



# Qualys API

Quick Reference

October 06, 2023

Copyright 2017-2023 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

<b>Vulnerability Management and Policy Compliance API</b> .....	<b>5</b>
Scans .....	5
Authentication .....	7
Authentication Vaults .....	14
Scanner Appliances .....	16
Option Profiles .....	17
KnowledgeBase .....	20
Reports .....	22
Report Templates .....	24
Remediation .....	27
Compliance Info .....	27
Users .....	30
Activity Log v2 .....	31
Activity Log v1 .....	31
<b>Cloud Agent API</b> .....	<b>32</b>
Agent Management .....	32
Activation Key .....	33
Configuration Profile .....	33
<b>Asset Management &amp; Tagging API</b> .....	<b>35</b>
Networks .....	35
Assets .....	35
Asset Groups .....	38
Tag .....	39
List users with their tags .....	40
Host Asset .....	40
Asset .....	40
Host Instance Vulnerability .....	41
Asset Data Connector .....	41
AWS Asset Data Connector .....	42
AWS Authentication Record .....	42
<b>Continuous Monitoring API</b> .....	<b>44</b>
Alerts .....	44
Profiles .....	44
Rulesets .....	44
Rules .....	45
<b>Web Application Scanning API</b> .....	<b>46</b>

Web Application .....	46
Authentication .....	47
Scan .....	48
Schedule .....	49
Option Profile .....	52
Report .....	52
Report Creation .....	53
Findings .....	55
Burp .....	56
<b>Web Application Firewall API .....</b>	<b>57</b>
Web Applications .....	57
Web Servers .....	58
Healthchecks .....	59
SSL Certificates .....	60
Custom Response Pages .....	61
Security Policies .....	62
HTTP Profiles .....	63
Custom Rules .....	64
Clusters .....	65
Appliances .....	66
<b>Malware Detection API.....</b>	<b>67</b>
Malware Detections .....	67
<b>Security Assessment Questionnaire API.....</b>	<b>68</b>
SAQ users .....	68
SAQ templates .....	69
<b>Portal version API.....</b>	<b>71</b>
Portal version .....	71
<b>API Server URL.....</b>	<b>72</b>
Qualys API Server URL .....	72
Still need help? .....	72
<b>Good to Know.....</b>	<b>73</b>
Notations .....	73
GET and POST .....	73
Date/Time .....	73
API Notes .....	73
Curl Client .....	73
Allowed Operators .....	73
Looking for more? .....	73

# Vulnerability Management and Policy Compliance API

Use these API calls to manage vulnerability and compliance scans and report on scan results.

[Scans](#) | [Authentication](#) | [Scanner Appliances](#) | [Option Profiles](#) | [KnowledgeBase](#) | [Reports](#) | [Report Templates](#) | [Remediation](#) | [Compliance Info](#) | [Users](#) | [Activity Log v2](#) | [Activity Log v1](#)

Looking for more information?

[Qualys API \(VM, PC\) User Guide](#)

[Qualys API \(VM, PC\) XML/DTD Reference](#)

## Scans

### Manage Scans

VM Scans - /api/2.0/fo/scan/

Compliance Scans - /api/2.0/fo/scan/compliance/

SCAP Scans - /api/2.0/fo/scan/scap/

### List Scans: (GET + POST)

**action**={list}&  
**echo\_request**={0|1}&  
**scan\_ref**={value}&  
**state**={Running|Paused|Canceled|Finished|Error|Queued|Loading}&  
**processed**={0|1}&  
**type**={On-Demand|Scheduled|API}&  
**target**={ip,range...}&  
**user\_login**={login}&  
**launched\_after\_datetime**={date/time}&  
**launched\_before\_datetime**={date/time}&  
**show\_agrs**={0|1}&  
**show\_op**={0|1}&  
**show\_status**={0|1}&  
**show\_last**={0|1}&  
**pci\_only**={0|1}&  
**ignore\_target**={0|1}&  
**client\_id**= {value}&  
**client\_name**={value}&  
**ec2\_instance\_ids**={value}&  
**scap\_scan\_since**={date}&  
**no\_scap\_scan\_since**={date}&

### Manage Scans: (POST)

**action**={cancel|pause|resume}&  
**echo\_request**={0|1}&  
**scan\_ref**={value}&

### Download Scan Results: (GET + POST)

**action**={fetch}&  
**echo\_request**={0|1}&  
**scan\_ref**={value}&  
**\*ips**={ip,range...}&  
**\*mode**={brief|extended}&  
**\*output\_format**={csv|json|csv\_extended|json\_extended}&

**Notes:** \* means VM scan only

### Share PCI Scan: (GET + POST)

**action**={share|status}& \*POST for share  
**echo\_request**={0|1}&  
**scan\_ref**={value}&  
**merchant\_username**={value}&

### VM Scan Summary: (GET + POST)

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

**action**={list}&  
**output\_format**={value}&  
**scan\_reference**={value}&  
**scan\_datetime\_since**={value}&  
**scan\_datetime\_until**={value}&  
**include\_scan\_input**={0|1}&  
**include\_scan\_details**={0|1}&  
**include\_hosts\_summary**={0|1}&  
**include\_detections\_summary**={0|1}&  
**include\_hosts\_summary\_categories**={value}&

### Scan Summary: (GET + POST)

/api/2.0/fo/scan/summary

**action**={list}&  
**scan\_date\_since**={value}&  
**scan\_date\_to**={value}&  
**output\_format**={value}&  
**tracking\_method**={value}&  
**include\_dead**={0|1}&  
**include\_excluded**={0|1}&  
**include\_unresolved**={0|1}&  
**include\_cancelled**={0|1}&  
**include\_notvuln**={0|1}&  
**include\_blocked**={0|1}&  
**include\_duplicate**={0|1}&

include\_aborted={0|1}&

### List Last 'N' Scan References for a Schedule: (GET)

/api/2.0/fo/scan/scanner

**action**={list}&  
**schedule\_scan\_ids**={value1, value2,...}&  
**schedule\_executions\_count**={value}& (1-10)  
**output\_format**={XML|JSON}&

### Scanner Details: (GET + POST)

/api/2.0/fo/scan/scanner

**action**={list}&  
**scan\_date\_since**={value}&  
**scan\_date\_to**={value}&  
**ips**={value}&  
**output\_format**=XML&

### Launch Scan

VM Scan - /api/2.0/fo/scan/

Compliance Scan - /api/2.0/fo/scan/compliance/

### Launch Scan: (POST)

**action**={launch}&  
**echo\_request**={0|1}&  
**scan\_ref**={value}&  
**scan\_title**={value}&  
**target\_from**={assets|tags}&  
**ip**={value}&  
**asset\_groups**={value}&  
**asset\_group\_ids**={value}&  
**exclude\_ip\_per\_scan**={value}&  
**tag\_include\_selector**={all|any}&  
**tag\_exclude\_selector**={all|any}&  
**tag\_set\_by**={id|name}&  
**tag\_set\_include**={value}&  
**tag\_set\_exclude**={value}&  
**use\_ip\_nt\_range\_tags**={0|1}&  
**use\_ip\_nt\_range\_tags\_include**={0|1}&  
**use\_ip\_nt\_range\_tags\_exclude**={0|1}&  
**iscanner\_id**={value1,value2...}&  
**iscanner\_name**={value1,value2...}&  
**default\_scanner**={0|1}&  
**scanners\_in\_ag**={0|1}&  
**scanners\_in\_tagset**={0|1}&  
**scanners\_in\_network**={value}

**option\_title**={value}&  
**option\_id**={value}&  
**priority**={value}& (0-9) \*default is 0  
**runtime\_http\_header**={value}&  
**connector\_name**={value}& \*for EC2 scan  
**ec2\_endpoint**={value}& \*for EC2 scan  
**ip\_network\_id**={id}&  
**fqdn**={value}&  
**client\_id**={value}&  
**client\_name**={value}&  
**ec2\_instance\_ids**={value}&

### Scheduled Scans

VM Scans - /api/2.0/fo/schedule/scan/

### List Scheduled Scans: (GET)

**action**={list}&  
**echo\_request**={0|1}&  
**id**={value}&  
**active**={0|1}&  
**show\_notifications**={0|1}&  
**client\_id**={value}&  
**client\_name**={value}&

### Create Scheduled Scan: (POST)

**action**={create}&  
**echo\_request**={0|1}&  
**scan\_title**={value}&  
**active**={0|1}&  
**option\_title**={value}&  
**option\_id**={value}&  
**iscanner\_id**={value1,value2...}&  
**iscanner\_name**={value1,value2...}&  
**ip**={value}&  
**asset\_groups**={value}&  
**asset\_group\_ids**={value}&  
**default\_scanner**={0|1}&  
**scanners\_in\_ag**={0|1}&  
**scanners\_in\_tagset**={0|1}&  
**exclude\_ip\_per\_scan**={value}&  
**ip\_network\_id**={id}&  
**runtime\_http\_header**={value}&  
**target\_from**={assets|tags}&  
**tag\_include\_selector**={all|any}&  
**tag\_exclude\_selector**={all|any}&  
**tag\_set\_by**={id|name}&  
**tag\_set\_include**={value}&  
**tag\_set\_exclude**={value}&

```
use_ip_nt_range_tags={0|1}&
use_ip_nt_range_tags_include={0|1}&
use_ip_nt_range_tags_exclude={0|1}&
connector_name={value}& *for EC2 scan
connector_uuid={value}& *for EC2 scan
ec2_endpoint={value}& *for EC2 scan
ec2_only_classic={value}& *for EC2 scan
occurrence={daily|weekly|monthly}&
frequency_days={value}& (1-365)
frequency_weeks={value}& (1-52)
weekdays={sunday|monday|tuesday|
wednesday|thursday|friday|saturday}&
frequency_months={value}& (1-12)
day_of_month={value}& (1-31)
day_of_week={value}& (0-6, where 0 is
sunday)
week_of_month={first|second|third|fourth|
last}&
start_date={date}&
start_hour={value}& (0-23)
start_minute={value}& (0-59)
time_zone_code={value}&
observe_dst={yes|no}&
recurrence={value}&
end_after={value}& (0-119)
end_after_mins={value}& (0-59)
pause_after_hours={value}& (1-119)
pause_after_mins={value}& (0-59)
resume_in_days={value}& (1-9)
resume_in_hours={value}& (0-23)
fqdn={value}&
client_id= {value}&
client_name={value}&
```

**Notes:** “end\_after\_mins” must be specified with “end\_after”. “pause\_after\_mins” must be specified with “pause\_after\_hours”. “resume\_in\_hours” must be specified with “pause\_after\_hours” and “resume\_in\_days”.

```
before_notify={0|1}&
before_notify_unit={days|hours|minutes}&
before_notify_time={value}&
before_notify_message={value}&
after_notify={0|1}&
after_notify_message={value}&
recipient_group_ids={value}&
```

**Notes:** “before\_notify\_time” must be specified with before\_notify=1. “before\_notify\_message” is only valid when before\_notify=1.

“after\_notify\_message” is only valid when after\_notify=1. “recipient\_group\_ids” is only valid when before\_notify=1 or after\_notify=1 is also specified.

### Update Scheduled Scan: (POST)

```
action={update}&
id={value}&
echo_request={0|1}&
set_start_time={0|1}&
client_id= {value}&
client_name={value}&
```

**Notes:** For updating the start time, these must be specified together: set\_start\_time=1, start\_date, start\_hour, start\_minute, time\_zone\_code, observe\_dst.

For Daily Scan, these must be specified together: occurrence=daily, frequency\_days.

For Weekly Scan, these must be specified together: occurrence=weekly, frequency\_weeks, weekdays.

For Monthly Scan, these must be specified together: occurrence=monthly, frequency\_months and day\_of\_month (for Nth day of month) or day\_of\_week, week\_of\_month (for Day in Nth week).

### Delete Scheduled Scan: (POST)

```
action={delete}&
id={value}&
echo_request={0|1}&
```

## Authentication

### Authentication Record List

/api/2.0/fo/auth/

### List Records (all types): (GET + POST)

```
action={list}&
echo_request={0|1}&
title={value}&
comments={value}&
```

```
ids={id,range...}&  
id_min={id}&  
id_max={id}&
```

## Authentication Record by Type List

```
/api/2.0/fo/auth/{type}/
```

where {type} is one of: unix, windows, oracle, oracle\_listener, snmp, ms\_sql, neo4j, ibm\_db2, vmware, vcenter, http, apache, ms\_iis, ibm\_websphere, mysql, tomcat, oracle\_weblogic, mongodb, mariadb, palo\_alto\_firewall, jboss, kubernetes, sapiq, sap\_hana, nginx

### List Records by Type: (GET + POST)

```
action={list}&
```

**Notes:** Same optional parameters as for authentication records list (all types) plus: details={Basic|All|None}&

## Authentication Records

```
/api/2.0/fo/auth/<type>/
```

where <type> is one of: unix (for Unix, Cisco, Checkpoint Firewall), windows, oracle, oracle\_listener, snmp, vmware, vcenter, apache, ms\_iis, ibm\_websphere, http, mysql, ms\_sql, docker, postgresql, sybase, tomcat, mongodb, mariadb, palo\_alto\_firewall, jboss, kubernetes, sapiq, sap\_hana, network\_ssh, neo4j, nginx, informixDB, infoblox,

### Manage Records: (GET + POST)

```
action={create|update|delete}&  
title={value}&  
ids={id,range...}&  
echo_request={0|1}&
```

**Notes:** “title” is required for a create request. “ids” is required for an update and delete request.

```
comments={value}&  
{target hosts} (*requirements below)  
{<type> credentials} (*requirements per record)
```

**Notes:** Comments, target hosts, and credentials specified for create and update requests only (not delete requests).

### {target hosts}:

```
ips={ip,range...}&  
add_ips={ip,range...}&  
remove_ips={ip,range...}&  
network_id={value}&
```

when Tag Support for Authentication Records is enabled (Windows, Unix):

```
asset_type={ips|asset_tags|ip_range_tag_rule}&  
tag_set_by={id|name}&  
tags_include={tag1,tag2...}&  
tags_exclude={tag1,tag2,...}&  
tag_include_selector={any|all}&  
tag_exclude_selector={any|all}&
```

**Notes:** “ips” is required for a create request (except for Windows, and except when Tag Support is enabled), optional for an update request. “add\_ips” and “remove\_ips” are for an update request only. “network\_id” is valid when the networks feature is enabled.

### {vault definition}:

```
login_type={basic|vault}& /set to vault to enable  
vault_id={value}&  
vault_type={value}&  
(vault parameters below are required except as indicated, * means optional)
```

#### ARCON PAM

```
vault_service_type={value}&
```

#### Azure Key

```
ak_secret_name={value}&
```

#### CA Access Control

```
end_point_name={value}&  
end_point_type={value}&  
end_point_container={value}&
```

#### CA PAM

```
vault_app_name={value}&  
vault_device_name={value}&  
vault_device_host={value}&
```

#### CyberArk PIM Suite

```
folder={value}&  
file={value}&
```

#### CyberArk AIM

```
folder={value}&
```



```
file={value}&
HashiCorp
secret_kv_path={value}&
secret_kv_name={value}&
secret_kv_key={value}&
Thycotic Secret Server
secret_name={value}&
Quest Vault
system_name={value}&
Lieberman ERPM
auto_discover_system_name={value}&
system_name_single_host={value}&
system_type={auto|windows|unix|oracle|mssql|ldap|system|custom}&
*custom_system_type=&{value}
*valid when system_type=custom
BeyondTrust PBPS
*system_type={value}&
*account_name={value}&
Wallix AdminBastion (WAB)
authorization_name={value}
target_name={value}
```

**{Unix record}:**

Login credentials:

```
username={value}&
password={value}&
login_type={basic|vault}& (vault definition)
vault_type={CA Access Control|CyberArk PIM Suite|CyberArk AIM|Hitachi ID PAM|Lieberman ERPM|Quest Vault|Thycotic Secret Server|BeyondTrust PBPS|Wallix AdminBastion}
cleartext_password={0|1}&
skip_password={0|1}&
{XML File}&
target_type={auto|A10|HP_COMWARE|CISCO_ASA_WITH_FIREPOWE}
```

**Notes:** Required for create request: “username”, “password” if cleartext\_password=1. {XML File} defines private key certificates and root delegations.

Kerberos auth details, if it is enabled on the target host:

```
use_kerberos={0|1}&
realm_discovery={value}&
service_realm={value}&
```

```
service_kdc={value}&
user_kdc={value}&
krb5_password={value}&
krb5_login_type={value}&
krb5_<vaultparameters>={value}&
```

Scanning:

```
port={value}& /PC scans only
use_agentless_tracking={0|1}&
agentless_tracking_path={value}&
```

**Notes:** If use\_agentless\_tracking=1, “agentless\_tracking\_path” is required.

**{Unix subtype record}:**

```
sub_type={cisco|checkpoint_firewall}&
```

Login credentials:

```
username={value}&
password={value}&
login_type={basic|vault}& (vault definition)
vault_type={CyberArk PIM Suite|CyberArk AIM}
cleartext_password={0|1}&
enable_password={value}& (Cisco only)
expert_password={value}& (Checkpoint only)
```

**Notes:** Required for create request: “username”, “password” if cleartext\_password=1.

Scanning:

```
port={value}& /PC scans only
```

**{Network SSH record}:**

Login credentials:

```
username={value}&
password={value}&
login_type={basic|vault}& (vault definition)
p2_login_type={basic|vault}& (vault definition)
*p2_<vault parameters>
vault_type={CA Access Control|CyberArk PIM Suite|CyberArk AIM|Hitachi ID PAM|Lieberman ERPM|Quest Vault|Thycotic Secret Server|BeyondTrust PBPS|Wallix AdminBastion}
**cleartext_password={0|1}&
password2={value}&
{XML File}&
target_type={auto|A10|HP_COMWARE|CISCO_ASA_WITH_FIREPOWE}
```

**Notes:**

\* If p2\_login\_type is vault then all vault parameter fields must be added with prefix 'p2\_'

\*\* Required for create request: "username", "password" if cleartext\_password=1. {XML File} defines private key certificates.

**{Windows record}:**

Login credentials:

**username**={value}&  
**password**={value}&  
login\_type={basic|vault}& ([vault definition](#))  
windows\_domain={value}&  
windows\_ad\_domain={value}&  
ntlm={0|1}&  
kerberos={0|1}&  
ntlmv2={0|1}&  
ntlm={0|1}&  
require\_smb\_signing={0|1}&  
minimum\_smb\_version={value}&

Scanning:

use\_agentless\_tracking={0|1}&

**{Oracle record}:**

Login credentials:

login\_type={basic|vault}& ([vault definition](#))  
**username**={value}&  
**password**={value}&  
vault\_type={ARCON PAM | Azure Key | BeyondTrust PBPS | CA Access Control | CyberArk PIM Suite| CyberArk AIM | HashiCorp | Lieberman ERPM | Quest Vault | Thycotic Secret Server}&  
vault\_id={value}&  
**sid**={value}&  
**servicename**={value}&  
port={num}&  
is\_cdb={0|1}& /PC scans only  
pc\_only={0|1}& /PC scans only

OS-dependent compliance checks:

perform\_windows\_os\_checks={0|1}&  
win\_ora\_home\_name={value}&  
win\_ora\_home\_path={value}&  
win\_init\_ora\_path={value}&  
win\_spfile\_ora\_path={value}&  
win\_listener\_ora\_path={value}&

win\_sqlnet\_ora\_path={value}&  
win\_tnsnames\_ora\_path={value}&  
perform\_unix\_os\_checks={0|1}&  
perform\_unix\_opatch\_checks={0|1}&  
unix\_ora\_home\_path={value}&  
unix\_init\_ora\_path={value}&  
unix\_spfile\_ora\_path={value}&  
unix\_listener\_ora\_path={value}&  
unix\_sqlnet\_ora\_path={value}&  
unix\_tnsnames\_ora\_path={value}&  
unix\_invptrloc={value}&

**{Oracle Listener record}:**

**password**={value}&

**{IBM DB2 record}:**

Login credentials:

**login\_type**={basic| vault}&  
**username**={value}&  
**password**={value}&  
**database**={value}&  
**port**={value}&  
pc\_only={0|1}& /PC scans only

OS-dependent compliance checks:

win\_db2dir={value}  
win\_prilogfile={value}  
win\_seclogfile={value}  
win\_terlogfile={value}  
win\_mirlogfile={value}  
unix\_db2dir={value}  
unix\_prilogfile={value}  
unix\_seclogfile={value}  
unix\_terlogfile={value}  
unix\_mirlogfile={value}

**Notes:** All check parameters are required if you want OS-dependent compliance checks to be run.

**{MySQL record}:**

username={value}&  
password={value}&  
database={value}&  
port={value}&  
windows\_config\_file={value}&  
unix\_config\_file={value}&  
ssl\_verify={value}&  
hosts={value}&  
client\_cert={value}&  
client\_key={value}&

```
kerberos={0|1}&  
ntlmv2={0|1}&  
ntlm={0|1}&  
member_domain={value}& or ips={value}&
```

**Notes:** All parameters are required for create request, except client\_cert and client\_key (which must be specified together).

**{Neo4j record}:**

```
username={value}&  
password={value}&  
login_type={basic|vault}&  
database={value}&  
port={value}&  
ssl_verify={value}&  
hosts={value}&  
neo4j_version={value}&  
unix_base_path={value}&  
unix_conf_path={value}&  
neo4j_auto_path={0|1}&
```

**{Nginx record}:**

```
unix_bin_path={value}&  
unix_conf_path={value}&  
unix_prefix_path={0|1}&
```

**{Infoblox record}:**

Login credentials:

```
username={value}&  
password={value}&  
login_type={basic|vault}& (vault definition)  
vault_type={CyberArk PIM Suite|Thycotic  
Secret Server|BeyondTrust PBPS|Wallix  
AdminBastion|Hashicorp|Azure key}&  
api_version={value}&  
ssl_verify={0|1}&
```

**{InformixDB record}:**

Login credentials:

```
username={value}&  
password={value}&  
login_type={basic}&
```

**{SNMP record}:**

```
version={v1|v2c|v3}&
```

SNMPv1 and SNMPv2c:

```
community_strings={value,value...}&
```

**Notes:** “community\_strings” is optional for create and update requests.

SNMPv3:

```
username={value}&  
password={value}&  
auth_alg={MD5|SHA1}&  
encrypt_password={value}&  
priv_alg={DES|AES}&  
security_engine_id={value}&  
context_engine_id={value}&  
context={value}&
```

**Notes:** All SNMPv3 parameters are optional. However, when one is specified, others are required as follows. 1) It is required that “username”, “password” and auth\_alg” are all defined for record. 2) It is required that “encrypt\_password” and “priv\_alg” are all defined for record. 3) For an update request “auth\_alg” and “priv\_alg” may be set to empty, in which case the data is not encrypted.

**{VMware record}:**

```
username={value}&  
password={value}&  
port={value}&  
hosts={value}&  
ssl_verify={all|skip|none}&  
login_type=&  
is_disconnect={0|1}&
```

**Notes:** “username” and “password” are required for a create request, optional for an update request.

**{vCenter record}:**

```
username={value}&  
password={value}&  
port={value}&  
hosts={value}&  
ssl_verify={all|skip|none}&  
login_type={basic|vault}&
```

**Notes:** “username” and “password” are required for a create request, optional for an update request.

**{Apache Web Server record}:**

```
unix_apache_config_file={value}&  
unix_apache_control_command={value}&  
windows_apache_config_file={value}&  
windows_apache_control_command=  
{value}&  
status={0|1}&  
is_system_created={0|1}&
```

**{IBM WebSphere App Server record}:**

```
unix_installation_dir={value}&  
unix_dir_mode={installation_dir|server_dir}&  
windows_installation_dir={value}
```

**{Tomcat Server record}:**

```
installation_path={value}&  
instance_path={value}&  
auto_discover_instances={0|1}&  
installation_path_windows={value}&  
instance_path_windows={value}&  
service_name={value}&
```

**Notes:** “installation\_path” or “installation\_path\_windows” is required for a create request.

**{HTTP record}:**

```
username={value}&  
password={value}&  
vhost={value}&  
realm={value}&  
ssl={0|1}&
```

**Notes:** “vhost” or “realm” is required for a create request. “ips” parameter is not valid for this record type.

**{MongoDB record}:**

```
unix_conf_file={value}&  
database_name={value}&  
port={value}&  
ssl_verify={0|1}&  
hosts={value}&  
credential_type={local|external}&  
cleartext={0|1}&  
login_type={basic|vault|pkcert}& (vault definition)  
username={value}&  
password={value}&
```

```
vault_type={BeyondTrust PBPS | CA Access Control | CyberArk PIM Suite| CyberArk AIM |Quest Vault | Thycotic Secret Server}&  
vault_id={value}&  
private_key={value}&  
private_key_vault_id={value}&  
passphrase={value}&  
certificate={value}&  
require_cert={0|1}&
```

**Notes:** Required for create request when login\_type=basic: “username” and “password”.

Required for create request when login\_type=vault: “username”, “vault\_type” and “vault\_id”. Required for create request when login\_type=pkcert: “private\_key” and “passphrase” (when passphrase\_vault\_id is not specified.) “hosts” required if ssl\_verify=1.

**{MariaDB record}:**

```
ssl_verify={0|1}&  
hosts={value}&  
database={value}&  
port={value}&  
windows_conf_file={value}&  
unix_conf_file={value}&  
client_cert={value}&  
client_key={value}&
```

Login credentials:

```
login_type={basic|vault}&  
username={value}&  
password={value}&
```

**Notes:** “username” and “password” are required for a create request, optional for an update request.

**{Palo Alto Networks Firewall record}:**

```
username={value}&  
password={value}&  
login_type=vault& (vault definition)  
vault_id={value}&  
vault_type={CyberArk PIM Suite | CyberArk AIM | Quest Vault | Thycotic Secret Server | BeyondTrust PBPS}&
```

**Notes:** “password” or “login\_type=vault” is required for create request.

**{Boss Server record}:**

windows\_working\_mode={value}&

Following parameters are required if Windows working mode is selected.

windows\_home\_path={value}&  
windows\_base\_path={value}&  
windows\_conf\_dir\_path={value}&  
windows\_conf\_file\_path={value}&  
windows\_conf\_host\_file\_path={value}&  
unix\_working\_mode={value}&

Following parameters are required if Unix working mode is selected.

unix\_home\_path={value}&  
unix\_base\_path={value}&  
unix\_conf\_dir\_path={value}&  
unix\_conf\_file\_path={value}&  
unix\_conf\_host\_file\_path={value}&

## PC scans only

**{Azure MS SQL record}:**

(PC scans only)

username={value}&  
password={value}&  
login\_type={basic|vault}& ([vault definition](#))  
vault\_type={ARCON PAM|BeyondTrust  
PBPS|CA Access Control|CyberArk  
AIM|CyberArk PIMSuite|HashiCorp|  
Lieberman ERPM|Quest Vault|Thycotic Secret  
Server}  
port={value}&  
database\_name={value}&  
- or - auto\_discover\_databases={0|1}&

**{Docker record}:**

(PC scans only)

docker\_daemon\_conf\_file={value}  
docker\_command={value}

**{Kubernetes record}:**

(PC scans only)

unix\_bin\_path={value}  
unix\_conf\_path={value}

**{MS SQL record}:**

(PC scans only)

username={value}&  
password={value}&  
port={value}&  
db\_local={0|1}&  
windows\_domain={value}&  
auth\_os\_type={unix|windows}&  
mssql\_unix\_insta\_path={value}&  
mssql\_unix\_conf\_path={value}&  
instance={value}& default is “MSSQLSERVER”  
- or - auto\_discover\_instances={0|1}&  
database={value}& default is “master”  
- or - auto\_discover\_databases={0|1}&  
port={value}&  
- or - auto\_discover\_ports={0|1}&

**Notes:** When “db\_local” is unspecified for a create request, the flag is set to 1 (MS SQL Server credentials). “windows\_domain” is required when “db\_local=0”, otherwise it is invalid.

**{Oracle WebLogic Server record}:**

(PC scans only)

installation\_path={value}&  
auto\_discover={0|1}&  
domain={value}&

**{PostgreSQL record}:**

(PC scans only)

pgsql\_unix\_conf\_file={value}&  
username={value}&  
password={value}&  
login\_type={basic|vault}& ([vault definition](#))  
vault\_type={CA Access Control|CyberArk PIM  
Suite|CyberArk AIM |Hitachi ID PAM|Quest  
Vault|Thycotic Secret Server|BeyondTrust  
PBPS}  
pgsql\_db\_name={value}&  
port={value}&  
ssl\_verify={0|1}&  
hosts={value}&  
client\_key\_type={basic|vault}&  
client\_key={value}&  
client\_key\_vault\_type={CyberArk  
AIM|BeyondTrust PBPS}&  
client\_key\_vault\_id={value}&  
passphrase\_type={basic|vault}&

```
passphrase={value}&  
client_cert={value}&  
passphrase_vault_type={CA Access  
Control|CyberArk PIM Suite|CyberArk AIM  
|Hitachi ID PAM|Quest Vault|Thycotic Secret  
Server|BeyondTrust PBPS}&  
passphrase_vault_id={value}&
```

**Notes:** Required for create request: “password” if login\_type=basic.

#### {SAP Hana record}:

(PC scans only)

```
database={value}&  
port={value}&  
unix_conf_path={value}&  
ssl_verify={0|1}&  
hosts={value}&  
username={value}&  
password={value}&  
password_encryption={0|1}  
login_type={basic|vault}& (vault definition)  
vault_type={Arcon PAM|Azure Key|  
BeyondTrust PBPS|CyberArk AIM|CyberArk  
PIM Suite|HashiCorp|Thycotic Secret Server}&  
vault_id={value}&
```

**Notes:** Required for a create request: “password” if login\_type=basic, “unix\_conf\_path” if the record will be used for scanning Unix hosts, “hosts” if ssl\_verify=1.

#### {SAP IQ record}:

(PC scans only)

```
username={value}&  
password={value}&  
password_encryption={0|1}  
login_type={basic|vault}& (vault definition)  
vault_type={Arcon PAM|Azure Key|  
BeyondTrust PBPS|CA Access Control|CA PAM,  
CyberArk AIM|CyberArk PIM Suite|HashiCorp|  
Hitachi ID PAM|Lieberman ERPM|Quest Vault|  
Thycotic Secret Server|Wallix AdminBastion  
(WAB)}&  
port={value}&  
database={value}&  
install_dir={value}&
```

**Notes:** Required for a create request: “password” if login\_type=basic, “install\_dir” if record will be used for scanning Unix hosts.

#### {Sybase record}:

(PC scans only)

```
username={value}&  
password={value}&  
login_type={basic|vault}& (vault definition)  
vault_type={CyberArk PIM Suite|CyberArk  
AIM |Quest Vault|Thycotic Secret Server|  
Lieberman ERPM}  
port={value}&  
database={value}&  
install_dir={value}&
```

**Notes:** Required for a create request: “password” if login\_type=basic, “install\_dir” if record will be used for scanning Unix hosts.

## Authentication Vaults

/api/2.0/fo/vault/

### List Vaults: (GET + POST)

```
action={list}&  
echo_request={0|1}&  
title={value}&  
type={CyberArk PIM Suite|Thycotic Secret  
Server|Quest Vault|CA Access Control|Hitachi ID  
PAM|Lieberman ERPM|CyberArk AIM|BeyondTrust  
PBPS|Wallix AdminBastion (WAB)}&  
modified={date/time}&  
orderby={id|title|system_name|last_modified|  
last_modified_by}&  
sortorder={asc|desc}&  
limit={value}&  
offset={value}&
```

**Notes:** “sortorder” is valid only when “orderby” is specified. “limit” and “offset” must be specified together.

### Manage Vaults: (GET + POST)

```
action={create|update|delete}&  
title={value}&  
type={CyberArk PIM Suite|Thycotic Secret  
Server|Quest Vault|CA Access Control|Hitachi
```

ID PAM|Lieberman ERPM|BeyondTrust PBPS|Wallix  
AdminBastion (WAB)  
id={id}  
comments={value}&  
echo\_request={Q|1}&  
{settings}

**Notes:** “title” and “type” are required for a create request, optional for an update request. “comments” is optional for create and update request. “id” is required for an update and delete request. “settings” for create and update request, varies per vault type (see below).

#### ARCON PAM:

url={value}&\*  
ssl\_verify={1|0}&\*  
username={value}&\*  
password={value}&\*

**Notes:** bold means required for new vault

#### Azure Key:

url={value}&\*  
app\_id={value}&\*  
ssl\_verify={1|0}&\*  
certificate={value}&\*  
private\_key={value}&\*  
passphrase={value}&

**Notes:** bold means required for new vault

#### CA PAM:

url={value}&\*  
apikey\_name={value}&\*  
ssl\_verify={1|0}&\*  
apikey={value}&\*

**Notes:** bold means required for new vault

#### CA Access Control:

ca\_url={value}&\*  
ca\_api\_username={value}&\*  
ca\_ssl\_verify={1|0}&\*  
ca\_web\_username={value}&  
ca\_web\_password={value}&

**Notes:** bold means required for new vault

#### CyberArk PIM Suite:

server\_address={value}&\*  
port={value}&  
safe={value}&\*  
username={value}&\*  
password={value}&\*

#### HashiCorp:

url={value}&\*  
api\_version={value}&  
ssl\_verify={1|0}&\*  
if auth\_type={userpass}&\*  
path={value}&  
username={value}&\*  
password={value}&\*  
if auth\_type={cert}&\*  
path={value}&  
role\_name={value}&\*  
cert={value}&\*  
private\_key={value}&\*  
passphrase={value}&  
if auth\_type={cert}&\*  
path={value}&  
role\_id={value}&\*  
secret\_id={value}&

**Notes:** bold means required for new vault

#### Hitachi ID PAM:

url={value}&\*  
username={value}&\*  
password={value}&\*  
ssl\_verify={1|0}&\*

**Notes:** bold means required for new vault

#### Lieberman ERPM:

url={value}&\*  
domain={value}&  
username={value}&\*  
password={value}&\*  
ssl\_verify={1|0}&\*

**Notes:** bold means required for new vault

#### Quest Vault:

server\_address={value}&\*  
port={value}&  
username={value}&\*  
access\_key={value}&\*

**Notes:** bold means required for new vault

### Thycotic Secret Server:

**url**={value}&  
**username**={value}&  
**password**={value}&  
**domain**={value}&

**Notes:** bold means required for new vault

### CyberArk AIM:

**appid**={value}&  
**safe**={value}&  
**url**={value}&  
**ssl\_verify**={0|1}&  
cert={value}&  
private\_key={value}&  
private\_key\_pwd={value}&

**Notes:** bold means required for new vault

### Wallix AdminBastion (WAB)

**url**={value}&  
ssl\_verify={0|1}&  
**username**={value}&  
password={value}&  
appkey={value}

### BeyondTrust PBPS:

**appkey**={value}&  
**url**={value}&  
**username**={value}&  
password={value}&  
**ssl\_verify**={0|1}&  
cert={value}&  
private\_key={value}&  
private\_key\_pwd={value}&

**Notes:** bold means required for new vault

## Scanner Appliances

/api/2.0/fo/appliance/

### List Appliances: (GET + POST)

action={list}&  
echo\_request={0|1}&  
output\_mode={**brief**|full}&  
scan\_detail={0|1}&  
include\_cloud\_info={0|1}&  
busy={0|1}&  
scan\_ref={value}&  
name={value}&

ids={id1,id2...}&  
include\_license\_info={0|1}&  
network\_id={id}&  
type={physical|virtual|offline}&  
show\_tags={0|1}&  
platform\_provider={ec2|ec2\_compat|gce|azure|vCenter}&

**Notes:** “include\_license\_info” applies to virtual scanner appliances

### Virtual Scanners: (GET + POST)

echo\_request={0|1}&  
-----  
**action**={create}&  
**name**={value}&  
**asset\_group\_id**={value}&  
polling\_interval={60-360}& \*default is 180

**Notes:** “asset\_group\_id” is required for Unit Managers and Scanners with permission to create virtual scanners. Managers do not specify “asset\_group\_id”.

-----  
**action**={update}&  
**id**={id}&  
name={value}&  
comment={value}&  
polling\_interval={60-360}&  
set\_tags= {value}&  
add\_tags= {value}&  
remove\_tags= {value}&  
tag\_set\_by= {id|name}&  
enable\_ipv6={0|1}&  
\*set\_vlans={ID|IP\_ADDRESS|NETMASK|NAME}&  
\*set\_routes={IP\_ADDRESS|NETMASK|GATEWAY|NAME}&

\*Notes: Or “ (empty string) to delete all records

-----  
**action**={delete}&  
id={id}&

### Physical Scanners: (POST)

/api/2.0/fo/appliance/physical/  
**action**={update}&  
**id**={id}&  
name={string}&  
polling\_interval={60-360}& \*default is 180  
set\_vlans={value}&  
set\_tags= {value}&  
add\_tags= {value}&



```
remove_tags= {value}&  
tag_set_by= {id|name}&  
set_routes={value}&  
comment={value}&  
*set_vlans={ID|IP_ADDRESS|NETMASK|NAME}&  
*set_routes={IP_ADDRESS|NETMASK|GATEWAY|NAME}&
```

#### Assign Appliance to Network: (POST)

```
action={assign_network_id}&  
appliance_id={id}&  
network_id={id}&  
echo_request={0|1}&
```

#### Replace Appliance: (POST)

```
/api/2.0/fo/appliance/replace_iscanner/
```

```
action={replace}&  
echo_request={0|1}&  
old_scanner_name={value}&  
new_scanner_name={value}&  
do_not_copy_settings={0|1}&  
do_not_remove_new_scanner_from_objects={0|1}&
```

## Option Profiles

```
/api/2.0/fo/subscription/option_profile/
```

#### Export Option Profile: (GET)

```
/api/2.0/fo/subscription/option_profile/
```

```
action={export}&  
output_format={XML}&  
option_profile_id={value}&  
option_profile_title={value}&  
option_profile_type={user|compliance|pci}&
```

#### Import Option Profile: (POST)

```
/api/2.0/fo/subscription/option_profile/
```

```
action={import}&
```

**Notes:** When calling this API the user needs to pass the proper XML with Content-Type XML.

## VM Option Profiles

```
/api/2.0/fo/subscription/option_profile/vm/?
```

#### Create VM Option Profile: (POST)

```
action={create}&
```

```
title={value}&  
owner={value}&  
default={0|1}&  
global={0|1}&  
offline_scanner={0|1}&  
scan_tcp_ports={none|full|standard|light}&  
scan_tcp_ports_additional={port1,port2}&  
3_way_handshake={0|1}&
```

#### Scan

```
enable_max_scan_duration_per_asset={0|1}&  
max_scan_duration_per_asset_minutes=maximum  
scan_udp_ports={none|full|standard|light}&  
scan_udp_ports_additional={port1,port2}&  
authoritative_option={0|1}&  
scan_dead_hosts={0|1}&  
close_vuln_on_dead_hosts={0|1}&  
not_found_alive_times={value}&  
purge_host_data={0|1}&  
external_scanners_use={value}&  
scan_parallel_scaling={0|1}&  
scan_overall_performance={high|normal|low|custom}&  
scan_external_scanners={value}&  
scan_scanner_appliances={value}&  
scan_total_process={value}&  
scan_http_process={value}&  
scan_packet_delay={minimum|short|medium|long|maximum}&  
scan_intensity={normal|medium|low|minimum}&  
load_balancer={0|1}&  
password_brute_forcing_system={minimal|limited|standard|exhaustive}&  
password_brute_forcing_custom={value1,value2}&  
vulnerability_detection={complete|custom|runtime}&  
custom_search_list_ids={value1,value2}&  
custom_search_list_title={value1,value2}&  
basic_host_information_checks={0|1}&  
oval_checks={0|1}&  
all_qrds_checks={0|1}&  
exclude_search_list_ids={value1,value2}&  
authentication={value1,value2}&  
authentication_least_privilege=Unix&  
enable_additional_certificate_detection={0|1}&  
enable_dissolvable_agent={0|1}&
```

enable\_windows\_share\_enumeration={0|1}&  
enable\_lite\_os\_scan={0|1}&  
enable\_partial\_ssl\_tls\_auditing = {0|1}  
custom\_http\_header={value}&  
custom\_http\_definition\_key={value}&  
custom\_http\_definition\_header={value}&  
host\_alive\_testing={0|1}&  
not\_overwrite\_os={0|1}&  
test\_authentication={0|1}&

#### System Authentication

include\_system\_auth={0|1}&  
use\_system\_auth\_on\_duplicate={0|1}&  
use\_user\_auth\_on\_duplicate={0|1}&

#### Map

basic\_information\_gathering=[all|register|netblockonly|none]&  
map\_tcp\_ports\_standard\_scan={0|1}&  
map\_tcp\_ports\_additional={value1,value2}&  
map\_udp\_ports\_standard\_scan={0|1}&  
map\_udp\_ports\_additional={value1,value2}&  
perform\_live\_host\_sweep={0|1}&  
disable\_dns\_traffic={0|1}&  
map\_overall\_performance={high|normal|low|custom}&  
map\_external\_scanners={value}&  
map\_scanner\_appliances={value}&  
map\_netblock\_size={1024 IPs|4096 IPs|8192 IPs|16384 IPs|32768 IPs|65536 IPs}&  
map\_packet\_delay={minimum|short|medium|long|maximum}&  
map\_authentication={VMware | vCenter}&

#### Additional

additional\_tcp\_ports={0|1}&  
additional\_tcp\_ports\_standard\_scan={0|1}&  
additional\_tcp\_ports\_additional={value1,value2}&  
additional\_udp\_ports={0|1}&  
additional\_udp\_ports\_type={standard|custom}&  
additional\_udp\_ports\_custom={value1,value2}&  
icmp={0|1}&  
blocked\_resources={0|1}&  
protected\_ports={default|custom}&  
protected\_ports\_custom={value1,value2}&  
protected\_ips={all|custom}&  
protected\_ips\_custom={value1,value2}&

ignore\_firewall\_generated\_tcp\_rst\_packets={0|1}&  
ignore\_all\_tcp\_rst\_packets={0|1}&  
ignore\_firewall\_generated\_tcp\_syn\_ack\_packets={0|1}&  
not\_send\_tcp\_ack\_or\_syn\_ack\_packets\_during\_host\_discovery={0|1}&

#### Update VM Option Profile: (POST)

action={update}&  
id={value}&

For other parameters see [Create VM Option Profile](#)

#### List VM Option Profile: (GET + POST)

action={list}&

#### Delete VM Option Profile: (GET + POST)

action={delete}&  
id={value}&

### PCI Option Profiles

/api/2.0/fo/subscription/option\_profile/pci/?

#### Create PCI Option Profile: (POST)

action={create}&  
title={value}&  
owner={value}&  
global={0|1}&  
offline\_scanner={0|1}&  
scan\_parallel\_scaling={0|1}&  
**Scan**  
scan\_overall\_performance={high|normal|low|custom}&  
scan\_external\_scanners={value}&  
scan\_scanner\_appliances={value}&  
scan\_total\_process={value}&  
scan\_http\_process={value}&  
scan\_packet\_delay={minimum|short|medium|long|maximum}&  
scan\_intensity={normal|medium|low|minimum}&  
scan\_dead\_hosts={0|1}&  
close\_vuln\_on\_dead\_hosts={0|1}&  
not\_found\_alive\_times={value}&  
purge\_host\_data={0|1}&  
**Additional**  
additional\_tcp\_ports\_additional={value1,value2}&

### Update PCI Option Profile: (POST)

**action**={update}&  
**id**={value}&  
For other parameters see [Create PCI Option Profile](#)

### List PCI Option Profile: (GET + POST)

**action**={list}&

### Delete PCI Option Profile: (GET + POST)

**action**={delete}&  
**id**={value}&

## Compliance Option Profiles

/api/2.0/fo/subscription/option\_profile/pc/?

### Create Compliance Option Profile: (POST)

**action**={create}&  
**title**={value}&  
**owner**={value}&  
**global**={0|1}&  
**scan\_parallel\_scaling**={0|1}&  
**Scan**  
**scan\_overall\_performance**={high|normal|low|custom}&  
**scan\_external\_scanners**={value}&  
**scan\_scanner\_appliances**={value}&  
**scan\_total\_process**={value}&  
**scan\_http\_process**={value}&  
**scan\_packet\_delay**={minimum|short|medium|long|maximum}&  
**scan\_intensity**={normal|medium|low|minimum}&  
**scan\_by\_policy**={0|1}&  
**policy\_names**={value1,value2}&  
**policy\_ids**={value1,value2}&  
**auto\_update\_expected\_value**={0|1}&  
**fim\_controls\_enabled**={0|1}&  
**custom\_wmi\_query\_checks**={0|1}&  
**enable\_dissolvable\_agent**={0|1}&  
**enable\_password\_auditing**={0|1}&  
**custom\_password\_dictionary**={value1,value2}&  
**enable\_windows\_share\_enumeration**={0|1}&  
**enable\_windows\_directory\_search**={0|1}&  
**scan\_ports**={standard|targeted}&  
**mssql\_db\_udc\_restriction**={0|1}&  
**mssql\_db\_udc\_limit**={value}&  
**oracle\_db\_udc\_restriction**={0|1}&

**oracle\_db\_udc\_limit**={value}&  
**sybase\_db\_udc\_restriction**={0|1}&  
**sybase\_db\_udc\_limit**={value}&  
**postgresql\_db\_udc\_restriction**={0|1}&  
**postgresql\_db\_udc\_limit**={value}&  
**sapiq\_db\_udc\_restriction**={0|1}&  
**sapiq\_db\_udc\_limit**={value}&  
**db2\_db\_udc\_restriction**={0|1}&  
**db2\_db\_udc\_limit**={value}&  
**enable\_auth\_instance\_discovery**={0|1}&  
**auto\_auth\_types**={value}&  
**ibm\_was\_discovery\_mode**={value}&  
**oracle\_template\_id**={value}&  
**oracle\_template\_name**={value}&  
**include\_system\_auth**={0|1}&  
**use\_system\_auth\_on\_duplicate**={0|1}&  
**use\_user\_auth\_on\_duplicate**={0|1}&  
**Instance Data Collection**  
**enable\_instance\_data\_collection**={0|1}&  
**instance\_data\_collection\_auth\_types**={value}&  
&  
**enable\_os\_based\_instance\_discovery**={0|1}&  
**os\_based\_instance\_disc\_technologies**

### Additional

**additional\_tcp\_ports**={0|1}&  
**additional\_tcp\_ports\_standard\_scan**={0|1}&  
**additional\_tcp\_ports\_additional**={value1,value2}&  
**additional\_udp\_ports**={0|1}&  
**additional\_udp\_ports\_type**={standard|custom}&  
**additional\_udp\_ports\_custom**={value1,value2}&  
**icmp**={0|1}&  
**blocked\_resources**={0|1}&  
**protected\_ports**={default|custom}&  
**protected\_ports\_custom**={value1,value2}&  
**protected\_ips**={all|custom}&  
**protected\_ips\_custom**={value1,value2}&  
**ignore\_rst\_packets**={0|1}&  
**ignore\_firewall\_generated\_syn\_ack\_packets**={0|1}&  
**not\_send\_ack\_or\_syn\_ack\_packets\_during\_host\_discovery**={0|1}&

### Update Compliance Option Profile: (POST)

**action**={update}&  
**id**={value}&

For other parameters see [Create Compliance Option Profile](#)

### List Compliance Option Profile: (GET + POST)

**action**={list}&

### Delete Compliance Option Profile: (GET + POST)

**action**={delete}&  
**id**={value}&

## KnowledgeBase

### Vulnerabilities

/api/2.0/fo/knowledge\_base/vuln/

#### List Vulnerabilities: (GET + POST)

**action**={list}&  
**echo\_request**={0|1}&  
**details**={Basic|All|None}&  
**ids**={value}&  
**id\_min**={value}&  
**id\_max**={value}&  
**is\_patchable**={0|1}&  
**last\_modified\_after**={date/time}&  
**last\_modified\_before**={date/time}&  
**last\_modified\_by\_user\_after**={date/time}&  
**last\_modified\_by\_user\_before**={date/time}&  
**last\_modified\_by\_service\_after**={date/time}&  
**last\_modified\_by\_service\_before**={date/time}&  
&  
**published\_after**={date/time}&  
**published\_before**={date/time}&  
**discovery\_method**={value}&  
**discovery\_auth\_types**={value}&  
**show\_pci\_reasons**={0|1}&  
**show\_supported\_modules\_info**={0|1}&  
**show\_disabled\_flag**={0|1}&  
**show\_qid\_change\_log**={0|1}&

**Notes:** Subscription authorization is required to use. For “discovery\_method” a valid value is: Remote, Authenticated, RemoteOnly, AuthenticatedOnly, or RemoteAndAuthenticated.

#### Edit Vulnerabilities: (POST)

/api/2.0/fo/knowledge\_base/vuln/  
**action**={edit}&  
**qid**={value}&

**severity**={value}&  
**disable**={0|1}&  
**threat\_comment**={value}&  
**impact\_comment**={value}&  
**solution\_comment**={value}&  
**include\_system\_option\_profiles**={0|1}

**Note:** Providing at least one optional parameter is mandatory.

#### Reset a Vulnerabilities: (POST)

**action**={reset}&  
**qid**={value}

#### List Edited Vulnerabilities: (POST)

**action**={custom}&

**Note:** Get a list of all edited vulnerabilities.

## KnowledgeBase QVS Download in JSON Format

/api/2.0/fo/knowledge\_base/qvs/

#### List QVS Information from KnowledgeBase: (GET + POST)

**action**={list}&  
**details**={Basic|All}&  
**CVEs**={value}&  
**qvs\_last\_modified\_before**={date}&  
**qvs\_last\_modified\_after**={date}&  
**qvs\_min**={value}&  
**qvs\_max**={value}&  
**nvd\_published\_before**={date}&  
**nvd\_published\_after**={date}&

## Static Search Lists

/api/2.0/fo/qid/search\_list/static/

#### List Static Search Lists: (GET + POST)

**action**={list}&  
**echo\_request**={0|1}&  
**ids**={id1,id2...}&

#### Create Static Search List: (POST)

**action**={create}&  
**echo\_request**={0|1}&  
**title**={value} &

qids={num1,num2...}&  
global={0|1}&  
comments={value}&

#### Update Static Search List: (POST)

action={update}&  
echo\_request={Q|1}&  
id={value}&  
title={value}&  
qids={num1,num2...}&  
add\_qids={num1,num2...}&  
remove\_qids={num1,num2...}&  
global={0|1}&  
comments={value}&

#### Delete Static Search List: (POST)

action={delete}&  
echo\_request={Q|1}&  
id={value}&

### Dynamic Search Lists

/api/2.0/fo/qid/search\_list/dynamic/

#### List Dynamic Search Lists: (GET + POST)

action={list}&  
echo\_request={Q|1}&  
ids={id1,id2...}&  
show\_qids={0|1}&  
show\_option\_profiles={0|1}&  
show\_distribution\_groups={0|1}&  
show\_report\_templates={0|1}&  
show\_remediation\_policies={0|1}&

#### Create Dynamic Search List: (POST)

action={create}&  
echo\_request={Q|1}&  
title={value}&  
global={0|1}&  
comments={value}&  
Criteria for Dynamic Search List (below)

#### Update Dynamic Search List: (POST)

action={update}&  
echo\_request={Q|1}&  
id={value}&  
title={value}&  
global={0|1}&  
comments={value}&  
unset\_user\_modified\_date={empty value}&

unset\_published\_date={empty value}&  
unset\_service\_modified\_date={empty value}&  
Criteria for Dynamic Search List (below)

#### Criteria for Dynamic Search List:

vuln\_title={value}&  
not\_vuln\_title={0|1}&  
discovery\_methods={value}&  
auth\_types={value}&  
user\_configuration={value}&  
categories={value}&  
not\_categories={0|1}&  
confirmed\_severities={value}&  
potential\_vulnerabilities={value}&  
ig\_severities={value}&  
vendor\_ids={value}&  
not\_vendor\_ids={0|1}&  
products={value}&  
not\_products={0|1}&  
cvss\_base={value}&  
cvss\_base\_operand={1|2}&  
cvss\_temp={value}&  
cvss\_temp\_operand={1|2}&  
cvss\_access\_vector={value}&  
cvss3\_base={value}&  
cvss3\_base\_operand={1|2}&  
cvss3\_temp={value}&  
cvss3\_temp\_operand={1|2}&  
cvss\_access\_vector={value}&  
patch\_available={0|1}&  
virtual\_patch\_available={0|1}&  
cve\_ids\_filter={1|2}& (1: Exact Match, 2:  
Contains)  
cve\_ids={value}&  
not\_cve\_ids={0|1}&  
exploitability={value}&  
malware\_associated={value}&  
vendor\_refs={value}&  
not\_vendor\_refs={0|1}&  
bugtraq\_id={value}&  
not\_bugtraq\_id={0|1}&  
vuln\_details={value}&  
compliance\_details={value}&  
compliance\_types={value}&  
qualys\_top\_lists={value}&  
qids\_not\_exploitable={0|1}&  
non\_running\_services={0|1}&  
sans\_20={0|1}&  
nac\_nam={0|1}&

```
vuln_provider={0|1}&  
user_modified_date_between={value}&  
user_modified_date_today={0|1}&  
user_modified_date_in_previous={value}&  
user_modified_date_within_last_days={value}&  
&  
not_user_modified={0|1}&  
service_modified_date_between={value}&  
service_modified_date_today={0|1}&  
service_modified_date_in_previous={value}&  
service_modified_date_within_last_days={valu  
e}&  
not_service_modified={0|1}&  
published_date_between={value}&  
published_date_today={0|1}&  
published_date_in_previous={value}&  
published_date_within_last_days={value}&  
not_published={0|1}&  
supported_modules={value}&
```

#### Delete Dynamic Search List: (POST)

```
action={delete} &  
echo_request={Q|1}&  
id={value}&
```

## Reports

### Manage Reports

/api/2.0/fo/report/

#### List Reports: (GET + POST)

```
action={list}&  
echo_request={Q|1}&  
id={value}&  
state={Running|Finished|Submitted|  
Canceled|Errors}&  
user_login={login}&  
expires_before_datetime={date/time}&  
client_id= {value}&  
client_name={value}&
```

#### Manage Reports: (POST)

```
action={cancel|delete}&  
echo_request={Q|1}&  
id={value}&
```

#### Download Report: (POST)

```
action={fetch}&
```

```
echo_request={Q|1}&  
client_id= {value}&  
client_name={value}&  
StatusChangedSince={YYYY-MM-DD}&
```

### Launch Report

/api/2.0/fo/report/

#### Launch Report (all types): (POST)

```
action={launch}&  
echo_request={Q|1}&  
template_id={value}&  
report_title={value}&  
pdf_password={passwd}&  
recipient_group={group,group... 50 max}&  
hide_header={0|1}&  
use_tags={0|1}&  
tag_include_selector={all|any}&  
tag_exclude_selector={all|any}&  
tag_set_by={id|name}&  
tag_set_include={value}&  
tag_set_exclude={value}&  
recipient_group_id={value}&
```

#### Map Report:

```
report_type={Map}&  
echo_request={Q|1}&  
output_format={pdf|html|mht|xml|csv|docx}&  
domain={value}&  
ip_restriction={value}&  
report_refs={value}&
```

#### Scan Report (Scan Based Findings):

```
report_type={Scan}&  
echo_request={Q|1}&  
output_format={pdf|html|mht|xml|csv}&  
report_refs={ref,ref...}&  
ip_restriction={value}&
```

#### Scan Report (Host Based Findings):

```
report_type={Scan}&  
echo_request={Q|1}&  
output_format={pdf|html|mht|xml|csv}&  
ips={value}&  
ips_network_id={id}&  
asset_group_ids={id,id...}&
```

#### Qualys Patch Report:

```
echo_request={Q|1}&
```

output\_format={pdf|online|xml|csv}&  
ips={value}&  
asset\_group\_ids={id,id...}&

### Remediation Report:

report\_type={Remediation}&  
echo\_request={0|1}&  
**output\_format**={pdf|html|mht|csv}&  
asset\_group\_ids={id,id...}&  
assignee\_type={User|All}&  
ips={value}&

### Compliance Report:

report\_type={Compliance}&  
echo\_request={0|1}&  
**output\_format**={pdf|html|mht}&

**Notes:** "mht" is not valid for PCI report.

ips={value}&  
asset\_group\_ids={id,id...}&  
report\_refs={ref,ref...}&

**Notes:** "report\_refs" is required for a PCI report, and not valid for other compliance reports.

### Compliance Policy Report:

report\_type={Policy}&  
echo\_request={0|1}&  
**output\_format**={pdf|html|mht|xml|csv}&  
**policy\_id**={value}&  
asset\_group\_ids={value}&  
ips={value}&  
instance\_string={value}&  
host\_id={value}&  
instance\_string={value}&

### Scorecard Report

/api/2.0/fo/report/scorecard/

#### Launch Scorecard: (POST)

**action**={launch}&  
echo\_request={0|1}&  
**name**={value}&  
report\_title={value}&  
**output\_format**={pdf|html|mht|xml|csv}&  
hide\_header={0|1}& (for CSV only)  
pdf\_password={passwd}&  
recipient\_group={group,group... 50 max}&  
recipient\_group\_id={distgroup1,distgroup2}&  
source={asset\_groups|business\_unit}&

asset\_groups={value,value...}&  
all\_asset\_groups={0|1}&  
business\_unit={value}&  
division={value}&  
function={value}&  
location={value}&  
patch\_quids={qid,qid...} (10 max)&  
missing\_quids={qid,qid}& (2 max)

### Scheduled Report

/api/2.0/fo/schedule/report/

#### List Scheduled Reports: (GET)

**action**={list}&  
id={value}&  
is\_active={true|false}&

#### Launch Scheduled Report: (POST)

**action**={launch\_now}&  
**id**={value}&

### Asset Search Report

/api/2.0/fo/report/asset/

#### Asset Search Report: (GET + POST)

**action**={search}&  
output\_format={csv|xml}&  
tracking\_method={IP|DNS|NETBIOS|EC2|AGENT}&  
ips={value}&  
ips\_network\_id={value}&  
asset\_group\_ids={value}&  
asset\_groups={value}&  
assets\_in\_my\_network\_only={0|1}&  
ec2\_instance\_status={RUNNING|TERMINATED|PENDING|STOPPING|SHUTTING\_DOWN|STOPPED}&  
\*ec2\_instance\_id={value}&  
\*ec2\_instance\_id\_modifier={value}&  
azure\_vm\_state={STARTING|RUNNING|STOPPING|STOPPED,DEALLOCATING,DEALLOCATED,UNKNOWN.}&  
azure\_vm\_id={value}&  
  
display\_ag\_titles={0|1}&  
ports={value}&  
services={value}&

```
qids={value}&
qid_with_text={value}&
qid_with_modifier={beginning with|
containing|matching|ending with}&
use_tags={0|1}&
tag_set_by={id|name}&
tag_include_selector={any|all}&
tag_exclude_selector={any|all}&
tag_set_include={value}&
tag_set_exclude={value}&
first_found_days={value}&
first_found_modifier={within|not within}&
last_vm_scan_days={value}&
last_vm_scan_modifier={within|not within}&
last_pc_scan_days={value}&
last_pc_scan_modifier={within|not within}&
dns_name={value}&
dns_modifier={beginning with|
containing|matching|ending with|not empty}&
netbios_name={value}&
netbios_modifier={beginning with|
containing|matching|ending with|not empty}&
os_cpe_name={value}&
os_cpe_modifier={beginning with|
containing|matching|ending with|not empty}&
os_name={value}&
os_modifier={beginning with|
containing|matching|ending with}&
Notes: *ec2_instance_id_modifier is valid only
when
```

\*ec2\_instance\_id is specified

## Report Templates

### Scan Template

#### Create Scan Template (POST)

/api/2.0/fo/report/template/scan/

**action=create**

**report\_format=xml**

title={value}&

owner={value}&

**Target**

scan\_selection={HostBased|ScanBased}&

include\_trending={0|1}&

limit\_timeframe={0|1}&

selection\_type={day|month|weeks|date|none|s  
cans}&

selection\_range={1|3|5|7|15|30|60|90}&

```
asset_groups={value}&
asset_group_ids={value}&
network={value}&
ips={value|xml}&
tag_set_by={name|id}&
tag_include_selector={ALL|ANY}&
tag_set_include={value}&
tag_exclude_selector={ALL|ANY}&
tag_set_exclude={value}&
host_with_cloud_agents={all|scan|agent}&
display_text_summary={0|1}&
graph_business_risk={0|1}&
graph_vuln_over_time={0|1}&
graph_status={0|1}&
graph_potential_status={0|1}&
graph_severity={0|1}&
```

**Display**

```
graph_potential_severity={0|1}&
```

```
graph_ig_severity={0|1}&
```

```
graph_top_categories={0|1}&
```

```
graph_top_vulns={0|1}&
```

```
graph_os={0|1}&
```

```
graph_services={0|1}&
```

```
graph_top_ports={0|1}&
```

```
display_custom_footer={0|1}&
```

```
display_custom_footer_text={value}&
```

```
sort_by={host|vuln|os|group|service|port}&
```

```
cvss={all|cvssv2|cvssv3}&
```

```
host_details={0|1}&
```

```
metadata_ec2_instances={0|1}&
```

```
cloud_provider_metadata={0|1}&
```

```
qualys_system_ids={0|1}&
```

```
include_text_summary={0|1}&
```

```
include_vuln_details={0|1}&
```

```
include_vuln_details_threat={0|1}&
```

```
include_vuln_details_impact={0|1}&
```

```
include_vuln_details_solution={0|1}&
```

```
include_vuln_details_vpatch={0|1}&
```

```
include_vuln_details_compliance={0|1}&
```

```
include_vuln_details_exploit={0|1}&
```

```
include_vuln_details_malware={0|1}&
```

```
include_vuln_details_results={0|1}&
```

```
include_vuln_details_reopened={0|1}&
```

```
include_vuln_details_appendix={0|1}&
```

```
include_trurisk_details={0|1}&
```

```
exclude_account_id={0|1}&
```

**Filters**

```
selective_vulns={complete|custom}&
```

```
search_list_ids={value}&
```



```
exclude_qid_option={Q1}&  
exclude_search_list_ids={value}&  
included_os={value}&  
status_new={0|1}&  
status_active={0|1}&  
status_reopen={0|1}&  
status_fixed={0|1}&  
vuln_active={0|1}&  
vuln_disabled={Q1}&  
vuln_ignored={Q1}&  
potential_active={Q1}&  
potential_disabled={Q1}&  
potential_ignored={Q1}&  
ig_active={Q1}&  
ig_disabled={Q1}&  
ig_ignored={Q1}&  
display_non_running_kernels={Q1}&  
exclude_non_running_kernel={Q1}&  
exclude_non_running_services={Q1}&  
exclude_qids_not_exploitable_due_to_config  
uration={Q1}&  
exclude_superceded_patches={Q1}&  
categories_list={value}&
```

#### Services and Ports

```
required_services={value}&  
unauthorized_services={value}&  
required_ports={value}&  
unauthorized_ports={value}&
```

#### User Access

```
global={Q1}&  
report_access_users={value}&
```

#### Update Scan Template (PUT)

```
/api/2.0/fo/report/template/scan/
```

```
template_id={value}&  
action=update  
report_format=xml&
```

#### Delete Scan Template (POST)

```
/api/2.0/fo/report/template/scan/
```

```
action=delete  
template_id={value}&
```

#### Export Scan Template (GET)

```
/api/2.0/fo/report/template/scan/
```

```
action=export  
report_format=xml  
template_id={value}&
```

## PCI Scan Template API

Notes: Go to Scan Template API. The same parameters used to define PCI Scan Template settings. All parameters (all are optional). In addition the following parameters are used.

#### Create PCI Scan Template (POST)

```
/api/2.0/fo/report/template/pciscan/
```

**action=create**

**report\_format=xml**

```
custom_pci_ranking={Q1}&  
customized_ranking_medium_from={0|1|2|3|4|  
5|6|7|8|9|10}&
```

```
customized_ranking_high_from={0|1|2|3|4|5|6|  
7|8|9|10}&
```

```
customized_ranking_comments={value}&  
customized_ranking_qid_searchlist_commen  
ts={<search list id1/name1> | <SEVERITY> |  
<comments>, <search list id2/name2> |  
SEVERITY> | <comments>}&
```

#### Update PCI Scan Template (PUT)

```
/api/2.0/fo/report/template/pciscan/
```

**action=update**

**report\_format=xml**

```
template_id={value}&
```

#### Delete PCI Scan Template (POST)

```
/api/2.0/fo/report/template/pciscan/
```

**action=delete**

```
template_id={value}&
```

#### Export PCI Scan Template (GET)

```
/api/2.0/fo/report/template/pciscan/
```

**action=export**

**report\_format=xml**

```
template_id={value}&
```

## Patch Template

#### Create Patch Template (POST)

```
/api/2.0/fo/report/template/patch/
```

**action=create**

**report\_format=xml**

```
title={value}&
```

```
owner={value}&
```

Target

```
patch_evaluation={qidbased|classic}&
asset_groups
asset_group_ids={value}&
tag_set_by={name|id}&
tag_include_selector={ALL|ANY}&
tag_set_exclude={value}&
tag_exclude_selector={ALL|ANY}&
network={value}&
ips={value}&
Display
group_by={HOST|PATCH|OS|AG}&
include_table_of_qids_fixed={0|1}&
include_patch_links={0|1}&
include_patches_from_unspecified_vendors={
0|1}&
include_cloud_metadata={0|1}&
patch_severity_by={assigned|highest}&
patch_cvss_score_by={assigned|highest|
none}&
cvss={all|cvssv2|cvssv3}&
display_custom_footer={0|1}&
display_custom_footer_text={value}&
exclude_account_id={0|1}&
Filters
selective_vulns={complete|custom}&
search_list_ids={value}&
exclude_qid_option={0|1}&
exclude_search_list_ids={value}&
display_non_running_kernels={0|1}&
exclude_non_running_kernel={0|1}&
exclude_non_running_services={0|1}&
exclude_qids_not_exploitable_due_to_config
uration={0|1}&
selective_patches={complete|custom}&
exclude_patch_qid_option={0|1}&
patch_search_list_ids={value}&
exclude_patch_search_list_ids={value}&
found_since_days={7|30|90|365|NoLimit}&
User Access
global={0|1}&
report_access_users={value}&
```

### Update Scan Template (PUT)

```
/api/2.0/fo/report/template/patch/
```

```
action=update
report_format=xml
template_id={value}&
```

### Delete Scan Template (POST)

```
/api/2.0/fo/report/template/patch/
```

```
action=delete
template_id={value}&
```

### Export Scan Template (GET)

```
/api/2.0/fo/report/template/patch/
```

```
action=export
report_format=xml
template_id={value}&
```

## Map Template

### Create Map Template (POST)

```
/api/2.0/fo/report/template/map/
```

```
action=create
report_format=xml
title={value}&
owner={value}&
global={0|1}&
Display
map_sort_by={ipaddress|dns|netbios|router|o
peratingsystem}&
map_related_info_lastscandate={0|1}&
map_related_info_assetgroups={0|1}&
map_related_info_authenticationrecords={0|1
}&
map_related_info_discoverymethod={0|1}&
display_custom_footer={0|1}&
display_custom_footer_text={value}&
map_exclude_account_id={0|1}&
Filters
map_included_hosttypes_innetblock={0|1}&
map_included_hosttypes_scannable={0|1}&
map_included_hosttypes_live={0|1}&
map_included_hosttypes_approved={0|1}&
map_included_hosttypes_outofnetblock={0|1
}&
map_included_hosttypes_notscannable={0|1
}&
map_included_hosttypes_notlive={0|1}&
map_included_hosttypes_rogue={0|1}&
Included Discovery Methods
map_idm_tcp={0|1}&
map_idm_udp={0|1}&
map_idm_traceroute={0|1}&
map_idm_other={0|1}&
map_idm_dns={0|1}&
```

```
map_idm_icmp={0|1}&  
map_idm_auth={0|1}&  
Included Status Levels  
map_included_statuses_added={0|1}&  
map_included_statuses_removed={0|1}&  
map_included_statuses_active={0|1}&  
dns_exclusions={none|DNS|DNS-DNSZone}&  
included_os={value}&
```

### Update Map Template (PUT)

```
/api/2.0/fo/report/template/map/
```

```
action=update  
report_format=xml  
template_id={value}&
```

### Delete Map Template (POST)

```
/api/2.0/fo/report/template/map/
```

```
action=delete  
template_id={value}&
```

### Export Map Template (GET)

```
/api/2.0/fo/report/template/map/
```

```
action=export  
report_format=xml  
template_id={value}&
```

## Remediation

### ticket\_list.php? (GET + POST)

```
{ticket-selection}  
show_vuln_details={0|1}&
```

### ticket\_edit.php? (GET + POST)

```
{ticket-selection}  
change_assignee={login}&  
change_state={OPEN|RESOLVED|IGNORED}  
reopen_ignored_days={value}&  
add_comment={value}&  
network_id={value}&
```

### ticket\_delete.php? (GET + POST)

```
{ticket-selection}
```

### {ticket-selection}:

```
ticket_numbers={num,range...}&  
since_ticket_number={num}&  
until_ticket_number={num}&  
ticket_assignee={login}&
```

```
overdue={0|1}&  
invalid={0|1}&  
states={OPEN|RESOLVED|CLOSED|  
IGNORED}&  
modified_since_datetime={date/time}&  
ips={ip,range...}&  
asset_groups={value,value...}&  
dns_contains={string}&  
netbios_contains={string}&  
vuln_severities={1,2,3,4,5}&  
potential_vuln_severities={1,2,3,4,5}&  
qids={value,value... 10 max}&  
vuln_title_contains={string}&  
vuln_details_contains={string}&  
vendor_ref_contains={string}&  
network_id={value}&
```

### ticket\_list\_deleted.php? (GET + POST)

```
ticket_numbers={num,range...}&  
since_ticket_number={num}&  
until_ticket_number={num}&  
deleted_since_datetime={date/time}&  
deleted_before_datetime={date/time}&
```

## Ignore Vulnerability

### /ignore\_vuln/index.php (GET +POST)

```
action={ignore|restore}&  
qids={value,value... 10 max}&  
comments={value}&  
(*asset_groups={value,value...}&  
(*ips={ip,range...}&  
(*tag_set_include={value}&  
(*tag_set_exclude={value}&  
(*tag_set_by={id|name}&  
(*tag_include_selector={all|any}&  
(*tag_exclude_selector={all|any}&  
(*use_ip_nt_range_tags_include={0|1}&  
(*use_ip_nt_range_tags_exclude={0|1}&  
(*dns_contains={string}&  
(*netbios_contains={string}&  
reopen_ignored_days={1-730}&  
reopen_ignored_date={date}&  
network_id={value}&
```

Notes: One of these (\*) is required

## Compliance Info

### Controls / Policies

#### List Controls: (GET + POST)

/api/2.0/fo/compliance/control/

**action**={list}&  
**echo\_request**={0|1}&  
**details**={Basic|All|None}&  
**ids**={id,range...}&  
**id\_min**={id}&  
**id\_max**={id}&  
**updated\_after\_datetime**={date/time}&  
**created\_after\_datetime**={date/time}&  
**truncation\_limit**={value}

#### List Policies: (GET + POST)

/api/2.0/fo/compliance/policy/

/api/2.0/fo/compliance/fdcc/policy/

**action**={list}&  
**echo\_request**={0|1}&  
**details**={Basic|All|None}&  
**ids**={id,range...}&  
**id\_min**={id}&  
**id\_max**={id}&  
**updated\_after\_datetime**={date/time}&  
**created\_after\_datetime**={date/time}&

#### Policy Export: (GET + POST)

/api/2.0/fo/compliance/policy/

**action**=export&  
**echo\_request**={0|1}&  
**id**={value}& -or- **title**={value}&  
**show\_user\_controls**={0|1}&  
**show\_appendix** = {0|1}  
IS\_CONTROL\_DISABLE

#### Policy Import: (POST)

/api/2.0/fo/compliance/policy/

**action**=import&  
**echo\_request**={0|1}&  
**xml\_file**&  
**title**={value}&  
**create\_user\_controls**={0|1}&

#### Policy - Manage Asset Groups: (POST)

/api/2.0/fo/compliance/policy/

**action**={add\_asset\_group\_ids|  
set\_asset\_group\_ids|remove\_asset\_group\_ids}&  
**echo\_request**={0|1}&  
**id**={value}&  
**asset\_group\_ids**={value}&  
**evaluate\_now**={0|1}&

#### Policy - Manage Asset Tags: (POST)

/api/2.0/fo/compliance/policy/

**action**={add\_asset\_tags|  
set\_asset\_tags|remove\_asset\_tags}&  
**id**={value}&  
**evaluate\_now**={0|1}&  
**tag\_include\_selector**={all|any}&  
**tag\_exclude\_selector**={all|any}&  
**tag\_set\_by**={id|name}&  
**tag\_set\_include**={tag id|name}&  
**tag\_set\_exclude**={tag id|name}

#### List Posture Info: (GET + POST)

/api/2.0/fo/compliance/posture/info/

**action**={list}&  
**policy\_id**={id} or **policy\_ids**={id1,id2,...}&  
**echo\_request**={0|1}&  
**output\_format**={xml|csv|csv\_no\_metadata}&  
**details**={Basic|Light|All|None}&  
**hide\_evidence**={0|1}&  
**show\_extended\_evidence**={0|1}&  
**ips**={ip,range...}&  
**host\_ids**={id,id...}&  
**control\_ids**={id,id...}&  
**ids**={id,range...}&  
**id\_min**={id}&  
**id\_max**={id}&  
**status\_changes\_since**={date/time}&  
**evaluation\_date**={date/time}&  
**asset\_group\_ids**={value}&  
**status**={Passed|Failed|Error}&  
**show\_remediation\_info**={0|1}&  
**truncation\_limit**={value}&  
**cause\_of\_failure**={0|1}&  
**criticality\_labels**={value}&  
**criticality\_values**={value}&  
**include\_dp\_name**={value}&  
**tag\_set\_by**={id|name}&  
**tag\_include\_selector**={all|any}&  
**tag\_exclude\_selector**={all|any}&  
**tag\_set\_include**={value}&  
**tag\_set\_exclude**={value}&

filter\_hosts={0|1}&

**Notes:** Up to 10 policies for “policy\_ids”.

### Get Policy List (GET)

/pcrs/1.0/posture/policy/list

**Note:** This API requires Request header:  
Authorization <token>.

lastEvaluationDate={date}&

### Resolve Host IDs (GET)

/pcrs/1.0/posture/hostids

**Note:** This API requires Request header:  
Authorization <token>.

policyId={value}&

### Get Posture Info (POST)

/pcrs/1.0/posture/postureInfo

**Note:** This API requires Request header:  
Authorization <token> and Request Body.

compressionRequired={0|1}&  
evidenceRequired={0|1}&  
lastEvaluationDate={date}&  
lastScanDate={date}&

### Policy Merge: (GET + POST)

/api/2.0/fo/compliance/policy/

action={merge}&  
id={id}&  
merge\_policy\_id={id} or {policy XML data}&  
replace\_cover\_page={0|1}&  
replace\_asset\_groups={0|1}&  
add\_asset\_groups={0|1}&  
add\_new\_technologies={0|1}&  
add\_new\_controls={0|1}&  
update\_section\_heading={0|1}&  
update\_existing\_controls={0|1}&  
preview\_merge={0|1}&

## Exceptions

### List Exceptions: (GET + POST)

/api/2.0/fo/compliance/exception/

action={list}&  
exception\_number={value}&  
ip={value}&  
network\_name={value}&

status={value}&  
control\_id={value}&  
control\_statement={value}&  
policy\_id={value}&  
technology\_name={value}&  
assignee\_id={value}&  
created\_by={value}&  
modified\_by={value}&  
details={Basic|All|None}&  
is\_active={0|1}&  
created\_after\_date={mm/dd/yyyy}&  
updated\_after\_date={mm/dd/yyyy}&  
expired\_before\_date={mm/dd/yyyy}&  
expired\_after\_date={mm/dd/yyyy}&  
exception\_numbers={value}&  
exception\_number\_min={value}&  
exception\_number\_max={value}&  
truncation\_limit={value}&

### Request Exceptions: (POST)

/api/2.0/fo/compliance/exception/

action={request}&  
control\_id={value}&  
host\_id={value}&  
policy\_id={value}&  
technology\_id={value}&  
instance\_string={value}&  
assignee\_id={value}&  
comments={value}&  
reopen\_on\_evidence\_change={0|1}&

### Update Exceptions: (POST)

/api/2.0/fo/compliance/exception/

action={update}&  
exception\_numbers={value}&  
comments={value}&  
reassign\_to={value}&  
reopen\_on\_evidence\_change={0|1}&  
status={Pending|Approved|Rejected}&  
end\_date={mm/dd/yyyy}&

### Delete Exceptions: (POST)

/api/2.0/fo/compliance/exception/

action={delete}&  
exception\_numbers={value}&

## ARF Report

### SCAP Scan Results: (GET + POST)

/api/2.0/fo/compliance/scap/arf/

**scan\_id**={id}&  
**ips**={ip,range...}&  
**ips\_network\_id**={value}&

## Cyberscope Report

### SCAP Scan Results: (GET + POST)

/api/2.0/fo/asset/host/cyberscope/fdcc/scan/

**scan\_id**={id}&  
**scan\_ref**={ref}&  
**ips**={ip,range...}&  
**organisation\_name1**={name1}&  
**organisation\_name2**={name2}&  
**organisation\_name3**={name3}&

**Notes:** “scan\_id” or “scan\_ref” is required.

### SCAP Policy Results: (GET + POST)

/api/2.0/fo/asset/host/cyberscope/fdcc/policy/

**policy\_id**={id}&  
**ips**={ip,range...}&  
**ag\_ids**={id,id...}&  
**organisation\_name1**={name1}&  
**organisation\_name2**={name2}&  
**organisation\_name3**={name3}&

**Notes:** All FDCC scanned hosts for the FDCC policy are included unless the filters “ip” and/or “ag\_ids” are specified.

### SCAP Global Results: (GET + POST)

/api/2.0/fo/asset/host/cyberscope/

**ips**={ip,range...}&  
**ag\_ids**={id,id...}&  
**organisation\_name1**={name1}&  
**organisation\_name2**={name2}&  
**organisation\_name3**={name3}&

**Notes:** “ips” or “ag\_ids” is required. VM scan data is reported in the datapoint <sr:DataPoint id: “vulnerability\_management\_product\_vulnerabilities”>

### SCAP Policy List: (GET + POST)

/api/2.0/fo/compliance/fdcc\_policy/

**action**={list}&  
**echo\_request**={0|1}  
**details**={Basic|All|None}  
**ids**={value}  
**id\_min**={value}  
**id\_max**={value}

## Users

### user.php? (GET + POST)

Add User:

**action**={add}&  
**send\_email**={0|1}&  
**user\_role**={manager|unit\_manager|scanner|reader|contact|administrator}&  
**business\_unit**={Unassigned|{value}}&

Edit User:

**action**={edit}&  
**login**={login}&

Permissions Info (Add or Edit User):

**asset\_groups**={value,value...}&

**Notes:** 1) “asset\_groups” applies only to Scanner, Reader and Contact.

General Info (Add or Edit User):

**first\_name**={value}&  
**last\_name**={value}&  
**title**={value}&  
**phone**={value}&  
**fax**={value}&  
**email**={value}&  
**address1**={value}&  
**address2**={value}&  
**city**={value}&  
**country**={value}&  
**state**={value}&  
**zip\_code**={value}&  
**external\_id**={value}&  
**time\_zone\_code**={code or null to set to browser’s timezone}&

**Notes:** 1) Required contact info for add request in bold above. For edit request, all contact info is optional. 2) “state” is required for some country codes.

Activate/Deactivate Request:

```
action={activate|deactivate}&  
login={login}&
```

#### **user\_list.php? (GET + POST)**

```
external_id_contains={string}&  
external_id_assigned={0|1}&
```

#### **action\_log\_report.php? (GET POST)**

```
date_from={date/time}&  
date_to={date/time}&  
user_login={login}&
```

#### **password\_change.php? (GET POST)**

```
user_logins={login,login...|all}&  
email={0|1}&
```

## Activity Log v2

(/api/2.0/fo/activity\_log/)

#### **Export user activity log (GET + POST)**

```
action={list}&  
user_action={value}&  
action_details={user_logged in|user_logged  
out}&  
username={value}&  
user_role={Manager|Unit  
Manager|Auditor|Scanner|Reader|KnowledgeB  
ase Only|Remediation User|Contact}&  
since_datetime={YYYY-MM-DD HH:ii:ss}&  
until_datetime={YYYY-MM-DD HH:ii:ss}&  
output_format=CSV  
truncation_limit={value}&
```

## Activity Log v1

#### **action\_log\_report.php Function**

(/msp/action\_log\_report.php)

```
action={list}&  
date_from={YYYY-MM-DD HH:ii:ss}  
date_to={YYYY-MM-DD HH:ii:ss}  
user_login={value}
```

# Cloud Agent API

Use these API calls to manage, activate, and configure your cloud agents.

[Agent Management](#) | [Activation Key](#) | [Configuration Profile](#)

Looking for more information?

[Qualys Cloud Agent API User Guide](#)

## Agent Management

### Current agent count

/qps/rest/2.0/count/am/hostasset (POST)

Filters (optional):

id (Long)  
name (String)  
created (Date)  
updated (Date)  
tagName (String) /Cloud Agent

**Notes:** To get a count of agents installed, nothing other than the filter tagName EQUALS Cloud Agent is recommended. The more filters added to the request will result in a more refined count.

### List agents

/qps/rest/2.0/search/am/hostasset (POST)

Required:

tagName (String) /Cloud Agent

Optional:

[Click here](#) for AM and Tagging API User Guide

### Activate a single agent

/qps/rest/2.0/activate/am/asset/<id>?module=<value>,<value>(POST)

\*see module parameter values

### Activate agents in bulk

/qps/rest/2.0/activate/am/asset?module=<value>,<value> (POST)

\*see module parameter values

Filters (optional):

id (Long)  
name (String)  
created (Date)  
updated (Date)  
tagName (String) /Cloud Agent

**Notes:** To activate all agents installed, nothing other than the filter tagName EQUALS Cloud Agent is recommended. The more filters added to the request we'll activate a more refined list of agents.

### Deactivate a single agent

/qps/rest/2.0/deactivate/am/asset/<id>?module=<value>,<value> (POST)

\*see module parameter values

### Deactivate agents in bulk

/qps/rest/2.0/deactivate/am/asset?module=<value>,<value> (POST)

\*see module parameter values

Filters (optional):

id (Long)  
name (String)  
created (Date)  
updated (Date)  
tagName (String) /Cloud Agent

**Notes:** To deactivate all agents installed, nothing other than the filter tagName EQUALS Cloud Agent is recommended. The more filters added to the request we'll deactivate a more refined list of agents.

### \*module parameter values

These values are supported:

AGENT\_VM - for VM module

AGENT\_PC - for PC module

AGENT\_FIM - for FIM module

AGENT\_IOC - for IOC module



## Uninstall a single agent

/qps/rest/2.0/uninstall/am/asset/<id> (POST)

## Uninstall agents in bulk

/qps/rest/2.0/uninstall/am/asset (POST)

### Filters (optional):

id (Long)  
name (String)  
created (Date)  
updated (Date)  
tagName (String) /Cloud Agent

**Notes:** The use of NOT EQUALS operator is not supported during agent uninstall. This is to avoid unintended consequences of Tags and Assets being deleted or updated.

## Activation Key

### Get a single activation key

/qps/rest/1.0/get/ca/agentactkey/<id> (GET)

### Search activation keys

/qps/rest/1.0/search/ca/agentactkey/ (POST)

### Filters (optional):

type (string)  
countPurchased (Integer)  
expireDate (Date)  
modules (string)  
tags (string)  
isDisabled (boolean)

### Create an activation key

/qps/rest/1.0/create/ca/agentactkey/ (POST)

### Filters (optional):

type (string)  
countPurchased (Integer)  
expireDate (Date)  
modules (string)  
tags (string)

### Delete an activation key

/qps/rest/1.0/delete/ca/agentactkey/<id> (POST)

## Update an activation key

/qps/rest/1.0/update/ca/agentactkey/<id> (POST)

### Filters (optional):

id (Integer)  
type (string)  
countPurchased (Integer)  
expireDate (Date)  
modules (string)  
tags (string)  
isDisabled (boolean)  
applyOnAgents (boolean)

## Configuration Profile

### Get a single configuration profile

/qps/rest/1.0/get/ca/agentconfig/<id> (GET)

### Search configuration profiles

/qps/rest/1.0/search/ca/agentconfig/ (POST)

### Filters (optional):

name (string)  
id (Integer)

### Create a configuration profile

/qps/rest/1.0/create/ca/agentconfig/ (POST)

### Filters (optional):

name (string)  
description (string)  
priority (Integer)  
isDefault (Integer)  
suspendScanning (boolean)  
tags (string)  
blackoutConfig (string)  
performanceProfile (string)  
id (Integer)

### Delete a configuration profile

/qps/rest/1.0/delete/ca/agentconfig/<id> (POST)

## Update a configuration profile

/qps/rest/1.0/update/ca/agentconfig/ (POST)

Filters (optional):

name (string)

description (string)

priority (Integer)

isDefault (Integer)

suspendScanning (boolean)

tags (string)

blackoutConfig (string)

performanceProfile (string)

id (Integer)

# Asset Management & Tagging API

Use these API calls to manage assets, tags and access to your assets.

[Networks](#) | [Assets](#) | [Asset Groups](#) | [Tag](#) | [Host Asset](#) | [Asset](#) | [Host Instance Vulnerability](#) | [Asset Data Connector](#) | [Asset Data Connector](#) | [AWS Asset Data Connector](#) | [AWS Authentication Record](#)

Looking for more information?

[Qualys API \(VM, PC\) User Guide](#)

[Qualys API \(VM, PC\) XML/DTD Reference](#)

[Qualys Asset Management & Tagging API User Guide](#)

## Networks

/api/2.0/fo/network/

### Network List: (GET + POST)

```
action={list}&
echo_request={Q|1}&
ids={id1,id2...}&
```

### Network: (POST)

```
action={create|update}&
name={value}&
echo_request={Q|1}&
```

## Assets

### IP Assets

/api/2.0/fo/asset/ip/

### List IPs: (GET + POST)

```
action={list}&
echo_request={Q|1}&
ips={ip,range...}&
tracking_method={IP|DNS|NETBIOS}&
compliance_enabled={0|1}&
network_id={id}&
certview_enabled={Q|1}
```

### Add IPs: (POST)

```
action={add}&
echo_request={Q|1}&
ips={value} -or- {POSTed CVS raw data}&
```

```
tracking_method={value}&
enable_vm={0|1}&
enable_pc={0|1}&
owner={value}&
ud1 | ud2 | ud3={value}&
comment={value}&
ag_title={value}&
```

### Update IPs: (POST)

```
action={update}&
echo_request={Q|1}&
ips={value} -or- {POSTed CVS raw data}&
network_id={value}&
tracking_method={value}&
host_dns={name} -or- host_netbios={name}&
owner={value}&
ud1={value}&
ud2={value}&
ud3={value}&
comment={value}&
```

## Host Assets

/api/2.0/fo/asset/host/

### Host List: (GET + POST)

```
action={list}&
echo_request={Q|1}&
details={Basic|Basic/AGs|All|All/AGs|None}&
show_asset_id={Q|1}&
ips={ip,range...}&
ipv6={ip,range...}&
ids={id,range...}&
ag_ids={value,value...}&
ag_titles={value,value...}&
id_min={id}&
id_max={id}&
no_vm_scan_since={date/time}&
vm_scan_since={date/time}&
no_compliance_scan_since={date/time}&
compliance_scan_since={date/time}&
vm_processed_before={date}&
vm_processed_after={date}&
vm_scan_date_before={date}&
vm_scan_date_after={date}&
vm_auth_scan_date_before={date}&
vm_auth_scan_date_after={date}&
compliance_enabled={0|1}&
os_pattern={PCRE regex}&
use_tags={0|1}&
```

```
tag_set_by={id|name}&  
tag_include_selector={all|any}&  
tag_exclude_selector={all|any}&  
tag_set_include={value}&  
tag_set_exclude={value}&  
show_tags={0|1}&  
truncation_limit={value}&  
network_ids={id1,id2...}&  
host_metadata={all|ec2|google|azure}&  
host_metadata_fields={value1,value2}&  
show_cloud_tags={0|1}&  
cloud_tag_fields={value}&  
show_ars={0|1}&  
ars_min={value}&  
ars_max={value}&  
show_ars_factors={0|1}&  
show_trurisk={0|1}&  
trurisk_min={value}&  
trurisk_max={value}&  
show_trurisk_factors={0|1}&
```

#### Host Update: (POST)

```
action={update}&  
echo_request={0|1}&  
ips={ip,range...}&  
ids={value}&  
ag_ids={value,value...}&  
ag_titles={value,value...}&  
network_id={value}&  
network_name={value}&  
tracking_method={value}&  
host_dns={value}&  
host_netbios={value}&  
new_tracking_method={value}&  
new_owner={value}&  
new_ud1={value}&  
new_ud2={value}&  
new_ud3={value}&  
new_comment={value}&
```

#### Purge Hosts: (POST)

```
action={purge}&  
echo_request={0|1}&  
*ips={ip,range...}&  
*ids={id,range...}&  
*ag_ids={value,value...}&  
*ag_titles={value,value...}&  
no_vm_scan_since={date/time}&
```

```
no_compliance_scan_since={date/time}&  
data_scope={vm|pc|vm,pc}&  
compliance_enabled={0|1}&  
os_pattern={PCRE regex}&  
network_ids={id1,id2...}&
```

**Notes:** If `compliance_enabled=1` is specified in the same request as `data_scope`, then vulnerability and compliance data will both be purged regardless of the `data_scope` value.

#### Patch List: (GET)

```
host_id={value}&  
output_format={xml}&
```

#### Host Detection Assets

/api/2.0/fo/asset/host/vm/detection/

#### Host Detection List: (GET + POST)

```
action={list}&  
echo_request={0|1}&  
show_asset_id={0|1}&  
ids={id,range...}&  
id_min={id}&  
id_max={id}&  
ips={ip,range...}&  
ipv6={ip,range...}&  
include_vuln_type={confirmed|potential}&  
ag_ids={value,value...}&  
ag_titles={value,value...}&  
use_tags={0|1}&  
tag_set_by={id|name}&  
tag_include_selector={all|any}&  
tag_exclude_selector={all|any}&  
tag_set_include={value}&  
tag_set_exclude={value}&  
show_tags={0|1}&  
vm_scan_since={date/time}&  
no_vm_scan_since={date/time}&  
max_days_since_last_vm_scan={date|time}&  
compliance_enabled={0|1}&  
os_pattern={PCRE regex}&  
qids={value}&  
severities={value}&  
show_igs={0|1}&  
show_results={0|1}&  
show_reopened_info={0|1}&  
output_format={XML|CSV}
```

```
CSV_NO_METADATA|CSV_NO_METADATA_
MS_EXCEL|CSV_MS_EXCEL}&
suppress_duplicated_data_from_csv={0|1}&
truncation_limit={value}&
status={New,Active,Re-Opened,Fixed}&
*include_search_list_titles={value}&
*exclude_search_list_titles={value}&
*include_search_list_ids={value}&
*exclude_search_list_ids={value}&
active_kernels_only={0|1|2|3}&
network_ids={id1,id2...}&
detection_processed_before={date}&
detection_processed_after={date}&
detection_updated_before={date}&
detection_updated_since={date}&
max_days_since_detection_updated={value}&
detection_last_tested_since={date}&
detection_last_tested_since_days={value}&
detection_last_tested_before={date}&
detection_last_tested_before_days={value}&
host_metadata={all|ec2|google|azure}&
host_metadata_fields={value1,value2}&
show_cloud_tags={Q|1}&
cloud_tag_fields={value}&
filter_superseded_qids={Q|1}&
show_qds={Q|1}&
qds_min={value}&
qds_max={value}&
show_qds_factors={Q|1}&
```

**Notes:** 1) \*include/exclude cannot be specified with “qids” or “severities” in same request. Search list titles and IDs cannot be included/excluded in the same request. “show\_igs” is required if included search lists contain only Information Gathered.

2) A request with “max\_days\_since\_vm\_scan” cannot also include “vm\_scan\_since” or “no\_vm\_scan\_since”.

3) A request with “max\_days\_since\_detection\_updated” cannot also include “detected\_updated\_since”.

## Excluded Hosts

### Excluded Hosts List: (GET + POST)

/api/2.0/fo/asset/excluded\_ip/

```
action={list}&
```

```
echo_request={Q|1}&
ips={ip,range...}&
network_id={id}&
```

Filter by asset groups:

```
ag_ids={value}&
ag_titles={value}&
```

**Notes:** “ag\_ids” and “ag\_titles” are mutually exclusive and cannot be specified together.

Filter by asset tags:

```
use_tags={Q|1}&
tag_include_selector={any|all} &
tag_exclude_selector={any|all}&
tag_set_by={id|name}&
tag_set_include={value}&
tag_set_exclude={value}&
```

**Notes:** “use\_tags=1” must be specified with other tag filter parameters.

### Excluded Hosts Change History: (GET + POST)

/api/2.0/fo/asset/excluded\_ip/history/

```
action={list}&
echo_request={Q|1}&
ips={ip,range...}&
ids={id,range...}&
id_min={id}&
id_max={id}&
network_id={id}&
```

### Manage Excluded Hosts: (POST)

/api/2.0/fo/asset/excluded\_ip/

```
action={add|remove|remove_all}&
echo_request={Q|1}&
ips={ip,range...}&
comment={value}&
expiry_days={value}& (for action=add)
dg_names={value}& (for action=add)
network_id={value}&
```

**Notes:** “ips” is invalid for “remove\_all”.

## Virtual Host Assets

/api/2.0/fo/asset/vhost/

### Virtual Host List: (GET + POST)

```
action={list}&
echo_request={0|1}&
ip={ip}&
port={port}&
```

### Virtual Host: (POST)

```
action={create|update|delete|add_fqdn|
delete_fqdn}&
echo_request={0|1}&
ip={ip}&
port={port}&
fqdn={fqdn}&
```

**Notes:** “fqdn” is invalid for “delete\_fqdn”.

### IPv6 Host Assets

/api/2.0/fo/asset/ip/v4\_v6/

### IPv6 Mapping Records List: (GET + POST)

```
action={list}&
echo_request={0|1}&
id_min={id}&
id_max={id}&
ipv4_filter={value}&
ipv6_network={value}&
output_format={csv|xml}&
truncation_limit={value}&
```

**Notes:** Subscription authorization is required.

### Add IPv6 Mapping Records: (POST)

```
action={add}&
echo_request={0|1}&
csv_data={value}&
xml_data={value}&
all_or_nothing={0|1}&
```

**Notes:** Subscription authorization is required to use. “csv\_data” or “xml\_data” is required

### Remove IPv6 Mapping Records: (POST)

```
action={remove}&
echo_request={0|1}&
csv_data={value}&
xml_data={value}&
```

**Notes:** Subscription authorization is required to use. “csv\_data” or “xml\_data” is required

### Restricted IPs

/api/2.0/fo/setup/restricted\_ips/

### Manage Restricted IPs: (GET + POST)

```
action={list|activate|add|delete|replace|clear}
&
echo_request={0|1}&
enable={0|1}&
ips={value} or CSV raw data upload&
output_format={CSV|XML}
```

### Asset Data

#### asset\_data\_report.php? (GET)

```
template_title={value}&
template_id={value}&
```

**Notes:** one parameter is required

#### asset\_range\_info.php? (GET)

```
target_ips={ip,range...}&
target_asset_groups={value,value...}&
```

**Notes:** one or both parameters is required

#### get\_host\_info.php? (GET)

```
host_ip={ip}&
host_dns={hostname}&
host_netbios={hostname}&
vuln_severity={1,2,3,4,5|all|none}&
potential_vuln_severity={1,2,3,4,5|all|none}&
ig_severity={1,2,3,4,5|all|none}&
general_info={0|1}&
vuln_details={0|1}&
ticket_details={0|1}&
```

**Notes:** One of these parameters is required: host\_ip or host\_dns or host\_netbios

### Asset Groups

/api/2.0/fo/asset/group/

### Asset Group List: (GET + POST)

```
action={list}&
echo_request={0|1}&
ids={id,id,id...}&
id_min={id}&
id_max={id}&
```

```
truncation_limit={value}&
network_ids={id,id.id...}&
unit_id={value}&
user_id={value}&
show_attributes={None or All or a comma-
separated list of: TITLE, OWNER,
OWNER_USER_NAME, NETWORK_IDS,
LAST_UPDATE, IP_SET, APPLIANCE_LIST,
DOMAIN_LIST, DNS_LIST, NETBIOS_LIST,
EC2_ID_LIST, HOST_IDS, USER_IDS, UNIT_IDS,
BUSINESS_IMPACT, CVSS, COMMENTS}
```

### Add Asset Group: (POST)

```
action={add}&
echo_request={Q|1}&
title={value}&
network_id={value}&
comments={value}&
division={value}&
location={value}&
function={value}&
business_impact={critical|high|medium|low|
none}&
ips={value}&
appliance_ids={value}&
default_appliance_id={value}&
domains={value}&
dns_names={value}&
netbios_names={value}&
cvss_enviro_cdp={high|medium-high|low-
medium|low|none}&
cvss_enviro_td={high|medium|low|none}&
cvss_enviro_cr={high|medium|low}&
cvss_enviro_ir={high|medium|low}&
cvss_enviro_ar={high|medium|low}&
```

### Edit/Delete Asset Group: (POST)

```
action={edit}&
echo_request={Q|1}&
id={value}&
{Edit only parameters below}
set_title={value}&
set_comments={value}&
set_division={value}&
set_location={value}&
set_function={value}&
set_business_impact={critical|high|medium|lo
w
|none }&
add|remove|set_ips={value}&
```

```
add|remove|set_appliance_ids={value}&
set_default_appliance_id={value}&
add|remove|set_domains={value}&
add|remove|set_dns_names={value}&
add|remove|set_netbios_names={value}&
set_cvss_enviro_cdp={high|medium-high|low-
medium|low|none}&
set_cvss_enviro_td={high|medium|low|none}
&
set_cvss_enviro_cr={high|medium|low}&
set_cvss_enviro_ir={high|medium|low}&
set_cvss_enviro_ar={high|medium|low}&
```

## Tag

### Get details on a tag

/qps/rest/2.0/get/am/tag<id> (GET + POST)

Required:  
id (long)

### Create a tag

/qps/rest/2.0/create/am/tag (POST)

### Update a tag

/qps/rest/2.0/update/am/tag/<id> (POST)

/qps/rest/2.0/update/am/tag (POST)

### Search tags

/qps/rest/2.0/search/am/tag (POST)

Filters:  
id (Long)  
name (string)  
parent (long)  
ruleType (STATIC, GROOVY, OS\_REGEX,  
NETWORK\_RANGE, NAME\_CONTAINS,  
INSTALLED\_SOFTWARE, OPEN\_PORTS,  
VULN\_EXIST, ASSET\_SEARCH)  
color (string formatted as #FFFFFF where F  
can be any value between 0-9 and A-F)

### Count tags

/qps/rest/2.0/count/am/tag (POST)

## Delete tag

/qps/rest/2.0/delete/am/tag/<id> (POST)

/qps/rest/2.0/delete/am/tag (POST)

## Evaluate tag

/qps/rest/2.0/evaluate/am/tag/<id> (POST)

/qps/rest/2.0/evaluate/am/tag (POST)

## List users with their tags

### Get details on a user

/qps/rest/2.0/get/admin/user/<id> (GET + POST)

Required:  
id (long)

### Search users

/qps/rest/1.0/search/admin/user (GET + POST)

### Count users

/qps/rest/2.0/count/admin/user (POST)

## Host Asset

### Get details on a host asset

/qps/rest/2.0/get/am/hostasset/<id> (GET + POST)

Required:  
id (long)

### Create a host asset

/qps/rest/2.0/create/am/hostasset (POST)

### Update host asset

/qps/rest/2.0/update/am/hostasset/<id> (POST)

/qps/rest/2.0/update/am/hostasset (POST)

### Search host assets

/qps/rest/2.0/search/am/hostasset (POST)

Filters:  
qwebHostId (long)

lastVulnScan (date)  
lastComplianceScan (date)  
informationGatheredUpdated (date)  
os (string)  
dnsHostName (string)  
netbiosName (string)  
netbiosNetworkID (string)  
networkGuid (string)  
trackingMethod (AssetTrackingMethod)  
port (integer)  
installedSoftware (string)

### Count host assets

/qps/rest/2.0/count/am/hostasset (GET + POST)

### Delete host asset

/qps/rest/2.0/delete/am/hostasset/<id> (POST)

/qps/rest/2.0/delete/am/hostasset/ (POST)

### Activate host asset

/qps/rest/2.0/activate/am/hostasset/<id>?module=QWEB\_VM (POST)

/qps/rest/2.0/activate/am/hostasset?module=QWEB\_VM (POST)

/qps/rest/2.0/activate/am/hostasset/<id>?module=QWEB\_PC (POST)

/qps/rest/2.0/activate/am/hostasset?module=QWEB\_PC (POST)

## Asset

### Get details on an asset

/qps/rest/2.0/get/am/asset/<id> (GET + POST)

Required:  
id (long)

### Update asset

/qps/rest/2.0/update/am/asset/<id> (POST)

/qps/rest/2.0/update/am/asset (POST)

### Search assets

/qps/rest/2.0/search/am/asset (POST)



Filters:  
id (long)  
name (string)  
created (date)  
updated (date)  
type (UNKNOWN, HOST, SCANNER, WEBAPP, MALWARE\_DOMAIN)  
tagName (string)  
tagId (string)

## Count assets

/qps/rest/2.0/count/am/asset (POST)

## Delete asset

/qps/rest/2.0/delete/am/asset/<id> (POST)

/qps/rest/2.0/delete/am/asset (POST)

## Activate asset

/qps/rest/2.0/activate/am/asset/<id>?module=QWEB\_VM (POST)

/qps/rest/2.0/activate/am/asset?module=QWEB\_VM (POST)

/qps/rest/2.0/activate/am/asset/<id>?module=QWEB\_PC (POST)

/qps/rest/2.0/activate/am/asset?module=QWEB\_PC (POST)

## Host Instance Vulnerability

### Get details on a vulnerability

/qps/rest/2.0/get/am/hostinstancevuln/<id> (GET + POST)

Filter (optional):  
id (long)

### Search vulnerabilities

/qps/rest/2.0/search/am/hostinstancevuln (POST)

Filters (optional):  
id (long)  
name (string)  
parentTagId (long)

ruleType (STATIC, GROOVY, OS\_REGEX, NETWORK\_RANGE, NAME\_CONTAINS, INSTALLED\_SOFTWARE, OPEN\_PORTS, VULN\_EXIST, ASSET\_SEARCH)  
color (string formatted as #FFFFFF where F can be any value between 0-9 and A-F)

## Count vulnerabilities

/qps/rest/2.0/count/am/hostinstancevuln (POST)

## Asset Data Connector

### Get details on a connector

/qps/rest/2.0/get/am/assetdataconnector/<id> (GET + POST)

Filter (optional):  
id (Integer)

### Update connector

/qps/rest/2.0/update/am/assetdataconnector/<id> (POST)

/qps/rest/2.0/update/am/assetdataconnector (POST)

### Search connectors

/qps/rest/2.0/search/am/assetdataconnector (POST)

Filters:  
id (long)  
name (string)  
lastSync (date)  
lastError (date)  
connectorState (PENDING, RUNNING, SUCCESS or Error)  
activation (VM or PC)  
defaultTags.name (string)  
defaultTag (long)  
disabled (Boolean)

## Count connectors

/qps/rest/2.0/count/am/assetdataconnector (POST)

## Delete connector

/qps/rest/2.0/delete/am/assetdataconnector/id>  
(POST)

/qps/rest/2.0/delete/am/assetdataconnector  
(POST)

## Run connector

/qps/rest/2.0/run/am/assetdataconnector/<id>  
(POST)

/qps/rest/2.0/run/am/assetdataconnector/<id>  
(POST)

## AWS Asset Data Connector

### Get details on an AWS connector

/qps/rest/2.0/get/am/awsassetdataconnector/<id>  
(GET + POST)

Filter (optional):  
id (Integer)

### Create AWS connector

/qps/rest/2.0/create/am/awsassetdataconnector  
(POST)

Optional:  
isGovCloudConfigured (Boolean)

### Update AWS connector

/qps/rest/2.0/update/am/awsassetdataconnector/  
<id> (POST)

/qps/rest/2.0/update/am/awsassetdataconnector  
(POST)

Optional:  
isGovCloudConfigured (Boolean)

### Search AWS connectors

/qps/rest/2.0/search/am/awsassetdataconnector  
(POST)

Filters:  
id (long)  
name (string)  
lastSync (date)  
lastError (date)

connectorState (PENDING, RUNNING,  
SUCCESS or Error)  
activation (VM or PC)  
defaultTags.name (string)  
allRegions (Boolean)  
serviceType (AwsServiceType)  
endpoint.region (string)  
authRecord (long)  
authRecord.name (string)  
disabled (Boolean)

## Count AWS connectors

/qps/rest/2.0/count/am/awsassetdataconnector  
(POST)

## Delete AWS connector

/qps/rest/2.0/delete/am/awsassetdataconnector/i  
d> (POST)

/qps/rest/2.0/delete/am/awsassetdataconnector  
(POST)

## Run AWS connector

/qps/rest/2.0/run/am/awsassetdataconnector/<id  
> (POST)

/qps/rest/2.0/run/am/awsassetdataconnector/<id  
> (POST)

## AWS Authentication Record

### Get details on AWS record

/qps/rest/2.0/get/am/awsauthrecord/<id>  
(GET + POST)

Filter (optional):  
id (Integer)

### Create AWS record

/qps/rest/2.0/create/am/awsauthrecord (POST)

### Update AWS record

/qps/rest/2.0/update/am/awsauthrecord/<id>  
(POST)

/qps/rest/2.0/update/am/awsauthrecord (POST)

## Search AWS records

/qps/rest/2.0/search/am/awsauthrecord (POST)

Filters:

id (long)

name (string)

description (string)

created (date)

modified (date)

## Count AWS records

/qps/rest/2.0/count/am/awsauthrecord (POST)

## Delete AWS record

/qps/rest/2.0/delete/am/awsauthrecord/id>  
(POST)

/qps/rest/2.0/delete/am/awsauthrecord (POST)

# Continuous Monitoring API

Use these API calls to manage alerts, profiles, rule sets, and rules to monitor your assets.

[Alerts](#) | [Profiles](#) | [Rulesets](#) | [Rules](#)

Looking for more information?

[Qualys Continuous Monitoring API User Guide](#)

## Alerts

### Search alerts

/qps/rest/1.0/search/cm/alert (POST)

Filters (optional):

id (Integer)  
eventType (HOST\_FOUND, HOST\_UPDATED, HOST\_PURGED, PORT\_OPEN, PORT\_CHANGED, PORT\_CLOSED, SOFTWARE\_ADDED, SOFTWARE\_REMOVED, SSL\_NEW, SSL\_EXPIRED, SSL\_EXPIRY, TICKET\_OPEN, TICKET\_RESOLVED, TICKET\_CLOSED, VULN\_OPEN, VULN\_CLOSED, VULN\_REOPENED, VULN\_ACTIVE, VULN\_PREDICTION\_ADDED, VULN\_PREDICTION\_CHANGED, VULN\_PREDICTION\_CLOSED)  
ipAddress (Text)  
hostname (Text)  
isHidden (Boolean)  
eventDate (Date)  
alertDate (Date)  
profileTitle (Text)

### View details on an alert

/qps/rest/1.0/get/cm/alert/<id> (GET, POST)

Required:

id (Integer) /alert ID

### Download alerts

/qps/rest/1.0/download/cm/alert (POST)

Required:

format (csv|cef)

Filters (optional):

id (Integer)  
eventType (Keyword - see Search above)  
ipAddress (Text)  
hostname (Text)  
isHidden (Boolean)  
eventDate (Date)  
alertDate (Date)  
profileTitle (Text)

## Profiles

### Search profiles

/qps/rest/1.0/search/cm/profile (POST)

Filters (optional):

id (Integer)  
title (Text)  
uuid (Integer)  
frequency (FREQ\_NEVER, FREQ\_5\_MINUTES, FREQ\_20\_MINUTES, FREQ\_1\_HR, FREQ\_2\_HRS, FREQ\_6\_HRS, FREQ\_12\_HRS, FREQ\_WEEKLY, FREQ\_DAILY)  
isActive (Boolean)  
ruleSetTitle (Text)

### View details on an profile

/qps/rest/1.0/get/cm/profile/<id> (GET, POST)

Required:

id (Integer) /profile ID

## Rulesets

### Search rulesets

/qps/rest/1.0/search/cm/ruleset (POST)

Filters (optional):

id (Integer)  
title (Text)  
description (Text)  
dateCreated (Date)  
dateUpdated (Date)

### View details on a ruleset

/qps/rest/1.0/get/cm/ruleset/<id> (GET, POST)

Required:

id (Integer) /ruleset ID

## Rules

### Search rules

/qps/rest/1.0/search/cm/rule (POST)

Filters (optional):

id (Integer)

ruleType (HOST, VULN, PORT, SSL, SW)

### View details on a rule

/qps/rest/1.0/get/cm/rule/<id> (POST)

Required:

id (Integer) /rule ID

# Web Application Scanning API

Use these API calls to scan and report on web applications.

[Web Application](#) | [Authentication](#) | [Scan](#) | [Schedule](#) | [Option Profile](#) | [Report](#) | [Report Creation](#) | [Findings](#) | [Burp](#)

Looking for more information?

[Qualys Web Application Scanning API User Guide](#)

## Web Application

### Current web application count

/qps/rest/3.0/count/was/webapp (GET + POST)

Filters (optional):

id (Integer)  
name (Text)  
url (Text)  
tags.name (Text)  
tags.id (Integer)  
createdDate (Date)  
updatedDate (Date)  
isScheduled (Boolean)  
isScanned (Boolean)  
lastScan.status (SUBMITTED, RUNNING, FINISHED, CANCELED, ERROR)  
lastScan.date (Date)

### Search web applications

/qps/rest/3.0/search/was/webapp (POST)

Filters (optional):

id (Integer)  
name (Text)  
url (Text)  
tags.name (Text)  
tags.id (Integer)  
createdDate (Date)  
updatedDate (Date)  
isScheduled (Boolean)  
isScanned Boolean)  
lastScan.date (Date)  
lastScan.status (SUBMITTED, RUNNING, FINISHED, CANCELED, ERROR)

### Get details for a web application

/qps/rest/3.0/get/was/webapp/<id> (GET)

Required:

id (Integer) /web application ID

### Create a web application

/qps/rest/3.0/create/was/webapp (POST)

Required:

name (Text)

url (Text)

Optional:

[Click here](#) for WAS API User Guide

### Update a web application

/qps/rest/3.0/update/was/webapp/<id> (POST)

Required:

id (Integer)

Optional:

[Click here](#) for WAS API User Guide

### Delete web applications

/qps/rest/3.0/delete/was/webapp/<id> (POST)

/qps/rest/3.0/delete/was/webapp/<filters> (POST)

Required:

id (Integer) /web application ID

Filters (optional):

name (Text)

url (Text)

tags.name (Text)

tags.id (Integer)

createdDate (Date)

updatedDate (Date)

isScheduled (Boolean)

isScanned (Boolean)

lastScan.status (SUBMITTED, RUNNING, FINISHED, CANCELED, ERROR)

lastScan.date (Date)

### Purge web applications

/qps/rest/3.0/purge/was/webapp/<id> (POST)

/qps/rest/3.0/purge/was/webapp/<filters> (POST)

Required:

id (Integer) /web application ID

Filters (optional):  
name (Text)  
url (Text)  
tags.name (Text)  
tags.id (Integer)  
createdDate (Date)  
updatedDate (Date)  
isScheduled (Boolean)  
isScanned (Boolean)  
lastScan.status (SUBMITTED, RUNNING,  
FINISHED, CANCELED, ERROR)  
lastScan.date (Date)

## Authentication

### Current authentication record count

/qps/rest/3.0/count/was/webappauthrecord  
(POST + GET)

Filters (optional):  
id (Integer)  
name (Text)  
tags (Integer)  
tags.id (Integer)  
tags.name (Text)  
createdDate (Date)  
updatedDate (Date)  
lastScan.date (Date)  
lastScan.authStatus (NOT\_USED,  
SUCCESSFUL, FAILED, PARTIAL)  
isUsed (Boolean)  
contents (FORM\_STANDARD,  
FORM\_CUSTOM, FORM\_SELENIUM,  
SERVER\_BASIC, SERVER\_DIGEST)

### Search authentication records

/qps/rest/3.0/search/was/webappauthrecord  
(POST)

Filters (optional):  
id (Integer)  
name (Text)  
tags (Integer)  
tags.id (Integer)  
tags.name (Text)  
createdDate (Date)  
updatedDate (Date)  
lastScan.date (Date)

lastScan.authStatus (NOT\_USED,  
SUCCESSFUL, FAILED, PARTIAL)  
isUsed (Boolean)  
contents (FORM\_STANDARD,  
FORM\_CUSTOM, FORM\_SELENIUM,  
SERVER\_BASIC, SERVER\_DIGEST)

### Get details for an authentication record

/qps/rest/3.0/get/was/webappauthrecord/<id>  
(GET)

Required:  
id (Integer) /Authentication record ID

### Create a new authentication record

/qps/rest/3.0/create/was/webappauthrecord  
(POST)

Required:  
name (Text)  
WebAuthRecord (Text)

Optional:  
tags  
comments

### Update an authentication record

/qps/rest/3.0/update/was/webappauthrecord/<id>  
(POST)

Required:  
id (Integer) /Authentication record ID

### Delete authentication records

/qps/rest/3.0/delete/was/webappauthrecord/<id>  
(POST)  
/qps/rest/3.0/delete/was/webappauthrecord  
(POST)

Filters (optional):  
id (Integer)  
name (Text)  
tags  
createdDate (Date)  
updatedDate (Date)  
lastScan.date (Date)  
lastScan.authStatus (Text)  
isUsed (Boolean)  
contents

## Scan

### Current scan count

/qps/rest/3.0/count/was/wasscan (POST + GET)

Filters (optional):

id (Integer)  
name (Text)  
webApp.name (Text)  
webApp.id (Integer)  
webApp.tags (with operator="NONE")  
webApp.tags.id (Integer)  
reference (Text)  
launchedDate (Date)  
type (DISCOVERY, VULNERABILITY)  
mode (MANUAL, SCHEDULED, API)  
status (SUBMITTED, RUNNING, FINISHED, ERROR, CANCELED)  
authStatus (NONE, NOT\_USED, SUCCESSFUL, FAILED, PARTIAL)  
resultsStatus (NOT\_USED, NO\_HOST\_ALIVE, NO\_WEB\_SERVICE, PROCESSING, SCAN\_RESULTS\_INVALID, TIME\_LIMIT\_REACHED, SERVICE\_ERROR, SCAN\_INTERNAL\_ERROR, SUCCESSFUL, TO\_BE\_PROCESSED)

### Search scans

/qps/rest/3.0/search/was/wasscan (POST)

Filters (optional):

id (Integer)  
name (Text)  
webApp.name (Text)  
webApp.id (Integer)  
webApp.tags (with operator="NONE")  
webApp.tags.id (Integer)  
reference (Text)  
launchedDate (Date)  
type (DISCOVERY, VULNERABILITY)  
mode (MANUAL, SCHEDULED, API)  
status (SUBMITTED, RUNNING, FINISHED, ERROR, CANCELED)  
authStatus (NONE, NOT\_USED, SUCCESSFUL, FAILED, PARTIAL)

resultsStatus (NOT\_USED, NO\_HOST\_ALIVE, NO\_WEB\_SERVICE, PROCESSING, SCAN\_RESULTS\_INVALID, TIME\_LIMIT\_REACHED, SERVICE\_ERROR, SCAN\_INTERNAL\_ERROR, SUCCESSFUL, TO\_BE\_PROCESSED)

### Get scan details

/qps/rest/3.0/get/was/wasscan/<id> (GET)

Required:

id (Integer) /Scan ID

### Launch a new scan (single web application)

/qps/rest/3.0/launch/was/wasscan (POST)

Required:

name (Text)  
target.webApp.id (Integer)  
type (DISCOVERY, VULNERABILITY)  
profile.id (Integer) \*

Optional:

target.scannerAppliance.type (EXTERNAL, INTERNAL, scannerTags)  
target.scannerAppliance.friendlyName (Text)  
target.webAppAuthRecord.id (Integer) - or -  
target.webAppAuthRecord.isDefault (Boolean)  
options  
proxy.id (Integer)  
dnsOverride.id (Integer)  
cancelOption set to DEFAULT - Forces the use of the target web app's cancelScans option if set, else fall back to the one passed in to the API while launching the scan  
cancelOption set to SPECIFIC - Always use the cancel scan option passed while launching the scan  
sendMail (Boolean)

[Click here](#) for WAS API User Guide

**Notes:** \* The element profile (Text) is required unless the target has a default option profile.



## Launch a new scan (multiple web application)

/qps/rest/3.0/launch/was/wasscan (POST)

### Required:

name (Text)  
target.webApps.id (Integer) or target.tags.id (Integer)  
target.tags.included.option (ALL or ANY)<sup>1</sup>  
target.tags.included.tagList.Tag.id (Integer)<sup>1</sup>  
type (DISCOVERY or VULNERABILITY)  
profile.id (Integer) \*

### Optional:

target.authRecordOption  
target.profileOption  
target.scannerOption  
target.randomizeScan  
[Click here](#) for WAS API User Guide

**Notes:** \* The element profile (Text) is required unless the target has a default option profile.

<sup>1</sup> The element target must have at least tags or web applications specified.

## Retrieve the status of a scan

/qps/rest/3.0/status/was/wasscan/<id> (GET)

### Required:

id (Integer) /Scan ID

## Retrieve the results of a scan

/qps/rest/3.0/download/was/wasscan/<id> (GET)

/qps/rest/2.0/download/was/wasscan/<id> (GET)

### Required:

id (Integer) /Scan ID

## Cancel an unfinished scan

/qps/rest/3.0/cancel/was/wasscan/<id> (POST)

### Required:

id (Integer) /Scan ID

## Delete an existing scan

/qps/rest/3.0/delete/was/wasscan/<id> (POST)

/qps/rest/3.0/delete/was/wasscan (POST)

### Filters (optional):

id (Integer)  
name (Text)  
webApp.name (Text)  
webApp.id (Integer)  
reference (Text)  
launchedDate (Date)  
type (DISCOVERY, VULNERABILITY)  
mode (MANUAL, SCHEDULED, API)  
status (SUBMITTED, RUNNING, FINISHED, ERROR, CANCELED)  
authStatus (NONE, NOT\_USED, SUCCESSFUL, FAILED, PARTIAL)  
resultsStatus (NOT\_USED, NO\_HOST\_ALIVE, NO\_WEB\_SERVICE, PROCESSING, SCAN\_RESULTS\_INVALID, TIME\_LIMIT\_REACHED, SERVICE\_ERROR, SCAN\_INTERNAL\_ERROR, SUCCESSFUL, TO\_BE\_PROCESSED)

## Schedule

### Current schedule count

/qps/rest/3.0/count/was/wasscanschedule (POST + GET)

### Filters (optional):

id (Integer)  
name (Text)  
owner.id (Text)  
createdDate (Date)  
updatedDate (Date)  
type (DISCOVERY, VULNERABILITY)  
webApp.name (Text)  
webApp.id (Integer)  
webApp.tags (with operator="NONE")  
webApp.tags.id (Integer)  
active (Boolean)  
invalid (Boolean)

## Search schedules

/qps/rest/3.0/search/was/wasscanschedule (POST)

Filters (optional):

id (Integer)  
name (Text)  
owner.id  
createdDate (Date)  
active (Boolean)  
type (DISCOVERY, VULNERABILITY)  
webApp.name (Text)  
webApp.id (Integer)  
webApp.tags (with operator="NONE")  
webApp.tags.id (Integer)  
updatedDate (Date)  
invalid (Boolean)  
lastScan (with operation="NONE")  
lastScan.launchedDate (Date)  
lastScan.status (SUBMITTED, RUNNING, FINISHED, ERROR, CANCELED)  
multi (Boolean)

## Get schedule details

/qps/rest/3.0/get/was/wasscanschedule/<id>  
(GET)

Required:

id (Integer) /Scan ID

## Create a schedule (single web application)

/qps/rest/3.0/create/was/wasscanschedule (POST)

Required:

name (Text)  
target.webApp.id (Integer)  
type (DISCOVERY, VULNERABILITY)  
profile.id (Integer)\*  
startDate (Date)  
timeZone (Text)  
occurrenceType (ONCE, DAILY, WEEKLY, MONTHLY)  
notification (Boolean)  
reschedule (Boolean)  
Optional:  
target.scannerAppliance.type (EXTERNAL, INTERNAL, scannerTags)  
target.scannerAppliance.friendlyName (Text)  
target.webAppAuthRecord.id (Integer) - or -

target.webAppAuthRecord.isDefault (Boolean)  
options  
proxy.id (Integer)  
dnsOverride.id (Integer)  
cancelOption set to DEFAULT - Forces the use of the target web app's cancelScans option if set, else fall back to the one passed in to the API while launching the scan  
cancelOption set to SPECIFIC - Always use the cancel scan option passed while launching the scan  
sendMail (Boolean)  
[Click here](#) for WAS API User Guide

**Notes:** \* The element profile (Text) is required unless the target has a default option profile.

## Create a schedule (multiple web application)

/qps/rest/3.0/create/was/wasscanschedule (POST)

Required:

name (Text)  
target.webApps.id (Integer) or target.tags.id (Integer)  
target.tags.included.option (ALL or ANY)  
target.tags.included.tagList.Tag.id (Integer)  
type (DISCOVERY, VULNERABILITY)  
profile.id (Integer)\*  
startDate (Date)  
timeZone (Text)  
occurrenceType (ONCE, DAILY, WEEKLY, MONTHLY)  
notification (Boolean)  
reschedule (Boolean)  
Optional:  
target.authRecordOption  
target.profileOption  
target.scannerOption  
target.randomizeScan  
target.authRecordOption  
target.scannerAppliance.type (EXTERNAL, INTERNAL, scannerTags)  
target.scannerAppliance.friendlyName (Text)  
cancelOption set to DEFAULT - Forces the use of the target web app's cancelScans option if set, else fall back to the one passed in to the API while launching the scan

cancelOption set to SPECIFIC - Always use the cancel scan option passed while launching the scan

sendMail (Boolean)

[Click here](#) for WAS API User Guide

**Notes:** \* The element profile (Text) is required unless the target has a default option profile.

## Update a schedule

/qps/rest/3.0/update/was/wasscanschedule/<id> (POST)

Required:

id (Integer) /Schedule ID

Optional:

[Click here](#) for WAS API User Guide

## Activate an existing schedule

/qps/rest/3.0/update/was/wasscanschedule/<id> (POST)

/qps/rest/3.0/activate/was/wasscanschedule/<filters> (POST)

Required:

id (Integer) /Schedule ID

Filters (optional):

name (Text)

webApp.id (Integer)

webApp.name (Text)

owner.id (Integer)

type (VULNERABILITY, DISCOVERY)

active (Boolean)

invalid (Boolean)

createdDate (Date)

updatedDate (Date)

## Deactivate an existing schedule

/qps/rest/3.0/update/was/wasscanschedule/<id> (POST)

/qps/rest/3.0/deactivate/was/wasscanschedule/<filters> (POST)

Required:

id (Integer) /Schedule ID

Filters (optional):

name (Text)

webApp.id (Integer)

webApp.name (Text)

owner.id (Integer)

type (VULNERABILITY, DISCOVERY)

active (Boolean)

invalid (Boolean)

createdDate (Date)

updatedDate (Date)

## Delete one or more existing schedules

/qps/rest/3.0/delete/was/wasscanschedule/<id> (POST)

/qps/rest/3.0/delete/was/wasscanschedule/<filters> (POST)

Required:

id (Integer) /Schedule ID

Filters (optional):

name (Text)

webApp.id (Integer)

webApp.name (Text)

owner.id (Integer)

type (VULNERABILITY, DISCOVERY)

active (Boolean)

invalid (Boolean)

createdDate (Date)

updatedDate (Date)

## Download one or more schedules to iCalendar

/qps/rest/3.0/download/was/wasscanschedule/<id> (POST)

/qps/rest/3.0/download/was/wasscanschedule/<filters> (POST)

Filters (optional):

name (Text)

owner.id (Integer)

createdDate (Date)

active (Boolean)

type (VULNERABILITY, DISCOVERY)

webApp.name (Text)

webApp.id (Integer)

updatedDate (Date)

invalid (Boolean)

## Option Profile

### Current option profile count

/qps/rest/3.0/count/was/optionprofile (POST + GET)

Filters (optional):

id (Integer)  
name (Text)  
tags  
tags.id (Integer)  
tags.name (Text)  
createdDate (Date)  
updatedAt (Date)  
usedByWebApps (Boolean with operator: EQUALS, NOT EQUALS)  
usedBySchedules (Boolean with operator: EQUALS, NOT EQUALS)  
owner.id (Long with operator: EQUALS, IN, NOT EQUALS, GREATER, LESSER)  
owner.name (text with operator: CONTAINS, EQUALS, NOT EQUALS)  
owner.username (text with operator: CONTAINS, EQUALS, NOT EQUALS)

### Search option profiles

/qps/rest/3.0/search/was/optionprofile (POST)

Filters (optional):

id (Integer)  
name (Text)  
tags  
tags.id (Integer)  
tags.name (Text)  
createdDate (Date)  
updatedAt (Date)  
usedByWebApps (Boolean with operator: EQUALS, NOT EQUALS)  
usedBySchedules (Boolean with operator: EQUALS, NOT EQUALS)  
owner.id (Long with operator: EQUALS, IN, NOT EQUALS, GREATER, LESSER)  
owner.name (text with operator: CONTAINS, EQUALS, NOT EQUALS)  
owner.username (text with operator: CONTAINS, EQUALS, NOT EQUALS)

### Get details for an option profile

/qps/rest/3.0/get/was/optionprofile/<id> (GET)

Required:

id (Integer) /Option profile ID

### Create a new option profile

/qps/rest/3.0/create/was/optionprofile (POST)

Required:

name (Text) /Option profile name

### Update an option profile

/qps/rest/3.0/update/was/optionprofile/<id> (POST)

Required:

id (Integer) /Option profile ID

### Delete an option profile

/qps/rest/3.0/delete/was/optionprofile/<id> (POST)

/qps/rest/3.0/delete/was/optionprofile (POST)

Optional:

name (Text)  
owner (Text)  
tags  
createdDate (Date)  
updatedAt (Date)  
usedByWebApps (Boolean)  
usedBySchedules (Boolean)

## Report

### Current report count

/qps/rest/3.0/count/was/report (GET, POST)

Filters (optional):

id (Integer)  
name (Text)  
tags.id (Integer)  
tags.name (Text)  
creationDate (Date)

type (WAS\_SCAN\_REPORT,  
WAS\_WEBAPP\_REPORT,  
WAS\_SCORECARD\_REPORT,  
WAS\_CATALOG\_REPORT,  
DATALIST\_REPORT)  
format (HTML\_ZIPPED, HTML\_BASE64, PDF,  
PDF\_ENCRYPTED, CSV, XML, POWERPOINT,  
WORD)  
status (RUNNING, ERROR, COMPLETE)

## Search reports

/qps/rest/3.0/search/was/report (POST)

### Filters (optional):

id (Integer)  
name (Text)  
tags.id (Integer)  
tags.name (Text)  
creationDate (Date)  
type (Keyword)  
format (Keyword)  
status (Keyword)

## Get details on a report

/qps/rest/3.0/get/was/report/<id> (GET, POST)

### Required:

id (Integer) /report ID

## Get report status

/qps/rest/3.0/status/was/report/<id> (GET, POST)

### Required:

id (Integer) /report ID

## Download a report

/qps/rest/3.0/download/was/report/<id> (GET,  
POST)

### Required:

id (Integer) /report ID

## Send an encrypted PDF report

/qps/rest/3.0/send/was/report/<id> (POST)

### Required:

id (Integer) /report ID  
distributionList (Text)

## Update a report

/qps/rest/3.0/update/was/report/<id> (POST)

### Required:

id (Integer) /report ID  
tags (Text)  
showPatched (applies to Web App Report,  
Scan Report only - SHOW\_BOTH (is default),  
SHOW\_ONLY, SHOW\_NONE)

## Delete one or more reports

/qps/rest/3.0/delete/was/report/<id> (POST)

/qps/rest/3.0/delete/was/report/<filters> (POST)

### Required:

id (Integer) /web application ID

### Filters (optional):

name (Text)  
tags.id (Integer)  
tags.name (Text)  
creationDate (Date)  
type (Keyword)  
format (Keyword)  
status (Keyword)

## Report Creation

### Report Creation Request

/qps/rest/3.0/create/was/report (POST)

name (Text)  
type (WAS\_SCAN\_REPORT,  
WAS\_WEBAPP\_REPORT,  
WAS\_SCORECARD\_REPORT,  
WAS\_CATALOG\_REPORT)  
format (HTML\_ZIPPED, HTML\_BASE64, PDF,  
PDF\_ENCRYPTED, CSV, XML, POWERPOINT)  
tags.id (Integer)  
tags.name (Text)  
password (Text)  
distributionList (\*)  
config (one and only one subelement is  
required: webAppReport, scanReport,  
catalogReport, scorecardReport)

**Notes:** (\*) indicates data type.

## Web Application Report

target.tags (Tag)  
target.tags.included.option (ALL or ANY)<sub>1</sub>  
target.tags.included.tagList.Tag.id (Integer)<sub>1</sub>  
target.webapps (WebApp)\*  
filters.searchlists (SearchList)\*  
filters.url (Text)  
filters.status (WebAppFindingStatus)\*  
filters.remediation\*  
showPatched (SHOW\_ONLY, SHOW\_NONE, SHOW\_BOTH - default)  
target.scannerTags.set.Tag.id (Integer)  
target.tags.excluded.option (ALL or ANY)  
target.tags.excluded.tagList.Tag.id (Integer)  
display.contents (WebAppReportContent)\*  
display.graphs (WebAppReportGraph)\*  
display.groups (WebAppReportGroup)\*  
display.options (rawLevels)\*

**Notes:** (\*) indicates data type.

**1** The element target must have at least tags or web applications specified.

## Scan Report

target.scans (WasScan)\*  
filters.searchlists (SearchList)\*  
filters.url (Text)  
filters.status (ScanFindingStatus)\*  
filters.remediation (\*)  
showPatched (SHOW\_ONLY, SHOW\_NONE, SHOW\_BOTH - default)  
display.contents (ScanAppReportContent)\*  
display.graphs (ScanAppReportGraph)\*  
display.groups (ScanAppReportGroup)\*  
display.options (rawLevels)\*

**Notes:** (\*) indicates data type.

## Scorecard Report

target.tags (Tag)\*  
target.tags.included.option (ALL or ANY)<sub>1</sub>  
target.tags.included.tagList.Tag.id (Integer)<sub>1</sub>  
filters.searchlists (SearchList)\*  
filters.scanDate (DatetimeRange)\*  
filters.scanStatus  
(WasScanConsolidatedStatus)\*  
filters.scanAuthStatus (WasScanAuthStatus)\*

target.scannerTags.set.Tag.id (Integer)  
target.tags.excluded.option (ALL or ANY)  
target.tags.excluded.tagList.Tag.id (Integer)  
display.contents (ScorecardReportContent)\*  
display.graphs (ScorecardReportGraph)\*  
display.groups (ScorecardReportGroup)\*  
display.options (rawLevels)\*

**Notes:** (\*) indicates data type.

**1** The element target must have at least tags or web applications specified

## Catalog Report

filters.scanDate (DatetimeRange)\*  
filters.url (Text)  
filters.ip (Text)  
filters.os (Text)  
filters.status (EntryStatus)\*  
display.contents (WebAppReportContent)\*  
display.graphs (WebAppReportGraph)\*  
display.groups (WebAppReportGroup)\*  
display.options (rawLevels)\*

**Notes:** (\*) indicates data type.

## Report Template Count

qps/rest/3.0/count/was/reporttemplate (POST)  
id (Integer)  
name (Text)  
type (Text)

## Search Report Template

qps/rest/3.0/search/was/reporttemplate (POST)  
id (Integer)  
name (Text)  
type (Text)

## Get details of Report Template

qps/rest/3.0/get/was/reporttemplate/<id> (GET)  
Required:  
id (Integer) /report template ID

## Findings

### Current finding count

/qps/rest/3.0/count/was/finding (POST)

Filters (optional):

id (Integer)  
qid (Integer)  
name (Text)  
type (VULNERABILITY, SENSITIVE\_CONTENT,  
or INFORMATION\_GATHERED)  
url (Text)  
webApp.tags.id (Integer)  
webApp.tags.name (Text)  
status (NEW, ACTIVE or REOPENED)  
patch (Integer-Long)  
webApp.id (Integer)  
webApp.name (Text)  
severity (Integer)  
externalRef (String)  
ignoredDate (Date)  
ignoredReason (FALSE\_POSITIVE,  
RISK\_ACCEPTED or NOT\_APPLICABLE)  
group (XSS, SQL, INFO, PATH, CC, SSN\_US or  
CUSTOM)  
owasp.name (Text)  
owasp.code (Integer)  
wasc.name (Text)  
wasc.code (Integer)  
cwe.id (Integer)  
firstDetectedDate (Date)  
lastDetectedDate (Date)  
lastTestedDate (Date)  
timesDetected (Integer)

### Search findings

/qps/rest/3.0/search/was/finding (POST)

Filters (optional):

id (Integer)  
qid (Integer)  
name (Text)  
type (VULNERABILITY, SENSITIVE\_CONTENT,  
or INFORMATION\_GATHERED)  
url (Text)  
webApp.tags.id (Integer)  
webApp.tags.name (Text)  
status (NEW, ACTIVE or REOPENED)  
patch (Integer-Long)

webApp.id (Integer)  
webApp.name (Text)  
severity (Integer)  
externalRef (String)  
ignoredDate (Date)  
ignoredReason (FALSE\_POSITIVE,  
RISK\_ACCEPTED or NOT\_APPLICABLE)  
group (Keyword: XSS, SQL, INFO, PATH, CC,  
SSN\_US or CUSTOM)  
owasp.name (Text)  
owasp.code (Integer)  
wasc.name (Text)  
wasc.code (Integer)  
cwe.id (Integer)  
firstDetectedDate (Date)  
lastDetectedDate (Date)  
lastTestedDate (Date)  
timesDetected (Integer)

### Get details on a finding

/qps/rest/3.0/get/was/finding/<id> (GET, POST)

Required:

id (Integer) /finding ID

### Ignore findings

/qps/rest/3.0/ignore/was/finding (POST)

Filters:

id (Integer)  
qid (Integer)  
name (Text)  
type (VULNERABILITY, SENSITIVE\_CONTENT,  
or INFORMATION\_GATHERED)  
url (Text)  
webApp.tags.id (Integer)  
webApp.tags.name (Text)  
status (NEW, ACTIVE or REOPENED)  
webApp.id (Integer)  
webApp.name (Text)  
severity (Integer)  
ignoredDate (Date)  
ignoredReason (FALSE\_POSITIVE,  
RISK\_ACCEPTED or NOT\_APPLICABLE)  
group (Keyword: XSS, SQL, INFO, PATH, CC,  
SSN\_US or CUSTOM)  
owasp.name (Text)  
owasp.code (Integer)  
wasc.name (Text)

wasc.code (Integer)  
cwe.id (Integer)  
firstDetectedDate (Date)  
lastDetectedDate (Date)  
lastTestedDate (Date)  
timesDetected (Integer)

## Activate findings

/qps/rest/3.0/activate/was/finding/<id> (POST)

/qps/rest/3.0/activate/was/finding/<findings>  
(POST)

### Filters:

id (Integer)  
qid (Integer)  
name (Text)  
type (VULNERABILITY, SENSITIVE\_CONTENT,  
or INFORMATION\_GATHERED)  
url (Text)  
webApp.tags.id (Integer)  
webApp.tags.name (Text)  
status (NEW, ACTIVE or REOPENED)  
webApp.id (Integer)  
webApp.name (Text)  
severity (Integer)  
ignoredDate (Date)  
ignoredReason (FALSE\_POSITIVE,  
RISK\_ACCEPTED or NOT\_APPLICABLE)  
group (XSS, SQL, INFO, PATH, CC, SSN\_US or  
CUSTOM)  
owasp.name (Text)  
owasp.code (Integer)  
wasc.name (Text)  
wasc.code (Integer)  
cwe.id (Integer)  
firstDetectedDate (Date)  
lastDetectedDate (Date)  
lastTestedDate (Date)  
timesDetected (Integer)

## Edit findings severity

/qps/rest/3.0/editSeverity/was/finding/<id>  
(POST)

/qps/rest/3.0/editSeverity/was/finding/<findings>  
(POST)

### Filters:

id (Integer)

new Severity level {1, 2, 3, 4, 5} (Integer)  
comments (Text)

## Restore findings severity

/qps/rest/3.0/restoreSeverity/was/finding<id>  
(POST)

### Required:

id (Integer)

## Retest findings

/qps/rest/3.0/retest/was/finding/<id>

/qps/rest/3.0/retest/was/finding/<findings>  
(POST)

### Required:

id (Integer)

## Burp

### Import Burp Scan Reports

/qps/rest/3.0/import/was/burp (POST)

### Required:

webAppId (Integer)

Burp Scanner Report in XML format

### Optional:

purgeResults (Boolean)

closeUnreportedIssues (Boolean)

fileName (String)



# Web Application Firewall API

Use these API calls to manage web applications, clusters, and appliances.

[Web Applications](#) | [Web Servers](#) | [Healthchecks](#) | [SSL Certificates](#) | [Custom Response Pages](#) | [Security Policies](#) | [HTTP Profiles](#) | [Custom Rules](#) | [Clusters](#) | [Appliances](#)

Looking for more information?

[Qualys Web Application Firewall API User Guide](#)

## Web Applications

### Current web application count

`/qps/rest/2.0/count/waf/webapp/` (GET)

### Get details on a web application

`/qps/rest/2.0/get/waf/webapp/<id>` (GET)

Required:

`id` (Integer) /web application ID

### Search web applications

`/qps/rest/2.0/search/waf/webapp/` (POST)

Filters (optional):

`id` (Long)  
`uuid` (UUID)  
`name` (Text)  
`url` (Text)  
`tags.tag.id` (Long)  
`tags.tag.name` (Text)  
`owner.id` (Text)  
`owner.username` (Text)  
`owner.lastname` (Text)  
`created` (Date)  
`updated` (Date)  
`urls.value` (Text)  
`healthcheck.id` (Long)  
`healthcheck.uuid` (UUID)  
`healthcheck.name` (Text)  
`failureResponseCode` (Long)  
`webServer.id` (Long)  
`weberver.uuid` (UUID)

`webServername` (Text)  
`webServerTimeout` (Long)  
`certificate.id` (Long)  
`certificate.uuid` (UUID)  
`certificate.name` (Text)  
`status`  
`deployed` (Date)  
`synced` (Date)  
`blockingMode` (Boolean)  
`createdBy.id` (Long)  
`createdBy.username` (Text)  
`createdBy.firstname` (Text)  
`createdBy.lastname` (Text)  
`updatedBy.id` (Long)  
`updatedBy.username` (Text)  
`updatedBy.firstname` (Text)  
`updatedBy.lastname` (Text)  
`custompage.id` (Long)  
`customPage.uuid` (UUID)  
`customPage.name` (Text)  
`securityPolicy.id` (Long)  
`securityPolicy.uuid` (UUID)  
`securityPolicy.name` (Text)  
`httpProfile.id` (Long)  
`httpProfile.uuid` (UUID)  
`httpProfile.name` (Text)  
`sslEnabled` (Boolean)  
`clusters.cluster.id` (Long)  
`clusters.cluster.name` (Text)  
`clusters.cluster.uuid` (UUID)  
`persistenceEnabled` (Boolean)  
`scanTrustEnabled` (Boolean)

### Create web application

`/qps/rest/2.0/create/waf/webapp` (POST)

Required:

`name` (Text)  
`url` (Text)  
`webServer.id` (Long)  
`securityPolicy.id` (Long)  
`httpProfile.id` (Long)  
`updateSchedule.enabled` (Boolean)

Optional:

[Click here](#) for WAF API User Guide

## Update web application

/qps/rest/2.0/update/waf/webapp/<id> (POST)

/qps/rest/2.0/update/waf/webapp (POST)

Optional:

name (Text)  
url (Text)  
webServer.id (Long)  
webServerTimeout (Long)  
securityProfile.id (Long)  
httpProfile.id (Long)  
persistencyEnabled (Boolean)  
persistencyToken  
healthcheck.id (Long)  
failureResponseCode (Long)  
certificate.id (Long)  
sslProtocols (Text)  
sslCiphers (Text)  
blockingMode (Boolean)  
customPage.id (Long)  
scanTrustEnabled (Boolean)  
customRules.CustomRule.id (Long)  
clusters.cluster.id (Long)  
lastComment (Text)  
updateSchedule.enabled (Boolean)  
updateSchedule.weekDays (Text)  
updateSchedule.startTime (Integer)  
updateSchedule.timezone.code (Text)  
updateSchedule.timezone.offset (Text)  
updateSchedule.freezeEndDate (Date)  
urls  
urls.string (text)  
tags

[Click here](#) for WAF API User Guide

## Delete web application

/qps/rest/2.0/delete/waf/webapp/<id> (POST)

Required:

id (Long) /web application ID

## Delete web applications (bulk)

/qps/rest/2.0/delete/waf/webapp (POST)

Filters (optional):

see [Search web applications](#)

## Web Servers

### Current web server count

/qps/rest/2.0/count/waf/webserver/ (GET)

### Get details on a web server

/qps/rest/2.0/get/waf/webserver/<id> (GET)

Required:

id (Integer) /web server ID

### Search web servers

/qps/rest/2.0/search/waf/webserver/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
loadBalancingAlgorithm (Text)  
addresses.url (Text)  
addresses.weight (Integer)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
owner.lastname (Text)  
created (Date)  
updated (date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)

## Create web server

/qps/rest/2.0/create/waf/webserver (POST)

Required:

name (Text)  
loadBalancingAlgorithm (Text)  
addresses.WebServerAddresses

Optional:

description (Text)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update web server

/qps/rest/2.0/update/waf/webserver/<id> (POST)

/qps/rest/2.0/update/waf/webserver (POST)

Optional:

name (Text)  
description (Text)  
loadBalancingAlgorithm (Text)  
addresses.WebServerAddress  
tags

## Delete web server

/qps/rest/2.0/delete/waf/webserver/<id> (POST)

Required:

id (Long) /web server ID

## Delete web server (bulk)

/qps/rest/2.0/delete/waf/webserver (POST)

Filters (optional):

see [Search web servers](#)

## Healthchecks

### Current healthcheck count

/qps/rest/2.0/count/waf/healthcheck/ (GET)

### Get details on a healthcheck

/qps/rest/2.0/get/waf/healthcheck/<id> (GET)

Required:

id (Integer) /healthcheck ID

### Search healthchecks

/qps/rest/2.0/search/waf/healthcheck/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
lmethod  
path (Text)  
expectedResponseCode (Long)  
intervalUp (Long)  
intervalDown (Long)  
intervalFlapping (Long)  
nbSuccessesUp (Long)  
nbFailuresDown (Long)  
timeout (Long)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)

## Create healthcheck

/qps/rest/2.0/create/waf/healthcheck (POST)

Required:

name (Text)  
method  
path (Text)  
loadBalancingResponseCode (Long)  
intervalUp (Long)  
intervalDown (Long)  
intervalFlapping (Long)  
nbSuccessesUp (Long)  
nbFailuresDown (Long)  
timeout (Long)

Optional:

description (Text)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update healthcheck

/qps/rest/2.0/update/waf/healthcheck/<id>  
(POST)  
/qps/rest/2.0/update/waf/healthcheck (POST)

Optional:

name (Text)  
description (Text)  
method  
path (Text)  
expectedResponseCode (Long)  
intervalUp (Long)  
intervalDown (Long)  
nbSuccessesUp (Long)  
nbFailuresDown (Long)  
timeout (Long)  
tags

## Delete healthcheck

/qps/rest/2.0/delete/waf/healthcheck/<id> (POST)

Required:

id (Long) /healthcheck ID

## Delete healthcheck (bulk)

/qps/rest/2.0/delete/waf/healthcheck (POST)

Filters (optional):

see [Search healthchecks](#)

## SSL Certificates

### Current SSL certificates count

/qps/rest/2.0/count/waf/certificate/ (GET)

### Get details on SSL certificate

/qps/rest/2.0/get/waf/certificate/<id> (GET)

Required:

id (Integer) /SSL certificate ID

### Search SSL certificates

/qps/rest/2.0/search/waf/certificate/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)

### Create SSL certificate

/qps/rest/2.0/create/waf/certificate (POST)

Required:

name (Text)  
passphrase (Text)  
token (Text)

Optional:

description (Text)  
pkcs12 (Text)

certificate (Text)  
privateKey (Text)  
chain (Text)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update SSL certificate

/qps/rest/2.0/update/waf/certificate/<id> (POST)

/qps/rest/2.0/update/waf/certificate (POST)

Optional:  
name (Text)  
description (Text)  
pkcs12 (Text)  
certificate (TextO)  
privateKey (Text)  
passphrase (Text)  
token (Text)  
chain (Text)  
tags

## Delete SSL certificate

/qps/rest/2.0/delete/waf/certificate/<id> (POST)

Required:  
id (Long) /SSL certificate ID

## Delete SSL certificate (bulk)

/qps/rest/2.0/delete/waf/certificate (POST)

Filters (optional):  
see [Search SSL certificates](#)

## Custom Response Pages

### Current custom response page count

/qps/rest/2.0/count/waf/custompage/ (GET)

### Get details on custom response page

/qps/rest/2.0/get/waf/custompage/<id> (GET)

Required:  
id (Integer) /custom response page ID

### Search custom response pages

/qps/rest/2.0/search/waf/custompage/ (POST)

### Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
body (Text)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)

## Create custom response page

/qps/rest/2.0/create/waf/custompage (POST)

Required:  
name (Text)  
body (Text)  
Optional:  
description (Text)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update custom response page

/qps/rest/2.0/update/waf/custompage/<id> (POST)

/qps/rest/2.0/update/waf/custompage (POST)

Optional:  
name (Text)  
description (Text)  
body (Text)  
tags

## Delete custom response page

/qps/rest/2.0/delete/waf/custompage/<id> (POST)

Required:

id (Long) /custom response page ID

## Delete custom response page (bulk)

/qps/rest/2.0/delete/waf/custompage (POST)

Filters (optional):

see [Search custom response pages](#)

## Security Policies

### Current security policy count

/qps/rest/2.0/count/waf/securitypolicy/ (GET)

### Get details on security policy

/qps/rest/2.0/get/waf/securitypolicy/<id> (GET)

Required:

id (Integer) /security policy ID

### Search security policies

/qps/rest/2.0/search/waf/securitypolicy/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
system (Integer)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)

webApps.webApp.uuid (UUID)

webApps.webApp.name (Text)

## Create security policy

/qps/rest/2.0/create/waf/securitypolicy (POST)

Required:

name (Text)

Optional:

description (Text)  
applicationSecurity (Keyword)  
threatLevel.loggingThreshold (Integer)  
threatLevel.blockingThreshold (Integer)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update security policy

/qps/rest/2.0/update/waf/securitypolicy/<id> (POST)

/qps/rest/2.0/update/waf/securitypolicy (POST)

Optional:

id (Integer)  
name (Text)  
description (Text)  
applicationSecurity (Keyword)  
threatLevel.loggingThreshold (Integer)  
threatLevel.blockingThreshold (Integer)  
tags

## Delete security policy

/qps/rest/2.0/delete/waf/securitypolicy/<id> (POST)

Required:

id (Long) /security policy ID

## Delete security policy (bulk)

/qps/rest/2.0/delete/waf/securitypolicy (POST)

Filters (optional):

see [Search security policies](#)

## HTTP Profiles

### Current HTTP profile count

/qps/rest/2.0/count/waf/httpprofile/ (GET)

### Get details on HTTP profile

/qps/rest/2.0/get/waf/httpprofile/<id> (GET)

Required:

id (Integer) /HTTP profile ID

### Search HTTP profiles

/qps/rest/2.0/search/waf/httpprofile/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
system (Integer)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)

### Create HTTP profile

/qps/rest/2.0/create/waf/httpprofile (POST)

Required:

name (Text)  
requestMethod.allowAll -or-  
requestMethod.denyAll  
requestHeader

requestContentType.allowAll -or-  
requestContentType.denyAll  
detectProtocolAnomalies (Boolean)  
serverCloacking  
serverCloacking.value (Text)  
suppressSensitiveHeaders (Boolean)  
onErrorMessages (Keyword)  
onSensitiveFileTypes (Keyword)  
cookieProtection  
discourageContentTypeSniffing (Boolean)  
forceDefaultContentType (Keyword)  
forceDefaultContentType.value (Text)  
forceDefaultCharacterEncoding  
forceDefaultCharacterEncoding.value (Text)  
contentSecurityPolicyHeader  
contentSecurityPolicyHeader.value (Text)  
discourageClickjacking  
browserXSSPProtection  
webServiceProtection.xmlParsing.enabled  
(Boolean)  
webServiceProtection.jsonParsing.enabled  
(Boolean)

Optional:

description (Text)  
requestMethod.allowAll.detectInvalid  
(Boolean)  
requestMethod.allowA..DetectTraceTrack  
(Boolean)  
requestHeader.detectInvalid (Boolean)  
requestHeader.detectRepeated (Boolean)  
requestHeader.detectChunked (Boolean)  
requestContentType.allowAll.detectFileUploa  
ds (Boolean)  
serverCloacking.enabled (Boolean)  
cookieProtection.type  
cookieProtection.value (Text)  
forceDefaultContentType.enabled (Boolean)  
forceDefaultCharacterEncoding.type  
(Keyword)  
contentSecurityPolicyHeader.enabled  
(Boolean)  
webServiceProtection.xmlParsing.size  
(Integer)  
webServiceProtection.xmlParsing.items  
(Integer)  
webServiceProtection.xmlParsing.level  
(Integer)

webServiceProtection.jsonParsing.size  
(Integer)  
webServiceProtection.jsonParsing.items  
(Integer)  
webServiceProtection.jsonParsing.level  
(Integer)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update HTTP profile

/qps/rest/2.0/update/waf/httpprofile/<id> (POST)  
/qps/rest/2.0/update/waf/httpprofile (POST)

Optional:  
see [Create HTTP profile](#)

## Delete HTTP profile

/qps/rest/2.0/delete/waf/httpprofile/<id> (POST)

Required:  
id (Long) /HTTP profile ID

## Delete HTTP profile (bulk)

/qps/rest/2.0/delete/waf/httpprofile (POST)

Filters (optional):  
see [Search HTTP profiles](#)

## Custom Rules

### Current custom rule count

/qps/rest/2.0/count/waf/customrule (GET)

### Get details on custom rule

/qps/rest/2.0/get/waf/customrule/<id> (GET)

Required:  
id (Integer) /custom rule ID

### Search custom rules

/qps/rest/2.0/search/waf/customrule/ (POST)

Filters (optional):  
id (Long)  
uuid (UUID)  
name (Text)

description (Text)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)

## Create custom rule

/qps/rest/2.0/create/waf/customrule (POST)

Required:  
name (Text)  
conditions  
action  
Optional:  
description (Text)  
tags  
tags.tag.id (Long)  
tags.tag.name (Text)

## Update custom rule

/qps/rest/2.0/update/waf/customrule/<id> (POST)  
/qps/rest/2.0/update/waf/customrule (POST)

Optional:  
name (Text)  
description (Text)  
conditions  
action  
tags

## Delete custom rule

/qps/rest/2.0/delete/waf/customrule/<id> (POST)

Required:  
id (Long) /custom rule ID



## Delete custom rule (bulk)

/qps/rest/2.0/delete/waf/customrule (POST)

Filters (optional):

see [Search custom response pages](#)

## Clusters

### Current cluster count

/qps/rest/2.0/count/waf/cluster (GET)

### Get details on clusters

/qps/rest/2.0/get/waf/cluster/<id> (GET)

Required:

id (Integer) /cluster ID

### Search clusters

/qps/rest/2.0/search/waf/cluster (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
tags.tag.id (Long)  
tags.tag.name (Text)  
owner.id (Long)  
owner.username (Text)  
owner.firstname (Text)  
owner.lastname (Text)  
created (Date)  
updated (Date)  
createdBy.id (Long)  
createdBy.username (Text)  
createdBy.firstname (Text)  
createdBy.lastname (Text)  
updatedBy.id (Long)  
updatedBy.username (Text)  
updatedBy.firstname (Text)  
updatedBy.lastname (Text)  
token (Text)  
syncDate (Date)  
status (Text)  
deploymentStatus (Text)  
deployed (Date)  
errorResponse.action  
errorResponse.customPage.id (Long)

errorResponse.customPage.uuid (UUID)  
errorResponse.redirect.url (Text)  
errorResponse.redirect.status (Long)  
appliances.appliance.id. (Long)  
appliances.appliance.uuid. (UUID)  
appliances.appliance.name (Text)  
webApps.webApp.id (Long)  
webApps.webApp.uuid (UUID)  
webApps.webApp.name (Text)  
trustedIPs.string (Text)

### Create cluster

/qps/rest/2.0/create/waf/cluster (POST)

Required:

name (Text)

Optional:

[Click here](#) for WAF API User Guide

### Update cluster

/qps/rest/2.0/update/waf/cluster/<id> (POST)

/qps/rest/2.0/update/waf/cluster (POST)

Optional:

name (Text)  
description (Text)  
errorResponse  
errorResponse.block  
errorResponse.redirect.url (Text)  
errorResponse.redirect.status (Long)  
errorResponse.customPage.id (Long)  
errorResponse.customPage.uuid (UUID)  
errorResponse.customPage.name (Text)  
tags  
trustedIPs.string (Text)

### Delete cluster

/qps/rest/2.0/delete/waf/cluster/<id> (POST)

Required:

id (Integer) /cluster ID

### Delete clusters (bulk)

/qps/rest/2.0/delete/waf/cluster (POST)

Filters (optional):

see [Search clusters](#)

## Appliances

### Current appliance count

/qps/rest/2.0/count/waf/appliance (GET)

### Get details on appliance

/qps/rest/2.0/get/waf/appliance/<id> (GET)

Required:

id (Integer) /appliance ID

### Search appliances

/qps/rest/2.0/search/waf/appliance (POST)

Optional:

id (Long)  
uuid (UUID)  
name (Text)  
hostname (Text)  
lastPollDate  
applianceCreated  
applianceVersion (Text)  
status (Long)  
pollStatus  
heartbeatGenerated  
heartbeatProcessed  
systemOs (Text)  
systemRam (Long)  
systemType (Text)  
systemEc2InstanceId (Text)  
systemEc2InstanceType (Text)  
systemEc2AmiId (Text)  
systemCpusCount (Long)  
systemCpusCores (Long)  
systemCpusSpeed (Float)  
systemCpusModel (Text)  
configRulesVersion (Text)  
configVersion (Text)  
configGenerated  
ip (Text)  
cluster.id (Long)  
cluster.uuid (UUID)  
cluster.name (Text)

### Delete appliance

/qps/rest/2.0/delete/waf/appliance/<id> (POST)

Required:

id (Long) /appliance ID

# Malware Detection API

Use these API calls to get information about malware detections.

## Malware Detections

Looking for more information?

[Qualys Malware Detection API User Guide](#)

## Malware Detections

### Current malware detections

/qps/rest/1.0/download/md/detection (POST)

Required:

format (csv|cef)

Filters (optional):

id (Integer)

qid (Integer)

url (Text)

type (Keyword ie BEHAVIORAL)

showDeactivatedSite (Boolean)

severity (Keyword i.e. HIGH)

### Search malware detections

/qps/rest/1.0/search/md/detection (POST)

Filters:

id (Integer)

qid (Integer)

type (Keyword ie BEHAVIORAL)

showDeactivatedSite (Boolean)

severity (Keyword i.e. HIGH)

### Get details on malware detection

/qps/rest/1.0/get/md/detection/<id> (GET, POST)

Required:

id (Integer) /malware detection ID

# Security Assessment Questionnaire API

Use these API calls to manage SAQ users and templates.

[SAQ users](#) | [SAQ templates](#)

Looking for more information?

[Qualys Security Assessment Questionnaire API User Guide](#)

## SAQ users

### Current user count

/qps/rest/1.0/count/saq/user/ (GET, POST)

Filters (optional):

id (Integer) /user ID  
uuid (Integer)  
firstName (Text)  
lastName (Text)  
company (Text)  
title (Text)  
emailAddress (Text)  
userName (Text)  
tags.tag.id (Text)  
tags.tag.name (Text)

### Get details on user

/qps/rest/1.0/get/saq/user/ <id> (GET)

Required:

id (Integer) /user ID

### Search users

/qps/rest/1.0/search/saq/user/ (POST)

Filters (optional):

id (Integer) /user ID  
uuid (Integer)  
firstName (Text)  
lastName (Text)  
company (Text)  
title (Text)  
emailAddress (Text)  
userName (Text)  
tags.tag.id (Integer)

tags.tag.name (Text)

### Create user

/qps/rest/1.0/create/saq/user/ (POST)

Required:

firstName (Text)  
lastName (Text)  
company (Text)  
emailAddress (Text)

Optional:

title (Text)  
tags (List)  
tags.tag.id (Integer)  
tags.tag.name (Text))

### Update user

/qps/rest/1.0/update/saq/user/<id> (POST)

/qps/rest/1.0/update/saq/user/ (POST)

Required to update single user:

id (Integer) /user ID

Optional:

firstName (Text)  
lastName (Text)  
company (Text)  
emailAddress (Text)  
title (Text)  
tags (List)  
tags.tag.id (Integer)  
tags.tag.name (Text))

Optional for bulk update:

id (Integer)  
uuid (Integer)

### Delete user

/qps/rest/1.0/delete/saq/user/<id> (POST)

Required:

id (Long) /user ID

### Delete users (bulk)

/qps/rest/1.0/delete/saq/user/ (POST)

Filters (optional):

see [Search users](#)

## SAQ templates

### Current library template count

/qps/rest/1.0/count/saq/librarytemplate/  
(GET, POST)

Filters (optional):

id (Integer) /library template ID  
uuid (Integer)  
name (Text)  
description (Text)  
category (Text)  
familyId (Integer)  
revision (Integer)  
isLibrary (Boolean)  
questionCnt (Integer)  
state (Text)

### Get details on library template

/qps/rest/1.0/get/saq/librarytemplate/ <id> (GET)

Required:

id (Integer) /library template ID

### Search library templates

/qps/rest/1.0/search/saq/librarytemplate/ (POST)

Filters (optional):

id (Long)  
uuid (UUID)  
name (Text)  
description (Text)  
category (Text)  
familyId (Integer)  
revision (Integer)  
isLibrary (Boolean)  
questionCnt (Integer)  
state (Text)

### Current template count

/qps/rest/1.0/count/saq/template/ (GET, POST)

Filters (optional):

id (Integer) /template ID  
uuid (Integer)  
name (Text)  
description (Text)  
category (Text)  
familyId (Integer)

revision (Integer)  
isLibrary (Boolean)  
questionCnt (Integer)  
state (Text)

### Get details on template

/qps/rest/1.0/get/saq/template/ <id> (GET)

Required:

id (Integer) /template ID

### Search templates

/qps/rest/1.0/search/saq/template/ (POST)

Filters (optional):

id (Integer) /template ID  
uuid (Integer)  
name (Text)  
description (Text)  
category (Text)  
familyId (Integer)  
revision (Integer)  
isLibrary (Boolean)  
questionCnt (Integer)  
state (Text)

### Create template from library

/qps/rest/1.0/createfromlibrary/saq/template/  
(POST)

Required:

id (Integer) /library template ID

### Create template

/qps/rest/1.0/create/saq/template/ (POST)

Several required and optional elements are supported

[Click here](#) for SAQ API User Guide

## Update template

/qps/rest/1.0/update/saq/template/<id> (POST)

/qps/rest/1.0/update/saq/template/ (POST)

Required to update single template:

id (Integer) /library template ID

Several optional elements are supported

[Click here](#) for SAQ API User Guide

## Create new version of existing template

/qps/rest/1.0/newversion/saq/template/<id>

(POST)

Required:

id (Long) /template ID

## Publish template

/qps/rest/1.0/publish/saq/template/<id> (POST)

Required:

id (Long) /template ID

## Delete template

/qps/rest/1.0/delete/saq/template/<id> (POST)

Required:

id (Long) /template ID

## Delete template (bulk)

/qps/rest/1.0/delete/saq/template/ (POST)

Filters (optional):

see [Search library templates](#)

# Portal version API

Find out the version of Portal and its sub-modules (in your subscription).

## Portal version

`/qps/rest/portal/version` (GET)

Returns the version information based on the username supplied in the request.

# API Server URL

## Qualys API Server URL

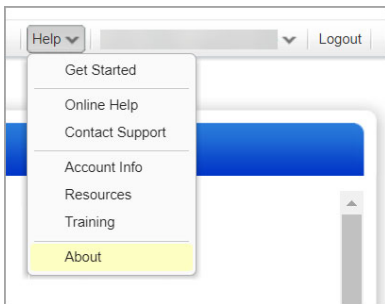
The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

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

## Still need help?

You can easily find the API server URL to use. Just log in to your Qualys account.

Go to Help > About.



You'll see the API Server URL for your account under Security Operations Center (SOC).

General Information	
<b>Qualys Web Service</b>	
Application Version:	10.0.0.1-1
Online Help Version:	10.0.18-5
SCAP Module Version:	1.2
<b>Qualys External Scanners</b>	
Security Operations Center (SOC):	64.39.96.0/20 (64.39.96.1-64.39.111.254) 2602:FDAA:0:2108::/64 2600:0C02:1020:2881::/64 2600:C08:2015:4400::/64 2600:0C02:1020:2111::/64 2600:0C02:1020:2224::/64
Scanner Version:	11.9.22-1
Vulnerability Signature Version:	2.4.896-3
Scanner Services	3.3.3.3-1
<b>Qualys Scanner Appliances</b>	
Security Operations Center (SOC):	- qualysguard.qg2.apps.qualys.com:443 - qgadmin.qg2.apps.qualys.com:443 - qualysapi.qg2.apps.qualys.com:443 - distribution.qg2.apps.qualys.com:443 - monitoring.qg2.apps.qualys.com:443 - scanservice1.qg2.apps.qualys.com:443



# Good to Know

## Notations

Required attributes are in bold. For example “**ref**={value}” indicates a required parameter.

Defaults are underlined. For example {Q|1} indicates “0” is the default value for the Boolean attribute.

## GET and POST

Functions support the GET method only, the POST method only or both GET and POST as indicated.

## Date/Time

Date/time format is YYYY-MM-DD[THH:MM:SSZ] where time is optional.

## API Notes

- 1) Authentication is performed using basic auth (using API v1 or APIv2) or session-based authentication (API v2 only) by the SSL socket connection.
- 2) There are known limits for the amount of data that can be sent using the GET method. These limits are dependent on the toolkit used. There is no fundamental limit with sending data using the POST method.
- 3) Variables and values must be URL-encoded.
- 4) Returned XML responses usually include numeric error codes.
- 5) UTF-8 encoding is used internally and for the returned XML.
- 6) Role-based privileges (Manager, Scanner, and Reader) apply to most API calls.
- 7) Blanks in “string type values” can be encoded as plus characters(+).

## Curl Client

Use the **curl** client to issue API requests directly from the Linux Command Line.

Example using basic authentication (example uses Qualys US Platform 1):

```
curl -s -k -H 'X-Requested-With: curl demoapp' -u username:password 'https://{SERVER}.qualys.com/api/2.0/fo/scan/?action=list'
```

Example using session based authentication (example uses Qualys US Platform 1):

```
curl -s -k -H 'X-Requested-With: curl demoapp' -D headers.15 -b 'QualysSession=SESSION_ID; path=/api; secure' 'https://{SERVER}.qualys.com/api/2.0/fo/scan/?action=list'
```

See the **curl(1)** man page for further details.

## Allowed Operators

Supported using the following APIs: Asset Management and Tagging, Cloud Agent, Continuous Monitoring, Malware Detection, Web Application Firewall, Web Application Scanning.

### Allowed Operators

Integer	EQUALS, NOT EQUALS, GREATER, LESSER, IN
Text	CONTAINS, EQUALS, NOT EQUALS
Date	EQUALS, NOT EQUALS, GREATER, LESSER
Keyword	EQUALS, NOT EQUALS, IN
Boolean	(true/false) EQUALS, NOT EQUALS

## Looking for more?

[Click here](#) for all our current API User Guides