Qualys API

Quick Reference

June 4, 2018

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

Table of Contents

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? No problem. Click
API v1 guide for Qualys API v1 User Guide
API v2 guide for Qualys API v2 User Guide

Scans

API v2 guide

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_ags={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}&

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}&

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}&

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}&

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}&
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}&
client_id= {value}&
client_name={value}&
ec2_instance_ids={value}&

Scheduled Scans

API v2 guide

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}&
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)
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

API v2 guide

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, ibm_db2, vmware, http, apache, ms_iis, ibm_websphere, mysql, tomcat, oracle_weblogic, mongodb, palo_alto_firewall

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, apache, ms_iis, ibm_websphere, http, mysql, ms_sql, docker, postgresql, sybase, tomcat, mongodb, palo_alto_firewall

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}&
Notes: "ips" is required for a create request (except Windows), optional for an update request. "add_ips" and "remove_ips" are for an update request only.
{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)
CyberArk PIM Suite
folder={value}&
file={value}&
CyberArk AIM
folder={value}&
file={value}&
Thycotic Secret Server
secret_name={value}&
Quest Vault
system_name={value}&
CA Access Control
end_point_name={value}&
end_point_type={value}&
end_point_container={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}&
Notes: Required for create request: "username", "password" if cleartext_password=1. {XML File} defines private key certificates and root delegations.

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

{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:
username={value}&
password={value}&
sid={value}&
servicename={value}&
port={num}&
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:
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).

{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}&

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}&

{IBM WebSphere App Server record}:
unix_install_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}&
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}&

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.

{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.

PC scans only

{Docker record}:
(PC scans only)
docker_deamon_conf_file={value}
docker_command={value}

{MS SQL record}:
(PC scans only)
username={value}&
password={value}&
port={value}&
db_local={0|1}&
windows_domain={value}&
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.
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}&

{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.

{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 v2 guide

/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={0|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).

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}&*
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 v2 guide

/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}&

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}&
*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}&

Assign Appliance to Network: (POST)

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

Assign Appliance to Network: (POST)

/api/2.0/fo/appliance/replace_iscanner/
action={replace}&
echo_request={0|1}&
old_scaner_name={value}&
new_scanner_name={value}&
do_not_copy_settings={0|1}&
do_not_remove_new_scanner_from_objects={0|1}&

Option Profiles

API v2 guide

/api/2.0/fo/subscription/option_profile/

Export Option Profile: (POST)

/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.

KnowledgeBase

API v2 guide

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}&
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.

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={0|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={0|1}&
id={value}&

Dynamic Search Lists

/api/2.0/fo/qid/search_list/dynamic/

List Dynamic Search Lists: (GET + POST)

action={list}&

echo_request={0|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={0|1}&
title={value}&
global={0|1}&
comments={value}&
Criteria for Dynamic Search List (below)

Update Dynamic Search List: (POST)

action={update}&
echo_request={0|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={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={value}&
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={0|1}&
id={value}&

Reports

API v2 guide

Manage Reports

/api/2.0/fo/report/

List Reports: (GET + POST)

action={list}&
echo_request={0|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={0|1}&
id={value}&

Download Report: (POST)

action={fetch}&
echo_request={0|1}&
client_id= {value}&
client_name={value}&

Launch Report

/api/2.0/fo/report/

Launch Report (all types): (POST)

action={launch}&
echo_request={0|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={0|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={0|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={0|1}&
output_format={pdf|html|mht|xml|csv}&
ips={value}&
ips_network_id={id}&
asset_group_ids={id,id…}&

Qualys Patch Report:

echo_request={0|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_qids={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 v2 guide

/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}&
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

API v2 guide

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|scans}&
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}&
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}&
exclude_account_id={0|1}&
Filters
selective_vulns={complete|custom}&
search_list_ids={value}&
exclude_qid_option={0|1}&
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={0|1}&
vuln_ignored={0|1}&
potential_active={0|1}&
potential_disabled={0|1}&
potential_ignored={0|1}&
ig_active={0|1}&
ig_disabled={0|1}&
ig_ignored={0|1}&
display_non_running_kernels={0|1}&
exclude_non_running_kernel={0|1}&
exclude_non_running_services={0|1}&
exclude_qids_not_exploitable_due_to_configuration={0|1}&
exclude_superceded_patches={0|1}&
categories_list={value}&
Services and Ports
required_services={value}&
unauthorized_services={value}&
required_ports={value}&
unauthorized_ports={value}&
User Access
global={0|1}&
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={0|1}&
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_comments={<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}&
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_configuration={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|operatingsystem}&
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

API v1 guide

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

API v1 guide

ignore_vuln.php? (GET +POST)

action={ignore|restore}&
qids={value,value… 10 max}&
comments={value}&
(*)asset_groups={value,value…}&
(*)ips={ip,range…}&
(*)dns_contains={string}&
(*)netbios_contains={string}&
reopen_ignored_days={1-730}&
network_id={value}&

Notes: One of these (*) is required

Compliance Info

API v2 guide

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}&

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}&
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}&
asset_group_ids={value}
status={Passed|Failed|Error}&
show_remediation_info={0|1}&
truncation_limit={value}&
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}
Notes: Up to 10 policies for "policy_ids".

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_managment_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

API v1 guide

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…}&
ui_interface_style={standard_blue|navy_blue|coral_red|olive_green|accessible_high_contrast}&

Notes: 1) "asset_groups" applies only to Scanner, Reader and Contact. 2) For an add request, "ui_interface_style" is set to standard_blue when unspecified.

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 v2 guide

(/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|KnowledgeBase 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

API v1 guide

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? No problem. Click

CA API guide for Qualys Cloud Agent API User Guide

Agent Management CA API guide

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

CA API guide

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

CA API guide

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? No problem. Click

API v1 guide for Qualys API v1 User Guide

API v2 guide for Qualys API v2 User Guide

Network API v2 guide for Qualys API Network Support Guide

AM API v2 guide for Qualys Asset Management and Tagging API v2 User Guide

Networks

Network API v2 guide

/api/2.0/fo/network/

Network List: (GET + POST)

action={list}&
echo_request={0|1}&
ids={id1,id2…}&

Network: (POST)

action={create|update}&
name={value}&
echo_request={**0**|1}&

Assets

API v2 guide

IP Assets

/api/2.0/fo/asset/ip/

List IPs: (GET + POST)

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

Add IPs: (POST)

action={add}&
echo_request={0|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={0|1}&
ips={value} –or- {POSTed CVS raw data}&
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={0|1}&
details={Basic|Basic/AGs|All|All/AGs|None}&
ips={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={value}&
host_metadata_fields={accountId|region|availabilityZone|instanceId|instanceType|imageId|kernelId}

Notes: host_metadata supports fetching only EC2 assets.

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}&
compliance_enabled={0|1}&
os_pattern={PCRE regex}&
network_ids={id1,id2...}&

Host Detection Assets

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

Host Detection List: (GET + POST)

action={list}&
echo_request={**0**|1}&
ids={id,range...}&
id_min={id}&
id_max={id}&
ips={ip,range...}&
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}&
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...}&
dectection_processed_before={date}
dectection_processed_after={date}
detection_updated_before={date}
detection_updated_since={date}&
max_days_since_detection_updated={value}&
*host_metadata={value}&
host_metadata_fields={accountId|region|availabilityZone|instanceId|instanceType|imageId|kernelId}

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”.

4) host_metadata supports fetching only EC2 assets.

Excluded Hosts

Excluded Hosts List: (GET + POST)

/api/2.0/fo/asset/excluded_ip/

action={list}&
echo_request={0|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={0|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={0|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={0|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

API v1 guide

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 v2 guide

/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={0|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={0|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|low
|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

AM API v2 guide

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)
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 color (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

AM API v2 guide

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

AM API v2 guide

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)
networdGuid (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

AM API v2 guide

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

AM API v2 guide

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 color (0-9 and A-F)

Count vulnerabilities

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

Asset Data Connector

AM API v2 guide

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

AM API v2 guide

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/id> (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

AM API v2 guide

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? No problem. Click **CM API guide** for Qualys Continuous Monitoring API User Guide

Alerts

CM API guide

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

CM API guide

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

CM API guide

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

CM API guide

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? No problem. Click

WAS API guide for Qualys Web Application Scanning API User Guide

Web Application

WAS API guide

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

WAS API guide

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

WAS API guide

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)[1]
target.tags.included.tagList.Tag.id (Integer)[1]
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.

[1] 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

WAS API guide

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

WAS API guide

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)
updatedDate (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)
updatedDate (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)
updatedDate (Date)
usedByWebApps (Boolean)
usedBySchedules (Boolean)

Report

WAS API guide

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

WAS API guide

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)[1]
target.tags.included.tagList.Tag.id (Integer)[1]
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)[1]
target.tags.included.tagList.Tag.id (Integer)[1]
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

WAS API guide

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

WAS API guide

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? No problem. Click

WAF API guide for Qualys Web Application Firewall API User Guide

Web Applications

WAF API guide

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)
persistencyEnabled (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
serverCloaking.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)
serverCloaking.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

WAF API guide

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 (TextO
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)
errorResonse.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

WAF API guide

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? No problem. Click

MD API guide for Qualys Malware Detection API User Guide

Malware Detections **MD API guide**

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? No problem. Click

SAQ API guide for Qualys Security Assessment Questionnaire API User Guide

SAQ users

SAQ API guide

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

SAQ API guide

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

What API Server URL to use

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

Qualys US Platform 1
https://qualysapi.qualys.com

Qualys US Platform 2
https://qualysapi.qg2.apps.qualys.com

Qualys US Platform 3
https://qualysapi.qg3.apps.qualys.com

Qualys EU Platform 1
https://qualysapi.qualys.eu

Qualys EU Platform 2
https://qualysapi.qg2.apps.qualys.eu

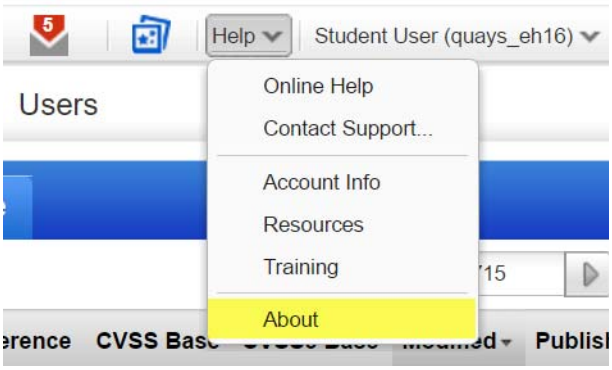
Qualys India Platform 1
https://qualysapi.qg1.apps.qualys.in

Qualys Private Cloud Platform
https://qualysapi.<customer_base_url>

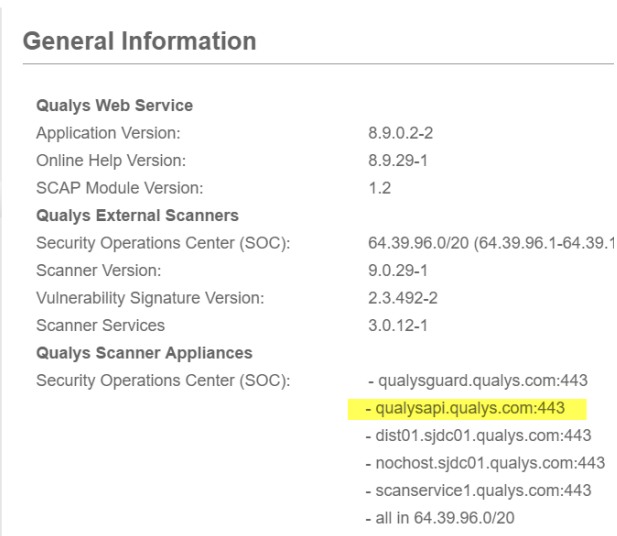
Still need help?

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).



Good to Know

Notations

Required attributes are in bold. For example "**ref**={value} indicates a required parameter.

Defaults are underlined. For example {0|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 latest API User Guides