Qualys Cloud Platform (VM, PC) v8.x

API Release Notes

Version 8.22

December 4, 2019

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Qualys API Server URL

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

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

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

Cloud Perimeter Scan API: New Input Parameter to Include Micro and Nano Instances into Scan

APIs affected	/api/2.0/fo/scan/cloud/perimeter/job/index.php?
New or Updated API	Updated
DTD or XSD changes	No

It's now possible to include micro/nano instances for scanning when launching a Cloud Perimeter scan for EC2 instances. To support scanning micro and nano instance types, we added a new optional parameter "include_micro_nano_instances" to the Cloud Perimeter Scan API. By default, this parameter is disabled, meaning the value is set to 0. To enable this parameter, set the value of the parameter to "include_micro_nano_instances = 1". There are no changes to the XML output or DTD.

This option is only available if micro and nano instances type is activated for your account.

Note - You'll see these changes in your account only when available on your platform. Please reach out to Qualys Support if you need more information.

Create/Update Cloud Perimeter Scan to include micro and nano instances

Sample - Create

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&module=vm&active=0&schedule=now&option_title=Initial
Options&connector_uuid=9ef995a8-0708-4155-a3f2-49a3cfcb2b7b
&include_micro_nano_instances=1&platform_type=vpc_peered&region_code=us-
east-1
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?"
```

Sample - Update

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=update&id=1640258&include_micro_nano_instances=0
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?"
```

Cloud Perimeter Scan API: New Input Parameter to Include Connector's Load Balancers into Scan

APIs affected	/api/2.0/fo/scan/cloud/perimeter/job/index.php?
New or Updated API	Updated
DTD or XSD changes	No

You can now specify in the Cloud Perimeter Scan API to include public load balancers from the selected connector in the scan job. We added a new optional input parameter "include_lb_from_connector" in the API to support this feature. Note there are no changes to the XML output or DTD.

By default, this parameter is disabled that is value is set to 0. To enable this parameter, set the value of the parameter to "include_lb_from_connector = 1". You also have the option to use the elb_dns parameter to specify one or more load balancer DNS names to include them in the scan job.

This option is available only if your account has Cloud View subscription and your platform has access to cloud view base URL "qweb_cloud_view_base_url". Please reach out to Qualys Support if you need more information.

Create/Update Cloud Perimeter Scan to include public load balancers

Sample - Create

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&module=vm&active=0&schedule=now&option_title=Initial
Options&connector_uuid=9ef995a8-0708-4155-a3f2-49a3cfcb2b7b
&include_lb_from_connector=1
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?"
```

Sample - Update

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=update&id=1645230&include_lb_from_connector=0
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?"
```

Schedule Scans for Policy Compliance

APIs affected	/api/2.0/fo/schedule/scan/compliance
New or Updated API	New
DTD or XSD changes	Yes

This API provides you the ability to create, update, list, and delete schedule scans for Policy Compliance.

Permissions

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

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

List compliance scan schedules

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

[GET]

Input Parameters

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

API request:

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

XML output:

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

```
            <SCAN>
                <ID>57363</ID>
                <ACTIVE>1</ACTIVE>
                <TITLE>
                    <![CDATA[My Scan Schedule api6]]>
                </TITLE>
                <USER_LOGIN>quays_sp1</USER_LOGIN>
                <TARGET>
                    <![CDATA[10.10.10.185]]>
                </TARGET>
                <NETWORK_ID>
                    <![CDATA[0]]>
                </NETWORK_ID>
                <ISCANNER_NAME>
                    <![CDATA[pyscandsp]]>
                </ISCANNER_NAME>
                <ASSET_GROUP_TITLE_LIST>
                    <ASSET_GROUP_TITLE>
                        <![CDATA[policyred7]]>
                    </ASSET_GROUP_TITLE>
                </ASSET_GROUP_TITLE_LIST>
                <OPTION_PROFILE>
                    <TITLE>
                        <![CDATA[duplicate IO]]>
                    </TITLE>
                    <DEFAULT_FLAG>0</DEFAULT_FLAG>
                </OPTION_PROFILE>
                <SCHEDULE>
                    <DAILY frequency_days="5" />
                    <START_DATE_UTC>2019-11-
19T22:00:00Z</START_DATE_UTC>
                    <START_HOUR>14</START_HOUR>
                    <START_MINUTE>0</START_MINUTE>
                    <NEXTLAUNCH_UTC>2019-11-
19T22:00:00</NEXTLAUNCH_UTC>
                    <TIME_ZONE>
                        <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
                      <TIME_ZONE_DETAILS>(GMT-0800) United States:
America/Los_Angeles</TIME_ZONE_DETAILS>
                    </TIME_ZONE>
                    <DST_SELECTED>1</DST_SELECTED>
                </SCHEDULE>
```

```
                    <NOTIFICATIONS />
                </SCAN>
            </COMPLIANCE_SCHEDULE_SCAN_LIST>
        </RESPONSE>
    </COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD update:

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

```
<!-- QUALYS COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT
(REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, COMPLIANCE_SCHEDULE_SCAN_LIST?)>
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_LIST (SCAN+)>
<!ELEMENT SCAN (ID, SCAN_TYPE?, ACTIVE, TITLE?, CLIENT?,
USER_LOGIN, TARGET, NETWORK_ID?, ISCANNER_NAME?, EC2_INSTANCE?,
CLOUD_DETAILS?, ASSET_GROUP_TITLE_LIST?, ASSET_TAGS?,
EXCLUDE_IP_PER_SCAN?, USER_ENTERED_IPS?, ELB_DNS?,
OPTION_PROFILE?, SCHEDULE, NOTIFICATIONS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT CLIENT (ID,NAME)>
<!ELEMENT TARGET (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT ISCANNER_NAME (#PCDATA)>
```

```
<!ELEMENT EC2_INSTANCE (CONNECTOR_UUID, EC2_ENDPOINT,
EC2_ONLY_CLASSIC?)>
<!ELEMENT CONNECTOR_UUID (#PCDATA)>
<!ELEMENT EC2_ENDPOINT (#PCDATA)>
<!ELEMENT EC2_ONLY_CLASSIC (#PCDATA)>


<!ELEMENT CLOUD_DETAILS (PROVIDER, CONNECTOR, SCAN_TYPE,
CLOUD_TARGET)>
<!ELEMENT PROVIDER (#PCDATA)>
<!ELEMENT CONNECTOR (ID?, UUID, NAME)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT REGION (UUID, CODE?, NAME?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT VPC_SCOPE (#PCDATA)>
<!ELEMENT VPC_LIST (VPC+)>
<!ELEMENT VPC (UUID)>

<!ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT ASSET_TAGS (TAG_INCLUDE_SELECTOR, TAG_SET_INCLUDE,
TAG_EXCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, USE_IP_NT_RANGE_TAGS)>
<!ELEMENT TAG_INCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_INCLUDE (#PCDATA)>
<!ELEMENT TAG_EXCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_EXCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS (#PCDATA)>
<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ELEMENT USER_ENTERED_IPS (RANGE+)>
<!ELEMENT ELB_DNS (DNS+)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
<!ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>
<!ELEMENT DEFAULT_FLAG (#PCDATA)>


<!ELEMENT SCHEDULE ((DAILY|WEEKLY|MONTHLY), START_DATE_UTC,
```

```
START_HOUR, START_MINUTE, END_AFTER_HOURS?, END_AFTER_MINUTES?,
PAUSE_AFTER_HOURS?, PAUSE_AFTER_MINUTES?, RESUME_IN_DAYS?,
RESUME_IN_HOURS?, NEXTLAUNCH_UTC?, TIME_ZONE, DST_SELECTED,
MAX_OCCURRENCE?)>
<!ELEMENT DAILY EMPTY>
<!ATTLIST DAILY
       frequency_days  CDATA #REQUIRED>

<!-- weekdays is comma-separated list of weekdays e.g. 0,1,4,5 -->
<!ELEMENT WEEKLY EMPTY>
<!ATTLIST WEEKLY
       frequency_weeks  CDATA #REQUIRED
       weekdays   CDATA #REQUIRED>

<!-- either day of month, or (day of week and week of month) must
be provided -->
<!ELEMENT MONTHLY EMPTY>
<!ATTLIST MONTHLY
       frequency_months  CDATA #REQUIRED
       day_of_month  CDATA  #IMPLIED
       day_of_week  (0|1|2|3|4|5|6)  #IMPLIED
       week_of_month  (1|2|3|4|5)  #IMPLIED>

<!-- start date of the task in UTC -->
<!ELEMENT START_DATE_UTC (#PCDATA)>
<!-- User Selected hour -->
<!ELEMENT START_HOUR (#PCDATA)>
<!-- User Selected Minute -->
<!ELEMENT START_MINUTE (#PCDATA)>
<!ELEMENT END_AFTER_HOURS (#PCDATA)>
<!ELEMENT END_AFTER_MINUTES (#PCDATA)>
<!ELEMENT PAUSE_AFTER_HOURS (#PCDATA)>
<!ELEMENT PAUSE_AFTER_MINUTES (#PCDATA)>
<!ELEMENT RESUME_IN_DAYS (#PCDATA)>
<!ELEMENT RESUME_IN_HOURS (#PCDATA)>
<!ELEMENT NEXTLAUNCH_UTC (#PCDATA)>
<!ELEMENT TIME_ZONE (TIME_ZONE_CODE, TIME_ZONE_DETAILS)>


<!-- timezone code like US-CA -->
<!ELEMENT TIME_ZONE_CODE (#PCDATA)>
```

```
<!-- timezone details like (GMT-0800) United States (California):
Los Angeles, Sacramento, San Diego, San Francisco-->
<!ELEMENT TIME_ZONE_DETAILS (#PCDATA)>

<!-- Did user select DST? 0-not selected 1-selected -->
<!ELEMENT DST_SELECTED (#PCDATA)>
<!ELEMENT MAX_OCCURRENCE (#PCDATA)>

<!-- notifications -->
<!ELEMENT NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?,
DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>
```

Create Compliance Scan Schedule

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

[POST]

Create a scan schedule in the user's account.

Input Parameters

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

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

Sample - Create compliance scan schedule

API request:

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

XML output:

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

Sample - Create compliance scan schedule and cancel after 45 minutes

API request:

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

XML output:

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

Sample - Create compliance scan schedule using all scanners in network

API request:

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

XML output:

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

Update Compliance Scan Schedule

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

[POST]

Update a scan schedule in the user's account.

Input Parameters

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

Type	Parameter List
Request	action=update (required)
echo_request={**0**|1}	(Optional) Specify 1 to echo the request's input parameters (names and values) in the XML output. Otherwise parameters are not displayed in the output.
Scan Title	scan_title
id={value}	(Required)The ID of the scan schedule you want to update.
Status	active=0|1
Compliance Profile	option_id or option_title
Scanner Appliance	iscanner_id, iscanner_name, default_scanner, scanners_in_ag, scanners_in_network, scanners_in_tagset
Asset IPs/Groups	ip, asset_group_ids or asset_groups, exclude_ip_per_scan

Type	Parameter List
Asset Tags	target_from=tags, use_ip_nt_range_tags, tag_include_selector, tag_exclude_selector, tag_set_by, tag_set_exclude, tag_set_include
Network	ip_network_id (when the Network Support feature is enabled)
Start Time	Must be specified together: set_start_time=1, start_date, start_hour, start_minute, time_zone_code, observe_dst
recurrence={value}	(Optional) The number of times the scan will be run before it is deactivated. For example, if you set recurrence=2, the scan schedule will be deactivated after it runs 2 times. By default no value is set. A valid value is an integer from 1 to 99.
Daily Scan	Must be specified together: occurrence=daily, frequency_days
Weekly Scan	Must be specified together: occurrence=weekly, frequency_weeks, weekdays
Monthly Scan	Must be specified together: occurrence=monthly, frequency_months, Nth day of month: day_of_month, Day in Nth week: day_of_week, week_of_month
End	end_after, end_after_mins
Pause and Resume	pause_after_hours, pause_after_mins, resume_in_days, resume_in_hours
Notifications	before_notify, before_notify_unit, before_notify_time, before_notify_message, after_notify, after_notify_message, recipient_group_ids

Sample - Update compliance scan schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"http://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/?
action=update&id=57360&option_id=39594"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
```

```
    <RESPONSE>
        <DATETIME>2019-11-19T12:04:44Z</DATETIME>
        <TEXT>Edit scheduled Scan Completed successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>57360</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Delete Compliance Scan Schedule

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

[POST]

Delete a scan schedule in the user's account.

Input Parameters

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

Sample - Delete compliance scan schedule

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-19T12:10:45Z</DATETIME>
```

```
            <TEXT>Schedule scan deleted successfully</TEXT>
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>57360</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Scan List Parameters

Request type

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

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

Parameter	Description
scan_ref={value}	(Optional) Show only a scan with a certain scan reference code. When unspecified, the scan list is not restricted to a certain scan. For a compliance scan the format is: compliance/98765456.12345
scan_id={value}	(Optional) Show only a scan with a certain compliance scan ID.
state={value}	(Optional) Show only one or more scan states. By default, the scan list is not restricted to certain states. A valid value is: Running, Paused, Canceled, Finished, Error, Queued (scan job is waiting to be distributed to scanner(s)), or Loading (scanner(s) are finished and scan results are being loaded onto the platform). Multiple values are comma separated.
processed={0|1}	(Optional) Specify 0 to show only scans that are not processed. Specify 1 to show only scans that have been processed. When not specified, the scan list output is not filtered based on the processed status.

Parameter	Description
type={value}	(Optional) Show only a certain scan type. By default, the scan list is not restricted to a certain scan type. A valid value is: On-Demand, Scheduled, or API.
target={value}	(Optional) Show only one or more target IP addresses. By default, the scan list includes all scans on all IP addresses. Multiple IP addresses and/or ranges may be entered. Multiple entries are comma separated. You may enter an IP address range using the hyphen (-) to separate the start and end IP address, as in: 10.10.10.1-10.10.10.2
user_login={value}	(Optional) Show only a certain user login. The user login identifies a user who launched scans. By default, the scan list is not restricted to scans launched by a particular user. Enter the login name for a valid Qualys user account.
launched_after_datetime={date}	(Optional) Show only scans launched after a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”. When launched_after_datetime and launched_before_datetime are unspecified, the service selects scans launched within the past 30 days. A date/time in the future returns an empty scans list.
launched_before_datetime={date}	(Optional) Show only scans launched before a certain date and time (optional). The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”. When launched_after_datetime and launched_before_datetime are unspecified, the service selects scans launched within the past 30 days. A date/time in the future returns a list of all scans (not limited to scans launched within the past 30 days).
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.

Show/Hide - These parameters specify whether certain information will be shown in the XML output.

Parameter	Description
show_ags={**0**|1}	(Optional) Specify 1 to show asset group information for each scan in the XML output. By default, asset group information is not shown.
show_op={**0**|1}	(Optional) Specify 1 to show option profile information for each scan in the XML output. By default, option profile information is not shown.
show_status={0|**1**}	(Optional) Specify 0 to not show scan status for each scan in the XML output. By default, scan status is shown.
show_last={**0**|1}	(Optional) Specify 1 to show only the most recent scan (which meets all other search filters in the request) in the XML output. By default, all scans are shown in the XML output.
pci_only={**0**|1}	(Optional) Specify 1 to show only external PCI scans in the XML output. When pci_only=1 is specified, the XML output will not include other types of scans run with other option profiles.
ignore_target={**0**|1}	(Optional) Specify 1 to hide target information from the scan list. Specify 0 to display the target information.

Scan Parameters

Input parameters used to launch a scan are below.

Parameter	Description
action={launch}	(Required) Specify “launch” to launch a new scan.
echo_request={**0**|1}	(Optional) Specify 1 to list the input parameters in the XML output. When unspecified, parameters are not listed in the XML output.
scan_title={value}	(Optional) The scan title. This can be a maximum of 2000 characters (ascii).
target_from={**assets**|tags}	(Optional) Specify “assets” (the default) when your scan target will include IP addresses/ranges and/or asset groups. Specify “tags” when your scan target will include asset tags.
ip={value}	(Optional) The IP addresses to be scanned. You may enter individual IP addresses and/or ranges. Multiple entries are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	ip is valid only when target_from=assets is specified.

Parameter	Description
asset_groups={value}	(Optional) The titles of asset groups containing the hosts to be scanned. Multiple titles are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	asset_groups is valid only when target_from=assets is specified. These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.
asset_group_ids={value}	(Optional) The IDs of asset groups containing the hosts to be scanned. Multiple IDs are comma separated. One of these parameters is required: ip, asset_groups or asset_group_ids.
	asset_group_ids is valid only when target_from=assets is specified. These parameters are mutually exclusive and cannot be specified in the same request: asset_groups and asset_group_ids.
exclude_ip_per_scan={value}	(Optional) The IP addresses to be excluded from the scan when the scan target is specified as IP addresses (not asset tags). You may enter individual IP addresses and/or ranges. Multiple entries are comma separated.
	exclude_ip_per_scan is valid only when target_from=assets is specified.
tag_include_selector={all|**any**}	(Optional) Select “any” (the default) to include hosts that match at least one of the selected tags. Select “all” to include hosts that match all of the selected tags.
	tag_include_selector is valid only when target_from=tags is specified.
tag_exclude_selector={all|**any**}	(Optional) Select “any” (the default) to exclude hosts that match at least one of the selected tags. Select “all” to exclude hosts that match all of the selected tags.
	tag_exclude_selector is valid only when target_from=tags is specified.
tag_set_by={**id**|name}	(Optional) Specify “id” (the default) to select a tag set by providing tag IDs. Specify “name” to select a tag set by providing tag names.
	tag_set_by is valid only when target_from=tags is specified.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
	tag_set_include is valid only when target_from=tags is specified.

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

Parameter	Description
scanners_in_ag={**0**|1}	(Optional) Specify 1 to distribute the scan to the target asset groups' scanner appliances. Appliances in each asset group are tasked with scanning the IPs in the group. By default up to 5 appliances per group will be used and this can be configured for your account (please contact your Account Manager or Support). For an Express Lite user, Internal Scanning must be enabled in the user's account.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. scanners_in_ag is valid when the scan target is specified using one of these parameters: asset_groups, asset_group_ids.
scanners_in_tagset={**0**|1}	(Optional) Specify 1 to distribute the scan to scanner appliances that match the asset tags specified for the scan target.
	One of these parameters must be specified in a request for an internal scan: iscanner_name, iscanner_id, default_scanner, scanners_in_ag, scanners_in_tagset. When none of these are specified, External scanners are used. scanners_in_tagset is valid when the target_from=tags is specified.
scanners_in_network={value}	(Optional) Specify 1 to distribute the scan to all scanner appliances in the network.
option_title={value}	(Optional) The title of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
option_id={value}	(Optional) The ID of the option profile to be used.
	One of these parameters must be specified in a request: option_title or option_id. These are mutually exclusive and cannot be specified in the same request.
ip_network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) The ID of a network used to filter the IPs/ranges specified in the"ip" parameter. Set to a custom network ID (note this does not filter IPs/ranges specified in "asset_groups" or "asset_group_ids"). Or set to "0" (the default) for the Global Default Network - this is used to scan hosts outside of your custom networks.

Parameter	Description
runtime_http_header={value}	(Optional) Set a custom value in order to drop defenses (such as logging, IPs, etc) when an authorized scan is being run. The value you enter will be used in the "Qualys-Scan:" header that will be set for many CGI and web application fingerprinting checks. Some discovery and web server fingerprinting checks will not use this header.
client_id={value}	(Optional) Id assigned to the client (Consultant type subscriptions).
client_name={value}	(Optional) Name of the client (Consultant type subscriptions). Note: The client_id and client_name parameters are mutually exclusive and cannot be specified together in the same request.
include_agent_targets={**0**|1}	(Optional) Specify 1 when your scan target includes agent hosts. This lets you scan private IPs where agents are installed when these IPs are not in your PC license. Supported capabilities - This parameter is supported for internal scans using scanner appliance(s). This option is not supported for scans using External scanners. - This parameter is supported when launching on demand scans only. It is not supported for scheduled scans. Parameter iscanner_id or iscanner_name must be specified in the same request.

Scan Schedule Parameters

Scan Schedule - Occurrence

Parameter	Description
occurrence=daily	Required for a daily scan.
frequency_days={value}	Required for a daily scan. The scan will run every N number of days. Value is an integer from 1 to 365.
occurrence=weekly	Required for a weekly scan.
frequency_weeks={value}	Required for a weekly scan. The scan will run every N number of weeks. Value is an integer from 1 to 52.
weekdays={value}	Required for a weekly scan. The scan will run on the one or more weekdays. Value is one or more days: sunday, monday, tuesday, wednesday, thursday, friday, saturday. Multiple days are comma separated.
occurrence=monthly	Required for a monthly scan.

Parameter	Description
frequency_months={value}	Required for a monthly scan. The scan will run every N number of months. Value is an integer from 1 to 12.
day_of_month={value}	Required for monthly scan - Nth day of the month. The scan will run on the Nth day of the month. Value is an integer from 1 to 31.
day_of_week={value}	Required for monthly scan - day in Nth week. The scan will run on this day of the week. Value is and integer from 0 to 6, where 0 is Sunday and 2 is Tuesday.
week_of_month={value}	Required for monthly scan - day in Nth week. The scan will run on this week of the month. Value is one of: first, second, third, fourth, last.

Scan Schedule - Start Time

Parameter	Description
start_date={mm/dd/yyyy}	(Optional) By default the start date is the date when the schedule is created. You can define another start date in mm/dd/yyyy format.
start_hour={hour}	(Required) The hour when a scan will start. The hour is an integer from 0 to 23, where 0 represents 12 AM, 7 represents 7 AM, and 22 represents 10 PM.
start_minute={minute}	(Required) The minute when a scan will start. A valid value is an integer from 0 to 59.
time_zone_code={value}	(Required) The time zone code for starting a scan, in upper case. For example, the time zone code for US California is US-CA. Valid codes are returned by the Time Zone Code API (/msp/time_zone_code_list.php).
observe_dst={yes|**no**}	(Optional) Specify yes to observe Daylight Saving Time (DST). This parameter is valid when the time zone code specified in time_zone_code supports DST.
recurrence={value}	(Optional) The number of times the scan will be run before it is deactivated. For example, if you set recurrence=2, the scan schedule will be deactivated after it runs 2 times. By default no value is set. A valid value is an integer from 1 to 99.
end_after={value}	(Optional) End a scan after some number of hours. A valid value is from 0 to 119.
end_after_mins={value}	(Optional) End a scan after some number of minutes. A valid value is an integer from 0 to 59. Must be specified with end_after. For example, to end the scan after 2 hours and 30 minutes, you would specify end_after=2 and end_after_mins=30.

Parameter	Description
	When end_after is set to 0, the minimum value for end_after_mins is 15.
pause_after_hours={value}	(Optional) Pause a scan after some number of hours if the scan has not finished by then. A valid value is an integer from 0 to 119.
pause_after_mins={value}	(Optional) Pause a scan after some number of minutes if the scan has not finished by then. A valid value is an integer from 0-59.
	Must be specified with pause_after_hours. For example, to pause the scan after 2 hours and 30 minutes, you would specify pause_after_hours=2 and pause_after_mins=30.
	When pause_after_hours is set to 0, the minimum value for pause_after_mins is 15.
resume_in_days={value}	(Optional) Resume a paused scan in some number of days. A valid value is an integer from 0 to 9 or Manually.
resume_in_hours={value}	(Optional) Resume a paused scan in some number of hours. A valid value is an integer from 0-23.
	Must be specified with pause_after_hours and resume_in_days. For example, to resume your scan in 5 hours, specify resume_in_days=0 and resume_in_hours=5. To resume your scan in 1 day and 12 hours, specify resume_in_days=1 and resume_in_hours=12. Note - The value you set for pause will determine the minimum value for resume. For example, if you set the scan to pause after 1 hour then you can set it to resume in 2 or more hours. If you set the scan to pause between 1-2 hours (from 1hr, 1min to 1 hr, 59min) then you can set it to resume in 3 hours or more.
set_start_time={**0**|1}	(Optional for Update only) Specify set_start_time=1 to update any of the start time parameters.
	Must be specified with all start time parameters together: start_date, start_hour, start_minute, time_zone_code, observe_dst

Scan Schedule - Notifications

Parameter	Description
before_notify={0|1}	(Optional) Specify before_notify=1 to send a notification before the scan starts. When not specified during a create request no notification is sent. When not specified during an update request we keep the previous setting.

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

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

Scan Schedule - Consultant type subscriptions

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

Specify Network ID while Creating Virtual Hosts

APIs affected	/api/2.0/fo/asset/vhost/
New or Updated API	Updated
DTD or XSD changes	No

You can now specify the network_id while creating the Virtual Host through API. Network support must be enabled to specify the network_id. If network support is enabled and you do not provide a network_id, then the Default Global Network is considered. You can specify only one network_id.

Input Parameters

Parameter	Description
network_id={value}	(Optional and valid when the networks feature is enabled). The network ID for the record.

Sample - Create New Virtual Host in a Network

Specify network_id to create a virtual host in the specified network.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=create&network_id=5004&ip=10.10.10.20
&port=8080&fqdn=example1.fqdn.com,example2.fqdn.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:27:52Z</DATETIME>
        <TEXT>Virtual host successfully created.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update the Virtual Host in a Network

Specify network_id to identify the virtual host you want to update.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=update&network_id=5004&ip=10.10.10.20
&port=8080&fqdn=example1.fqdn.com,example2.fqdn.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:27:52Z</DATETIME>
        <TEXT>Virtual host successfully updated.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Add FQDNs to the Virtual Host in a Network

Specify network_id to identify the virtual host you want to add FQDNs to.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d
"action=add_fqdn&network_id=5004&ip=10.10.10.20&port=8080&fqdn=exa
mple5.fqdn.com,example6.fqdn.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:38:57Z</DATETIME>
        <TEXT>Virtual host FQDN(s) successfully added.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete FQDNs from the Virtual Host in a Network

Specify network_id to identify the virtual host you want to remove FQDNs from.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d
"action=delete_fqdn&network_id=5004&ip=10.10.10.20&port=8080&fqdn=
example1.fqdn.com,example5.fqdn.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:39:35Z</DATETIME>
        <TEXT>Virtual host FQDN(s) successfully deleted.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Delete the Virtual Host in a Network

Specify network_id to identify the virtual host you want to delete.

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=delete&network_id=5004&ip=10.10.10.20&port=8080"
"https://qualysapi.qualys.com/api/2.0/fo/asset/vhost/"
```

XML output:

```
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-11-22T07:40:09Z</DATETIME>
        <TEXT>Virtual host successfully deleted.</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```

KnowledgeBase API now Supports Edit and Reset Actions for WAS QIDs

APIs affected	/api/2.0/fo/knowledge_base/vuln/
New or Updated API	No
DTD or XSD changes	No

Starting in this release, you can edit and reset WAS QIDs in the same way as other QIDs using the KnowledgeBase API. Managers have permissions to edit a vulnerability, reset a vulnerability.

Input Parameters

You can change the severity level and/or add comments to Threat, Impact or Solution. Providing at least one optional parameter is mandatory.

Parameter	Description
action=edit	(Required) POST method is required
qid={value}	(Required) QID of the vulnerability to be edited.
severity={value}	(Optional) Severity level between 1 to 5. Changing the severity level of a vulnerability impacts how the vulnerability appears in reports and how it is eventually prioritized for remediation. For example, by changing a vulnerability from a severity 2 to a severity 5, remediation tickets for the vulnerability could have a higher priority and shorter deadline for resolution.
disable={**0**|1}	(Optional) Specify 1 to disable the vulnerability. Default is 0. When you disable a vulnerability it is globally filtered out from all hosts in all scan reports. The vulnerability is also filtered from host information, asset search results and your dashboard. You may include disabled vulnerabilities in scan reports by changing report filter settings.
threat_comment	(Optional) Threat comments in plain text.
impact_comment	(Optional) Impact comments in plain text.
solution_comment	(Optional) Solution comments in plain text.

Comments added for Threat, Impact, or Solution are appended to the service-provided descriptions in the vulnerability details.

Edit a WAS vulnerability to raise the vulnerability severity level to 3

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=edit&severity=3&qid=150198"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2019-12-03T08:51:59Z</DATETIME>
        <TEXT>Custom Vuln Data has been updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>qid</KEY>
                <VALUE>150198</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Reset a vulnerability

You can change the vulnerability settings back to original.

Parameter	Description
action=reset	(Required) POST method is required
qid={value}	(Required) QID of the vulnerability to be reset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=reset&qid=150198"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

XML output:

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

```
    <RESPONSE>
        <DATETIME>2019-12-02T08:55:11Z</DATETIME>
        <TEXT>Custom Vuln Data has been reset successfully</TEXT>
    </RESPONSE>
</SIMPLE_RETURN>
```