Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.18

March 16, 2022 (Updated April 12, 2022)

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.

Compliance Policy - Manage Asset Tags using API

APIs affected	/api/2.0/fo/compliance/policy/
New or Updated API	Updated
DTD or XSD changes	No

Starting in this release, you can manage the asset tags assigned to a compliance policy using the API. You can add, remove, and set asset tags for a policy.

Good to Know

- Asset Tagging service must be enabled for your subscription.

- You must have permission to modify the policy you want to update.

Input Parameters

With the new API actions, you can add, remove, and set assets tags for a policy.

The set asset tag action will overwrite the existing asset tags for a policy. The set tag API does not check whether any asset tags are added to the policy and will overwrite the existing asset tags for a policy.

The add asset tag action will check whether the asset tags are already associated with the policy and only add the asset tags that are newly-provided in the API request.

Use the following input parameters to manage asset tags in compliance policies. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
action={value}	(Required) Specify one of the following actions (using POST): - set_asset_tags - Specify this action to overwrite the asset tags for a policy. Any assigned asset tags not specified in the request will be removed from the policy. - add_asset_tags - Specify this action to add asset tags to the policy. When specified, we will check whether the asset tags specified in the request are already associated with the policy and only add the asset tags that are new to the policy. - remove_asset_tags - Specify this action to remove asset tags from the policy. **Note**: With the remove_asset_tags action, you must set either tag_set_include or tag_set_exclude parameter, or both the parameters.

Parameter	Description
id={value}	(Required) Policy ID for the policy you want to update.
evaluate_now={0|1}	(Optional) Specify evaluate_now=1 to immediately evaluate the policy against assigned assets, and select the Evaluate Now check box in the UI Policy Editor. When this check box is selected we'll start policy evaluation each time you save changes to the policy from the UI or API.
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_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_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_include={tag id|name}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={tag id|name}	(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.

Sample Adding Asset Tags

In this sample, we are adding an asset tag to a policy.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=add_as
set_tags"
```

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>2022-01-19T06:35:40Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
```

```
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Removing Asset Tags

In this sample, we are removing an asset tag from a policy.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=remove
_asset_tags"
```

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>2022-01-19T06:35:40Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Setting Asset Tags

In this sample, we are setting asset tags for a policy.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"id=4201701&tag_set_include=118766028&tag_include_selector=all
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=set_as
set_tags"
```

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>2022-01-19T06:28:30Z</DATETIME>
        <TEXT>Compliance Policy successfully modified.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4201701</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

New Parameter in Launch Map API for Network-enabled Subscription

APIs affected	/msp/map-2.php
New or Updated API	Updated
DTD or XSD changes	Yes

The Launch Map API is used to launch a Qualys network map for one or more domains for initiating network discovery.

We added the input parameter **network_id** to the Launch Map API, which allows users to map domains/netblocks in a custom network. This option is only available in subscriptions with the Network Support feature enabled.

Launch Map

The table below shows the new input parameter. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
network_id={value}	(Optional, and valid only when the Network Support feature is enabled for the user's account) Restrict the request to a certain custom network by specifying the network ID. When unspecified, we default to "0" for Global Default Network.

Sample API

In this sample, the user has passed network_id=4234545 as part of the API request for network enabled account.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"map_title=my_map&domain=mydomain.com:10.10.10.10-
10.10.10.20&iscanner_name=my_scanner&option=Initial
Options&network_id=4234545&save_report=yes"
"https://qualysapi.qualys.com/msp/map-2.php"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE MAP_REQUEST SYSTEM "https://qualysapi.qualys.com/map-2.dtd">
<MAP_REQUEST>
<!-- QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ -->
<!-- MAPREF= map/1234567890.12345 -->
<!-- map is running on mydomain.com -->
```

```
<!-- keep-alive -->
.
.

<MAP value="map/1234567890.12345">
<HEADER>
  <KEY value="USERNAME">joe_user</KEY>
  <KEY value="COMPANY"><![CDATA[My Company]]></KEY>
  <KEY value="DATE">2022-02-14T10:41:28Z</KEY>
  <KEY value="TITLE"><![CDATA[my_map]]></KEY>
  <KEY value="TARGET">mydomain.com</KEY>
  <KEY value="NBHOST_TOTAL">2</KEY>
  <KEY value="DURATION">00:06:22</KEY>
  <KEY value="SCAN_HOST">my_scanner(Scanner 12.9.25-1, Vulnerability
  Signatures 2.5.402-2)</KEY>
  <KEY value="REPORT_TYPE">API</KEY>
  <KEY value="STATUS">FINISHED</KEY>
  <KEY value="NETWORK_ID">4234545</KEY>
  <KEY value="OPTIONS"><![CDATA[Information gathering: All Hosts, Perform
  live host sweep, Standard TCP port list, Standard UDP port list, Disable
  DNS traffic, Netblock: 10.10.10.10-10.10.10.20, ICMP Host Discovery]]>
  </KEY>
  <USER_ENTERED_DOMAINS>
        <DOMAIN><![CDATA[mydomain.com]]></DOMAIN>
        <NETBLOCK>
          <RANGE>
            <START>10.10.10.10</START>
            <END>10.10.10.20</END>
          </RANGE>
        </NETBLOCK>
      </USER_ENTERED_DOMAINS>
      <OPTION_PROFILE>
        <OPTION_PROFILE_TITLE option_profile_default="0"><![CDATA[Initial
        Options]]></OPTION_PROFILE_TITLE>
      </OPTION_PROFILE>
    </HEADER>
<IP value="10.10.10.10" network="Custom_network_3" network_id="4234545">
<DISCOVERY method="TCP RST" />
</IP>
<IP value="10.10.10.11" network="Custom_network_3" network_id="4234545">
<DISCOVERY method="TCP RST" />
</IP>
      .
      .
<IP value="10.10.10.20" network="Custom_network_3" network_id="4234545">
      <DISCOVERY method="TCP RST" />
    </IP>
  </MAP>
</MAP_REQUEST>
```

DTD update:

DTD: <platform API server>/map-2.dtd

```
<!-- QUALYS MAP-2 DTD -->
<!ELEMENT MAP_REQUEST (MAP*|ERROR*) >
<!-- value is the report ref -->
<!ELEMENT MAP (HEADER?,(IP+|ERROR)?)>
<!ATTLIST MAP
value CDATA #IMPLIED>
<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>
<!-- INFORMATION ABOUT THE MAP -->
<!ELEMENT HEADER (KEY+, ASSET_GROUPS?, USER_ENTERED_DOMAINS?,
OPTION_PROFILE?)>
<!ELEMENT KEY (#PCDATA)*>
<!ATTLIST KEY
value CDATA #IMPLIED>
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN+, NETBLOCK*)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT NETBLOCK (RANGE+)>
<!ELEMENT RANGE (START+, END+)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
<!ELEMENT OPTION_PROFILE (OPTION_PROFILE_TITLE)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ATTLIST OPTION_PROFILE_TITLE
option_profile_default CDATA #IMPLIED
<!-- value is the IP -->
<!-- type is the kind of server : router, mail server ... -->
<!-- "port" is deprecated, replaced by "discovery" -->
<!ELEMENT IP ((PORT*,DISCOVERY*,LINK*)|LINK+)?>
<!ATTLIST IP
value CDATA #REQUIRED
name CDATA #IMPLIED
type CDATA #IMPLIED
os CDATA #IMPLIED
netbios CDATA #IMPLIED
account CDATA #IMPLIED
network CDATA #IMPLIED
network_id CDATA #IMPLIED>
<!-- value indicates an open port on a server (deprecated) -->
<!ELEMENT PORT (#PCDATA)*>
<!ATTLIST PORT
value CDATA #REQUIRED>
```

```
<!-- value indicates a method that discovered this machine -->
<!ELEMENT DISCOVERY (#PCDATA)*>
<!ATTLIST DISCOVERY
method CDATA #REQUIRED>
<!-- value of a link, indicates the need to go trough a server to see -->
<!-- another (ie. gateway or router) -->
<!ELEMENT LINK EMPTY>
<!ATTLIST LINK
value CDATA #REQUIRED>
```

CSV Header Text Updated in Compliance Policy Reports

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

We made a change to the CSV header text for Control and Host data in custom Compliance Policy Reports.

In Compliance Policy Reports using a custom report template with control statistics enabled, discrepancies were observed in the header information in the CSV format as compared to HTML and PDF formats. In CSV format, control and host data was displayed under the header “Control Summary” and “Host Statistics” respectively; whereas, in PDF and HTML reports, the same data was visible under the header “Control Statistics (Percentage of Hosts Passed per Control)” and “Host Statistics (Percentage of Control Passed per Host)” respectively.

This release makes the header text consistent across all report formats and the header text in CSV reports has been updated to **Control Statistics (Percentage of Hosts Passed per Control)** for control information and **Host Statistics (Percentage of Control Passed per Host)** for host-specific information.

You can download Compliance Policy Reports from the UI or fetch reports using the API. See a sample CSV report below.

Download Policy Report in CSV Format

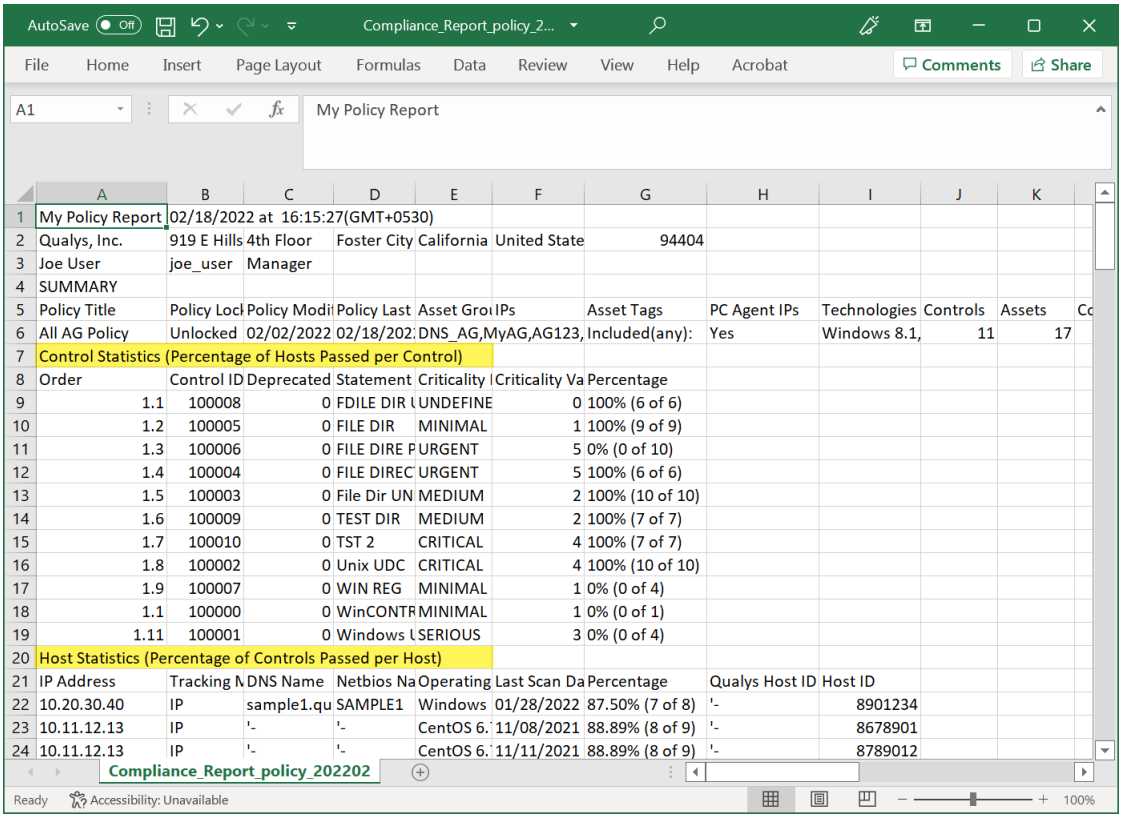
In this sample, we’re downloading a Compliance Policy Report in CSV format. The report includes control statistics. In the output, you’ll see the new header text.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=123456"
```

CSV output:

In the sample CSV policy compliance report, the updated header text is highlighted.



	A	B	C	D	E	F	G	H	I	J	K
1	My Policy Report	02/18/2022 at 16:15:27(GMT+0530)									
2	Qualys, Inc.	919 E Hills	4th Floor	Foster City	California	United State	94404				
3	Joe User	joe_user	Manager								
4	SUMMARY										
5	Policy Title	Policy Locl	Policy Modi	Policy Last	Asset Grou	IPs	Asset Tags	PC Agent IPs	Technologies	Controls	Assets
6	All AG Policy	Unlocked	02/02/2022	02/18/202	DNS_AG,MyAG,AG123,		Included(any):	Yes	Windows 8.1,	11	17
7	Control Statistics (Percentage of Hosts Passed per Control)										
8	Order	Control ID	Deprecated	Statement	Criticality I	Criticality Va	Percentage				
9	1.1	100008	0	FDILE DIR U	UNDEFINE	0	100% (6 of 6)				
10	1.2	100005	0	FILE DIR	MINIMAL	1	100% (9 of 9)				
11	1.3	100006	0	FILE DIRE P	URGENT	5	0% (0 of 10)				
12	1.4	100004	0	FILE DIREC	URGENT	5	100% (6 of 6)				
13	1.5	100003	0	File Dir UN	MEDIUM	2	100% (10 of 10)				
14	1.6	100009	0	TEST DIR	MEDIUM	2	100% (7 of 7)				
15	1.7	100010	0	TST 2	CRITICAL	4	100% (7 of 7)				
16	1.8	100002	0	Unix UDC	CRITICAL	4	100% (10 of 10)				
17	1.9	100007	0	WIN REG	MINIMAL	1	0% (0 of 4)				
18	1.1	100000	0	WinCONTR	MINIMAL	1	0% (0 of 1)				
19	1.11	100001	0	Windows U	SERIOUS	3	0% (0 of 4)				
20	Host Statistics (Percentage of Controls Passed per Host)										
21	IP Address	Tracking N	DNS Name	Netbios Na	Operating	Last Scan Da	Percentage	Qualys Host ID	Host ID		
22	10.20.30.40	IP	sample1.qu	SAMPLE1	Windows	01/28/2022	87.50% (7 of 8)	'-	8901234		
23	10.11.12.13	IP	'-	'-	CentOS 6.	11/08/2021	88.89% (8 of 9)	'-	8678901		
24	10.11.12.13	IP	'-	'-	CentOS 6.	11/11/2021	88.89% (8 of 9)	'-	8789012		

Support for Compressed Reports with PCRS

API affected	/api/2.0/fo/report/
New or Updated APIs	No (affects report output only)
DTD or XSD changes	No

Policy Compliance Reporting Service (PCRS) is a new reporting service to improve performance in Policy Compliance report generation. With PCRS, report generation is enhanced to be more efficient and faster. We are starting by enhancing policy reports in CSV format by automatically compressing large size reports. When you run a policy report in CSV format, the report will be in ZIP format if the report size is between 1 GB and 5 GB; while reports less than 1 GB will be in CSV format. Similar improvements to other report formats will be added soon. You can download reports from the user interface or fetch reports by using APIs.

We had previously announced the introduction of PCRS, and we're now ready to enable PC customers with this service. PCRS will be automatically enabled for PC customers starting in 30 days from the time of this notification. Contact Qualys Support if you do not want this feature to be enabled for your subscription.

See this previous notification: Qualys Cloud Platform (PCRS) API Notification

Download reports from the UI

To download reports from the UI, go to the **Reports** data list, select the report you want to download and click **Download** from the Quick Actions menu. If the policy CSV report size is more than 1 GB, it will be downloaded as a .zip file.

Fetch reports using the API

Important: If you are currently using the Report API to launch and fetch compliance policy reports in CSV format, then it's important to note that once PCRS is enabled for your subscription, any CSV compliance policy report that is over 1GB in size will be compressed automatically and you will get a ZIP file instead of a CSV file. You'll need to update your code or work with your 3rd party vendor to monitor the response header and if the report is compressed, add a step to uncompress the ZIP file before parsing the data.

When fetching a report using the API, the response header will indicate if the report is compressed or not. See the API samples that follow.

- In case of compressed reports, header content-type is - application/zip

- In case of uncompressed reports, header content-type is - text/csv

Sample: Report size more than 1 GB

In this sample, the report being downloaded is more than 1GB in size.

API Request

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

Response Header

You'll notice that the header Content-Type is "application/zip"

```
* About to connect() to qualysapi.xxx.qualys.com port <PORT NUMBER> (#0)
*   Trying xx.xx.x.xxx ...
* Connected to qualysapi.xxx.qualys.com (xx.xx.x.xxx) port <PORT NUMBER>
(#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: CN=*.xxx.qualys.com,OU=Engineering,O="Qualys,
Inc.",L=Foster City,ST=California,C=US
*       start date: Sep 16 09:45:00 2020 GMT
*       expire date: Sep 16 09:45:00 2022 GMT
*       common name: *.xxx.qualys.com
*       issuer: E=xx@qualys.com,CN=Qualys Ops
T2v1,OU=Operations,O="Qualys, Inc.",L=Redwood City,ST=California,C=US
* Server auth using Basic with user '<USER NAME>'
> POST /api/2.0/fo/report/ HTTP/1.1
> Authorization: <AUTHORIZATION TOKEN>
> User-Agent: curl/7.29.0
> Host: qualysapi.xxx.qualys.com
> Accept: */*
> X-Requested-With:curl demo2
> Content-Length: 22
> Content-Type: application/x-www-form-urlencoded
>
} [data not shown]
* upload completely sent off: 22 out of 22 bytes
< HTTP/1.1 200 OK
< Date: Thu, 07 Oct 2021 11:15:03 GMT
< Server: Qualys
```

```
< Strict-Transport-Security: max-age=63072000;
< X-XSS-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< X-RateLimit-Limit: 300
< X-RateLimit-Window-Sec: 3600
< X-Concurrency-Limit-Limit: 2
< X-Concurrency-Limit-Running: 0
< X-RateLimit-ToWait-Sec: 0
< X-RateLimit-Remaining: 297
< Content-Length: 221540169
< Connection: keep-alive
< Content-Disposition: attachment; filename=<FILENAME>.zip
< Content-Type: application/zip
```

Sample: Report size less than 1 GB

In this sample, the report being downloaded is less than 1GB in size.

API Request

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

Response Header

You'll notice that the header Content-Type is "text/csv;charset=UTF-8"

```
* About to connect() to qualysapi.xxx.qualys.com port <PORT NUMBER> (#0)
*   Trying xx.xx.x.xxx...
* Connected to qualysapi.xxx.qualys.com (xx.xx.x.xxx) port <PORT NUMBER>
(#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* skipping SSL peer certificate verification
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* Server certificate:
*       subject: CN=*.xxx.qualys.com,OU=Engineering,O="Qualys,
Inc.",L=Foster City,ST=California,C=US
*       start date: Sep 16 09:45:00 2020 GMT
*       expire date: Sep 16 09:45:00 2022 GMT
*       common name: *.xxx.qualys.com
*       issuer: E=xx@qualys.com,CN=Qualys Ops
T2v1,OU=Operations,O="Qualys, Inc.",L=Redwood City,ST=California,C=US
* Server auth using Basic with user '<user name>'
> POST /api/2.0/fo/report/ HTTP/1.1
> Authorization: <AUTHORIZATION TOKEN>
> User-Agent: curl/7.29.0
> Host: qualysapi.xxx.qualys.com
```

```
> Accept: */*
> X-Requested-With:curl demo2
> Content-Length: 22
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 22 out of 22 bytes
< HTTP/1.1 200 OK
< Date: Thu, 07 Oct 2021 11:16:21 GMT
< Server: Qualys
< Strict-Transport-Security: max-age=63072000;
< X-XSS-Protection: 1; mode=block
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< X-RateLimit-Limit: 300
< X-RateLimit-Window-Sec: 3600
< X-Concurrency-Limit-Limit: 2
< X-Concurrency-Limit-Running: 0
< X-RateLimit-ToWait-Sec: 0
< X-RateLimit-Remaining: 296
< Content-Length: 294850
< Connection: keep-alive
< Content-Disposition: attachment;
filename=Compliance_Report_PCRA_326___xxx.csv
< Content-Type: text/csv;charset=UTF-8
```

Issues Addressed

- Now you'll get an appropriate error message when updating a host in a custom network using the API and the host_id specified does not belong to the network_id specified or the network_id was not specified.
- We fixed an issue where the Update Schedule Scan API incorrectly returned an error message in the API response stating that a virtual or physical scanner is needed to scan private IPs. Now users can scan private and non-internal IPs in same scan job with virtual/physical scanner.
- We fixed an issue where the user could not create a Windows authentication record with the same IP present in a different network via API. Now users can create a Windows record if the IP is in a different network. An error for the duplicate network is displayed if a user tries to create a Windows record in the same network with the same IP.
- When the customer was using asset tags-related parameters in the Posture API call, the posture data was not getting filtered properly.
- Improved UI and API validation error messages and documentation to explain that if the Network Support feature is enabled for your subscription, then authentication records for application technologies must have the same network selection as the corresponding Unix/Windows authentication record for the host running the application.
- We fixed an issue for AGMS-enabled subscriptions so users will now get the correct assigned asset group list returned from the User List API (/msp/user_list.php).