID, QID, TYPE, SEVERITY?, PORT?,
PROTOCOL?, FQDN?, SSL?, INSTANCE?, RESULTS?,
STATUS?, FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?, QDS?, QDS_FACTORS?,
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?, ASSET_CVE?)>
<!ELEMENT UNIQUE_VULN_ID (#PCDATA)>
<!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 QDS (#PCDATA)>
<!ATTLIST QDS severity CDATA #REQUIRED>
<!ELEMENT QDS_FACTORS (QDS_FACTOR)*>
<!ELEMENT QDS_FACTOR (#PCDATA)>
<!ATTLIST QDS_FACTOR name CDATA #REQUIRED>
<!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

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.
/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.

XPath	element specifications / notes
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST (HOST+)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST	(ID, ASSET_ID?, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?, OS?, OS_CPE?, DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?, CLOUD_RESOURCE_ID?, 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?, CLOUD_PROVIDER_TAGS?, 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/ASSET_ID (#PCDATA)	Asset ID of the host.
/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/DNS_DATA	(HOSTNAME?, DOMAIN?, FQDN?)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/HOSTNAME (#PCDATA)	The DNS hostname for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/DOMAIN (#PCDATA)	The domain name for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS_DATA/FQDN (#PCDATA)	The Fully Qualified Domain Name (FQDN) for the asset.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER (#PCDATA)	Cloud provider of the asset. These will be populated for all cloud assets (Azure, EC2, Google).
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_SERVICE (#PCDATA)	Cloud service of the asset. For example: (VM for Azure, EC2 for AWS).
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_RESOURCE_ID (#PCDATA)	Cloud resource ID of the asset.

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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?)
/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/CLOUD_PROVIDER_TAGS (CLOUD_TAG+)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG /NAME (#PCDATA)	The name of the cloud tag.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG /VALUE (#PCDATA)	The value of the cloud tag.
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/CLOUD_PROVIDER_TAGS/CLOUD_TAG /LAST_SUCCESS_DATE (#PCDATA)	Tag last success date/time, fetched from instance.

XPath	element specifications / notes
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST (DETECTION+)	
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION	(UNIQUE_VULN_ID, QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?, INSTANCE?, RESULTS?, STATUS?, FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?, QDS?, QDS_FACTORS?, 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?, ASSET_CVE?)
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/UNIQUE_VULN_ID (#PCDATA)	The unique ID of the vulnerability detection. It distinguishes each vulnerability detection uniquely across different assets, ports, services, etc.
/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.
/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.

XPath	element specifications / notes
/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/QDS (#PCDATA)	The Qualys Detection Score (QDS) for the vulnerability detection. The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability. QDS has a range from 1 to 100 with these severity levels: - Critical (90-100) - High (70-89) - Medium (40-69) - Low (1-39)
attribute: severity	severity is <i>required</i> and corresponds to the QDS score
/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/QDS_FACTORS (QDS_FACTOR)	Factors that contributed to the QDS.
attribute: name	name is <i>required</i> for each contributing factor
/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.
/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.

XPath	element specifications / notes
/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 not exploitable because it was found on non-running port/service. A value of 0 indicates that it is exploitable because it was found on a 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 not exploitable due to the current host configuration. A value of 0 indicates that it is 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.
/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.

XPath	element specifications / notes
/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

API used

[platform API server](#)/api/2.0/fo/asset/excluded_ip/?action=list

DTD for Excluded Host List Output

[platform API server](#)/api/2.0/fo/asset/excluded_ip/ip_list_output.dtd

A recent DTD 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

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.

XPath	element specifications / notes
/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

API used

[<platform API server>](#)/api/2.0/fo/asset/excluded_ip/history/?action=list

DTD for Excluded Host Change History Output

[<platform API server>](#)/api/2.0/fo/asset/excluded_ip/history/history_list_output.dtd

A recent DTD 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

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.
/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.

XPath	element specifications / notes
/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

API used

[platform API server](#)/api/2.0/fo/asset/vhost/?action=list

DTD for Virtual Host List Output

[platform API server](#)/api/2.0/fo/asset/vhost/vhost_list_output.dtd

A recent DTD 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

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 echo_request=1.
/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 echo_request=1.
/VIRTUAL_HOST_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.

XPath	element specifications / notes
/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 echo_request=1.
/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 echo_request=1.
/VIRTUAL_HOST_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.
/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

API used

<platform API server>/api/2.0/fo/asset/ip/v4_v6/?action=list

DTD for IPv6 Mapping Records List Output

<platform API server>/api/2.0/fo/asset/ip/v4_v6/ip_map_list_output.dtd

A recent DTD 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

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 echo_request=1.
/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 echo_request=1.
/IP_MAP_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.
/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 echo_request=1.
/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 echo_request=1.
/IP_MAP_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.
/IP_MAP_LIST_OUTPUT/RESPONSE	(DATETIME, IP_MAP_LIST?)
/IP_MAP_LIST_OUTPUT/RESPONSE/DATETIME	(#PCDATA) The date and time of the Qualys response.

XPath	element specifications / notes
/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.

vCenter - ESXi Mapping Records List Output

API used

[<platform API server>](#)/api/2.0fo/auth/vcenter/vcenter_mapping/?action=list

DTD for IPv6 Mapping Records List Output

[<platform API server>](#)/api/2.0/fo/auth/vcenter/vcenter_mapping/vcenter_esxi_map_list_output.dtd

A recent DTD is shown below.

```
<!-- QUALYS VCENTER_ESXI_MAP_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT VCENTER_ESXI_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, VCENTER_ESXI_MAP_LIST?, WARNING?)>
<!ELEMENT VCENTER_ESXI_MAP_LIST (VCENTER_ESXI_MAP+)>
<!ELEMENT VCENTER_ESXI_MAP (VCENTER_IP, ESXI_IP, MAPPING_DATA_SOURCE?)>
<!ELEMENT VCENTER_IP (#PCDATA)>
<!ELEMENT ESXI_IP (#PCDATA)>
<!ELEMENT MAPPING_DATA_SOURCE (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```

XPaths for vCenter - ESXi Mapping Records List Output

XPath	element specifications / notes
/VCENTER_ESXI_MAP_LIST_OUT (REQUEST?,RESPONSE) PUT	
/VCENTER_ESXI_MAP_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/VCENTER_ESXI_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 echo_request=1.
/VCENTER_ESXI_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 echo_request=1.
/VCENTER_ESXI_MAP_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.
/VCENTER_ESXI_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+))	
/VCENTER_ESXI_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE))	
/VCENTER_ESXI_MAP_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name. This element appears only when the API request includes the parameter echo_request=1.
/VCENTER_ESXI_MAP_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.
/VCENTER_ESXI_MAP_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.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE (DATETIME, VCENTER_ESXI_MAP_LIST?, WARNING?)	
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the Qualys response.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST (VCENTER_ESXI_MAP+)	
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST/VCENTER_ESXI_MAP (VCENTER_IP, ESXI_IP, MAPPING_DATA_SOURCE?)	
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST/VCENTER_ESXI_MAP/VCENTER_IP (#PCDATA)	A vCenter IP address for a mapping record.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST/VCENTER_ESXI_MAP/ESXI_IP (#PCDATA)	An ESXi IP address for a mapping record.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST/VCENTER_ESXI_MAP/MAPPING_DATA_SOURCE (#PCDATA)	The mapping data source for a mapping record.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/VCENTER_ESXI_MAP_LIST/WARNING (CODE?, TEXT, URL?)	
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/WARNING/CODE (#PCDATA)	

XPath	element specifications / notes
	A warning code.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/WARNING/TEXT	(#PCDATA)
	Warning message text.
/VCENTER_ESXI_MAP_LIST_OUTPUT/RESPONSE/WARNING/URL	(#PCDATA)
	Warning URL.

Restricted IPs List Output

API used

[platform API server](#)/api/2.0/fo/setup/restricted_ips/?action=list

DTD for Restricted IPs List Output

[platform API server](#)/api/2.0/fo/setup/restricted_ips/restricted_ips_output.dtd

A recent DTD 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

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 echo_request=1 .
/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 echo_request=1 .

XPath	element specifications / notes
/RESTRICTED_IPS_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.
/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 echo_request=1.
/RESTRICTED_IPS_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.
/RESTRICTED_IPS_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter echo_request=1.
/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

API used

[platform API server](#)/api/2.0/fo/asset/ip/ action=update

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 Restricted IPs List Output

[platform API server](#)/api/2.0/fo/asset/ip/duplicate_hosts_error.dtd

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

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 echo_request=1.
/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 echo_request=1.
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.
/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 echo_request=1.
/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 echo_request=1.
/DUPLICATE_HOSTS_ERROR_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any. This element appears only when the API request includes the parameter echo_request=1.
/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)
/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.

XPath	element specifications / notes
/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

API used

[platform API server](#)/api/2.0/fo/asset/group/?action=list

DTD for Asset Group List Output

[platform API server](#)/api/2.0/fo/asset/group/asset_group_list_output.dtd

A recent DTD is shown 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?, OWNER_USER_NAME?
)>

<!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)>

<!-- OWNER_USER_NAME -->
<!ELEMENT OWNER_USER_NAME (#PCDATA)>

<!-- WARNING -->
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

```

XPaths for 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 echo_request=1.
/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 echo_request=1.
/ASSET_GROUP_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request. This element appears only when the API request includes the parameter echo_request=1.
/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 echo_request=1.
/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 echo_request=1.
/ASSET_GROUP_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.
/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.
/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.

XPath	element specifications / notes
/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)
/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.

XPath	element specifications / notes
/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.
/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/ASSET_GROUP_LIST/ASSET_GROUP/OWNER_USER_NAME (#PCDATA)	The asset group owner name is displayed.
/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

API used

[<platform API server>](#)/api/2.0/fo/report/asset/?action=search

DTD for Asset Search Report Output

[<platform API server>](#)/asset_search_report_v2.dtd

A recent DTD is shown 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|FILTER_AZURE_
VM_ID|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|FILTER_AZURE_VM_STATE)+)>

<!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)>

<!ELEMENT FILTER_NETBIOS (#PCDATA)>
<!ATTLIST FILTER_NETBIOS criterion CDATA #IMPLIED>
<!ELEMENT FILTER_AZURE_VM_ID (#PCDATA)>

<!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 FILTER_AZURE_VM_STATE (#PCDATA)>
<!ELEMENT TOTAL (#PCDATA)>
<!-- HOST_LIST -->

<!ELEMENT HOST_LIST ((HOST|WARNING)*)>

<!ELEMENT HOST (ERROR | (IP, HOST_TAGS?, TRACKING_METHOD,
DNS?, CLOUD_PROVIDER?, CLOUD_SERVICE?, CLOUD_RESOURCE_ID?,
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 CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#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

XPath	element specifications / notes
/ASSET SEARCH REPORT	(ERROR (HEADER, HOST_LIST?))
/ASSET SEARCH REPORT/ERROR (#PCDATA)	An error message.
attribute: number	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)	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.

XPath	element specifications / notes
/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 FILTER_AZURE_VM_ID 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 FILTER_LAST_SCAP_SCAN_DATE FILTER_AZURE_VM_STATE)
/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*)	
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ INCLUDED_TAGS	attribute: scope 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.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ EXCLUDED_TAGS (ASSET_TAG*)	
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS/ EXCLUDED_TAGS	attribute: scope 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.
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/ASSET_TAGS (#PCDATA)	The asset tags selected for the report.

XPath	element specifications / notes
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_DNS (#PCDATA)	The DNS hostname.
attribute: criterion	criterion is <i>deprecated</i> .
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_NETBIOS (#PCDATA)	The NetBIOS hostname.
attribute: criterion	criterion is <i>deprecated</i> .
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_AZURE_VM_ID (#PCDATA)	The Azure VM ID of the host.
/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: criterion	criterion is <i>deprecated</i> .
/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: criterion	criterion is <i>deprecated</i> .
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_LAST_SCAN_DATE (#PCDATA)	The date and time of the most recent vulnerability scan.
attribute: criterion	criterion is <i>deprecated</i> .
/ASSET SEARCH REPORT/ERROR/HEADER/FILTERS/FILTER_LAST_COMPLIANCE_SCAN_DATE (#PCDATA)	The date and time of the most recent compliance scan.
attribute: criterion	criterion is <i>deprecated</i> .
/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/FILTERS/FILTER_AZURE_VM_STATE (#PCDATA)	The Azure virtual machine state. Possible values are: STARTING, RUNNING, STOPPING, STOPPED, DEALLOCATING, DEALLOCATED, UNKNOWN.

XPath	element specifications / notes
/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?, CLOUD_PROVIDER?, CLOUD_SERVICE?, CLOUD_RESOURCE_ID?, 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: network_id	network_id is <i>deprecated</i> .
/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/CLOUD_PROVIDER (#PCDATA)	Cloud provider of the asset. For example: (Azure, EC2, Google).
/ASSET SEARCH REPORT/ERROR/HOST_LIST/CLOUD_SERVICE (#PCDATA)	Cloud service of the asset. For example: (VM for Azure, EC2 for AWS).
/ASSET SEARCH REPORT/ERROR/HOST_LIST/CLOUD_RESOURCE_ID (#PCDATA)	Cloud resource ID of the asset.
/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)	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: format	format is <i>deprecated</i> .
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST (PORT_SERVICE+)	
/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)	

XPath	element specifications / notes
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/SERVICE (#PCDATA)	Hosts that has the specified open ports.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/DEFAULT_SERVICE (#PCDATA)	Hosts that has the specified services running on it.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/LAST_SCAN_DATE (#PCDATA)	Expected service to be running on the open ports
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/LAST_COMPLIANCE_SCAN_DATE (#PCDATA)	The date and time of the most recent vulnerability scan.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/PORT_SERVICE_LIST/PORT_SERVICE/FIRST_FOUND_DATE (#PCDATA)	The date and time of the most recent compliance scan.
/ASSET SEARCH REPORT/ERROR/HOST_LIST/WARNING (#PCDATA)	The date and time the host was first detected.
	A warning message. Attribute number is a warning code when available

Network List Output

API used

<platform API server>/api/2.0/fo/network/?action=list

DTD for Network List Output

<platform API server>/network_list_output.dtd

A recent DTD is shown 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

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.
/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)

XPath

element specifications / notes

The name of a scanner appliance assigned to the network.

Patch List Output

API used

[<platform API server>/api/2.0/fo/asset/patch/index.php](#)

DTD for Patch List Output

[<platform API server>/api/2.0/fo/asset/patch/host_patches.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS PATCH_LIST_OUTPUT DTD -->
<!ELEMENT PATCH_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 (SUBSCRIPTION_ID, HOST_ID, IP, DNS, NETBIOS, OS,
OS_CPE, NETWORK?, PATCH_INFO_LIST)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT PATCH_INFO_LIST (PATCH_INFO+)>
<!ELEMENT PATCH_INFO (DETECTION_QIDS, PATCH_QID, PATCH_SEVERITY,
PATCH_TITLE, PATCH_VENDOR_ID, PATCH_RELEASE_DATE, PATCH_LINKS? )>
<!ELEMENT DETECTION_QIDS (QID+)>
<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID cve_ids CDATA #IMPLIED>
<!ELEMENT PATCH_QID (#PCDATA)>
<!ATTLIST PATCH_QID cve_ids CDATA #IMPLIED>
<!ELEMENT PATCH_SEVERITY (#PCDATA)>
<!ELEMENT PATCH_TITLE (#PCDATA)>
<!ELEMENT PATCH_VENDOR_ID (#PCDATA)>
<!ELEMENT PATCH_RELEASE_DATE (#PCDATA)>
<!ELEMENT PATCH_LINKS (LINK+)>
```

```
<!ELEMENT LINK (#PCDATA)>
<!ATTLIST LINK os_sw CDATA #IMPLIED>
<!-- EOF -->
```

XPaths for Patch List Output

XPath	element specifications / notes
/PATCH_LIST_OUTPUT	(REQUEST?, RESPONSE)
/PATCH_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/PATCH_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/PATCH_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/PATCH_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/PATCH_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/PATCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/PATCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	The input parameter name.
/PATCH_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	The input parameter value.
/PATCH_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data.
/PATCH_LIST_OUTPUT/RESPONSE	(SUBSCRIPTION_ID, HOST_ID, IP, DNS, NETBIOS, OS, OS_CPE, NETWORK?, PATCH_INFO_LIST?)
/PATCH_LIST_OUTPUT/RESPONSE/SUBSCRIPTION_ID (#PCDATA)	Id assigned to the subscription.
/PATCH_LIST_OUTPUT/RESPONSE/HOST_ID (#PCDATA)	The host ID associated with the detection.
/PATCH_LIST_OUTPUT/RESPONSE/IP (#PCDATA)	The IP address of the host.
/PATCH_LIST_OUTPUT/RESPONSE/DNS (#PCDATA)	DNS hostname for the host.
/PATCH_LIST_OUTPUT/RESPONSE/NETBIOS (#PCDATA)	NetBIOS hostname for the asset.
/PATCH_LIST_OUTPUT/RESPONSE/OS (#PCDATA)	The operating system on a host.
/PATCH_LIST_OUTPUT/RESPONSE/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.)

XPath	element specifications / notes
/PATCH_LIST_OUTPUT/RESPONSE/NETWORK	(#PCDATA)
	The network name.
/PATCH_LIST_OUTPUT/RESPONSE/PATCH_INFO_LIST	(DETECTION_QIDS, PATCH_QID, PATCH_SEVERITY, PATCH_TITLE, PATCH_VENDOR_ID, PATCH_RELEASE_DATE, PATCH_LINKS?)
	Patch information (detection QID, patch QID, patch severity, patch title, patch vendor, patch release date and patch links).

Chapter 6 - VM Reports XML

This section covers report XML returned from VM Report API requests.

[Report List Output](#)

[Schedule Report List Output](#)

[Scan Report Template Output](#)

[PCI Scan Template Output](#)

[Patch Template Output](#)

[Map Template Output](#)

[Map Report Output](#)

[Patch Report \(XML\) Output](#)

[VM Scan Report Output](#)

Report List Output

API used

[platform API server](#)/api/2.0/fo/report/?action=list

DTD for Report List Output

[platform API server](#)/api/2.0/fo/report/report_list_output.dtd

A recent 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 CLIENT (ID,NAME)>
<!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

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.

XPath	element specifications / notes
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT	(ID,NAME)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT/ID (#PCDATA)	Id assigned to the client. (only for Consultant type subscriptions)
/SCAN_LIST_OUTPUT/RESPONSE/SCAN_LIST/SCAN/CLIENT /NAME (#PCDATA)	Name of the client. (only for Consultant type subscriptions)
/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.
/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 Output

API used

[<platform API server>](#)/api/2.0/fo/schedule/report/?action=list

DTD for Schedule Report List Output

[<platform API server>](#)/api/2.0/fo/schedule/report/schedule_report_list_output.dtd

A recent 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

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.

XPath	element specifications / notes
/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)	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 <i>required</i> 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 <i>required</i> for a report that runs after some number of weeks (from 1 to 52) attribute: weekdays weekdays is <i>required</i> 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 <i>required</i> for a report that runs after some number of months (from 1 to 12) attribute: day_of_month day_of_month is <i>implied</i> 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 <i>implied</i> 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	

XPath	element specifications / notes
attribute: week_of_month	week_of_month is <i>implied</i> 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.
/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

API used

[platform API server](#)/api/2.0/fo/report/template/scan/?action=export

DTD for Scan Report Template Output

[platform API server](#)/api/2.0/fo/report/template/scan/scanreporttemplate_info.dtd

A recent 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

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.
/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	

XPath	element specifications / notes
/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

API used

[platform API server](#)/api/2.0/fo/report/template/pciscan/?action=export

DTD for PCI Scan Template Output

[platform API server](#)/api/2.0/fo/report/template/pciscan/pciscanreporttemplate_info.dtd

A recent 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

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)
	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	

XPath	element specifications / notes
/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

API used

[platform API server](#)/api/2.0/fo/report/template/patch/?action=export

DTD for Patch Template Output

[platform API server](#)/api/2.0/fo/report/template/patch/patchreporttemplate_info.dtd

A recent 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

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.
/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

API used

[<platform API server>](#)/api/2.0/fo/report/template/map/?action=export

DTD for Map Template Output

[<platform API server>](#)/api/2.0/fo/report/template/map/mapreporttemplate_info.dtd

A recent 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

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	
/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)	
	The selected operating system.

Map Report Output

API used

<platform API server>/api/2.0/fo/report/?action=fetch

<platform API server>/msp/map_report.php

DTD for Map Report Output

<platform API server>/map.dtd

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

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.
/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.

XPath	element specifications / notes
/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.
/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.

Patch Report (XML) Output

API used

[platform API server](#)/api/2.0/fo/report/?action=fetch

DTD for Patch Report Output

[platform API server](#)/patch_report.dtd

A recent DTD is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS PATCH REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT PATCH_REPORT (ERROR | (HEADER, (SUMMARY | (REPORT_SUMMARY,
PATCH_SUMMARY)), PATCH_LIST_BY_HOST?, PATCH_LIST_BY_AG?,
PATCH_LIST_BY_OS?, PATCH_LIST_BY_QID?, NON_RUNNING_KERNELS?))>
<!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)>

<!-- SUMMARY DETAILS -->
<!ELEMENT SUMMARY (REPORT_SUMMARY, PATCH_SUMMARY)>

<!ELEMENT REPORT_SUMMARY (TITLE, ASSET_GROUPS?, IPS?, ASSET_TAGS?,
GROUP_BY, CREATED_ON, NETWORK?)>
  <!ELEMENT ASSET_GROUPS (#PCDATA)>
  <!ELEMENT TITLE (#PCDATA)>
  <!ELEMENT IPS (#PCDATA)>
  <!ELEMENT ASSET_TAGS (#PCDATA)>
  <!ELEMENT GROUP_BY (#PCDATA)>
  <!ELEMENT CREATED_ON (#PCDATA)>

<!ELEMENT PATCH_SUMMARY (TOTAL_PATCHES, HOST_REQUIRING_PATCHES,
VULN_ADDRESSED)>
  <!ELEMENT TOTAL_PATCHES (#PCDATA)>
  <!ELEMENT HOST_REQUIRING_PATCHES (#PCDATA)>
```

```

    <!-- ELEMENT VULN_ADDRESSED (#PCDATA)>

<!-- PATCH_LIST_BY_HOST -->
<!-- ELEMENT PATCH_LIST_BY_HOST (HOST_LIST?, PATCH_LINKS?)>

<!-- PATCH_LIST_BY_ASSET GROUP -->
<!-- ELEMENT PATCH_LIST_BY_AG (ASSET_GROUPS_LIST, PATCH_LINKS?)>

<!-- ELEMENT ASSET_GROUPS_LIST (ASSET_GROUP*)>
<!-- ELEMENT ASSET_GROUP (NAME?, TOTAL_PATCHES?, HOST_NEEDING_PATCHES?,
TOTAL_DETECTION_FIXED?, HOST_LIST?)>
    <!-- ELEMENT HOST_NEEDING_PATCHES (#PCDATA)>
    <!-- ELEMENT TOTAL_DETECTION_FIXED (#PCDATA)>

<!-- PATCH_LIST_BY_QID -->
<!-- ELEMENT PATCH_LIST_BY_QID (PATCH_LIST, PATCH_LINKS?)>
    <!-- ELEMENT PATCH_LIST (PATCH_INFO*)>

<!-- PATCH_LIST_BY_OS -->
<!-- ELEMENT PATCH_LIST_BY_OS (OS_LIST?, PATCH_LINKS?)>

<!-- ELEMENT OS_LIST (OS_DETAILS*)>
<!-- ELEMENT OS_DETAILS (NAME?, TOTAL_PATCHES?,
SUMMARY_HOSTS_NEEDING_PATCHES?, SUMMARY_TOTAL_DETECTIONS_FIXED?,
PATCH_LIST)>
    <!-- ELEMENT SUMMARY_HOSTS_NEEDING_PATCHES (#PCDATA)>
    <!-- ELEMENT SUMMARY_TOTAL_DETECTIONS_FIXED (#PCDATA)>

<!-- ELEMENT HOST_LIST (HOST*)>

<!-- ELEMENT HOST (IP?, DNS?, NETBIOS?, OS?, OS_CPE?, PATCH_COUNT?,
VULN_COUNT?, NETWORK?, CLOUD_PROVIDER?, CLOUD_PROVIDER_SERVICE?,
CLOUD_RESOURCE_TYPE?, CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?,
CLOUD_IMAGE_ID?, CLOUD_RESOURCE_METADATA?, PATCH_LIST?, DETECTION_INFO?
)>
    <!-- ELEMENT IP (#PCDATA)>
    <!-- ELEMENT DNS (#PCDATA)>
    <!-- ELEMENT NETBIOS (#PCDATA)>
    <!-- ELEMENT OS (#PCDATA)>
    <!-- ELEMENT OS_CPE (#PCDATA)>
    <!-- ELEMENT PATCH_COUNT (#PCDATA)>
    <!-- ELEMENT NETWORK (#PCDATA)>
    <!-- ELEMENT CLOUD_PROVIDER (#PCDATA)>
    <!-- ELEMENT CLOUD_PROVIDER_SERVICE (#PCDATA)>
    <!-- ELEMENT CLOUD_RESOURCE_TYPE (#PCDATA)>
    <!-- ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
    <!-- ELEMENT CLOUD_ACCOUNT (#PCDATA)>
    <!-- ELEMENT CLOUD_IMAGE_ID (#PCDATA)>

<!-- ELEMENT CLOUD_RESOURCE_METADATA (INSTANCE_ID?, PUBLIC_DNS_NAME?,
PUBLIC_IP_ADDRESS?, PRIVATE_IP_ADDRESS?, IMAGE_ID?, SPOT_INSTANCE?,
AVAILABILITY_ZONE?, VPC_ID?,

```

```

        GROUP_ID?, GROUP_NAME?, LOCAL_HOSTNAME?, INSTANCE_STATE?,
PRIVATE_DNS_NAME?, INSTANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?,
RESERVATION_ID?, MAC_ADDRESS?)>
    <!--ELEMENT INSTANCE_ID (#PCDATA)>
    <!--ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
    <!--ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
    <!--ELEMENT PRIVATE_IP_ADDRESS (#PCDATA)>
    <!--ELEMENT IMAGE_ID (#PCDATA)>
    <!--ELEMENT SPOT_INSTANCE (#PCDATA)>
    <!--ELEMENT AVAILABILITY_ZONE (#PCDATA)>
    <!--ELEMENT VPC_ID (#PCDATA)>
    <!--ELEMENT GROUP_ID (#PCDATA)>
    <!--ELEMENT GROUP_NAME (#PCDATA)>
    <!--ELEMENT LOCAL_HOSTNAME (#PCDATA)>
    <!--ELEMENT INSTANCE_STATE (#PCDATA)>
    <!--ELEMENT PRIVATE_DNS_NAME (#PCDATA)>
    <!--ELEMENT INSTANCE_TYPE (#PCDATA)>
    <!--ELEMENT ACCOUNT_ID (#PCDATA)>
    <!--ELEMENT REGION_CODE (#PCDATA)>
    <!--ELEMENT SUBNET_ID (#PCDATA)>
    <!--ELEMENT RESERVATION_ID (#PCDATA)>
    <!--ELEMENT MAC_ADDRESS (#PCDATA)>

<!--ELEMENT PATCH_INFO (PATCH_QID?, VENDOR_ID?, SEVERITY?, PATCH_TITLE?,
VULN_COUNT?, HOST_COUNT?, PATCH_PUBLISHED?, CVSS_BASE_SCORE?,
CVSS3_BASE_SCORE?, CVSS3_VERSION?, NETWORK?, DETECTION_INFO?,
HOST_LIST?)>
    <!--ELEMENT PATCH_QID (#PCDATA)>
    <!--ELEMENT VENDOR_ID (#PCDATA)>
    <!--ELEMENT SEVERITY (#PCDATA)>
    <!--ELEMENT PATCH_TITLE (#PCDATA)>
    <!--ELEMENT VULN_COUNT (#PCDATA)>
    <!--ELEMENT HOST_COUNT (#PCDATA)>
    <!--ELEMENT PATCH_PUBLISHED (#PCDATA)>
    <!--ELEMENT CVSS_BASE_SCORE (#PCDATA)>
    <!--ELEMENT CVSS3_BASE_SCORE (#PCDATA)>
    <!--ELEMENT CVSS3_VERSION (#PCDATA)>
    <!--ELEMENT DETECTION_INFO (DETECTION*)>

    <!--ELEMENT DETECTION (VULN_QID?, VULN_SEVERITY?, VULN_TYPE?,
VULN_TITLE?, DETECTION_INSTANCE?, DETECTION_NORMALIZED_INSTANCE?,
DETECTION_DATE_LAST_FOUND?, CVSS_BASE_SCORE?, CVSS3_BASE_SCORE?,
CVSS3_VERSION?)>
        <!--ELEMENT VULN_QID (#PCDATA)>
        <!--ELEMENT VULN_SEVERITY (#PCDATA)>
        <!--ELEMENT VULN_TYPE (#PCDATA)>
        <!--ELEMENT VULN_TITLE (#PCDATA)>
        <!--ELEMENT DETECTION_INSTANCE (#PCDATA)>
        <!--ELEMENT DETECTION_NORMALIZED_INSTANCE (#PCDATA)>
        <!--ELEMENT DETECTION_DATE_LAST_FOUND (#PCDATA)>

<!-- PATCH_LINKS -->
<!--ELEMENT PATCH_LINKS (PATCH*)>

```

```
<!ELEMENT PATCH (PATCH_QID?, OS?, LINK?)>
<!ELEMENT NON_RUNNING_KERNELS (NON_RUNNING_KERNEL*)>
<!ELEMENT NON_RUNNING_KERNEL (QID?, IP?, SEVERITY?)>

<!ELEMENT LINK (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
```

XPaths for Patch Report Output

XPath	element specifications / notes
<!ELEMENT PATCH_REPORT (ERROR (HEADER, SUMMARY, PATCH_LIST_BY_HOST?, PATCH_LIST_BY_AG?, PATCH_LIST_BY_OS?, PATCH_LIST_BY_QID?,	
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>	The header section tells you who created the report and when, company information (name and address) and user information (username and role).
<!ELEMENT SUMMARY (REPORT_SUMMARY, PATCH_SUMMARY)>	
<!ELEMENT REPORT_SUMMARY (TITLE, GROUP_LIST, IP_LIST, TAG_LIST, GROUP_BY, CREATED_ON, NETWORK)>	
<!ELEMENT PATCH_SUMMARY (TOTAL_PATCHES, HOST_REQUIRING_PATCHES, VULN_ADDRESSED)>	The summary section tells you report details (title, group, IPs, when was it created) and detailed summary about the patch including total patches, how many hosts were patched, and how many vulnerabilities were addressed.
<!ELEMENT PATCH_LIST_BY_HOST (HOST_LIST?, PATCH_LINKS)>	The patch list by host gives details about the host (host list and patch links)
<!ELEMENT PATCH_LIST_BY_AG (ASSET_GROUPS, PATCH_LINKS)>	The patch list by asset group gives details about the asset groups (asset group name, total patches, how many hosts needed the patch, number of hosts that needed the patch, host list and the patch links)
<!ELEMENT PATCH_LIST_BY_QID (PATCH_LIST, PATCH_LINKS)>	The patch list by QID gives details about the host list and patch links.
<!ELEMENT PATCH_LIST_BY_OS (OS_LIST?, PATCH_LINKS)>	The patch list by OS gives details about the OS list (name, total patches, hosts that needed the patch, total detections that were fixed by the patch and the patch links.
<!ELEMENT HOST_LIST (HOST*)>	The host list section tells you various details about the host (IP, DNS, NETBIOS, OS, patch count, network, and patch list)
<!ELEMENT CLOUD_RESOURCE_METADATA (INSTANCE_ID?, PUBLIC_DNS_NAME?, PUBLIC_IP_ADDRESS?, PRIVATE_IP_ADDRESS?, IMAGE_ID?, SPOT_INSTANCE?, AVAILABILITY_ZONE?, VPC_ID?, GROUP_ID?, GROUP_NAME?, LOCAL_HOSTNAME?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INSTANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?, RESERVATION_ID?, MAC_ADDRESS?)>	The cloud resource metadata section shows cloud provider metadata for each host when cloud metadata is included in the patch report.
<!ELEMENT PATCH_INFO (PATCH_QID?, VENDOR_ID?, SEVERITY?, PATCH_TITLE?, VULN_COUNT?, HOST_COUNT?, PATCH_PUBLISHED?, CVSS_BASE_SCORE?, CVSS3_BASE_SCORE?, CVSS3_VERSION?, NETWORK?, DETECTION_INFO?, HOST_LIST?)>	

XPath	element specifications / notes
	Patch information (patch QID, vendor ID, severity, title, vulnerabilities fixed by the patch, patch published date, CVSS scores, CVSS3 version, and the detection information).
<!ELEMENT PATCH (PATCH_QID?, OS?, LINK?)>	
	Patch QID, OS and patch links.
<!ELEMENT NON_RUNNING_KERNELS (PATCH_QID?, IP?, SEVERITY?)>	
	The non running kernels section tells about the patch QID and severity.

VM Scan Report Output

This output is returned for a host based VM scan report.

API used

[<platform API server>/api/2.0/fo/report/?action=fetch](#)

DTD for VM Scan Report Output

[<platform API server>/asset_data_report.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS ASSET DATA REPORT DTD -->

<!ELEMENT ASSET_DATA_REPORT (ERROR | (HEADER, RISK_SCORE_PER_HOST?,
HOST_LIST?, GLOSSARY?, NON_RUNNING_KERNELS?, APPENDICES?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- HEADER -->

<!ELEMENT HEADER (COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE,
TARGET, RISK_SCORE_SUMMARY?)>

<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT TEMPLATE (#PCDATA)>
<!ELEMENT TARGET (USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST?,
ASSET_TAG_LIST?)>

<!ELEMENT USER_ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_IP_LIST (RANGE*)>
<!ELEMENT RANGE (START, END)>
<!ATTLIST RANGE network_id CDATA #IMPLIED>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>

<!ELEMENT COMBINED_IP_LIST (RANGE*)>

<!ELEMENT ASSET_TAG_LIST (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>
```

```

<!-- AVERAGE RISK_SCORE_SUMMARY -->
<!ELEMENT RISK_SCORE_SUMMARY (TOTAL_VULNERABILITIES, AVG_SECURITY_RISK,
BUSINESS_RISK)>
<!ELEMENT TOTAL_VULNERABILITIES (#PCDATA)>
<!ELEMENT AVG_SECURITY_RISK (#PCDATA)>
<!ELEMENT BUSINESS_RISK (#PCDATA)>

<!-- RISK_SCORE_PER_HOST -->
<!ELEMENT RISK_SCORE_PER_HOST (HOSTS+)>
<!ELEMENT HOSTS (IP_ADDRESS, TOTAL_VULNERABILITIES, SECURITY_RISK)>
<!ELEMENT IP_ADDRESS (#PCDATA)>
<!ATTLIST IP_ADDRESS
  network_id CDATA #IMPLIED
>

<!ELEMENT SECURITY_RISK (#PCDATA)>

<!-- HOST_LIST -->
<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP?,IPV6?, TRACKING_METHOD, ASSET_TAGS?, HOST_ID,
ASSET_ID?, DNS?, NETBIOS?, QG_HOSTID?, CLOUD_PROVIDER?,
CLOUD_PROVIDER_SERVICE?, CLOUD_SERVICE?, CLOUD_RESOURCE_TYPE?,
CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?, EC2_INSTANCE_ID?, CLOUD_IMAGE_ID?,
IP_INTERFACES?,EC2_INFO?, CLOUD_RESOURCE_METADATA?, AZURE_VM_INFO?,
OPERATING_SYSTEM?, OS_CPE?, ARS?, TRURISK_SCORE?, ACS?, ASSET_GROUPS?,
VULN_INFO_LIST?))>

<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id CDATA #IMPLIED
  v6 CDATA #IMPLIED
>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT ASSET_TAGS (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (#PCDATA)>

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_TYPE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT CLOUD_ACCOUNT (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT CLOUD_IMAGE_ID (#PCDATA)>
<!ELEMENT IP_INTERFACES (IP*)>
<!ELEMENT EC2_INFO
(PUBLIC_DNS_NAME?, IMAGE_ID?, VPC_ID?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INS
TANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?)>
<!ELEMENT CLOUD_RESOURCE_METADATA (INSTANCE_ID?, PUBLIC_DNS_NAME?,

```

```

VM_ID?, VM_NAME?, PLATFORM?, HOST_NAME?, MACHINE_TYPE?,
MACHINE_STATE?, PROJECT_ID?, PUBLIC_IP_ADDRESS?, VPC_NETWORK?, ZONE?,
IMAGE_OFFER?, IMAGE_PUBLISHER?, IMAGE_VERSION?, SUBNET?, VM_STATE?,
PRIVATE_IP_ADDRESS?, IMAGE_ID?, SPOT_INSTANCE?, AVAILABILITY_ZONE?,
VPC_ID?, GROUP_ID?, GROUP_NAME?, LOCAL_HOSTNAME?, INSTANCE_STATE?,
PRIVATE_DNS_NAME?, INSTANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?,
RESERVATION_ID?, SIZE?, SUBSCRIPTION_ID?, LOCATION?,
RESOURCE_GROUP_NAME?, MAC_ADDRESS?)>
<!ELEMENT AZURE_VM_INFO
(PUBLIC_IP_ADDRESS?,IMAGE_OFFER?,IMAGE_VERSION?,SUBNET?,VM_STATE?,PRIVATE
_IP_ADDRESS?,SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?)>
<!ELEMENT INSTANCE_ID (#PCDATA)>
<!ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
<!ELEMENT IMAGE_ID (#PCDATA)>
<!ELEMENT SPOT_INSTANCE (#PCDATA)>
<!ELEMENT AVAILABILITY_ZONE (#PCDATA)>
<!ELEMENT VPC_ID (#PCDATA)>
<!ELEMENT GROUP_ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT INSTANCE_STATE (#PCDATA)>
<!ELEMENT LOCAL_HOSTNAME (#PCDATA)>
<!ELEMENT PRIVATE_DNS_NAME (#PCDATA)>
<!ELEMENT INSTANCE_TYPE (#PCDATA)>
<!ELEMENT ACCOUNT_ID (#PCDATA)>
<!ELEMENT REGION_CODE (#PCDATA)>
<!ELEMENT SUBNET_ID (#PCDATA)>
<!ELEMENT RESERVATION_ID (#PCDATA)>
<!ELEMENT MAC_ADDRESS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT VM_ID (#PCDATA)>
<!ELEMENT VM_NAME (#PCDATA)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT HOST_NAME (#PCDATA)>
<!ELEMENT MACHINE_TYPE (#PCDATA)>
<!ELEMENT MACHINE_STATE (#PCDATA)>
<!ELEMENT PROJECT_ID (#PCDATA)>
<!ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
<!ELEMENT VPC_NETWORK (#PCDATA)>
<!ELEMENT ZONE (#PCDATA)>
<!ELEMENT IMAGE_OFFER (#PCDATA)>
<!ELEMENT IMAGE_PUBLISHER (#PCDATA)>
<!ELEMENT IMAGE_VERSION (#PCDATA)><!ELEMENT SUBNET (#PCDATA)>
<!ELEMENT VM_STATE (#PCDATA)>
<!ELEMENT PRIVATE_IP_ADDRESS (#PCDATA)>
<!ELEMENT SIZE (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT LOCATION (#PCDATA)>
<!ELEMENT RESOURCE_GROUP_NAME (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT ARS (#PCDATA)>
<!ELEMENT TRURISK_SCORE (#PCDATA)>
<!ELEMENT ACS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>

```

```

<!ELEMENT VULN_INFO (QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?,
INSTANCE?, RESULT?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?,
VULN_STATUS?, LAST_FIXED?, FIRST_REOPENED?, LAST_REOPENED?,
TIMES_REOPENED?, CVSS_FINAL?, CVSS3_FINAL?, CVSS3_VERSION?,
TICKET_NUMBER?, TICKET_STATE?, ASSET_CVE?, QDS?)>

<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID id CDATA #REQUIRED>

<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>

<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!ELEMENT FIRST_FOUND (#PCDATA)>
<!ELEMENT LAST_FOUND (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!-- Note: VULN_STATUS is N/A for IGs -->
<!ELEMENT VULN_STATUS (#PCDATA)>
<!ELEMENT LAST_FIXED (#PCDATA)>
<!ELEMENT FIRST_REOPENED (#PCDATA)>
<!ELEMENT LAST_REOPENED (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>
<!ELEMENT CVSS_FINAL (#PCDATA)>
<!ELEMENT CVSS3_FINAL (#PCDATA)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_STATE (#PCDATA)>
<!ELEMENT QDS (#PCDATA)>

<!ELEMENT INSTANCE (#PCDATA)>

<!-- GLOSSARY -->

<!ELEMENT GLOSSARY (VULN_DETAILS_LIST)>

<!ELEMENT VULN_DETAILS_LIST (VULN_DETAILS+)>

<!ELEMENT VULN_DETAILS (QID, TITLE, SEVERITY, CATEGORY, CUSTOMIZED?,
THREAT, THREAT_COMMENT?, IMPACT, IMPACT_COMMENT?, SOLUTION,
SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, PCI_FLAG, LAST_UPDATE?,
CVSS_SCORE?, CVSS3_SCORE?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?,
BUGTRAQ_ID_LIST?)>
<!ATTLIST VULN_DETAILS id ID #REQUIRED>

<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>

```

```

<!ELEMENT CUSTOMIZED (DISABLED?, CUSTOM_SEVERITY?)>
<!ELEMENT DISABLED (#PCDATA)>
<!ELEMENT CUSTOM_SEVERITY (#PCDATA)>

<!ELEMENT THREAT (#PCDATA)>
<!ELEMENT THREAT_COMMENT (#PCDATA)>
<!ELEMENT IMPACT (#PCDATA)>
<!ELEMENT IMPACT_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>
<!ELEMENT CORRELATION (EXPLOITABILITY?, MALWARE?)>
<!ELEMENT EXPLOITABILITY (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 LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_SCORE (CVSS_BASE?, CVSS_TEMPORAL?)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_SCORE (CVSS3_BASE?, CVSS3_TEMPORAL?, CVSS3_VERSION?)>
<!ELEMENT CVSS3_BASE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#PCDATA)>

<!ELEMENT VENDOR_REFERENCE_LIST (VENDOR_REFERENCE+)>
<!ELEMENT VENDOR_REFERENCE (ID, URL)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT CVE_ID_LIST (CVE_ID)+>
<!ELEMENT CVE_ID (ID, URL)>

```

```

<!ELEMENT BUGTRAQ_ID_LIST (BUGTRAQ_ID+)>
<!ELEMENT BUGTRAQ_ID (ID,URL)>

<!ELEMENT COMPLIANCE (COMPLIANCE_INFO+)>
<!ELEMENT COMPLIANCE_INFO (COMPLIANCE_TYPE, COMPLIANCE_SECTION,
COMPLIANCE_DESCRIPTION)>
<!ELEMENT COMPLIANCE_TYPE (#PCDATA)>
<!ELEMENT COMPLIANCE_SECTION (#PCDATA)>
<!ELEMENT COMPLIANCE_DESCRIPTION (#PCDATA)>

<!-- APPENDICES -->

<!ELEMENT APPENDICES (NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?)>
<!ELEMENT NO_RESULTS (IP_LIST)>
<!ELEMENT IP_LIST (RANGE*)>
<!ELEMENT NO_VULNS (IP_LIST)>
<!ELEMENT TEMPLATE_DETAILS (VULN_LISTS?, SELECTIVE_VULNS?,
EXCLUDED_VULN_LISTS?, EXCLUDED_VULNS?, RESULTING_VULNS?, FILTER_SUMMARY?,
EXCLUDED_CATEGORIES?)>
<!ELEMENT VULN_LISTS (#PCDATA)>
<!ELEMENT SELECTIVE_VULNS (#PCDATA)>
<!ELEMENT EXCLUDED_VULN_LISTS (#PCDATA)>
<!ELEMENT EXCLUDED_VULNS (#PCDATA)>
<!ELEMENT RESULTING_VULNS (#PCDATA)>
<!ELEMENT FILTER_SUMMARY (#PCDATA)>
<!ELEMENT EXCLUDED_CATEGORIES (#PCDATA)>
<!ELEMENT NON_RUNNING_KERNELS (NON_RUNNING_KERNEL*)>
<!ELEMENT NON_RUNNING_KERNEL (NRK_QID*, IP*, SEVERITY*)>
<!ELEMENT NRK_QID (#PCDATA)>

```

XPaths for Asset Data Report

Report Section

XPath	element specifications / notes
/ASSET_DATA_REPORT	(ERROR (HEADER, RISK_SCORE_PER_HOST?, HOST_LIST?, GLOSSARY?, NON_RUNNING_KERNELS?, APPENDICES?))
/ASSET_DATA_REPORT/HEADER	(COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE, TARGET, RISK_SCORE_SUMMARY?) Report summary information.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST (HOSTS+)	Risk score summary per host. This is included when the report template has the Text Summary setting selected.
/ASSET_DATA_REPORT/HOST_LIST (HOST+)	Detected vulnerabilities for each host. For each detected vulnerability, information specific to its detection on the host is also provided.
/ASSET_DATA_REPORT/GLOSSARY (VULN_DETAILS_LIST)	Vulnerability information applicable to all hosts.
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS (VULN_DETAILS_LIST)	

XPath	element specifications / notes
/ASSET_DATA_REPORT/APPENDICES	(NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?) Additional data such as hosts with no scan results and template settings.
/ASSET_DATA_REPORT/ERROR	(#PCDATA) attribute: number number is <i>implied</i> and, if present, will be an error code.

Header

XPath	element specifications / notes
/ASSET_DATA_REPORT/HEADER	(COMPANY, USERNAME, GENERATION_DATETIME, TEMPLATE, TARGET, RISK_SCORE_SUMMARY?)
/ASSET_DATA_REPORT/HEADER/COMPANY	(#PCDATA) The company name.
/ASSET_DATA_REPORT/HEADER/USERNAME	(#PCDATA) The login ID for the user who generated the report.
/ASSET_DATA_REPORT/HEADER/GENERATION_DATETIME	(#PCDATA) The date and time when the report was generated, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HEADER/TEMPLATE	(#PCDATA) The title assigned to the template used to generate the report.
/ASSET_DATA_REPORT/HEADER/TARGET	(USER_ASSET_GROUPS?, USER_IP_LIST?, COMBINED_IP_LIST?, ASSET_TAG_LIST?)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_ASSET_GROUPS	(ASSET_GROUP_TITLE+)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_ASSET_GROUPS/ASSET_GROUP_TITLE	(#PCDATA) The title of an asset group that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST	(RANGE*)
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE	(START, END) network_id attribute identifies a network ID when the networks feature is enabled in the subscription.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE/START	(#PCDATA) The first IP address in a range of IPs that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/USER_IP_LIST/RANGE/END	(#PCDATA) The last IP address in a range of IPs that the user specified in the report template.
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST	(RANGE*)
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST /RANGE	(START, END) network_id attribute identifies a network ID when the networks feature is enabled in the subscription.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/RANGE/START (#PCDATA)	The first IP address in the combined IP range. This IP range combines IPs that the user specified in the report template (USER_IP_LIST) as well as IPs that make up the asset groups that the user specified in the report template (USER_ASSET_GROUPS).
/ASSET_DATA_REPORT/HEADER/TARGET/COMBINED_IP_LIST/RANGE/END (#PCDATA)	The last IP address in the combined IP range. This IP range combines IPs that the user specified in the report template (USER_IP_LIST) as well as IPs that make up the asset groups that the user specified in the report template (USER_ASSET_GROUPS).
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST (INCLUDED_TAGS, EXCLUDED_TAGS?)	
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST/INCLUDED_TAGS/ASSET_TAG (#PCDATA)	The list of asset tags included in the scan target. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/ASSET_DATA_REPORT/HEADER/TARGET/ASSET_TAG_LIST/EXCLUDED_TAGS/ASSET_TAG (#PCDATA)	The list of asset tags excluded from the scan target. The scope “all” means hosts matching all tags; scope “any” means hosts matching at least one of the tags.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY (TOTAL_VULNERABILITIES, AVG_SECURITY_RISK, BUSINESS_RISK)	
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/TOTAL_VULNERABILITIES (#PCDATA)	The sum of the vulnerabilities found on all hosts in the report.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/AVG_SECURITY_RISK (#PCDATA)	The average security risk calculated for the report.
/ASSET_DATA_REPORT/RISK_SCORE_SUMMARY/RISK, BUSINESS_RISK (#PCDATA)	
	The business risk score calculated for the report.

Security Risk Score per Host

XPath	element specifications / notes
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST (HOSTS+)	
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS	
	(IP_ADDRESS, TOTAL_VULNERABILITIES, SECURITY_RISK)
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/IP_ADDRESS (#PCDATA)	
	The IP address of a host. The attribute network_id is the host’s network ID when the networks feature is enabled in the subscription.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/TOTAL_VULNERABILITIES (#PCDATA)	The total number of vulnerabilities found on the host.
/ASSET_DATA_REPORT/RISK_SCORE_PER_HOST/HOSTS/SECURITY_RISK (#PCDATA)	
	The security risk score, either the average severity level detected or the highest severity level detected, based on the security risk setup setting for the subscription. For Express Lite, the average severity level is used.

Host List

The host list section includes a list of hosts in your report with detected vulnerabilities.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST (HOST+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST	(ERROR (IP?,IPV6?, TRACKING_METHOD, ASSET_TAGS?, HOST_ID, ASSET_ID?, DNS?, NETBIOS?, QG_HOSTID?, CLOUD_PROVIDER?, CLOUD_PROVIDER_SERVICE?, CLOUD_SERVICE?, CLOUD_RESOURCE_TYPE?, CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?, EC2_INSTANCE_ID?, CLOUD_IMAGE_ID?, IP_INTERFACES?,EC2_INFO?, CLOUD_RESOURCE_METADATA?, AZURE_VM_INFO?, OPERATING_SYSTEM?, OS_CPE?, ARS?, ACS?, ASSET_GROUPS?, VULN_INFO_LIST?))
/ASSET_DATA_REPORT/HOST_LIST/HOST/IP (#PCDATA)	The host's IP address. The attribute network_id identifies the host's network ID when the networks feature is enabled in the subscription. The attribute v6 identifies the hosts IPv6 IP address
/ASSET_DATA_REPORT/HOST_LIST/HOST/TRACKING_METHOD (#PCDATA)	The host's tracking method. This is one of: "ip", "dns", "netbios", "agent", "ec2".
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_TAGS (ASSET_TAG+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_TAGS/ASSET_TAG (#PCDATA)	An asset tag assigned to the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/DNS (#PCDATA)	The DNS host name when known. For an EC2 asset this is the private DNS name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/NETBIOS (#PCDATA)	The Microsoft Windows NetBIOS host name if appropriate, when known.
/ASSET_DATA_REPORT/HOST_LIST/HOST/QG_HOSTID (#PCDATA)	Qualys host ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_PROVIDER (#PCDATA)	Cloud provider of the asset. These will be populated for all cloud assets (Azure, EC2, Google).
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_PROVIDER_SERVICE (#PCDATA)	Cloud provider services of the asset. For example, compute engine.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_SERVICE (#PCDATA)	Cloud service of the asset. For example: (VM for Azure, EC2 for AWS).
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_TYPE (#PCDATA)	Cloud resource type of the asset. For example, virtual machine.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_ID (#PCDATA)	Cloud resource ID of the asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_ACCOUNT (#PCDATA)	Cloud account of the asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INSTANCE_ID (#PCDATA)	EC2 instance ID.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_IMAGE_ID (#PCDATA)	Cloud image ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/IP_INTERFACES (IP*)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/IP_INTERFACES/IP (#PCDATA)	Host IP interface.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO	(PUBLIC_DNS_NAME?, IMAGE_ID?, VPC_ID?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INSTANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?)
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/PUBLIC_DNS_NAME (#PCDATA)	EC2 instance public DNS name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/IMAGE_ID (#PCDATA)	EC2 instance image ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/VPC_ID (#PCDATA)	EC2 VPC ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/INSTANCE_STATE (#PCDATA)	EC2 instance state.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/PRIVATE_DNS_NAME (#PCDATA)	EC2 instance private DNS name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/INSTANCE_TYPE (#PCDATA)	Instance type of the EC2 instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/ACCOUNT_ID (#PCDATA)	Account ID of the EC2 instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/REGION_CODE (#PCDATA)	Region code of the EC2 instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/EC2_INFO/SUBNET_ID (#PCDATA)	Subnet ID of the EC2 instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA	(INSTANCE_ID?, PUBLIC_DNS_NAME?, VM_ID?, VM_NAME?, PLATFORM?, HOST_NAME?, MACHINE_TYPE?, MACHINE_STATE?, PROJECT_ID?, PUBLIC_IP_ADDRESS?, VPC_NETWORK?, ZONE?, IMAGE_OFFER?, IMAGE_PUBLISHER?, IMAGE_VERSION?, SUBNET?, VM_STATE?, PRIVATE_IP_ADDRESS?, IMAGE_ID?, SPOT_INSTANCE?, AVAILABILITY_ZONE?, VPC_ID?, GROUP_ID?, GROUP_NAME?, LOCAL_HOSTNAME?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INSTANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?, RESERVATION_ID?, SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?, MAC_ADDRESS?)
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/INSTANCE_ID (#PCDATA)	Instance id.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PUBLIC_DNS_NAME (#PCDATA)	Public DNS name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/VM_ID (#PCDATA)	Virtual Machine ID.

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/VM_NAME (#PCDATA)	Virtual Machine name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PLATFORM (#PCDATA)	Platform.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/HOST_NAME (#PCDATA)	Host name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/MACHINE_TYPE (#PCDATA)	Machine type.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/MACHINE_STATE (#PCDATA)	Machine state.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PROJECT_ID (#PCDATA)	Project ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PUBLIC_IP_ADDRESS (#PCDATA)	Public IP Address.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/VPC_NETWORK (#PCDATA)	VPC Network.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/ZONE (#PCDATA)	Cloud Provider Zone.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/IMAGE_OFFER (#PCDATA)	Image offering form the publisher
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/IMAGE_PUBLISHER (#PCDATA)	Image publisher.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/IMAGE_VERSION (#PCDATA)	Cloud provider image version.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/SUBNET (#PCDATA)	Subnet of your cloud provider.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/VM_STATE (#PCDATA)	Cloud provider virtual machine state.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PRIVATE_IP_ADDRESS (#PCDATA)	Private IP of cloud provider asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/IMAGE_ID (#PCDATA)	Cloud provider image ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/AVAILABILITY_ZONE (#PCDATA)	Instance availability zone.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/VPC_ID (#PCDATA)	Instance VPC ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/GROUP_ID (#PCDATA)	Instance group ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/GROUP_NAME (#PCDATA)	Instance group name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/INSTANCE_STATE (#PCDATA)	

XPath	element specifications / notes
	Instance state.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/PRIVATE_DNS_NAME (#PCDATA)	Private DNS name.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/INSTANCE_TYPE (#PCDATA)	Instance type.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/ACCOUNT_ID (#PCDATA)	Instance account ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/REGION_CODE (#PCDATA)	Region code of the instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/SUBNET_ID (#PCDATA)	Instance subnet ID.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/SUBSCRIPTION_ID (#PCDATA)	ID of subscription.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/LOCATION (#PCDATA)	Location of instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/RESOURCE_GROUP_NAME (#PCDATA)	Resource group name of the instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/CLOUD_RESOURCE_METADATA/MAC_ADDRESS (#PCDATA)	Mac address of the instance.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO	(PUBLIC_IP_ADDRESS?, IMAGE_OFFER?, IMAGE_VERSION?, SUBNET?, VM_STATE?, PRIVATE_IP_ADDRESS?, SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?)
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/PUBLIC_IP_ADDRESS (#PCDATA)	The IP address of the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/IMAGE_OFFER (#PCDATA)	Image offering from the publisher.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/IMAGE_VERSION (#PCDATA)	Azure VM image version.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/SUBNET (#PCDATA)	Subnet of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/VM_STATE (#PCDATA)	Azure virtual machine state. Possible values are: STARTING, RUNNING, STOPPING, STOPPED, DEALLOCATING, DEALLOCATED, UNKNOWN.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/PRIVATE_IP_ADDRESS (#PCDATA)	Private IP address of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/SIZE (#PCDATA)	Size of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/SUBSCRIPTION_ID (#PCDATA)	Subscription ID of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/LOCATION (#PCDATA)	

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/AZURE_VM_INFO/RESOURCE_GROUP_NAME (#PCDATA)	Location of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/OPERATING_SYSTEM (#PCDATA)	Resource group name of the Azure VM asset.
/ASSET_DATA_REPORT/HOST_LIST/HOST/OS_CPE (#PCDATA)	The operating system detected on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/ARS (#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_DATA_REPORT/HOST_LIST/HOST/ACS (#PCDATA)	The Asset Risk Score (ARS). The Asset Risk Score (ARS) is the overall risk score assigned to the asset based on multiple contributing factors. ARS has a range from 0 to 1000: - Severe (850-1000) - High (700-849) - Medium (500-699) - Low (0-499)
/ASSET_DATA_REPORT/HOST_LIST/HOST/ACS (#PCDATA)	The Asset Criticality Score (ACS).
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	The title of an asset group that the host belongs to. This list includes all asset groups that the host belongs to in the user's account.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST (VULN_INFO+)	
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO	(QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?, INSTANCE?, RESULT?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?, VULN_STATUS?, LAST_FIXED?, FIRST_REOPENED?, LAST_REOPENED?, TIMES_REOPENED?, CVSS_FINAL?, CVSS3_FINAL?, CVSS3_VERSION?, TICKET_NUMBER?, TICKET_STATE?, ASSET_CVE?, QDS?)
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/QID (#PCDATA)	The Qualys ID (QID) assigned to the vulnerability.
attribute: id	id is <i>required</i> and is a reference ID (CDATA) that corresponds to a QID defined under the Glossary section.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TYPE (#PCDATA)	The type of vulnerability check. A valid value is "Vuln" for a confirmed vulnerability, "Practice" for a potential vulnerability, or "Ig" for an information gathered.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/PORT (#PCDATA)	The port number that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/SERVICE (#PCDATA)	The service that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FQDN (#PCDATA)	The Fully Qualified Domain Name (FQDN) associated with the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/PROTOCOL (#PCDATA)	

XPath	element specifications / notes
	The protocol that the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/SSL (#PCDATA)	A flag indicating whether SSL was present on this host. If SSL was present, the SSL element appears with the value "true".
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/RESULT (#PCDATA)	Specific scan test results for the vulnerability, from the host assessment data.
attribute: format	format is <i>implied</i> and, if present, will be "table," indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FIRST_FOUND (#PCDATA)	The date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/LAST_FOUND (#PCDATA)	The date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TIMES_FOUND (#PCDATA)	The total number of times the vulnerability was detected on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/VULN_STATUS (#PCDATA)	The vulnerability status. (Note status levels do not apply to information gathered.) A valid value is "New" for an active vulnerability that was detected one time, Active for an active vulnerability that was detected at least two times, "Re-Opened" for an active vulnerability that was fixed and then re-opened, and "Fixed" for a vulnerability that was detected previously and is now fixed.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/LAST_FIXED (#PCDATA)	The last fixed date/time for the vulnerability on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FIRST_REOPENED (#PCDATA)	The date and time when the vulnerability was first reopened on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/LAST_REOPENED (#PCDATA)	The date and time when the vulnerability was last reopened on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TIMES_REOPENED (#PCDATA)	The number of times the vulnerability on the host has been reopened.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/CVSS_FINAL (#PCDATA)	The final CVSS score calculated for the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/CVSS3_FINAL (#PCDATA)	The final CVSS3 score calculated for the host. If Access Vector is not defined by NIST, this is the Temporal score.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/CVSS3_VERSION (#PCDATA)	The CVSS3 version that is currently supported.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TICKET_NUMBER (#PCDATA)	

XPath	element specifications / notes
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TICKET_STATE (#PCDATA)	The number of the ticket that applies to the vulnerability instance on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TICKET_STATE (#PCDATA)	The state/status of the ticket that applies to the vulnerability instance on the host.
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/QDS (#PCDATA)	The Qualys Detection Score (QDS). The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability. QDS has a range from 1 to 100 with these severity levels: - Critical (90-100) - High (70-89) - Medium (40-69) - Low (1-39)
/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/INSTANCE (#PCDATA)	The Oracle DB instance the vulnerability was detected on.
/ASSET_DATA_REPORT/HOST_LIST/HOST/ERROR (#PCDATA)	
attribute: number	number is <i>implied</i> and, if present, will be an error code.

Glossary

The Glossary element is included in the XML report output only when you enable vulnerability details in the report template.

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY (VULN_DETAILS_LIST)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST (VULN_DETAILS+)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS	(QID, TITLE, SEVERITY, CATEGORY, CUSTOMIZED?, THREAT, THREAT_COMMENT?, IMPACT, IMPACT_COMMENT?, SOLUTION, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, PCI_FLAG, LAST_UPDATE?, CVSS_SCORE?, CVSS3_SCORE?, VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/QID (#PCDATA)	The Qualys ID (QID) assigned to the vulnerability.
attribute: id	id is <i>required</i> and is a reference ID (CDATA) that corresponds to a QID listed in the Host List section.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/TITLE (#PCDATA)	The title of the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/SEVERITY (#PCDATA)	The severity level assigned to the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CATEGORY (#PCDATA)	The category of the vulnerability.

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED	(DISABLED?, CUSTOM_SEVERITY?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED/DISABLED	(#PCDATA)
	Identifies whether the vulnerability was disabled by a Manager users. If disabled, the vulnerabilities is filtered from reports.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CUSTOMIZED/CUSTOM_SEVERITY	(#PCDATA)
	Identifies whether the severity level was changed. Managers can change the severity level by editing the vulnerability in the Qualys KnowledgeBase.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/THREAT	(#PCDATA)
	The Qualys provided description of the threat.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/THREAT_COMMENT	(#PCDATA)
	User-defined description of the threat, if any.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/IMPACT	(#PCDATA)
	The Qualys provided description of the impact.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/IMPACT_COMMENT	(#PCDATA)
	User-defined description of the impact, if any.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/SOLUTION	(#PCDATA)
	The Qualys provided description of the solution. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading "Virtual Patches:". This includes a list of virtual patches and a link to more information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/SOLUTION_COMMENT	(#PCDATA)
	User-defined description of the solution, if any.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/PCI_FLAG	(#PCDATA)
	A flag that indicates whether the vulnerability must be fixed to pass a PCI compliance scan. 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.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION	(EXPLOITABILITY?, MALWARE?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY	(EXPLT_SRC)+
	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC	(SRC_NAME, EXPLT_LIST)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME	(#PCDATA)
	The name of a third party vendor or publicly available source of the vulnerability information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST	(EXPLT)+

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	The CVE reference for the exploitability information.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	A link to the exploit, when available.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE (MW_SRC)+	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/SRC_NAME (#PCDATA)	The name of the source of the malware information: Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST (MW_INFO)+	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)	
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	The malware name/ID assigned by Trend Micro.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	A list of the platforms that may be affected by the malware.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	A link to malware details.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/LAST_UPDATE (#PCDATA)	

XPath	element specifications / notes
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE	(CVSS_BASE?, CVSS_TEMPORAL?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/CVSS_BASE	(#PCDATA)
	CVSS2 Base score defined for the vulnerability.
attribute: source	Note: This attribute is never present in XML output for this release.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/ CVSS_TEMPORAL	(#PCDATA)
	CVSS2 Temporal score defined for the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS3_SCORE	(CVSS3_BASE?, CVSS3_TEMPORAL?, CVSS3_VERSION?)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS3_SCORE/CVSS3_BASE	(#PCDATA)
	CVSS3 Base score defined for the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS3_SCORE/ CVSS3_TEMPORAL	(#PCDATA)
	CVSS3 Temporal score defined for the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS3_SCORE/ CVSS3_VERSION (#PCDATA)	
	CVSS3 version that is currently supported.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/VENDOR_REFERENCE_LIST	(VENDOR_REFERENCE+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/VENDOR_REFERENCE_LIST/ VENDOR_REFERENCE	(ID, URL)
	The name of a vendor reference, and the URL to this vendor reference.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/reference_list/reference/ID	(#PCDATA)
	The name of a vendor reference, CVE name, or Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/reference_list/reference/URL	(#PCDATA)
	The URL to the vendor reference, CVE name, or Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVE_ID_LIST	(CVE_ID+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVE_ID_LIST/CVE_ID	(ID, URL)
	A CVE name assigned to the vulnerability, and the URL to this CVE name. 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.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/BUGTRAQ_ID_LIST	(BUGTRAQ_ID+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/BUGTRAQ_ID_LIST/BUGTRAQ_ID	

XPath	element specifications / notes
	(ID, URL)
	A Bugtraq ID assigned to the vulnerability, and the URL to this Bugtraq ID.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE	
	(COMPLIANCE_INFO+)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/COMPLIANCE_INFO	(COMPLIANCE_TYPE, COMPLIANCE_SECTION, COMPLIANCE_DESCRIPTION)
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_TYPE	(#PCDATA)
	The type of a compliance policy or regulation that is associated with the vulnerability. A valid value is: HIPAA, GLBA, CobIT or SOX.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_SECTION	(#PCDATA)
	The section of a compliance policy or regulation associated with the vulnerability.
/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/COMPLIANCE/COMPLIANCE_INFO/COMPLIANCE_DESCRIPTION	(#PCDATA)
	The description of a compliance policy or regulation associated with the vulnerability.

Non-Running Kernels

XPath	element specifications / notes
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS	(NON_RUNNING_KERNEL*)
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL	
	(NRK_QID*, IP*, SEVERITY*)
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/NRK_QID	(#PCDATA)
	The vulnerability QID with non-running kernel.
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/IP	(#PCDATA)
	The IP address related to the vulnerability with non-running kernel.
/ASSET_DATA_REPORT/NON_RUNNING_KERNELS/NON_RUNNING_KERNEL/SEVERITY	(#PCDATA)
	The severity level of the vulnerability with non-running kernel.

Appendices

XPath	element specifications / notes
/ASSET_DATA_REPORT/APPENDICES	(NO_RESULTS?, NO_VULNS?, TEMPLATE_DETAILS?)
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS	(IP_LIST)
	A list of IPs for which there are no available scan results. This includes hosts that were not “alive” at the time of the scan.
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST	(RANGE*)
	network_id attribute identifies the asset's network ID when the networks feature is enabled in the subscription.
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE	(START, END)
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE/START	(#PCDATA)
	The first IP address in the range.

XPath	element specifications / notes
/ASSET_DATA_REPORT/APPENDICES/NO_RESULTS/IP_LIST/RANGE/END (#PCDATA)	The last IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS (IP_LIST)	A list of IPs for which you have saved scan results but the results are not displayed because all vulnerability checks have been filtered out. To display these results, make changes to the filter settings in your report template. This appendix also lists IPs for which no vulnerabilities were detected by the service. Verify the scan options specified in your option profile.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST (RANGE*)	network_id attribute identifies the asset's network ID when the networks feature is enabled in the subscription.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE (START, END)	
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE/START (#PCDATA)	The first IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/NO_VULNS/IP_LIST/RANGE/END (#PCDATA)	The last IP address in the range.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS	(VULN_LISTS?, SELECTIVE_VULNS?, EXCLUDED_VULN_LISTS?, EXCLUDED_VULNS?, RESULTING_VULNS?, FILTER_SUMMARY?, EXCLUDED_CATEGORIES?)
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/VULN_LISTS (#PCDATA)	The title of each included search list when specified in the report template.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/SELECTIVE_VULNS (#PCDATA)	
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_VULN_LISTS (#PCDATA)	The title of each excluded search list when specified in the report template.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_VULNS (#PCDATA)	All excluded QIDs contained in the excluded search lists specified in the report template.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/RESULTING_VULNS (#PCDATA)	This element appears when both included search lists and excluded search lists were specified in the report template. When present, this element contains the resulting list of included QIDs, where all excluded QIDs have been removed. No value appears if there were no resulting QIDs.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/FILTER_SUMMARY (#PCDATA)	A summary of the filters set on the Filter tab in the report template. For example, you may filter particular status levels, severity levels and types of vulnerability checks (active, disabled and ignored) for vulnerabilities, potential vulnerabilities and information gathered.
/ASSET_DATA_REPORT/APPENDICES/TEMPLATE_DETAILS/EXCLUDED_CATEGORIES (#PCDATA)	A list of vulnerability categories that were filtered out of the report. Identify which vulnerability categories to include on the Filter tab in the report template.

Chapter 7 - VM Scorecard Reports XML

This section describes the XML output returned from VM Scorecard Report API requests.

[Asset Group Vulnerability Report](#)

[Ignored Vulnerabilities Report](#)

[Most Prevalent Vulnerabilities Report](#)

[Most Vulnerable Hosts Report](#)

[Patch Scorecard Report](#)

Asset Group Vulnerability Report

API used

[platform API server](#)/api/2.0/fo/report/scorecard/

DTD for Asset Group Vulnerability Report

[platform API server](#)/asset_group_scorecard.dtd

A recent DTD 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

XPath	element specifications / notes
/ASSET_GROUP_SCORECARD	(ERROR (HEADER, SUMMARY, RESULTS))
/ASSET_GROUP_SCORECARD/ERROR	(#PCDATA)
	An error message.
attribute: number	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.
/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.

XPath	element specifications / notes
/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

API used

[<platform API server>](#)/api/2.0/fo/report/scorecard/

DTD for Ignored Vulnerabilities Report

[<platform API server>](#)/ignored_vulns_scorecard.dtd

A recent DTD 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

XPath	element specifications / notes
/IGNORED_VULNS_SCORECARD	(ERROR (HEADER, SUMMARY, RESULTS))
/IGNORED_VULNS_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: number	An error code, when available
/IGNORED_VULNS_SCORECARD/HEADER	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/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.

XPath	element specifications / notes
/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.
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/DETECTION/VULN	(QID, TITLE, FIRST_FOUND_DATE?, SEVERITY, TYPE, CVSS_BASE?, CVSS_TEMPORAL?) Information about the vulnerability detected. CVSS Base and Temporal scores are included when the CVSS Scoring feature is enabled for the subscription.
/IGNORED_VULNS_SCORECARD/RESULTS/ASSET_GROUP_LIST/ASSET_GROUP/DETECTION_LIST/DETECTION/TICKET	(NUMBER, STATE_DAYS, LAST_MODIFIED_DATE, COMMENTS?, ASSIGNEE_NAME?, ASSIGNEE_EMAIL?) 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.

Most Prevalent Vulnerabilities Report

API used

[<platform API server>/api/2.0/fo/report/scorecard/](#)

DTD for Most Prevalent Vulnerabilities Report

[<platform API server>/most_prevalent_vulns_scorecard.dtd](#)

A recent DTD 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

XPath	element specifications / notes
/MOST_PREVALENT_VULNS_SCORECARD	(ERROR (HEADER, SUMMARY, RESULTS))
/MOST_PREVALENT_VULNS_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: number	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.
/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.

XPath	element specifications / notes
/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.
/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

API used

[<platform API server>](#)/api/2.0/fo/report/scorecard/

DTD for Most Vulnerable Hosts Report

[<platform API server>](#)/most_vulnerable_hosts_scorecard.dtd

A recent DTD is 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

XPath	element specifications / notes
/MOST_VULNERABLE_HOSTS_SCORECARD	(ERROR (HEADER, SUMMARY, RESULTS))
/MOST_VULNERABLE_HOSTS_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: number	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.
/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+)	

XPath	element specifications / notes
/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.
/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 Scorecard Report

API used

[<platform API server>](#)/api/2.0/fo/report/scorecard/

DTD for Patch Scorecard Report

[<platform API server>](#)/patch_scorecard.dtd

A recent DTD is 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 Scorecard Report

XPath	element specifications / notes
/PATCH_REPORT_SCORECARD	(ERROR (HEADER, SUMMARY, RESULTS))
/PATCH_REPORT_SCORECARD/ERROR (#PCDATA)	An error message.
attribute: number	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.
/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.

XPath	element specifications / notes
/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)	
/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.

XPath	element specifications / notes
/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?)	
/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.

XPath	element specifications / notes
/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.

Chapter 8 - VM Remediation Tickets XML

This section describes the XML output returned from VM Remediation Tickets API requests.

[Ticket List Output](#)

[Ticket Edit Output](#)

[Ticket Delete Output](#)

[Deleted Ticket List Output](#)

[Get Ticket Information Report](#)

[Ignore Vulnerability Output](#)

Ticket List Output

API used

[<platform API server>/msp/ticket_list.php](#)

DTD for Ticket List Output

[<platform API server>/ticket_list_output.dtd](#)

A recent DTD is below.

```
<!-- QUALYS TICKET LIST OUTPUT DTD -->

<!ELEMENT REMEDIATION_TICKETS (ERROR | (HEADER, (TICKET_LIST,
TRUNCATION?) ?) )>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Truncation warning -->
<!ELEMENT TRUNCATION (#PCDATA)>
<!ATTLIST TRUNCATION last CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?,
TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,
```

```

        POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,
        TICKET_ASSIGNEE?, QIDS?, SHOW_VULN_DETAILS?,
        VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?,
        VENDOR_REF_CONTAINS?, NETWORK_ID?, HOST_ID?,
SHOW_HOST_ID?) )+) >
<!ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT STATES (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT DNS_CONTAINS (#PCDATA)>
<!ELEMENT NETBIOS_CONTAINS (#PCDATA)>
<!ELEMENT VULN_SEVERITIES (#PCDATA)>
<!ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>
<!ELEMENT OVERDUE (#PCDATA)>
<!ELEMENT INVALID (#PCDATA)>
<!ELEMENT TICKET_ASSIGNEE (#PCDATA)>
<!ELEMENT QIDS (#PCDATA)>
<!ELEMENT SHOW_VULN_DETAILS (#PCDATA)>
<!ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>
<!ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>
<!ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT SHOW_HOST_ID (#PCDATA)>

<!-- AVOID COLISIONS BETWEEN LISTS ABOVE AND BELOW!-->
<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, CREATION_DATETIME, DUE_DATETIME,
        CURRENT_STATE, CURRENT_STATUS?, INVALID?, ASSIGNEE,
        DETECTION, STATS?, HISTORY_LIST?, VULNINFO?, DETAILS?)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT CREATION_DATETIME (#PCDATA)>
<!ELEMENT DUE_DATETIME (#PCDATA)>
<!ELEMENT CURRENT_STATE (#PCDATA)>
<!ELEMENT CURRENT_STATUS (#PCDATA)>
<!ELEMENT ASSIGNEE (NAME, EMAIL, LOGIN)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EMAIL (#PCDATA)>
<!ELEMENT LOGIN (#PCDATA)>

<!-- Target Asset -->
<!ELEMENT DETECTION (IP, HOST_ID?, DNSNAME?, NBHNAME?, PORT?, SERVICE?,
        PROTOCOL?,
        FQDN?, SSL?, INSTANCE?)>
<!ELEMENT IP (#PCDATA) >
<!ELEMENT HOST_ID (#PCDATA)>
<!-- DNS Hostname -->
<!ELEMENT DNSNAME (#PCDATA)>
<!-- NetBios Hostname -->
<!ELEMENT NBHNAME (#PCDATA)>
<!-- TCP Port of the vuln -->

```

```

<!ELEMENT PORT (#PCDATA)>
<!-- service name on the host-->
<!ELEMENT SERVICE (#PCDATA)>
<!-- Protocol -->
<!ELEMENT PROTOCOL (#PCDATA)>
<!-- FQDN -->
<!ELEMENT FQDN (#PCDATA)>
<!-- was this found using SSL -->
<!ELEMENT SSL (#PCDATA)>
<!-- Ticket Statistics -->
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATS (FIRST_FOUND_DATETIME, LAST_FOUND_DATETIME,
                  LAST_SCAN_DATETIME, TIMES_FOUND, TIMES_NOT_FOUND,
                  LAST_OPEN_DATETIME, LAST_RESOLVED_DATETIME?,
                  LAST_CLOSED_DATETIME?, LAST_IGNORED_DATETIME?)>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_SCAN_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT TIMES_NOT_FOUND (#PCDATA)>
<!ELEMENT LAST_OPEN_DATETIME (#PCDATA)>
<!ELEMENT LAST_RESOLVED_DATETIME (#PCDATA)>
<!ELEMENT LAST_CLOSED_DATETIME (#PCDATA)>
<!ELEMENT LAST_IGNORED_DATETIME (#PCDATA)>

<!-- Ticket History -->
<!ELEMENT HISTORY_LIST (HISTORY+)>
<!ELEMENT HISTORY (DATETIME, ACTOR,
                  STATE?, ADDED_ASSIGNEE?, REMOVED_ASSIGNEE?,
                  SCAN?, RULE?, COMMENT?) >
<!ELEMENT ACTOR (#PCDATA)>

<!-- Ticket state/status -->
<!ELEMENT STATE (OLD?, NEW)>
<!ELEMENT OLD (#PCDATA)>
<!ELEMENT NEW (#PCDATA)>

<!-- added assignee -->
<!ELEMENT ADDED_ASSIGNEE (NAME, EMAIL, LOGIN)>

<!-- removed assignee -->
<!ELEMENT REMOVED_ASSIGNEE (NAME, EMAIL, LOGIN)>

<!-- Scan Report that triggered ticket policy -->
<!ELEMENT SCAN (REF, DATETIME?)>
<!ELEMENT REF (#PCDATA)>

<!-- Ticket Creation Rule (Policy) -->
<!ELEMENT RULE (#PCDATA) >

<!-- Ticket Comment -->
<!ELEMENT COMMENT (#PCDATA) >
<!-- Ticket Vulnerability Information -->
<!ELEMENT VULNINFO (TITLE, TYPE, QID, SEVERITY, STANDARD_SEVERITY,

```

```

        CVE_ID_LIST?, VENDOR_REF_LIST?)>
<!--
    Severity is Qualys severity level 1 to 5 (possibly customized),
    whereas standard-severity is the original Qualys severity level
    1 to 5 (which may differ if the vuln has been customized by one
    of the users in the subscription).
-->
<!ELEMENT TITLE (#PCDATA)>
<!-- VULN|POSS -->
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT STANDARD_SEVERITY (#PCDATA)>

<!-- CVE ID (no URI) -->
<!ELEMENT CVE_ID_LIST (CVE_ID+)>
<!ELEMENT CVE_ID (#PCDATA) >
<!-- Vendor Reference (no URI) -->
<!ELEMENT VENDOR_REF_LIST (VENDOR_REF+)>
<!ELEMENT VENDOR_REF (#PCDATA) >

<!-- Ticket Vulnerability Details -->
<!ELEMENT DETAILS
(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)>
<!ELEMENT DIAGNOSIS (#PCDATA) >
<!ELEMENT CONSEQUENCE (#PCDATA) >
<!ELEMENT SOLUTION (#PCDATA) >

<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (EXPLT_SRC)+>
<!ELEMENT EXPLT_SRC (SRC_NAME, EXPLT_LIST)>
<!ELEMENT SRC_NAME (#PCDATA)>
<!ELEMENT EXPLT_LIST (EXPLT)+>
<!ELEMENT EXPLT (REF, DESC, LINK?)>
<!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 RESULT (#PCDATA) >

<!--
    If the "format" attribute is set to "table", then column
    values are separated by tab '\t', and rows are terminated
    by new line '\n'.
-->

```

```
-->  
<!ATTLIST RESULT format CDATA #IMPLIED>
```

XPaths for Ticket List Output

Ticket List - Header Information

XPath	element specifications / notes
/REMEDIATION_TICKETS	(ERROR (HEADER, (TICKET_LIST, TRUNCATION?)))
/REMEDIATION_TICKETS/ERROR (#PCDATA)	
attribute: number	number is <i>implied</i> and if present, is an error code
/REMEDIATION_TICKETS/TRUNCATION (#PCDATA)	
attribute: last	last is <i>implied</i> and if present, is the last ticket number included in the ticket list report. The ticket list is truncated after 1000 records.
/REMEDIATION_TICKETS/HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)	
/REMEDIATION_TICKETS/HEADER/USER_LOGIN (#PCDATA)	
	The Qualys user login name for the user that requested the ticket list report.
/REMEDIATION_TICKETS/HEADER/COMPANY (#PCDATA)	
	The company associated with the Qualys user.
/REMEDIATION_TICKETS/HEADER/DATETIME (#PCDATA)	
	The date and time when the ticket list report was requested. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT) like this: "2005-01-10T02:33:11Z".
/REMEDIATION_TICKETS/HEADER/WHERE	
	((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, SHOW_VULN_DETAILS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?, HOST_ID?, SHOW_HOST_ID?+)
	Ticket selection parameters that were specified as part of the ticket_list.php request. Only the specified parameters appear in the output. Ticket selection parameters are described below.
/REMEDIATION_TICKETS/HEADER/WHERE/MODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window are retrieved.
	The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".
/REMEDIATION_TICKETS/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME (#PCDATA)	
	The start date/time of the time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window are retrieved.
	The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT) like "2006-01-01" or "2006-05-25T23:12:00Z".
/REMEDIATION_TICKETS/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).

XPath	element specifications / notes
/REMEDATION_TICKETS/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	The lowest ticket number selected. Selected tickets will have numbers greater than or equal to the ticket number specified.
/REMEDATION_TICKETS/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	The highest ticket number selected. Selected tickets will have numbers less than or equal to the ticket number specified.
/REMEDATION_TICKETS/HEADER/WHERE/STATES (#PCDATA)	One or more ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/REMEDATION_TICKETS/HEADER/WHERE/IPS (#PCDATA)	One or more IP addresses and/or ranges.
/REMEDATION_TICKETS/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	The title of one or more asset groups.
/REMEDATION_TICKETS/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	A text string contained within the DNS host name.
/REMEDATION_TICKETS/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	A text string contained within the NetBIOS host name.
/REMEDATION_TICKETS/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	One or more vulnerability severity levels.
/REMEDATION_TICKETS/HEADER/WHERE/HOST_IDS (#PCDATA)	A text string with the asset host_id.
/REMEDATION_TICKETS/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	One or more potential vulnerability severity levels.
/REMEDATION_TICKETS/HEADER/WHERE/OVERDUE (#PCDATA)	When not specified, overdue and non-overdue tickets are selected. The value 1 indicates that only overdue tickets were requested. The value 0 indicates that only non-overdue tickets were requested.
/REMEDATION_TICKETS/HEADER/WHERE/INVALID (#PCDATA)	When not specified, both valid and invalid tickets are selected. The value 1 indicates that only invalid tickets were requested. The value 0 indicates that only valid tickets that were requested.
/REMEDATION_TICKETS/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	The user login of an active account.
/REMEDATION_TICKETS/HEADER/WHERE/QIDS (#PCDATA)	One or more Qualys IDs (QIDs).
/REMEDATION_TICKETS/HEADER/WHERE/SHOW_VULN_DETAILS (#PCDATA)	A flag identifying whether vulnerability details are included in the ticket list XML output. The value 1 indicates that vulnerability details were requested. The value 0 indicates that vulnerability details were not requested.
/REMEDATION_TICKETS/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	A text string contained within the vulnerability title.
/REMEDATION_TICKETS/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	A text string contained within vulnerability details.

XPath	element specifications / notes
/REMEDIATION_TICKETS/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	A text string contained within a vendor reference for the vulnerability.
/REMEDIATION_TICKETS/HEADER/WHERE/HOST_ID (#PCDATA)	The unique host ID assigned to the asset.
/REMEDIATION_TICKETS/HEADER/WHERE/SHOW_HOST_ID (#PCDATA)	A flag identifying whether host ID is included in the ticket list XML output. The value 1 indicates that host ID is included. The value 0 indicates that host ID is not included.

Ticket List - General Ticket Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST (TICKET+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET	(NUMBER, CREATION_DATETIME, DUE_DATETIME, CURRENT_STATE, CURRENT_STATUS?, INVALID?, ASSIGNEE, DETECTION, STATS?, HISTORY_LIST?, VULNINFO?, DETAILS?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/NUMBER (#PCDATA)	The number assigned to the ticket by Qualys.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CREATION_DATETIME (#PCDATA)	The date when the ticket was first created in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DUE_DATETIME (#PCDATA)	The due date for ticket resolution in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CURRENT_STATE (#PCDATA)	The current ticket state: OPEN, RESOLVED, or CLOSED.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/CURRENT_STATUS (#PCDATA)	The current ticket status: REOPENED, FIXED, IGNORED.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/INVALID (#PCDATA)	A flag indicating whether the ticket is currently invalid. The value 1 is returned when the ticket is invalid. The value 0 is returned when the ticket is valid.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE (NAME, EMAIL, LOGIN)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/NAME (#PCDATA)	The full name (first and last) of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/EMAIL (#PCDATA)	The email address of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/ASSIGNEE/LOGIN (#PCDATA)	The Qualys user login name for the assignee.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETECTION (#PCDATA)	See "Ticket List - Host Information" for descriptions of the DETECTION sub-elements.

XPath	element specifications / notes
/REMEDATION_TICKETS/TICKET_LIST/TICKET/STATS (#PCDATA)	See “Ticket List -Statistics” for descriptions of the STATS sub-elements.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST (#PCDATA)	See “Ticket List - History” for descriptions of the HISTORY sub-elements.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/VULNINFO (#PCDATA)	See “Ticket List — Vulnerability Information” for descriptions of the VULNINFO sub-elements.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETAILS (#PCDATA)	See “Ticket List — Vulnerability Details” for descriptions of the DETAILS sub-elements.

Ticket List - Host Information

XPath	element specifications / notes
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION	(IP, DNSNAME?, NBHNAME?, PORT?, SERVICE?, PROTOCOL?, FQDN?, SSL?, INSTANCE?)
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/IP (#PCDATA)	The IP address of the host.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/DNSNAME (#PCDATA)	The DNS host name when known.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/NBHNAME (#PCDATA)	The Microsoft Windows NetBIOS host name if appropriate, when known.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/HOST_ID (#PCDATA)	The unique host ID assigned to the asset.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/PORT (#PCDATA)	The port number that the vulnerability was detected on.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/SERVICE (#PCDATA)	The service that the vulnerability was detected on.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/PROTOCOL (#PCDATA)	The protocol that the vulnerability was detected on.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/FQDN (#PCDATA)	The fully qualified domain name of the host, when known.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/SSL (#PCDATA)	A flag indicating whether SSL was present on this host, when known. If SSL was present, the SSL element appears with the value TRUE.
/REMEDATION_TICKETS/TICKET_LIST/TICKET/DETECTION/INSTANCE (#PCDATA)	The Oracle DB instance the vulnerability was detected on.

Ticket List -Statistics

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS	(FIRST_FOUND_DATETIME, LAST_FOUND_DATETIME, LAST_SCAN_DATETIME, TIMES_FOUND, TIMES_NOT_FOUND, LAST_OPEN_DATETIME, LAST_RESOLVED_DATETIME?, LAST_CLOSED_DATETIME?, LAST_IGNORED_DATETIME?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/FIRST_FOUND_DATETIME (#PCDATA)	The date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_FOUND_DATETIME (#PCDATA)	The date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_SCAN_DATETIME (#PCDATA)	The date and time of the most recent scan of the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/TIMES_FOUND (#PCDATA)	The total number of times the vulnerability was detected on the host.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/TIMES_NOT_FOUND (#PCDATA)	The total number of times the host was scanned and the vulnerability was not detected.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_OPEN_DATETIME (#PCDATA)	The date of the most recent scan which caused the ticket state to be changed to Open, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_RESOLVED_DATETIME (#PCDATA)	The date of the most recent scan which caused the ticket state to be changed to Resolved, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_CLOSED_DATETIME (#PCDATA)	The date of the most recent scan which caused the ticket state to be changed to Closed, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_IGNORED_DATETIME (#PCDATA)	The most recent date and time when the ticket was marked as Ignored, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

Ticket List - History

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST (HISTORY+)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY	(DATETIME, ACTOR, STATE?, ADDED_ASSIGNEE?, REMOVED_ASSIGNEE?, SCAN?, RULE?, COMMENT?)
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/DATETIME (#PCDATA)	The date and time of the ticket history event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/ACTOR (#PCDATA)	

XPath

element specifications / notes

The Qualys user login name, identifying the user whose action prompted the ticket history event (such as user scan resulting in ticket state/status change, user ticket edit).

/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE (OLD?, NEW)	
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE/OLD (#PCDATA)	
	The old (previous) state of the ticket.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/STATE/NEW (#PCDATA)	
	The new (current) state of the ticket.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/ADDED_ASSIGNEE	
	(NAME, EMAIL, LOGIN)
	Qualys user who was added as the ticket assignee. For a complete description of the ADDED_ASSIGNEE sub-elements, see the ASSIGNEE description in the "Ticket List - General Ticket Information" table.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/REMOVED_ASSIGNEE	
	(NAME, EMAIL, LOGIN)
	Qualys user who was removed as the ticket assignee. For a complete description of the REMOVED_ASSIGNEE sub-elements, see the ASSIGNEE description in the "Ticket List - General Ticket Information" table.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN (REF, DATETIME?)	
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN/REF (#PCDATA)	
	The scan report reference for the scan that triggered the ticket update event. Note: For a new ticket created by a user, a scan report reference is not returned.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/SCAN/DATETIME (#PCDATA)	
	The date and time of the scan that triggered the ticket update event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/RULE (#PCDATA)	
	The name of the policy rule that triggered the automatic ticket creation.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/HISTORY_LIST/HISTORY/COMMENT (#PCDATA)	
	Comments added to the ticket by Qualys users.

Ticket List — Vulnerability Information

XPath

element specifications / notes

/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/VULNINFO	
	(TITLE, TYPE, QID, SEVERITY, STANDARD_SEVERITY, CVE_ID_LIST?, VENDOR_REF_LIST?)
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TITLE (#PCDATA)	
	The title of the vulnerability, from the Qualys KnowledgeBase.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TYPE (#PCDATA)	
	Type is VULN for a vulnerability, and POSS for a potential vulnerability.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/VULNINFO/QID (#PCDATA)	
	The Qualys ID (QID) assigned to the vulnerability, from the Qualys KnowledgeBase.
/REMEDIACTION_TICKETS/TICKET_LIST/TICKET/VULNINFO/SEVERITY (#PCDATA)	

XPath

element specifications / notes

The current severity level assigned to the vulnerability. This severity level may be different from the standard severity level if it was customized by a Manager user.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/STANDARD_SEVERITY (#PCDATA)

The standard or initial severity level assigned to the vulnerability by Qualys.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/CVE_ID_LIST (CVE_ID+)

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/CVE_ID_LIST/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.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/VENDOR_REF_LIST (VENDOR_REF+)

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/VENDOR_REF_LIST/VENDOR_REF (#PCDATA)

A vendor reference number assigned to the vulnerability.

Ticket List — Vulnerability Details

XPath

element specifications / notes

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS

(DIAGNOSIS?, CONSEQUENCE?, SOLUTION?, CORRELATION?, RESULT?)

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/DIAGNOSIS (#PCDATA)

A description of the threat that the vulnerability presents, from the Qualys KnowledgeBase.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CONSEQUENCES (#PCDATA)

A description of the potential impact if this vulnerability is exploited, from the Qualys KnowledgeBase.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/SOLUTION (#PCDATA)

A verified solution to fix the vulnerability, from the Qualys KnowledgeBase. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading "Virtual Patches:". This includes a list of virtual patches and a link to more information.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION (EXPLOITABILITY?, MALWARE?)

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY (EXPLT_SRC)+

The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.

/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC (SRC_NAME, EXPLT_LIST)

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/SRC_NAME (#PCDATA)	The name of a third party vendor or publicly available source of the vulnerability information.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST (EXPLT)+	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	The CVE reference for the exploitability information.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	A link to the exploit, when available.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE (MW_SRC)+	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/SRC_NAME (#PCDATA)	
	The name of the source of the malware information: Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST (MW_INFO)+	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)	
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	
	The malware name/ID assigned by Trend Micro.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	
	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	
	A list of the platforms that may be affected by the malware.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	
	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	

XPath	element specifications / notes
	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	
	A link to malware details.
/REMEDIATION_TICKETS/TICKET_LIST/TICKET/DETAILS/RESULT (#PCDATA)	
attribute: format	format is <i>implied</i> and if present, will be “table,” indicating that the results are a table that has columns separated by tabulation characters and rows separated by new-line characters

Ticket Edit Output

API used

[<platform API server>/msp/ticket_edit.php](#)

DTD for Ticket Edit Output

[<platform API server>/ticket_edit_output.dtd](#)

A recent DTD is below.

```
<!-- QUALYS TICKET EDIT OUTPUT DTD -->

<!ELEMENT TICKET_EDIT_OUTPUT (ERROR | (HEADER, CHANGES, SKIPPED))>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, UPDATE, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Edit criteria -->
<!ELEMENT UPDATE ((ASSIGNEE?, STATE?, COMMENT?, REOPEN_IGNORED_DAYS?)+) >
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT REOPEN_IGNORED_DAYS (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?,
    TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
    UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
    DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,
    POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,
    TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?,
    VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?)+) >
<!ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT STATES (#PCDATA)>
<!ELEMENT IPS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (#PCDATA)>
<!ELEMENT DNS_CONTAINS (#PCDATA)>
<!ELEMENT NETBIOS_CONTAINS (#PCDATA)>
<!ELEMENT VULN_SEVERITIES (#PCDATA)>
<!ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>
<!ELEMENT OVERDUE (#PCDATA)>
```

```

<!ELEMENT INVALID (#PCDATA)>
<!ELEMENT TICKET_ASSIGNEE (#PCDATA)>
<!ELEMENT QIDS (#PCDATA)>
<!ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>
<!ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>
<!ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>

<!-- AVOID COLISIONS BETWEEN LISTS ABOVE AND BELOW!-->
<!ELEMENT CHANGES (TICKET_NUMBER_LIST)?>
<!ATTLIST CHANGES count CDATA #IMPLIED>

<!ELEMENT TICKET_NUMBER_LIST (TICKET_NUMBER+)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>

<!ELEMENT SKIPPED (TICKET_LIST)?>
<!ATTLIST SKIPPED count CDATA #IMPLIED>

<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, REASON)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT REASON (#PCDATA)>

```

XPaths for Edit Ticket Output

Edit Ticket Output — Header Information

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT	(ERROR (HEADER, CHANGES, SKIPPED))
/TICKET_EDIT_OUTPUT/ERROR	(#PCDATA)
attribute: number	number is <i>implied</i> and, if present, is an error code.
/TICKET_EDIT_OUTPUT/HEADER	(USER_LOGIN, COMPANY, DATETIME, UPDATE, WHERE)
/TICKET_EDIT_OUTPUT/HEADER/USER_LOGIN	(#PCDATA)
	The Qualys user login name for the user that issued the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/COMPANY	(#PCDATA)
	The company associated with the Qualys user.
/TICKET_EDIT_OUTPUT/HEADER/DATETIME	(#PCDATA)
	The date and time of the ticket edit request. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/TICKET_EDIT_OUTPUT/HEADER/UPDATE	((ASSIGNEE?, STATE?, COMMENT?, REOPEN_IGNORED_DAYS?)+)
	The ticket update parameters specified with the ticket_edit.php request are described below.
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/ASSIGNEE	(#PCDATA)
	The user login ID of the current ticket assignee. The ticket assignee was updated by the ticket edit request.

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/STATE (#PCDATA)	The current ticket state. The ticket state was updated by the ticket edit request. A possible value is OPEN (for state/status Open and Open/Reopened), RESOLVED (for state Resolved), or IGNORED (for state/status Closed/Ignored).
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/COMMENT (#PCDATA)	A ticket comment. This comment was added by the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/UPDATE/REOPEN_IGNORED_DAYS (#PCDATA)	The number of days when the Closed/Ignored ticket will be reopened. The number was set by the ticket edit request.
/TICKET_EDIT_OUTPUT/HEADER/WHERE	((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?) +)
	The ticket selection parameters specified with the ticket_edit.php request are described below.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/MODIFIED_SINCE_DATETIME (#PCDATA)	The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window were selected. The date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME (#PCDATA)	The start date/time of a time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window were selected. The date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	One or more ticket numbers and/or ranges were selected. Ticket range start and end is separated by a dash (-).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	The lowest ticket number selected. Selected tickets have numbers greater than or equal to the ticket number specified.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	The highest ticket number selected. Selected tickets have numbers less than or equal to the ticket number specified.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/STATES (#PCDATA)	The selected ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/TICKET_EDIT_OUTPUT/HEADER/WHERE/IPS (#PCDATA)	The selected IP addresses and/or ranges. Tickets on these IP addresses/ranges were selected.

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	The title of one or more selected asset groups. Tickets on IPs in these asset groups were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	A text string contained within the DNS host name. Tickets with a DNS host name containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	A text string contained within the NetBIOS host name. Tickets with a NetBIOS host name containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	One or more vulnerability severity levels. Tickets with vulnerabilities having these severity levels were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	One or more potential vulnerability severity levels. Tickets with potential vulnerabilities having these severity levels were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/OVERDUE (#PCDATA)	The value 1 indicates that only overdue tickets were selected. The value 0 indicates that only non-overdue tickets were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/INVALID (#PCDATA)	The value 1 indicates that only invalid tickets were selected. The value 0 indicates that only valid tickets that were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	The user login of an active account who is the ticket assignee. Tickets with this assignee were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/QIDS (#PCDATA)	One or more Qualys IDs (QIDs). Tickets with these QIDs were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	A text string contained within the vulnerability title. Tickets with vulnerabilities containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	A text string contained within vulnerability details. Tickets with vulnerability details containing this text string were selected.
/TICKET_EDIT_OUTPUT/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	A text string contained within a vendor reference for the vulnerability. Tickets with a vendor reference containing this text string were selected.

Ticket Edit Output — Changed and Skipped Tickets

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/CHANGES (TICKET_NUMBER_LIST)	attribute: count count is <i>implied</i> and, if present, is the total number of tickets that were edited.
/TICKET_EDIT_OUTPUT/CHANGES/TICKET_NUMBER_LIST (TICKET_NUMBER+)	
/TICKET_EDIT_OUTPUT/CHANGES/TICKET_NUMBER_LIST/TICKET_NUMBER (#PCDATA)	The number of a ticket that was changed.

XPath	element specifications / notes
/TICKET_EDIT_OUTPUT/SKIPPED	(TICKET_LIST)
attribute: count	count is <i>implied</i> and, if present, is the total number of tickets that were not changed for some reason.
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST	(TICKET+)
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET	(NUMBER, REASON)
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET /NUMBER	(#PCDATA)
	The number of a ticket that was not changed for some reason.
/TICKET_EDIT_OUTPUT/SKIPPED/TICKET_LIST/TICKET /REASON	(#PCDATA)
	The reason why the ticket identified in the NUMBER element was not changed. Possible reasons are: "Nothing to change" "Ticket not found (# ticket number)" "Ticket cannot be moved from Closed into Resolved state" "The IP in this ticket is not in the user's account" "Mid-air collision detected" Note: The "Mid-air collision detected" reason is returned when two Qualys entities (end users, API requests, and/or the service itself) attempts to change a ticket at the same time. In this case, the first request is processed and any additional requests return an error.

Ticket Delete Output

API used

[<platform API server>/msp/ticket_delete.php](#)

DTD for Ticket Delete Output

[<platform API server>/patch_scorecard.dtd](#)

A recent DTD is below.

```
<!-- QUALYS TICKET DELETE OUTPUT DTD -->

<!ELEMENT TICKET_DELETE_OUTPUT (ERROR | (HEADER, RETURN?))>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?,
TICKET_NUMBERS?, SINCE_TICKET_NUMBER?,
UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?,
```

```
        DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?,  
        POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?,  
        TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?,  
        VULN_DETAILS_CONTAINS?,VENDOR_REF_CONTAINS?)+) >  
<!--ELEMENT MODIFIED_SINCE_DATETIME (#PCDATA)>  
<!--ELEMENT UNMODIFIED_SINCE_DATETIME (#PCDATA)>  
<!--ELEMENT TICKET_NUMBERS (#PCDATA)>  
<!--ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>  
<!--ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>  
<!--ELEMENT STATES (#PCDATA)>  
<!--ELEMENT IPS (#PCDATA)>  
<!--ELEMENT ASSET_GROUPS (#PCDATA)>  
<!--ELEMENT DNS_CONTAINS (#PCDATA)>  
<!--ELEMENT NETBIOS_CONTAINS (#PCDATA)>  
<!--ELEMENT VULN_SEVERITIES (#PCDATA)>  
<!--ELEMENT POTENTIAL_VULN_SEVERITIES (#PCDATA)>  
<!--ELEMENT OVERDUE (#PCDATA)>  
<!--ELEMENT INVALID (#PCDATA)>  
<!--ELEMENT TICKET_ASSIGNEE (#PCDATA)>  
<!--ELEMENT QIDS (#PCDATA)>  
<!--ELEMENT VULN_TITLE_CONTAINS (#PCDATA)>  
<!--ELEMENT VULN_DETAILS_CONTAINS (#PCDATA)>  
<!--ELEMENT VENDOR_REF_CONTAINS (#PCDATA)>  
  
<!--ELEMENT RETURN (MESSAGE?, CHANGES?)>  
<!--ATTLIST RETURN  
    status (FAILED|SUCCESS|WARNING) #REQUIRED  
    number CDATA #IMPLIED>  
  
<!--ELEMENT MESSAGE (#PCDATA)>  
<!--ELEMENT CHANGES (TICKET_NUMBER_LIST)>  
<!--ATTLIST CHANGES  
    count CDATA #REQUIRED>  
  
<!--ELEMENT TICKET_NUMBER_LIST (TICKET_NUMBER+)>  
<!--ELEMENT TICKET_NUMBER (#PCDATA)>
```

XPaths for Ticket Delete Output

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT	(ERROR (HEADER, RETURN?))
/TICKET_DELETE_OUTPUT/ERROR	(#PCDATA) attribute: number number is <i>implied</i> and, if present, is an error code.
/TICKET_DELETE_OUTPUT/HEADER	(USER_LOGIN, COMPANY, DATETIME, WHERE)
/TICKET_DELETE_OUTPUT/HEADER/USER_LOGIN	(#PCDATA) The Qualys user login name for the user who requested the delete function.
/TICKET_DELETE_OUTPUT/HEADER/COMPANY	(#PCDATA) The company associated with the Qualys user.
/TICKET_DELETE_OUTPUT/HEADER/DATETIME	(#PCDATA) The date and time when the function was run. The date appears in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT) like this: "2005-01-10T02:33:11Z".
/TICKET_DELETE_OUTPUT/HEADER/WHERE	((MODIFIED_SINCE_DATETIME?, UNMODIFIED_SINCE_DATETIME?, TICKET_NUMBERS?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, STATES?, IPS?, ASSET_GROUPS?, DNS_CONTAINS?, NETBIOS_CONTAINS?, VULN_SEVERITIES?, POTENTIAL_VULN_SEVERITIES?, OVERDUE?, INVALID?, TICKET_ASSIGNEE?, QIDS?, VULN_TITLE_CONTAINS?, VULN_DETAILS_CONTAINS?, VENDOR_REF_CONTAINS?) +) The ticket selection parameters specified with the ticket_delete.php request are described below.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/MODIFIED_SINCE_DATETIME	(#PCDATA) The start date/time of a time window when tickets were modified. The end of the time window is the date/time when the API function was run. Only tickets modified within this time window were selected. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/UNMODIFIED_SINCE_DATETIME	(#PCDATA) The start date/time of the time window when tickets were not modified. The end of the time window is the date/time when the API function was run. Only tickets that were not modified within this time window were retrieved. The start date/time appears in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/TICKET_NUMBERS	(#PCDATA) One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER	(#PCDATA) The lowest ticket number selected. Selected tickets have numbers greater than or equal to the ticket number specified.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER	(#PCDATA) The highest ticket number selected. Selected tickets have numbers less than or equal to the ticket number specified.

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT/HEADER/WHERE/STATES (#PCDATA)	The selected ticket states. Possible values are OPEN (for state/status Open or Open/Reopened), RESOLVED (for state Resolved), CLOSED (for state/status Closed/Fixed) and IGNORED (for state/status Closed/Ignored).
/TICKET_DELETE_OUTPUT/HEADER/WHERE/IPS (#PCDATA)	The selected IP addresses and/or ranges. Tickets on these IP addresses and/or ranges were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/ASSET_GROUPS (#PCDATA)	The title of one or more selected asset groups. Tickets on IP addresses in these asset groups were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/DNS_CONTAINS (#PCDATA)	A text string contained within the DNS host name. Tickets with a DNS host name containing this string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/NETBIOS_CONTAINS (#PCDATA)	A text string contained within the NetBIOS host name. Tickets with a NetBIOS host name containing this string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_SEVERITIES (#PCDATA)	One or more vulnerability severity levels. Tickets with vulnerabilities having these severity levels were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/POTENTIAL_VULN_SEVERITIES (#PCDATA)	One or more potential vulnerability severity levels. Tickets with potential vulnerabilities having these severity levels were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/OVERDUE (#PCDATA)	The value 1 indicates that only overdue tickets were selected. The value 0 indicates that only non-overdue tickets were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/INVALID (#PCDATA)	The value 1 indicates that only invalid tickets were selected. The value 0 indicates that only valid tickets were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/TICKET_ASSIGNEE (#PCDATA)	The user login of an active account who is the ticket assignee. Tickets with this assignee were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/QIDS (#PCDATA)	One or more Qualys IDs (QIDs). Tickets with these QIDs were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_TITLE_CONTAINS (#PCDATA)	A text string contained within the vulnerability title. Tickets with vulnerabilities containing this text string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VULN_DETAILS_CONTAINS (#PCDATA)	A text string contained within vulnerability details. Tickets with vulnerability details containing this text string were selected.
/TICKET_DELETE_OUTPUT/HEADER/WHERE/VENDOR_REF_CONTAINS (#PCDATA)	A text string contained within a vendor reference for the vulnerability. Tickets with a vendor reference containing this text string were selected.
/TICKET_DELETE_OUTPUT/RETURN (MESSAGE?, CHANGES?)	
attribute: status	status is <i>required</i> and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: number	number is <i>implied</i> and, if present, is an error code.

XPath	element specifications / notes
/TICKET_DELETE_OUTPUT/RETURN/MESSAGE (#PCDATA)	A descriptive message that corresponds to the status code.
/TICKET_DELETE_OUTPUT/RETURN/CHANGES (TICKET_NUMBER_LIST)	
attribute: count	count is <i>implied</i> and, if present, is the total number of tickets that were deleted.
/TICKET_DELETE_OUTPUT/RETURN/CHANGES/TICKET_NUMBER_LIST (TICKET_NUMBER+)	
/TICKET_DELETE_OUTPUT/RETURN/CHANGES/TICKET_NUMBER_LIST/TICKET_NUMBER (#PCDATA)	A single ticket number that was deleted.

Deleted Ticket List Output

API used

[<platform API server>/msp/ticket_list_deleted.php](#)

DTD for Deleted Ticket List Output

[<platform API server>/ticket_list_deleted_output.dtd](#)

A recent DTD is below.

```
<!-- QUALYS TICKET LIST DELETED OUTPUT DTD -->

<!ELEMENT TICKET_LIST_DELETED_OUTPUT
((HEADER, (TICKET_LIST|ERROR|TRUNCATION)*) | ERROR)>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- Truncation warning -->
<!ELEMENT TRUNCATION (#PCDATA)>
<!ATTLIST TRUNCATION last CDATA #IMPLIED>

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (USER_LOGIN, COMPANY, DATETIME, WHERE)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT DATETIME (#PCDATA)>

<!-- Search criteria -->
<!ELEMENT WHERE ((DELETED_SINCE_DATETIME?, DELETED_BEFORE_DATETIME?,
SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?,
TICKET_NUMBERS?) +)>
<!ELEMENT DELETED_SINCE_DATETIME (#PCDATA)>
<!ELEMENT DELETED_BEFORE_DATETIME (#PCDATA)>
<!ELEMENT SINCE_TICKET_NUMBER (#PCDATA)>
<!ELEMENT UNTIL_TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_NUMBERS (#PCDATA)>

<!-- Ticket information -->
```

```
<!ELEMENT TICKET_LIST (TICKET+)>
<!ELEMENT TICKET (NUMBER, DELETION_DATETIME)>
<!ELEMENT NUMBER (#PCDATA)>
<!ELEMENT DELETION_DATETIME (#PCDATA)>
```

XPaths for Deleted Ticket List Output

Deleted Ticket List - Header Information

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT	((HEADER,(TICKET_LIST ERROR TRUNCATION)*) ERROR)
/TICKET_LIST_DELETED_OUTPUT/ERROR (#PCDATA)	
attribute: number	number is <i>implied</i> and if present, is an error code.
/TICKET_LIST_DELETED_OUTPUT/TRUNCATION (#PCDATA)	
attribute: last	last is <i>implied</i> and if present, is the last ticket number included in the deleted ticket list. This list is truncated after 1000 records.
/TICKET_LIST_DELETED_OUTPUT/HEADER	(USER_LOGIN, COMPANY, DATETIME, WHERE)
/TICKET_LIST_DELETED_OUTPUT/HEADER/USER_LOGIN	The Qualys user login for the user that requested the deleted ticket list.
/TICKET_LIST_DELETED_OUTPUT/HEADER/COMPANY	The company associated with the Qualys user.
/TICKET_LIST_DELETED_OUTPUT/HEADER/DATETIME	The date and time when the ticket list report was requested, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE	((DELETED_SINCE_DATETIME?, DELETED_BEFORE_DATETIME?, SINCE_TICKET_NUMBER?, UNTIL_TICKET_NUMBER?, TICKET_NUMBERS?) +)
	Ticket selection parameters specified as part of the ticket_list_deleted.php request.
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/DELETED_SINCE_DATETIME (#PCDATA)	Tickets deleted since this date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/DELETED_BEFORE_DATETIME (#PCDATA)	Tickets deleted since this date/time, in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT).
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/SINCE_TICKET_NUMBER (#PCDATA)	Tickets since this ticket number. Selected tickets will have numbers greater than or equal to the ticket number specified.
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/UNTIL_TICKET_NUMBER (#PCDATA)	Tickets until this ticket number. Selected tickets will have numbers less than or equal to the ticket number specified.

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT/HEADER/WHERE/TICKET_NUMBERS (#PCDATA)	
	Tickets with certain ticket numbers. One or more ticket numbers and/or ranges. Ticket range start and end is separated by a dash (-).

Deleted Ticket List - General Ticket Information

XPath	element specifications / notes
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST (TICKET+)	
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET (NUMBER, DELETION_DATETIME)	
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET/NUMBER (#PCDATA)	
	The total number of deleted tickets.
/TICKET_LIST_DELETED_OUTPUT/TICKET_LIST/TICKET/DELETION_DATETIME (#PCDATA)	
	The date when the ticket was deleted, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

Get Ticket Information Report

API used

[<platform API server>/msp/get_tickets.php](#)

DTD for Get Ticket Info Output

[<platform API server>/remediation_tickets.dtd](#)

A recent DTD is below.

```
<!-- QUALYS REMEDIATION TICKET INFO DTD -->
<!ELEMENT REMEDIATION_TICKETS ((HEADER,ACCOUNT,(TICKET|ERROR)*) | ERROR)
>

<!-- Ticket Report error -->
<!ELEMENT ERROR (#PCDATA) >
<!ATTLIST ERROR number CDATA #IMPLIED >

<!-- Information about the Ticket Report -->
<!ELEMENT HEADER (KEY+) >
<!-- Header Keys, e.g.
      USERNAME: corp_xxn
      COMPANY: <![CDATA[corp name]]>
      DATE: yyyy-dd-mm-ddThh-mm-ssZ
-->

<!ELEMENT KEY (#PCDATA) >
<!ATTLIST KEY
      value CDATA #IMPLIED >

<!-- Account information -->
```

```
<!--ELEMENT ACCOUNT EMPTY -->
<!--ATTLIST ACCOUNT
      account-id CDATA #REQUIRED-->

<!--ELEMENT TICKET (ASSIGNEE+,HOST,STATS?,HISTORY+,VULNINFO?,DETAILS?) -->
<!--ATTLIST TICKET
      number NMTOKEN #REQUIRED
      created CDATA #IMPLIED
      due CDATA #IMPLIED
      state CDATA #REQUIRED
      status CDATA #IMPLIED
      ticket-id CDATA #REQUIRED
-->

<!-- Ticket Assignee - content is QualysGuard user login ID -->
<!--ELEMENT ASSIGNEE (#PCDATA) -->
<!--ATTLIST ASSIGNEE
      name CDATA #REQUIRED
      email CDATA #REQUIRED
-->

<!-- Target Asset -->
<!--ELEMENT HOST (DNSNAME?,NBHNAME?,PORT?,SERVICE?,PROTOCOL?,FQDN?,SSL?) -->
<!--ATTLIST HOST
      ip CDATA #REQUIRED-->
<!-- DNS Hostname -->
<!--ELEMENT DNSNAME (#PCDATA) -->
<!-- NetBios Hostname -->
<!--ELEMENT NBHNAME (#PCDATA) -->
<!-- TCP Port of the vuln -->
<!--ELEMENT PORT (#PCDATA) -->
<!-- service name on the host-->
<!--ELEMENT SERVICE (#PCDATA) -->
<!-- Protocol -->
<!--ELEMENT PROTOCOL (#PCDATA) -->
<!-- FQDN -->
<!--ELEMENT FQDN (#PCDATA) -->
<!-- was this found using SSL -->
<!--ELEMENT SSL (#PCDATA) -->

<!-- Ticket Statistics -->
<!--ELEMENT STATS EMPTY -->
<!--ATTLIST STATS
      first-found CDATA #REQUIRED
      last-found CDATA #REQUIRED
      last-scan CDATA #REQUIRED
      times-found CDATA #REQUIRED
      times-not-found CDATA #REQUIRED
      last-open CDATA #REQUIRED
      last-resolved CDATA #IMPLIED
      last-closed CDATA #IMPLIED
      last-ignored CDATA #IMPLIED
-->
```

```
<!-- Ticket History -->
<!ELEMENT HISTORY
(STATE?,ADDED_ASSIGNEES?,REMOVED_ASSIGNEES?,SCAN?,RULE?,COMMENT?) >
<!ATTLIST HISTORY
    added NMTOKEN #REQUIRED
    by CDATA #REQUIRED>

<!-- Ticket state/status -->
<!ELEMENT STATE EMPTY >
<!ATTLIST STATE
    old-state CDATA #IMPLIED
    new-state CDATA #IMPLIED>

<!-- added assignees -->
<!ELEMENT ADDED_ASSIGNEES (ASSIGNEE+) >

<!-- added assignees -->
<!ELEMENT REMOVED_ASSIGNEES (ASSIGNEE+) >

<!-- Scan Report that triggered ticket policy -->
<!ELEMENT SCAN EMPTY >
<!ATTLIST SCAN
    ref CDATA #REQUIRED
    date CDATA #REQUIRED
>

<!-- Ticket Creation Rule (Policy) -->
<!ELEMENT RULE (#PCDATA) >

<!-- Ticket Comment -->
<!ELEMENT COMMENT (#PCDATA) >

<!-- Ticket Vulnerability Information -->
<!ELEMENT VULNINFO (TITLE,CVE*,VENDOR*)>
<!-- severity is Qualys severity level 1 to 5 (possibly customized) -->

<!--
    standard-severity is the original Qualys severity level 1 to 5
    if it has been customized by the user
-->
<!ATTLIST VULNINFO
    type (VULN|POSS) #REQUIRED
    qid CDATA #REQUIRED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- CVE ID and optional URI to CVE website -->
<!ELEMENT CVE (#PCDATA) >
<!ATTLIST CVE
    id CDATA #REQUIRED
>

<!--
    Vendor Reference and optional URI to vendor website,
```

```

    e.g. name and location of vendor patch from Microsoft, RedHat, SUSE,
    Sun
-->
<!ELEMENT VENDOR (#PCDATA) >
<!ATTLIST VENDOR
    ref CDATA #REQUIRED>
<!ELEMENT TITLE (#PCDATA) >

<!-- Ticket Vulnerability Details -->
<!ELEMENT DETAILS
(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)>

<!ELEMENT DIAGNOSIS (#PCDATA) >
<!ELEMENT CONSEQUENCE (#PCDATA) >
<!ELEMENT SOLUTION (#PCDATA) >
<!ELEMENT CORRELATION (EXPLOITABILITY?,MALWARE?)>
<!ELEMENT EXPLOITABILITY (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 RESULT (#PCDATA) >
<!--
    If the "format" attribute is set to "table", then column
    values are separated by tab '\t', and rows are terminated
    by new line '\n'.
-->
<!ATTLIST RESULT
    format CDATA #IMPLIED
>

```

XPaths for Ticket Information Report

Tickets - Header Information

XPath	element specifications / notes
/REMEDIATION_TICKETS	((HEADER,ACCOUNT,TICKET*) ERROR)
/REMEDIATION_TICKETS/HEADER	(KEY)+
/REMEDIATION_TICKETS/HEADER/KEY	
attribute: value	value is <i>implied</i> and, if present, will be one of the following: USERNAME..... The Qualys user login name for the user that requested the ticket report. COMPANY The company associated with the Qualys user. DATE The date when the ticket report was requested in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/REMEDIATION_TICKETS/ACCOUNT	
attribute: account-id	account-id is <i>required</i> and will be the MD5 hash of the Qualys subscription ID associated with the Qualys user account specified in the header key USERNAME.
/REMEDIATION_TICKETS/ERROR	
attribute: number	number is <i>implied</i> and, if present, is an error code.

Tickets - General Ticket Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET	(ASSIGNEE+,HOST,STATS?,HISTORY+,VULNINFO?,DETAILS?)
attribute: number	value is <i>required</i> and is the remediation ticket number that appears in the Qualys user interface.
attribute: created	created is <i>implied</i> , and if present, will be the date when the ticket was first created in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
attribute: due	due is <i>implied</i> , and if present, will be the due date for ticket resolution in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
attribute: state	state is <i>required</i> and will be the current ticket state: OPEN, RESOLVED, or CLOSED.
attribute: status	status is <i>implied</i> , and if present, will be the current ticket status: REOPENED, FIXED, IGNORED.
attribute: ticket-id	ticket-id is <i>required</i> and will be the unique ID of the remediation ticket, used to identify the ticket within the Qualys application.
/REMEDIATION_TICKETS/TICKET/ASSIGNEE	
	The user login name of the assignee's Qualys user account.
attribute: name	name is <i>required</i> and is the full name (first and last) of the assignee, as defined in the assignee's Qualys user account.
attribute: email	email is <i>required</i> and is the email address of the assignee, as defined in the assignee's Qualys user account.
/REMEDIATION_TICKETS/TICKET/COMMENT	
	Comments added to the ticket by Qualys users.

Tickets - Host Information

XPath	element specifications / notes
/REMEDIACTION_TICKETS/TICKET/HOST	(DNSNAME?,NBHNAME?,PORT?,SERVICE?,PROTOCOL?,FQDN?,SSL?)
attribute: ip	ip is <i>required</i> and is the IP address that the ticket applies to, the IP address on which the vulnerability was detected.
/REMEDIACTION_TICKETS/TICKET/HOST/DNSNAME	The registered DNS host name.
/REMEDIACTION_TICKETS/TICKET/HOST/NBHNAME	The Microsoft Windows NetBIOS host name.
/REMEDIACTION_TICKETS/TICKET/HOST/PORT	The TCP port on which the vulnerability was detected.
/REMEDIACTION_TICKETS/TICKET/HOST/SERVICE	The service name of the host, found during information gathering.
/REMEDIACTION_TICKETS/TICKET/HOST/PROTOCOL	The protocol running on the host, when known.
/REMEDIACTION_TICKETS/TICKET/HOST/FQDN	The fully qualified domain name of the host, when known.
/REMEDIACTION_TICKETS/TICKET/HOST/SSL	A flag indicating whether SSL was present on this host when known. If SSL was present, the SSL element appears with the value TRUE.

Tickets - Statistics and History

XPath	element specifications / notes
/REMEDIACTION_TICKETS/TICKET/STATS	
attribute: first-found	first-found is <i>required</i> and will be the date and time when the vulnerability was first detected on the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: last-found	last-found is <i>required</i> and will be the date and time when the vulnerability was last detected on the host (from the most recent scan), in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: last-scan	last-scan is <i>required</i> and will be the date and time of the most recent scan of the host, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: times-found	times-found is <i>required</i> and will be the total number of times the vulnerability was detected on the host
attribute: times-not-found	times-not-found is <i>required</i> and will be the total number of times the host was scanned and the vulnerability not detected
attribute: last-open	last-open is <i>required</i> and will be the date of the most recent scan which caused the ticket state to be changed to Open, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: last-resolved	last-resolved is <i>implied</i> , and if present, will be the date of the most recent scan which caused the ticket state to be changed to Resolved, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)

XPath	element specifications / notes
attribute: last-closed	last-closed is <i>implied</i> , and if present, will be the date of the most recent scan which caused the ticket state to be changed to Closed, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
attribute: last-ignored	last-ignored is <i>implied</i> , and if present, will be the most recent date and time when the ticket was marked as Ignored, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
/REMEDIATION_TICKETS/TICKET/HISTORY	
(STATE?,ADDED_ASSIGNEES?,REMOVED_ASSIGNEES?,SCAN?,RULE?,COMMENT?)	
attribute: added	added is <i>required</i> and is the token name for the ticket history event
attribute: by	by is <i>required</i> and is the Qualys user login name, identifying the user whose action prompted the ticket history event (such as user scan resulting in ticket state/status change, user ticket edit)
/REMEDIATION_TICKETS/TICKET/HISTORY/STATE	
attribute: old-state	old-state is <i>implied</i> , and if present, will be the old (previous) state of the ticket
attribute: new-state	new-state <i>implied</i> , and if present, will be the new state of the ticket
/REMEDIATION_TICKETS/TICKET/HISTORY/ADDED_ASSIGNEES	
Qualys user login name of an assignee that was added.	
/REMEDIATION_TICKETS/TICKET/HISTORY/REMOVED_ASSIGNEES	
Qualys user login name of an assignee that was removed.	
/REMEDIATION_TICKETS/TICKET/HISTORY/SCAN	
attribute: ref	ref is <i>required</i> and is the scan report reference for the scan that triggered the ticket update event. Note: For a new ticket created by a user, a scan report reference is not returned.
attribute: date	date is <i>required</i> and is the date and time of the scan that triggered the ticket update event, in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT)
/REMEDIATION_TICKETS/TICKET/HISTORY/RULE	
The name of the policy rule that triggered the automatic ticket creation.	

Tickets - Vulnerability Information

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/VULNINFO	
(TITLE,CVE*,VENDOR*)	
attribute: type	type is <i>required</i> and is a vulnerability type flag, VULN for vulnerability and POSS for potential vulnerability
attribute: qid	qid is <i>required</i> and is the Qualys ID number assigned to the vulnerability
attribute: severity	severity is <i>required</i> and is the Qualys assigned severity level (from 1 to 5)
attribute: standard-severity	standard-severity is <i>implied</i> , and if present, will be a user-defined severity level (from 1 to 5)
/REMEDIATION_TICKETS/TICKET/VULNINFO/TITLE	
The title of the vulnerability as defined for the vulnerability in the Qualys Vulnerability KnowledgeBase.	

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/VULNINFO/CVE	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.
attribute: id	id is <i>required</i> and is the CVE name(s) associated with the Qualys vulnerability check associated with the ticket
/REMEDIATION_TICKETS/TICKET/VULNINFO/VENDOR	URI to the vendor Web site, when available
attribute: ref	ref is <i>required</i> and is a vendor reference name, like Microsoft, Red Hat, SUSE, Sun
/REMEDIATION_TICKETS/TICKET/DETAILS	(DIAGNOSIS?,CONSEQUENCE?,SOLUTION?,CORRELATION?,RESULT?)
/REMEDIATION_TICKETS/TICKET/DETAILS/DIAGNOSIS	A description of the threat posted by the vulnerability, from the Qualys KnowledgeBase. This element may be present only when get_tickets.php is specified with the vuln_details=1 parameter.
/REMEDIATION_TICKETS/TICKET/DETAILS/CONSEQUENCE	A description of the possible impact if the vulnerability is exploited, from the Qualys KnowledgeBase. This element may be present only when get_tickets.php is specified with the vuln_details=1 parameter.
/REMEDIATION_TICKETS/TICKET/DETAILS/SOLUTION	A verified solution to fix the vulnerability, from the Qualys KnowledgeBase. When virtual patch information is correlated with a vulnerability, the virtual patch information from Trend Micro appears under the heading "Virtual Patches:". This includes a list of virtual patches and a link to more information. This element may be present only when get_tickets.php is specified with the vuln_details=1 parameter.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION (EXPLOITABILITY?, MALWARE?)	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY (EXPLT_SRC)+	The <EXPLOITABILITY> element and its sub-elements appear only when there is exploitability information for the vulnerability from third party vendors and/or publicly available sources.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY/EXPLT_SRC (SRC_NAME, EXPLT_LIST)	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY/EXPLT_SRC/SRC_NAME (#PCDATA)	The name of a third party vendor or publicly available source of the vulnerability information.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST (EXPLT)+	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT (REF, DESC, LINK?)	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/ EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/REF (#PCDATA)	The CVE reference for the exploitability information.

XPath	element specifications / notes
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/DESC (#PCDATA)	The description provided by the source of the exploitability information (third party vendor or publicly available source).
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC/EXPLT_LIST/EXPLT/LINK (#PCDATA)	A link to the exploit, when available.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE (MW_SRC)+	The <MALWARE> element and its sub-elements appear only when there is malware information for the vulnerability from Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC (SRC_NAME, MW_LIST)	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/SRC_NAME (#PCDATA)	The name of the source of the malware information: Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST (MW_INFO)+	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO (MW_ID, MW_TYPE?, MW_PLATFORM?, MW_ALIAS?, MW_RATING?, MW_LINK?)	
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ID (#PCDATA)	The malware name/ID assigned by Trend Micro.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_TYPE (#PCDATA)	The type of malware, such as Backdoor, Virus, Worm or Trojan.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_PLATFORM (#PCDATA)	A list of the platforms that may be affected by the malware.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_ALIAS (#PCDATA)	A list of other names used by different vendors and/or publicly available sources to refer to the same threat.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_RATING (#PCDATA)	The overall risk rating as determined by Trend Micro: Low, Medium or High.
/REMEDIATION_TICKETS/TICKET/DETAILS/CORRELATION/MALWARE/MW_SRC/MW_LIST/MW_INFO /MW_LINK (#PCDATA)	A link to malware details.
/REMEDIATION_TICKETS/TICKET/DETAILS/RESULT	Specific scan test results for the vulnerability, from the host assessment data. This element may be present only when get_tickets.php is specified with the vuln_details=1 parameter.
attribute: format	format is <i>implied</i> and if present, will be the result format

Ignore Vulnerability Output

API used

<platform API server>/api/2.0/fo/ignore_vuln/index.php

DTD for Ignore Vulnerability Output

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

A recent DTD is below.

```
<!ELEMENT IGNORE_VULN_OUTPUT (REQUEST?,RESPONSE)>

<!-- "name" is the name of API -->
<!-- "at" attribute is the current platform date and time -->
<!ELEMENT REQUEST (#PCDATA)>
<!ATTLIST REQUEST
    name CDATA #REQUIRED
    username CDATA #REQUIRED
    at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RESPONSE (MESSAGE, IGNORED_LIST?, RESTORED_LIST?)>
<!ATTLIST RESPONSE
    status (FAILED|SUCCESS|WARNING) #REQUIRED
    number CDATA #IMPLIED>
<!ELEMENT MESSAGE (#PCDATA)*>

<!ELEMENT IGNORED_LIST (IGNORED+)>
<!ELEMENT IGNORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)*>
<!ELEMENT NETBIOS (#PCDATA)*>

<!ATTLIST IP network_id CDATA #IMPLIED>

<!ELEMENT RESTORED_LIST (RESTORED+)>
<!ELEMENT RESTORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
```

XPaths for Ignore Vulnerability Output

This section describes the XPaths for the ignore vulnerability output (ignore_vuln_output.dtd).

XPath	element specifications / notes
/IGNORE_VULN_OUTPUT	(API, RETURN)
/IGNORE_VULN_OUTPUT/API	(#PCDATA)
I attribute: name attribute: username attribute: at	name is <i>required</i> and is the API function name. username is <i>required</i> and is the user login of the API user. at is <i>required</i> and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/IGNORE_VULN_OUTPUT/RETURN	(MESSAGE, IGNORED_LIST?, RESTORED_LIST?)
attribute: status	status is <i>required</i> and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: number	number is <i>implied</i> and, if present, is an error code.
/IGNORE_VULN_OUTPUT/RETURN/MESSAGE	(#PCDATA)
	A descriptive message that corresponds to the status code.
/IGNORE_VULN_OUTPUT/RETURN/IGNORED_LIST	(IGNORED+)
/IGNORE_VULN_OUTPUT/RETURN/IGNORED_LIST/IGNORED	(TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)
/IGNORE_VULN_OUTPUT/RETURN/RESTORED_LIST	(RESTORED+)
/IGNORE_VULN_OUTPUT/RETURN/RESTORED_LIST/RESTORED	(TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/TICKET_NUMBER	(#PCDATA)
	The ticket number related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/QID	(#PCDATA)
	The QID related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/IP	(#PCDATA)
	The IP address related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/DNS	(#PCDATA)
	The DNS host name related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.
/IGNORE_VULN_OUTPUT/RETURN/{LIST}/{VULN}/NETBIOS	(#PCDATA)
	The NetBIOS host name related to a vulnerability that was ignored or restored. {LIST} stands for an ignored or restored list. {VULN} stands for an ignored or restored vulnerability.

Chapter 9 - Compliance XML

This section describes the XML output returned from Policy Compliance API requests.

[Compliance Control List Output](#)

[Compliance Policy List Output](#)

[Compliance Policy Export Output](#)

[Compliance Posture Info List 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

API used

[platform API server](#)/api/2.0/fo/compliance/control/?action=list

DTD for Compliance Control List Output

[platform API server](#)/api/2.0/fo/compliance/control/control_list_output.dtd

A recent DTD is shown below.

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!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?, USE_AGENT_ONLY?, AUTO_UPDATE?,
IGNORE_ERROR?, (IGNORE_ITEM_NOT_FOUND|ERROR_SET_STATUS)?,
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 USE_AGENT_ONLY (#PCDATA)>
<!ELEMENT AUTO_UPDATE (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
<!ELEMENT ERROR_SET_STATUS (#PCDATA)>
<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, 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?, SCRIPT_ID?, SCRIPT_NAME?,
OUTPUT_FILTER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DISABLE_CASE_SENSITIVE_SEARCH?, EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?,
DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!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 DB_QUERY (#PCDATA)>
<!ELEMENT SCRIPT_ID (#PCDATA)>
<!ELEMENT SCRIPT_NAME (#PCDATA)>
<!ELEMENT OUTPUT_FILTER (#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 FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_OBJECT_TYPES (#PCDATA)>
<!ELEMENT DIGEST_HASH (#PCDATA)>
<!ELEMENT PERMISSION_MONITOR (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT EXCLUDE_USER_OWNER (#PCDATA)>
<!ELEMENT EXCLUDE_GROUP_OWNER (#PCDATA)>

<!ELEMENT DATA_TYPE (#PCDATA)>
<!ELEMENT EVALUATE_AS_STRING (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?,
DB_QUERY?, DESCRIPTION?)>

```

```

<!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

Control List Output: Request

XPath	element specifications / notes
/CONTROL_LIST_OUTPUT	(REQUEST?, RESPONSE)
/CONTROL_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/CONTROL_LIST_OUTPUT/REQUEST/DATETIME	(#PCDATA) The date and time of the request.
/CONTROL_LIST_OUTPUT/REQUEST/USER_LOGIN	(#PCDATA) The user login ID of the user who made the request.
/CONTROL_LIST_OUTPUT/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST	(PARAM+)
/CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)
/CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY	(#PCDATA) An input parameter name.
/CONTROL_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE	(#PCDATA) An input parameter value.
/CONTROL_LIST_OUTPUT/REQUEST/POST_DATA	(#PCDATA) The POST data, if any.

Control List Output: Response

XPath	element specifications / notes
/CONTROL_LIST_OUTPUT (REQUEST?, RESPONSE)	
/CONTROL_LIST_OUTPUT/RESPONSE	(DATETIME, CONTROL_LIST ID_SET?, WARNING?)
/CONTROL_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST (CONTROL+)	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL	(ID, UPDATE_DATE, CREATED_DATE, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?, DEPRECATED?, DEPRECATED_DATE?, CHECK_TYPE?, COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, IGNORE_ERROR?, (IGNORE_ITEM_NOT_FOUND ERROR_SET_STATUS)?, , SCAN_PARAMETERS?, TECHNOLOGY_LIST, FRAMEWORK_LIST?)
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/ID (#PCDATA)	A compliance control ID.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/UPDATE_DATE (#PCDATA)	The date and time when the control was last updated.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CREATED_DATE (#PCDATA)	The date and time when the control was created.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CATEGORY (#PCDATA)	A category for a compliance control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SUB-CATEGORY (#PCDATA)	A sub-category for a compliance control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	A statement for a compliance control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY/LABEL (#PCDATA)	A criticality label (e.g. SERIOUS, CRITICAL, URGENT) assigned to the control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/DEPRECATED (#PCDATA)	The value 1 identifies a deprecated control. This element appears only for a deprecated control.
/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.

XPath	element specifications / notes
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/COMMENT (#PCDATA)	User defined comments.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/USE_AGENT_ONLY (#PCDATA)	Set to 1 when the "Use agent scan only" option is enabled for the control. When enabled the control is evaluated using scan data collected from a cloud agent scan only.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/AUTO_UPDATE (#PCDATA)	Set to 1 when the "Auto Update expected value" option is enabled for the control. When enabled the control's expected value for posture evaluation is replaced with the actual value collected from the cloud agent scan.
/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.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/(IGNORE_ITEM_NOT_FOUND ERROR_SET_STATUS)? (#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).
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS	(PATH_TYPE?, 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?, SCRIPT_ID?, SCRIPT_NAME?, OUTPUT_FILTER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?, INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?, DISABLE_CASE_SENSITIVE_SEARCH?, EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?, DESCRIPTION)
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/PATH_TYPE (#PCDATA)	Specify file location using the path types: Registry Key, File Search, File Path.

XPath	element specifications / notes
/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).
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/REG_KEY (#PCDATA)	A Windows registry key.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/REG_VALUE_NAME (#PCDATA)	A value for a Windows registry key.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_PATH (#PCDATA)	A pathname to a file or directory.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_QUERY (#PCDATA)	A query for a file content check.
/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.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/WMI_NS (#PCDATA)	A WMI namespace for a WMI query check.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/ WMI_QUERY (#PCDATA)	A WMI query for a WMI query check.
/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.
/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.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/GROUP_NAME (#PCDATA)	Windows local group name to get a list of members for.
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/BASE_DIR (#PCDATA)	For directory search, the base directory to start search from.
/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".

XPath	element specifications / notes
/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).
/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).
/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".
/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.
/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.
/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.
/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.
/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).
/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. Click here to find abbreviated SDDL names for well-known users and groups.
/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.
/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.

XPath	element specifications / notes
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS (WIN_BASIC_PERMISSIONS?, WIN_ADVANCED_PERMISSIONS?)	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS/WIN_BASIC_PERMISSIONS (WIN_BASIC_PERMISSIONS_TYPE+)	
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/WIN_PERMISSIONS/WIN_ADVANCED_PERMISSIONS (WIN_ADVANCED_PERMISSIONS_TYPE+)	
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/PERMISSIONS (SPECIAL, USER, GROUP, OTHER)	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/PERMISSIONS/SPECIAL (USER, GROUP, DELETION)	
/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.
/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.
/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.
/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).
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/USER_OWNER (#PCDATA)	For Unix Directory Search and Unix Directory Integrity controls, match files owned by certain users specified as comma separated list of user names and/or UUIDs.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/GROUP_OWNER (#PCDATA)	

XPath

element specifications / notes

For Unix Directory Search and Unix Directory Integrity controls, match files owned by certain groups specified as comma separated list of group names and/or GUIDs.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/SCRIPT_ID (#PCDATA)	For future use.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/SCRIPT_NAME (#PCDATA)	For future use.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/OUTPUT_FILTER (#PCDATA)	For future use.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/TIME_LIMIT (#PCDATA)	For a Unix directory search, the search time limit in seconds.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/MATCH_LIMIT (#PCDATA)	For a Unix directory search, the maximum number of objects matched.
/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.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)	The search time limit specified for a Unix File Content Check V2 control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)	The search match limit specified for a Unix File Content Check V2 control.
/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.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)	Disable the case-sensitive search in Unix agent UDCs (Directory Search and Directory Integrity).
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/EXCLUDE_USER_OWNER (#PCDATA)	(Supported only by Cloud Agent) For Unix Directory Search and Unix Directory Integrity controls, this is a flag (true or false) indicating whether to exclude the files owned by certain users specified as comma separated list of user names and/or UUIDs.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/EXCLUDE_GROUP_OWNER (#PCDATA)	(Supported only by Cloud Agent) For Unix Directory Search and Unix Directory Integrity controls, this is a flag (true or false) indicating whether to exclude the files owned by certain groups specified as comma separated list of group names and/or GUIDs.

XPath	element specifications / notes
/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.
/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
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/EVALUATE_AS_STRING (#PCDATA)	A scan parameter that identifies if the Evaluate as string option is enabled for Unix File Content Check UDC.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SCAN_PARAMETERS/DESCRIPTION (#PCDATA)	A description of the check's scan parameters.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST (TECHNOLOGY+)	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?, DB_QUERY?, DESCRIPTION?)>	
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/ID (#PCDATA)	A technology ID for a technology in a control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/NAME (#PCDATA)	A technology name for a technology in a control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/RATIONALE (#PCDATA)	The rationale description for a technology in a control.
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/DATAPOINT (CARDINALITY, OPERATOR, DEFAULT_VALUES)	
/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.
/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).
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/DATAPOINT/DEFAULT_VALUES (DEFAULT_VALUE+)	total is the total number of default values
/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/DATAPOINT/DEFAULT_VALUES/DEFAULT_VALUE (#PCDATA)	

XPath

element specifications / notes

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.

/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.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/DB_QUERY (#PCDATA)

SQL query defined by the user to be executed on the database for database udc.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/DESCRIPTION (#PCDATA)

Description of the SQL query defined by the user to be executed on the database for database udc.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST
(Framework+)

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework
(ID, NAME, REFERENCE_LIST)

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/ID
(#PCDATA)

A framework ID for a framework reference in a control.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/NAME
(#PCDATA)

A framework name for a framework reference in a control.

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST (REFERENCE+)

/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework/REFERENCE_LIST/REFERENCE (SECTION, COMMENTS)

/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.

/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.

/CONTROL_LIST_OUTPUT/RESPONSE/ID_SET (ID|ID_RANGE)+

/CONTROL_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)

A compliance control ID.

/CONTROL_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)

A range of compliance control IDs.

Control List Output: Warning

XPath	element specifications / notes
/CONTROL_LIST_OUTPUT/RESPONSE/WARNING (CODE, TEXT, URL?)	
/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).
/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).
/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

API used

[platform API server](#)/api/2.0/fo/compliance/policy/?action=list

DTD for Network List Output

[platform API server](#)/api/2.0/fo/compliance/policy/policy_list_output.dtd

A recent DTD 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?,TAG_SET_EXCLUDE?,
TAG_EXCLUDE_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 TAG_SET_EXCLUDE (TAG_ID+)>
<!ELEMENT TAG_EXCLUDE_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, REMEDIATION?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT CUSTOMIZED (#PCDATA)>
<!ELEMENT REMEDIATION (#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 (ASSET_INCLUDE_TAG_LIST?,
ASSET_EXCLUDE_TAG_LIST?)>

<!ELEMENT ASSET_INCLUDE_TAG_LIST (TAG+)>
<!ELEMENT ASSET_EXCLUDE_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

Compliance Policy List Output: Request

XPath	element specifications / notes
/POLICY_LIST_OUTPUT (REQUEST?, RESPONSE)	
/POLICY_LIST_OUTPUT/REQUEST	(DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)
/POLICY_LIST_OUTPUT/REQUEST/DATETIME (#PCDATA)	The date and time of the request.
/POLICY_LIST_OUTPUT/REQUEST/USER_LOGIN (#PCDATA)	The user login ID of the user who made the request.
/POLICY_LIST_OUTPUT/REQUEST/RESOURCE (#PCDATA)	The resource specified for the request.
/POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST (PARAM+)	
/POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM (KEY, VALUE)	
/POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/KEY (#PCDATA)	An input parameter name.
/POLICY_LIST_OUTPUT/REQUEST/PARAM_LIST/PARAM/VALUE (#PCDATA)	An input parameter value.
/POLICY_LIST_OUTPUT/REQUEST/POST_DATA (#PCDATA)	The POST data, if any.

Compliance Policy List Output: Response

XPath	element specifications / notes
/POLICY_LIST_OUTPUT (REQUEST?, RESPONSE)	
/POLICY_LIST_OUTPUT/RESPONSE	(DATETIME, (POLICY_LIST ID_SET)?, WARNING?, GLOSSARY?)
/POLICY_LIST_OUTPUT/RESPONSE/DATETIME (#PCDATA)	The date and time of the response.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST (POLICY+)	
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY	(ID, TITLE, CREATED?, LAST_MODIFIED?, LAST_EVALUATED?, STATUS?, IS_LOCKED?, EVALUATE_NOW?, ASSET_GROUP_IDS?, TAG_SET_INCLUDE?, TAG_INCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, TAG_EXCLUDE_SELECTOR?, INCLUDE_AGENT_IPS?, CONTROL_LIST?)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/ID (#PCDATA)	A compliance policy ID.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TITLE (#PCDATA)	A compliance policy title.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CREATED (#PCDATA)	The date/time when the policy was created.

XPath	element specifications / notes
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED	(DATETIME, BY)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED/DATETIME	(#PCDATA)
	The date/time when the policy was last updated.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_MODIFIED/BY	(#PCDATA)
	The user login ID of the user who last modified the policy.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_EVALUATED	(DATETIME)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/LAST_EVALUATED/DATETIME	(#PCDATA)
	The date/time when the policy was last evaluated.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/STATUS	(#PCDATA)
	The current status of the policy: active or inactive.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/IS_LOCKED	(#PCDATA)
	The current status of the policy: locked or unlocked.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/EVALUTE_NOW	(#PCDATA)
	Indicates whether the Evaluate Now option was selected in the policy.
/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: has_hidden_data	has_hidden_data 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.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_INCLUDE	(TAG_ID+)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_INCLUDE/TAG_ID	(#PCDATA)
	A tag set ID.
/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.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_EXCLUDE	(TAG_ID+)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_SET_EXCLUDE/TAG_ID	(#PCDATA)
	A tag set ID.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/TAG_EXCLUDE_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.
/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.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST	(CONTROL+)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL	(ID, STATEMENT, CRITICALITY?, DEPRECATED?, TECHNOLOGY_LIST?)
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/ID	(#PCDATA)
	A compliance control ID.

XPath	element specifications / notes
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/STATEMENT (#PCDATA)	A control statement.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/CRITICALITY (LABEL, VALUE)	
/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.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/CRITICALITY/VALUE (#PCDATA)	A criticality value (0-5) assigned to the control.
/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.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST (TECHNOLOGY+)	
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY (ID, NAME, RATIONALE, CUSTOMIZED, REMEDIATION?)	
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/ID (#PCDATA)	A technology ID for a control.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/NAME (#PCDATA)	A technology name for a control.
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/RATIONALE (#PCDATA)	The rationale description for a control technology.
/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).
/POLICY_LIST_OUTPUT/RESPONSE/POLICY_LIST/POLICY/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/REMEDIATION (#PCDATA)	Remediation information for the technology. Users can customize remediation details using the Policy Editor in the UI.
/POLICY_LIST_OUTPUT/RESPONSE/ID_SET (ID ID_RANGE)	
/POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID (#PCDATA)	A policy ID.
/POLICY_LIST_OUTPUT/RESPONSE/ID_SET/ID_RANGE (#PCDATA)	A range policy IDs.

Compliance Policy List Output: Warning

XPath	element specifications / notes
/POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST	(WARNING+)
/POLICY_LIST_OUTPUT/RESPONSE/WARNING_LIST/WARNING	(CODE?, TEXT, URL?)
/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).
/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).
/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

XPath	element specifications / notes
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY	(ASSET_GROUP_LIST?, ASSET_TAG_LIST?, USER_LIST?)
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST	(ASSET_GROUP+)
	A list of asset groups assigned to policies in the policy list output.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST/ASSET_GROUP	(ID, TITLE, IP_SET?)
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/ID	(#PCDATA)
	An asset group ID for an asset group assigned to the policy.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/TITLE	(#PCDATA)
	An asset group title for an asset group assigned to the policy.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_GROUP_LIST /ASSET_GROUP/IP_SET	(IP IP_RANGE)+
/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.
/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.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST	(TAG+)
	A list of asset tags assigned to policies in the policy list output.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST/TAG	(TAG_ID?, TAG_NAME?)
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST /TAG/TAG_ID	(#PCDATA)
	An asset tag ID for an asset tag assigned to the policy.

XPath	element specifications / notes
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/ASSET_TAG_LIST /TAG/TAG_NAME	(#PCDATA)
	An asset tag name for an asset tag assigned to the policy.
/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.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER	(USER_LOGIN, FIRST_NAME, LAST_NAME)
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /USER (#PCDATA)	
	A user login ID.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /FIRST_NAME (#PCDATA)	
	The first name of the account user.
/POLICY_LIST_OUTPUT/RESPONSE/GLOSSARY/USER_LIST /LAST_NAME (#PCDATA)	
	The last name of the account user.

Compliance Policy Export Output

API used

[<platform API server>/api/2.0/fo/compliance/policy/?action=export](#)

DTD for Compliance Policy Export Output

[<platform API server>/api/2.0/fo/compliance/policy/policy_export_output.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!-- $Revision: 62328 $ -->
<!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?, REMEDIATION?,
DATAPOINT?, USE_SCAN_VALUE?, DB_QUERY?, DESCRIPTION?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EVALUATE (CTRL*)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT REMEDIATION (#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|DBCOL|DT)+>
<!ELEMENT K (#PCDATA)>
<!ELEMENT OP (#PCDATA)>
<!ELEMENT CD (#PCDATA)>
<!ELEMENT L (#PCDATA)>
<!ELEMENT V (#PCDATA)>
<!ELEMENT FV (#PCDATA)>
<!ATTLIST FV set CDATA #IMPLIED>
<!ELEMENT DBCOL (#PCDATA)>
<!ELEMENT DT (#PCDATA)>

<!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,
IS_CONTROL_DISABLE?, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?,
COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, IGNORE_ERROR,
(IGNORE_ITEM_NOT_FOUND|ERROR_SET_STATUS)?, 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 USE_AGENT_ONLY (#PCDATA)>
<!ELEMENT AUTO_UPDATE (#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 ERROR_SET_STATUS (#PCDATA)>

```

```

<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, 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?, INTEGRITY_CHECK_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?,
INTEGRITY_CHECK_TIME_LIMIT?,FILE_CONTENT_CHECK_V2_TIME_LIMIT?,
FILE_CONTENT_CHECK_V2_MATCH_LIMIT?,INTEGRITY_CHECK_MATCH_LIMIT?,
DISABLE_CASE_SENSITIVE_SEARCH?,EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?,
INTEGRITY_CHECK_OBJECT_TYPES?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?,
SCRIPT_ID?, SCRIPT_NAME?, OUTPUT_FILTER?,
GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE,
EVALUATE_AS_STRING?, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!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 INTEGRITY_CHECK_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 DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT EXCLUDE_USER_OWNER (#PCDATA)>
<!ELEMENT EXCLUDE_GROUP_OWNER (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)>
<!ELEMENT FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_OBJECT_TYPES (#PCDATA)>
<!ELEMENT DIGEST_HASH (#PCDATA)>
<!ELEMENT PERMISSION_MONITOR (#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 EVALUATE_AS_STRING (#PCDATA)>
<!ELEMENT DB_QUERY (#PCDATA)>
<!ELEMENT SCRIPT_ID (#PCDATA)>
<!ELEMENT SCRIPT_NAME (#PCDATA)>
<!ELEMENT OUTPUT_FILTER (#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

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?)
/POLICY_EXPORT_OUTPUT/REQUEST/DATETIME	(#PCDATA)
	The date and time of the request.

XPath	element specifications / notes
/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

XPath	element specifications / notes
/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+)	total is the total number of sections
/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.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS ((CONTROL USER_DEFINED_CONTROL)*)	
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS (CONTROL*)	total 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+)	total is the total number of technologies
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES /TECHNOLOGY (ID, NAME?, EVALUATE?, RATIONALE?, REMEDIATION?, DATAPOINT?, USE_SCAN_VALUE?, DB_QUERY?, DESCRIPTION?)	
/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.
/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.

XPath	element specifications / notes
/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 DBCOL DT)+	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	set 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.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES/TECHNOLOGY/EVALUATE/CTRL /DP/DBCOL (#PCDATA)	Columns returned in scan result.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES/TECHNOLOGY/EVALUATE/CTRL /DP/DT (#PCDATA)	Data type to be defined to evaluate controls.
/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.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/CONTROL/TECHNOLOGIES/TECHNOLOGY/REMEDIATION (#PCDATA)	Remediation information available 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*)	total 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/CONTROL/TECHNOLOGIES/TECHNOLOGY/DB_QUERY (#PCDATA)	User defined SQL statement
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL	(ID, UDC_ID, CHECK_TYPE, IS_CONTROL_DISABLE?, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?, COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, 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 type of UDC check, such as Registry Key Existence, Registry Value Existence, Window File/Directory Existence, Window File/Directory Permission, Unix File Content Check, Unix Directory Search Check, etc.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_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/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_CONTROL/CATEGORY/NAME (#PCDATA)	The category name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SUB_CATEGORY (ID, NAME)	A sub-category for the control.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SUB_CATEGORY/ID (#PCDATA)	The sub-category ID.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SUB_CATEGORY/NAME (#PCDATA)	The sub-category name.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/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_CONTROL/COMMENT (#PCDATA)	User defined comments.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/USE_AGENT_ONLY (#PCDATA)	Set to 1 when the "Use agent scan only" option is enabled for the control. When enabled the control is evaluated using scan data collected from a cloud agent scan only.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/AUTO_UPDATE (#PCDATA)	Set to 1 when the "Auto Update expected value" option is enabled for the control. When enabled the control's expected value for posture evaluation is replaced with the actual value collected from the cloud agent scan.

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_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.
/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	(PATH_TYPE?, 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?, INTEGRITY_CHECK_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?, INTEGRITY_CHECK_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_TIME_LIMIT?, FILE_CONTENT_CHECK_V2_MATCH_LIMIT?, INTEGRITY_CHECK_MATCH_LIMIT?, DISABLE_CASE_SENSITIVE_SEARCH?, EXCLUDE_USER_OWNER?, EXCLUDE_GROUP_OWNER?, INTEGRITY_CHECK_OBJECT_TYPES?, WIN_FILE_SYS_OBJECT_TYPES?, MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?, WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?, SCRIPT_ID?, SCRIPT_NAME?, OUTPUT_FILTER?, GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, EVALUATE_AS_STRING?, DESCRIPTION)
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/PATH_TYPE (#PCDATA)	Specify file location using the path types: Registry Key, File Search, File Path.

XPath	element specifications / notes
/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.
/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)	

XPath	element specifications / notes
	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.
/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/DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)	
	Disable the case-sensitive search in Unix agent UDCs (Directory Search and Directory Integrity).

XPath	element specifications / notes
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/EXCLUDE_USER_OWNER (#PCDATA)	(Supported only by Cloud Agent) For Unix Directory Search and Unix Directory Integrity controls, this is a flag (true or false) indicating whether to exclude the files owned by certain users specified as comma separated list of user names and/or UIDs.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/EXCLUDE_GROUP_OWNER (#PCDATA)	(Supported only by Cloud Agent) For Unix Directory Search and Unix Directory Integrity controls, this is a flag (true or false) indicating whether to exclude the 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/FILE_CONTENT_CHECK_V2_TIME_LIMIT (#PCDATA)	The search time limit specified for a Unix File Content Check V2 control.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/FILE_CONTENT_CHECK_V2_MATCH_LIMIT (#PCDATA)	The search match limit specified for a Unix File Content Check V2 control.
/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.
/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/SCRIPT_ID (#PCDATA)	For future use.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/SCRIPT_NAME (#PCDATA)	

XPath	element specifications / notes
	For future use.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/OUTPUT_FILTER (#PCDATA)	
	For future use.
/POLICY_EXPORT_OUTPUT/RESPONSE/POLICY/SECTIONS/SECTION/CONTROLS/USER_DEFINED_CONTROL/SCAN_PARAMETERS/EVALUATE_AS_STRING (#PCDATA)	
	A scan parameter that identifies if the Evaluate as string option is enabled for Unix file content check
/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).
/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).

XPath	element specifications / notes
/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+)
/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).

XPath	element specifications / notes
/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 id .
/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 id 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 id 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 Info List Output

API used

[platform API server](#)/api/2.0/fo/compliance/posture/info/?action=list

DTD for Compliance Posture Info List Output

[platform API server](#)/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd

A recent DTD 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?, EVALUATION_DATE?, PREVIOUS_STATUS?,
FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?,
EXCEPTION?, EVIDENCE?, CAUSE_OF_FAILURE?)>
<!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 EVALUATION_DATE (#PCDATA)>
<!ELEMENT PREVIOUS_STATUS (#PCDATA)>
<!ELEMENT FIRST_FAIL_DATE (#PCDATA)>
<!ELEMENT LAST_FAIL_DATE (#PCDATA)>
<!ELEMENT FIRST_PASS_DATE (#PCDATA)>
<!ELEMENT LAST_PASS_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?, EXTENDED_EVIDENCE?,
STATISTICS?, EXTENDED_STATISTICS_ERROR? )>
<!ELEMENT BOOLEAN_EXPR (#PCDATA)>
<!ELEMENT DPV_LIST (DPV+)>
<!ELEMENT DPV (LABEL, (ERROR|V)+, TM_REF?)>
<!ATTLIST DPV lastUpdated CDATA #IMPLIED>
<!ELEMENT V (#PCDATA|H|R)*>
<!ATTLIST V fileName CDATA #IMPLIED>
<!ELEMENT H (C+)>
<!ELEMENT R (C+)>
<!ELEMENT EXTENDED_EVIDENCE (#PCDATA)>
<!ELEMENT STATISTICS (#PCDATA)>
<!ELEMENT EXTENDED_STATISTICS_ERROR (#PCDATA)>

<!ELEMENT CAUSE_OF_FAILURE (DIRECTORY_FIM_UDC, UNEXPECTED?, MISSING?,
ADDED_DIRECTORIES?, REMOVED_DIRECTORIES?, PERMISSON_CHANGED_DIRECTORIES?,
CONTENT_CHANGED_DIRECTORIES?)>
<!ELEMENT DIRECTORY_FIM_UDC (#PCDATA)>
<!ELEMENT UNEXPECTED (V*)>
<!ELEMENT MISSING (V*)>
<!ATTLIST MISSING logic CDATA #FIXED "OR">
<!ELEMENT ADDED_DIRECTORIES (V*)>
<!ELEMENT REMOVED_DIRECTORIES (V*)>
<!ELEMENT PERMISSON_CHANGED_DIRECTORIES (V*)>
<!ELEMENT CONTENT_CHANGED_DIRECTORIES (V*)>

<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT ERROR (#PCDATA)>
<!ELEMENT TM_REF (#PCDATA)>
<!ELEMENT C (#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?, DNS_DATA?, NETBIOS?, OS?,
OS_CPE?, QG_HOSTID?, ASSET_ID?, 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 DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)>
<!ELEMENT HOSTNAME (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT ASSET_ID (#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?, REFERENCE?, DEPRECATED?,
RATIONALE_LIST?)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT REFERENCE (#PCDATA)>
<!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

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.

XPath	element specifications / notes
/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?, POSTURE_MODIFIED_DATE?, EVALUATION_DATE?, PREVIOUS_STATUS?, FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?, EXCEPTION?, EVIDENCE?, CAUSE_OF_FAILURE?)
/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/EVALUATION_DATE (#PCDATA)	Date and time of last posture evaluation.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/POSTURE_MODIFIED_DATE (#PCDATA)	Date and time of modification for a compliance posture info record.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/PREVIOUS_STATUS (#PCDATA)	The previous status (passed or failed) of the controls before the compliance scan.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/FIRST_FAIL_DATE (#PCDATA)	In a set of compliance scans in which a control is failed in all the scans, this is the date and time of the first compliance scan in the set for the failed control.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/LAST_FAIL_DATE (#PCDATA)	The latest or most recent date and time when the compliance scan failed for controls..
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/FIRST_PASS_DATE (#PCDATA)	In a set of compliance scans in which a control is passed in all the scans, this is the date and time of the first compliance scan in the set for the passed control.

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/ LAST_PASS_DATE (#PCDATA)	The latest or most recent date and time when the compliance scan passed for controls.
/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.
/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/EXTENDED_EVIDENCE (BOOLEAN_EXPR, DPV_LIST?)	
	The Extended Evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/STATISTICS (BOOLEAN_EXPR, DPV_LIST?)	
	The Statistics will show information found during the control evaluation irrespective of whether the control Passed or Failed.

XPath	element specifications / notes
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/EXTENDED_STATISTICS_ERROR (BOOLEAN_EXPR, DPV_LIST?)	The Extended Statistics Error will show the error message in case of any error found during the compliance scan.
/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: lastUpdated	lastUpdated 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/(#PCDATA H R)*	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/V/H	
	Header name returned by the scan results.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/V/R	
	Row name returned by the scan results.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/V/C	
	Column name returned by the scan results.
/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/INFO/CAUSE_OF_FAILURE (DIRECTORY_FIM_UDC, UNEXPECTED?, MISSING?, ADDED_DIRECTORIES?, REMOVED_DIRECTORIES?, PERMISSON_CHANGED_DIRECTORIES?, CONTENT_CHANGED_DIRECTORIES?)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/DIRECTORY_FIM_UDC (#PCDATA)	
	Name of failed Directory Integrity Monitoring UDC (user defined control).
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/UNEXPECTED (V*)	
	For failed Directory Integrity Monitoring UDC, cause of failure is one or more unexpected values as listed.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/MISSING (V*)	

XPath

element specifications / notes

For failed Directory Integrity Monitoring UDC, cause of failure is one or more missing values as listed (with logic given as value attribute).

/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/
ADDED_DIRECTORIES (V*)

For failed Directory Integrity Monitoring UDC, cause of failure is one or more added files/directories as listed.

/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/
REMOVED_DIRECTORIES (V*)

For failed Directory Integrity Monitoring UDC, cause of failure is one or more removed files/directories as listed.

/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/
PERMISSION_CHANGED_DIRECTORIES (V*)

For failed Directory Integrity Monitoring UDC, cause of failure is permissions changed on one or more files/directories as listed.

/POSTURE_INFO_LIST_OUTPUT/RESPONSE/INFO_LIST/INFO/CAUSE_OF_FAILURE/
CONTENT_CHANGED_DIRECTORIES (V*)

For failed Directory Integrity Monitoring UDC, cause of failure is content changed on one or more files/directories as listed.

/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.

/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

XPath	element specifications / notes
/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.
/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?, DNS_DATA?, NETBIOS?, OS?, OS_CPE?, QG_HOSTID?, ASSET_ID?, 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/DNS_DATA (HOSTNAME?, DOMAIN?, FQDN?)	
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/DNS_DATA/HOSTNAME (#PCDATA)	The DNS hostname for the asset.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/DNS_DATA/DOMAIN (#PCDATA)	The domain name for the asset.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/DNS_DATA/FQDN (#PCDATA)	The Fully Qualified Domain Name (FQDN) for the asset.
/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.

XPath	element specifications / notes
/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/QG_HOSTID (#PCDATA)	The Qualys host ID assigned by Qualys. This is unique and persistent per host. Qualys host ID is assigned when the host is scanned and agentless tracking is enabled, or when a cloud agent is installed, whichever happens first.
/POSTURE_INFO_LIST_OUTPUT/RESPONSE/GLOSSARY/HOST_LIST/HOST/ASSET_ID (#PCDATA)	The unique asset ID assigned to each host asset in your subscription. You'll see the asset ID in several Asset Management APIs.
/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).
/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?, REFERENCE?, 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.

XPath	element specifications / notes
/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/REFERENCE (#PCDATA)	A control reference. This could be a CIS reference, STIG reference or user-defined reference.
/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/CONTROL/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.
/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.

XPath	element specifications / notes
/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.
/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/TM/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 online help.

Compliance Policy Report

API used

[platform API server](#)/api/2.0/fo/report/?action=fetch

DTD for Compliance Policy Report

[platform API server](#)/compliance_policy_report.dtd

A recent DTD is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE POLICY REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT COMPLIANCE_POLICY_REPORT (ERROR | (HEADER, (SUMMARY),
(RRESULTS)))>
<!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?, NEWWORK?)>
<!ELEMENT IP_LIST (IP*)>
<!ELEMENT NEWWORK (#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, QG_HOSTID?, 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 QG_HOSTID (#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?,
CAUSE_OF_FAILURE?, TECHNOLOGY, EVALUATION_DATE?, PREVIOUS_STATUS?,
FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?,
EVIDENCE?, EXCEPTION?, CONTROL_COMMENTS?)>
<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CONTROL_REFERENCES (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT CAUSE_OF_FAILURE (UNEXPECTED?, MISSING?)>
<!ELEMENT UNEXPECTED (V*)>
<!ELEMENT MISSING (V*)>
<!ATTLIST MISSING logic CDATA #FIXED "OR">
<!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 COLUMN_NAME (#PCDATA)>

```

```

<!ELEMENT CONTROL_COMMENTS (#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, QG_HOSTID?, DNS, NETBIOS,
OPERATING_SYSTEM, LAST_SCAN_DATE, PERCENTAGE,
NETWORK?,HOST_ID?,CLOUD_PROVIDER?,CLOUD_SERVICE?,CLOUD_RESOURCE_ID?,CLOUD
_RESOURCE_TYPE?, CLOUD_ACCOUNT_ID?,
CLOUD_IMAGE_ID?,CLOUD_RESOURCE_INFO?)>
<!ELEMENT CLOUD_RESOURCE_INFO (PUBLIC_IP_ADDRESS?, PRIVATE_IP_ADDRESS?,
VPC_ID?, SUBNET_ID?, INSTANCE_TYPE?, INSTANCE_STATE?, REGION_CODE?,
AVAILABILITY_ZONE?, PRIVATE_DNS_NAME?, PUBLIC_DNS_NAME? , GROUP_ID?,
GROUP_NAME?, RESERVATION_ID?, IS_SPOT_INSTANCE?, LOCAL_HOSTNAME?,
MAC_ADDRESS?)>

<!ELEMENT STATS (#PCDATA)>
<!ELEMENT SEARCH_DURATION (#PCDATA)>
<!ELEMENT ERRORS (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_TYPE (#PCDATA)>
<!ELEMENT CLOUD_ACCOUNT_ID (#PCDATA)>
<!ELEMENT CLOUD_IMAGE_ID (#PCDATA)>
<!ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
<!ELEMENT VPC_ID (#PCDATA)>
<!ELEMENT INSTANCE_STATE (#PCDATA)>
<!ELEMENT PRIVATE_DNS_NAME (#PCDATA)>
<!ELEMENT INSTANCE_TYPE (#PCDATA)>
<!ELEMENT REGION_CODE (#PCDATA)>
<!ELEMENT SUBNET_ID (#PCDATA)>
<!ELEMENT AVAILABILITY_ZONE (#PCDATA)>
<!ELEMENT PRIVATE_IP_ADDRESS (#PCDATA)>
<!ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
<!ELEMENT GROUP_ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT RESERVATION_ID (#PCDATA)>
<!ELEMENT LOCAL_HOSTNAME (#PCDATA)>
<!ELEMENT IS_SPOT_INSTANCE (#PCDATA)>
<!ELEMENT MAC_ADDRESS (#PCDATA)>

```

XPaths for Compliance Policy Report

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.
/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)

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/HEADER/FILTERS/HOST_INSTANCE (IP?, INSTANCE?)	Network of the IPs in the report.
/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.
/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)	

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_ERROR (#PCDATA)	The number of control instances with a Failed status in the report.
/COMPLIANCE_POLICY_REPORT/SUMMARY/CONTROL_INSTANCES/TOTAL_EXCEPTIONS (#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/CONTROLS_SUMMARY (CONTROL_INFO*)	The number of approved and pending exceptions in the policy report.
/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*)	

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST	(TRACKING_METHOD, QG_HOSTID?, 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.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/IP (#PCDATA)	The IP address for the host.
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/QG_HOSTID (#PCDATA)	The Qualys host ID assigned by Qualys. This is unique and persistent per host. Qualys host ID is assigned when the host is scanned and agentless tracking is enabled, or when a cloud agent is installed, whichever happens first.
/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.

XPath	element specifications / notes
/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?, CONTROL_COMMENTS?)
/COMPLIANCE_POLICY_REPORT/RESULTS/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CID	(#PCDATA) The control ID number assigned to the control.
/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))	

XPath	element specifications / notes
/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.
/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/HOST_LIST/HOST/CONTROL_LIST/CONTROL/CONTROL_COMMENTS (#PCDATA)	User-defined comments saved for the control.
/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: logic	logic 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: lastUpdated	lastUpdated 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?)	
/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.

XPath	element specifications / notes
/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, QG_HOSTID?, DNS, NETBIOS, OPERATING_SYSTEM, LAST_SCAN_DATE, PERCENTAGE, NETWORK?,HOST_ID?,CLOUD_PROVIDER?,CLOUD_SERVICE?,CLOUD_RESOURCE_ID?, CLOUD_RESOURCE_TYPE?,CLOUD_ACCOUNT_ID?, CLOUD_IMAGE_ID?,CLOUD_RESOURCE_INFO?)>	
/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/QG_HOSTID (#PCDATA)	The Qualys host ID assigned by Qualys. This is unique and persistent per host. Qualys host ID is assigned when the host is scanned and agentless tracking is enabled, or when a cloud agent is installed, whichever happens first.
/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.

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/HOST_ID (#PCDATA)	The host's unique ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_PROVIDER (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud provider (e.g. AWS).
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_SERVICE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud service (e.g. EC2).
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud resource ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_TYPE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud resource type (e.g. Instance).
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_ACCOUNT_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud account ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_IMAGE_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The cloud image ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO	(PUBLIC_IP_ADDRESS?, PRIVATE_IP_ADDRESS?, VPC_ID?, SUBNET_ID?, INSTANCE_TYPE?, INSTANCE_STATE?, REGION_CODE?, AVAILABILITY_ZONE?, PRIVATE_DNS_NAME?, PUBLIC_DNS_NAME?, GROUP_ID?, GROUP_NAME?, RESERVATION_ID?, IS_SPOT_INSTANCE?, LOCAL_HOSTNAME?, MAC_ADDRESS?)>
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/PUBLIC_IP_ADDRESS (#PCDATA)	(Applicable when cloud metadata is included in the report.) The public IP address.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/PRIVATE_IP_ADDRESS (#PCDATA)	(Applicable when cloud metadata is included in the report.) The private IP address.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/VPC_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The VPC ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/SUBNET_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The subnet ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/INSTANCE_TYPE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The instance type (e.g. t2.micro).

XPath	element specifications / notes
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/INSTANCE_STATE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The instance state (e.g. PENDING, RUNNING, TERMINATED, STOPPED).
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/REGION_CODE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The region code.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/AVAILABILITY_ZONE (#PCDATA)	(Applicable when cloud metadata is included in the report.) The availability zone in which the instance launched.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/PRIVATE_DNS_NAME (#PCDATA)	(Applicable when cloud metadata is included in the report.) The private DNS hostname.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/PUBLIC_DNS_NAME (#PCDATA)	(Applicable when cloud metadata is included in the report.) The public DNS hostname.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/GROUP_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The group ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/GROUP_NAME (#PCDATA)	(Applicable when cloud metadata is included in the report.) The group name.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/RESERVATION_ID (#PCDATA)	(Applicable when cloud metadata is included in the report.) The reservation ID.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/IS_SPOT_INSTANCE (#PCDATA)	(Applicable when cloud metadata is included in the report.) Indicates whether the instance is a Spot instance. A value of 0 means it is not a Spot instance. A value of 1 means it is a Spot instance.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/LOCAL_HOSTNAME (#PCDATA)	(Applicable when cloud metadata is included in the report.) The local hostname.
/COMPLIANCE_POLICY_REPORT/SUMMARY/HOST_STATISTICS/HOST_INFO/CLOUD_RESOURCE_INFO/MAC_ADDRESS (#PCDATA)	(Applicable when cloud metadata is included in the report.) The MAC address.

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 for Compliance Authentication Report

[<platform API server>/compliance_authentication_report.dtd](#)

A recent 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|AU
TH_NOT_ATTEMPTED|AUTH_NOT_INSTALLED|AUTH_TOTAL|PASSED_PERCENTAGE|FAILED_P
ERCENTAGE|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_N
OT_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_N
OT_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?,
HOST_ID?, ALL_ASSET_TAGS?)>
<!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)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT ALL_ASSET_TAGS (#PCDATA)>

```

XPaths for Compliance Authentication Report

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)

XPath	element specifications / notes
	An error message.
attribute: number	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)
/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+)	

XPath	element specifications / notes
/COMPLIANCE_AUTHENTICATION_REPORT/HEADER/FILTERS/ASSET_TAG_LIST/EXCLUDED_TAGS/TAG_ITEM (#PCDATA)	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.
	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.
/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.

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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.
/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 for Compliance Scorecard Report

[platform API server](#)/compliance_scorecard_report.dtd

A recent DTD 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_TITLE|TECHNOLOGY|CONTROL_INSTANCES|HOSTS_TOTAL|HOSTS_SCANNED|HOSTS_CHANGED|PASSED_TOTAL|PASSED_CHANGED|FAILED_TOTAL|FAILED_CHANGED|ERROR_TOTAL|ERROR_CHANGED|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

XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT	(ERROR (HEADER, (SUMMARY) (DETAILS)))
/COMPLIANCE_SCORECARD_REPORT/ERROR (#PCDATA COUNT PERCENT)	An error message.
attribute: number	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.

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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.
/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+))	

XPath	element specifications / notes
/COMPLIANCE_SCORECARD_REPORT/SUMMARY/REPORT_DISCOVERIES/BY_TECHNOLOGY/TOTAL_TECHNOLOGY (#PCDATA)	The number of technologies included in the report.
/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

API used

[<platform API server>](#)/api/2.0/fo/compliance/exception/?action=list

DTD for Network List Output

[<platform API server>](#)/api/2.0/fo/compliance/exception/exception_list_output.dtd

A recent DTD 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

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.
/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?)

XPath	element specifications / notes
/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)
/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.

XPath	element specifications / notes
/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.
/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

API used

[<platform API server>](#)/api/2.0/fo/compliance/exception/?action=update|delete

DTD for Exception Batch Return Output

[<platform API server>](#)/api/2.0/fo/compliance/exception/exception_batch_return.dtd

A recent DTD is shown below.

```
<!-- 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

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+)	

XPath	element specifications / notes
/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

API used

[<platform API server>](#)/api/2.0/fo/compliance/fdd_policy/?action=list

DTD for SCAP Policy List Output

[<platform API server>](#)/api/2.0/fo/compliance/fdcc_policy/fdcc_policy_list_output.dtd

A recent DTD 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

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?)

XPath	element specifications / notes
/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.
/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.

XPath	element specifications / notes
/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.

Chapter 10 - User XML

This section describes the XML output returned from User API requests.

[User Output](#)

[User List Output](#)

[User Action Log Report](#)

[Password Change Output](#)

User Output

API used

[<platform API server>/msp/user.php](#)

DTD for User Output

[<platform API server>/user_output.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS USER OUTPUT DTD -->

<!ELEMENT USER_OUTPUT (API, RETURN, USER?)>

<!-- "name" is the name of API -->
<!-- "at" is the current platform date and time -->
<!ELEMENT API (#PCDATA)>
<!ATTLIST API
    name CDATA #REQUIRED
    username CDATA #REQUIRED
    at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RETURN (MESSAGE?)>
<!ATTLIST RETURN
    status (FAILED|SUCCESS|WARNING) #REQUIRED
    number CDATA #IMPLIED>

<!ELEMENT MESSAGE (#PCDATA)>

<!-- USER element in case password needs to be returned in XML -->
<!ELEMENT USER (USER_LOGIN, PASSWORD)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT PASSWORD (#PCDATA)>
```

XPaths for User Output

XPath	element specifications / notes
/USER_OUTPUT	(API, RETURN, USER?)
/USER_OUTPUT/API	(#PCDATA)
attribute: name	name is <i>required</i> and is the API function name.
attribute: username	username is <i>required</i> and is the user login of the API user.
attribute: at	at is <i>required</i> and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).
/USER_OUTPUT/RETURN	(MESSAGE?)
attribute: status	status is <i>required</i> and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: number	number is <i>implied</i> and, if present, is an error code.
/USER_OUTPUT/RETURN/MESSAGE	(#PCDATA)
	A descriptive message that corresponds to the status code.
/USER_OUTPUT/USER	(USER_LOGIN, PASSWORD)
	The USER element (with sub-elements) is returned for a new user account when the user.php request included the send_email=0 input parameter.
/USER_OUTPUT/USER/USER_LOGIN	(#PCDATA)
	The user login ID for the new user account.
/USER_OUTPUT/USER/PASSWORD	(#PCDATA)
	The new and current password for the new user account.

User List Output

API used

<platform API server>/msp/user_list.php

DTD for User List Output

<platform API server>/user_list_output.dtd

A recent DTD is shown below.

```
<!-- QUALYS USER LIST OUTPUT DTD -->

<!ELEMENT USER_LIST_OUTPUT (ERROR | USER_LIST)>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT USER_LIST (USER*)>

<!ELEMENT USER (USER_LOGIN?, USER_ID?, EXTERNAL_ID?, CONTACT_INFO,
    ASSIGNED_ASSET_GROUPS?, USER_STATUS, CREATION_DATE,
    LAST_LOGIN_DATE?, USER_ROLE, MANAGER_POC?,
    BUSINESS_UNIT?, UNIT_MANAGER_POC?,
```

```
        UI_INTERFACE_STYLE?, PERMISSIONS?, NOTIFICATIONS?)>

<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT EXTERNAL_ID (#PCDATA)>

<!ELEMENT CONTACT_INFO (FIRSTNAME, LASTNAME, TITLE, PHONE, FAX, EMAIL,
                        COMPANY, ADDRESS1, ADDRESS2, CITY, COUNTRY, STATE,
                        ZIP_CODE, TIME_ZONE_CODE)>

<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT PHONE (#PCDATA)>
<!ELEMENT FAX (#PCDATA)>
<!ELEMENT EMAIL (#PCDATA)>
<!ELEMENT COMPANY (#PCDATA)>
<!ELEMENT ADDRESS1 (#PCDATA)>
<!ELEMENT ADDRESS2 (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>
<!ELEMENT TIME_ZONE_CODE (#PCDATA)>

<!ELEMENT ASSIGNED_ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>

<!ELEMENT USER_STATUS (#PCDATA)>
<!ELEMENT CREATION_DATE (#PCDATA)>
<!ELEMENT LAST_LOGIN_DATE (#PCDATA)>
<!ELEMENT USER_ROLE (#PCDATA)>
<!ELEMENT MANAGER_POC (#PCDATA)>
<!ELEMENT BUSINESS_UNIT (#PCDATA)>
<!ELEMENT UNIT_MANAGER_POC (#PCDATA)>
<!ELEMENT UI_INTERFACE_STYLE (#PCDATA)>

<!ELEMENT PERMISSIONS (CREATE_OPTION_PROFILES, PURGE_INFO, ADD_ASSETS,
                        EDIT_REMEDIATION_POLICY, EDIT_AUTH_RECORDS)>

<!ELEMENT CREATE_OPTION_PROFILES (#PCDATA)>
<!ELEMENT PURGE_INFO (#PCDATA)>
<!ELEMENT ADD_ASSETS (#PCDATA)>
<!ELEMENT EDIT_REMEDIATION_POLICY (#PCDATA)>
<!ELEMENT EDIT_AUTH_RECORDS (#PCDATA)>

<!ELEMENT NOTIFICATIONS (LATEST_VULN, MAP, SCAN, DAILY_TICKETS)>

<!ELEMENT LATEST_VULN (#PCDATA)>

<!ELEMENT MAP (#PCDATA)>
<!ELEMENT SCAN (#PCDATA)>
<!ELEMENT DAILY_TICKETS (#PCDATA)>
```

XPaths for User List Output

XPath	element specifications / notes
/USER_LIST_OUTPUT	(ERROR USER_LIST)
/USER_LIST_OUTPUT/ERROR	(#PCDATA)
attribute: number	number is <i>implied</i> and if present, will be an error code.
/USER_LIST_OUTPUT/USER_LIST	(USER*)
/USER_LIST_OUTPUT/USER_LIST/USER	(USER_LOGIN?, EXTERNAL_ID?, CONTACT_INFO, ASSIGNED_ASSET_GROUPS?, USER_STATUS, CREATION_DATE, LAST_LOGIN_DATE?, USER_ROLE, MANAGER_POC?, BUSINESS_UNIT?, UNIT_MANAGER_POC?, UI_INTERFACE_STYLE?, PERMISSIONS?, NOTIFICATIONS?)
/USER_LIST_OUTPUT/USER_LIST/USER/USER_LOGIN (#PCDATA)	The Qualys user login ID for the user's account.
/USER_LIST_OUTPUT/USER_LIST/USER/USER_ID (#PCDATA)	The unique ID for the user's account.
/USER_LIST_OUTPUT/USER_LIST/USER/EXTERNAL_ID (#PCDATA)	The user's custom external ID, if defined. If not defined, this element does not appear.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO	(FIRSTNAME, LASTNAME, TITLE, PHONE, FAX, EMAIL, COMPANY, ADDRESS1, ADDRESS2, CITY, COUNTRY, STATE, ZIP_CODE, TIME_ZONE_CODE)
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/FIRSTNAME (#PCDATA)	The user's first name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/LASTNAME (#PCDATA)	The user's last name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/TITLE (#PCDATA)	The user's job title.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/PHONE (#PCDATA)	The user's phone number.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/FAX (#PCDATA)	The user's fax number.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/EMAIL (#PCDATA)	The user's email address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/COMPANY (#PCDATA)	The user's company name.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ADDRESS1 (#PCDATA)	The first line of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ADDRESS2 (#PCDATA)	The second line of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/CITY (#PCDATA)	The user's city.

XPath	element specifications / notes
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/COUNTRY (#PCDATA)	The user's country.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/STATE (#PCDATA)	The user's state.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/ZIP_CODE (#PCDATA)	The zip code of the user's street address.
/USER_LIST_OUTPUT/USER_LIST/USER/CONTACT_INFO/TIME_ZONE_CODE (#PCDATA)	The user's time zone code This will be the browser's timezone (Auto) or a user-selected code (e.g. US-NY).
/USER_LIST_OUTPUT/USER_LIST/USER/ASSIGNED_ASSET_GROUPS (ASSET_GROUP_TITLE+)	
/USER_LIST_OUTPUT/USER_LIST/USER/ASSIGNED_ASSET_GROUPS/ASSET_GROUP_TITLE (#PCDATA)	The title of an asset group assigned to the user.
/USER_LIST_OUTPUT/USER_LIST/USER/USER_STATUS (#PCDATA)	The user status. Possible values are Active, Inactive and Pending Activation.
/USER_LIST_OUTPUT/USER_LIST/USER/CREATION_DATE (#PCDATA)	The date and time when the user account was created.
/USER_LIST_OUTPUT/USER_LIST/USER/LAST_LOGIN_DATE (#PCDATA)	The most recent date/time the user logged into Qualys using the user login ID specified in the <USER_LOGIN> element. This element is returned when the API request was made by a Manager or Unit Manager. For a Manager, the last login date is returned for all users in the subscription. For a Unit Manager, the last login date is returned for users in the Unit Manager's same business unit.
/USER_LIST_OUTPUT/USER_LIST/USER/USER_ROLE (#PCDATA)	The user role assigned to the user. Possible values are Manager, Unit Manager, Scanner, Reader and Contact.
/USER_LIST_OUTPUT/USER_LIST/USER/MANAGER_POC (#PCDATA)	A flag indicating whether the user is the Manager Point of Contact (POC) for the subscription. The value 1 is returned when this user is the Manager POC. The value 0 is returned when this user is not the Manager POC.
/USER_LIST_OUTPUT/USER_LIST/USER/BUSINESS_UNIT (#PCDATA)	The business unit the user belongs to. If the user is not part of a business unit then the value is "Unassigned".
/USER_LIST_OUTPUT/USER_LIST/USER/UNIT_MANAGER_POC (#PCDATA)	A flag indicating whether this user is the Unit Manager Point of Contact (POC) for the user's business unit. The value 1 is returned when this user is the Unit Manager POC. The value 0 is returned when this user is not the Unit Manager POC.
/USER_LIST_OUTPUT/USER_LIST/USER/UI_INTERFACE_STYLE (#PCDATA)	The user interface style applied to the user account. Possible values are standard_blue, navy_blue, coral_red, olive_green and accessible_high_contrast.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS	(CREATE_OPTION_PROFILES, PURGE_INFO, ADD_ASSETS, EDIT_REMEDIATION_POLICY, EDIT_AUTH_RECORDS)

XPath	element specifications / notes
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/CREATE_OPTION_PROFILES (#PCDATA)	A flag indicating whether the user is granted permission to create personal option profiles. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/PURGE_INFO (#PCDATA)	A flag indicating whether the user is granted permission to permanently delete saved host information. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/ADD_ASSETS (#PCDATA)	A flag indicating whether the Unit Manager is granted permission to add IPs and domains to the user's business unit, and thus to the subscription. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/EDIT_REMEDIATION_POLICY (#PCDATA)	A flag indicating whether the Unit Manager is granted permission to create and edit a remediation policy for the user's business unit. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/PERMISSIONS/EDIT_AUTH_RECORDS (#PCDATA)	A flag indicating whether the Unit Manager is granted permission to create and edit authentication records when all of the target hosts in the record are in the user's business unit. The value 1 is returned when the user is granted this permission. The value 0 is returned when the user is not granted this permission.
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS (LATEST_VULN, MAP, SCAN, DAILY_TICKETS)	
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/LATEST_VULN (#PCDATA)	A flag indicating how often the user receives the Latest Vulnerabilities email notification. Possible values are weekly, daily and none.
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/MAP (#PCDATA)	A flag indicating whether the user receives the Map Notification via email. The value will be one of: "ags" - the user receives the Map Notification (this option is set to "On" in the UI) "none" - the user does not receive the Map Notification (this option is set to "Off" in the UI)
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/SCAN (#PCDATA)	A flag indicating whether the user receives the Scan Summary Notification via email. The value will be one of: "ags" - the user receives the Scan Summary Notification (this option is set to "On" in the UI) "none" - the user does not receive the Scan Summary Notification (this option is set to "Off" in the UI)
/USER_LIST_OUTPUT/USER_LIST/USER/NOTIFICATIONS/DAILY_TICKETS (#PCDATA)	A flag indicating whether the user receives the Daily Trouble Tickets Updates email notification. The value 1 is returned when this notification should be sent to the user. The value 0 is returned when this notification should not be sent to the user.

User Action Log Report

API used

<platform API server>/msp/action_log_report.php

DTD for Action Log Report

<platform API server>/action_log_report.dtd

A recent DTD is shown below.

```
<!-- QUALYS ACTION LOG REPORT DTD -->

<!ELEMENT ACTION_LOG_REPORT (ERROR | (DATE_FROM, DATE_TO, USER_LOGIN?,
ACTION_LOG_LIST))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!ELEMENT DATE_FROM (#PCDATA)*>
<!ELEMENT DATE_TO (#PCDATA)*>
<!ELEMENT USER_LOGIN (#PCDATA)*>

<!ELEMENT ACTION_LOG_LIST (ACTION_LOG)*>
<!ELEMENT ACTION_LOG (DATE, MODULE, ACTION, DETAILS, USER, IP?)>
<!ELEMENT DATE (#PCDATA)>
<!ELEMENT MODULE (#PCDATA)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT DETAILS (#PCDATA)>

<!ELEMENT USER (USER_LOGIN, FIRSTNAME, LASTNAME, ROLE)>
<!ELEMENT FIRSTNAME (#PCDATA)>
<!ELEMENT LASTNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!ELEMENT IP (#PCDATA)>
```

XPaths for Action Log Report

XPath	element specifications / notes
/ACTION_LOG_REPORT	(ERROR (DATE_FROM, DATE_TO, USER_LOGIN?, ACTION_LOG_LIST))
/ACTION_LOG_REPORT/ERROR	(#PCDATA)
attribute: number	number is <i>implied</i> and if present, will be an error code.
/ACTION_LOG_REPORT/DATE_FROM	(#PCDATA)
	The start date and time of the time window for downloading action log entries, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT). Note: If the time is not specified as part of the “date_from” input parameter for the action log request, then the time is set to the start of the day: T00:00:00Z

XPath	element specifications / notes
/ACTION_LOG_REPORT/DATE_TO (#PCDATA)	The end date and time of the time window for downloading action log entries, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT). Note: If the “date_to” input parameter is not specified for the action log request, then the current date and time are used. If the date is specified but the time is not specified, then the time is set to the end of the day: T23:59:59Z
/ACTION_LOG_REPORT/USER_LOGIN (#PCDATA)	The Qualys user login ID specified to filter results. Note: This element appears only when the “user_login” input parameter is specified for the action log request.
/ACTION_LOG_REPORT/ACTION_LOG_LIST (ACTION_LOG)*	
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG	(DATE, MODULE, ACTION, DETAILS, USER, IP?)
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/DATE (#PCDATA)	The date and time when the action occurred, in YYYY-MMDDTHH:MM:SSZ format (UTC/GMT).
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/MODULE (#PCDATA)	The module affected by the action. See the Qualys online help for a listing.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/ACTION (#PCDATA)	The action performed. See the Qualys online help for a listing.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/DETAILS (#PCDATA)	Additional information about the action. For example, details may include map and scan targets, scan reference numbers and specific changes to account configurations.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER	(USER_LOGIN, FIRSTNAME, LASTNAME, ROLE)
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/USER_LOGIN (#PCDATA)	The Qualys user login ID for the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/FIRSTNAME (#PCDATA)	The first name of the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/LASTNAME (#PCDATA)	The last name of the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/USER/ROLE (#PCDATA)	The user role (Manager, Unit Manager, Scanner or Reader) assigned to the user who performed the action.
/ACTION_LOG_REPORT/ACTION_LOG_LIST/ACTION_LOG/IP (#PCDATA)	The IP address of the system used by the user to perform the action.

Password Change Output

API used

[<platform API server>/msp/password_change.php](#)

DTD for Password Change Output

[<platform API server>/password_change_output.dtd](#)

A recent DTD is shown below.

```
<!-- QUALYS PASSWORD CHANGE OUTPUT DTD -->

<!ELEMENT PASSWORD_CHANGE_OUTPUT (API,RETURN)>

<!-- "name" is the name of API -->
<!-- "at" attribute is the current platform date and time -->
<!ELEMENT API (#PCDATA)>
<!ATTLIST API
    name CDATA #REQUIRED
    username CDATA #REQUIRED
    at CDATA #REQUIRED>

<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RETURN (MESSAGE, CHANGES?, NO_CHANGES?)>
<!ATTLIST RETURN
    status (FAILED|SUCCESS|WARNING) #REQUIRED
    number CDATA #IMPLIED>
<!ELEMENT MESSAGE (#PCDATA)*>

<!ELEMENT CHANGES (USER_LIST)>
<!ATTLIST CHANGES count CDATA #IMPLIED>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, PASSWORD?, REASON?)>

<!ELEMENT NO_CHANGES (USER_LIST)>
<!ATTLIST NO_CHANGES count CDATA #IMPLIED>
```

XPaths for Password Change Report

XPath	element specifications / notes
/PASSWORD_CHANGE_OUTPUT	(API, RETURN)
/PASSWORD_CHANGE_OUTPUT/API	(#PCDATA)
attribute: name	name is <i>required</i> and is the API function name.
attribute: username	username is <i>required</i> and is the user login of the API user.
attribute: at	at is <i>required</i> and is the date/time when the function was run in YYYY-MM-DDTHH:MM:SSZ format (UTC/GMT).

XPath	element specifications / notes
/PASSWORD_CHANGE_OUTPUT/RETURN	(MESSAGE, CHANGES?, NO_CHANGES?)
attribute: status	status is <i>required</i> and is a status code, either SUCCESS, FAILED, or WARNING.
attribute: number	number is <i>implied</i> and, if present, is an error code.
/PASSWORD_CHANGE_OUTPUT/RETURN/MESSAGE	(#PCDATA)
	A descriptive message that corresponds to the status code.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES	(USER_LIST)
attribute: count	count is <i>implied</i> and, if present, is the total number of user accounts for which passwords were updated.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST	(USER+)
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER	(USER_LOGIN, PASSWORD?, REASON?)
	The USER element (with sub-elements) is returned for a user account when the password_change.php request included the email=0 input parameter.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/USER_LOGIN	(#PCDATA)
	The user login ID for a user account.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/PASSWORD	(#PCDATA)
	The new and current password for the user account.
/PASSWORD_CHANGE_OUTPUT/RETURN/CHANGES/USER_LIST/USER/REASON	(#PCDATA)
	The reason why the password for the user account was not updated. For example, if the user has running maps and/or scans.
/PASSWORD_CHANGE_OUTPUT/RETURN/NO_CHANGES	(USER_LIST)
attribute: count	count is <i>implied</i> and, if present, is the total number of user accounts which do not have changed passwords.
/PASSWORD_CHANGE_OUTPUT/RETURN/NO_CHANGES/USER_LIST	(USER+)

Appendix

- Simple Return
- Batch Return

Simple Return

The simple return is XML output returned from several API calls.

DTD for Simple Return

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

A recent 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

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.

XPath	element specifications / notes
/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/KEY (#PCDATA)	The response item value.

Batch Return

The batch return is XML output returned from several API calls.

DTD for Simple Return

[platform API server](#)/api/2.0/batch_return.dtd

A recent DTD is 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

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.
/SIMPLE_RETURN/REQUEST/RESOURCE	(#PCDATA) The resource specified for the request.
/BATCH_RETURN/REQUEST/PARAM_LIST	(PARAM+)
/BATCH_RETURN/REQUEST/PARAM_LIST/PARAM	(KEY, VALUE)

XPath	element specifications / notes
/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.