Qualys API

Network Support

July 14, 2017

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
1 (650) 801 6100

CONTENTS

About this guide

Welcome to the Qualys API. In this guide we'll describe the Network Support feature, first available with Qualys 7.13, using the Qualys API and how to deploy networks using your Qualys subscription.

Note the Network Support feature must be enabled in your account to use this feature and the API capabilities described in this guide. Your account must be configured with the API access permission.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,200 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

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

1

Get Started

We are pleased to introduce the new Network Support feature for Qualys Vulnerability Management (VM). Using this feature you can scan different networks that are configured with the same IP addresses/ranges.

Network Support must be enabled for your subscription in order for you to use this feature. Don't know if it's turned on? Just log into your account and go to VM > Assets. If you see the Networks tab (next to Domains) then it's turned on.

Good to know

- The Global Default Network, provided by Qualys, is used to scan assets that do not belong to custom networks.

- Initially, once we turn on Network Support for your account, scan configurations will be assigned to the Global Default Network. You can change the network for an appliance and schedule (UI only at this time) but not for an asset group.

Tell me the steps

It's easy to complete your first network scan. There's just a couple steps.

1) Set Up a Network - You'll need to give it a friendly name and assign it one or more scanner appliances. These appliances will be used to scan the IP addresses in the network. Tip - Each scanner appliance can be included in only 1 network. Learn more

2) Organize Assets by Network - This step is recommended. Create a new asset group, assign it to a network and add assets (IP addresses, domains) to it. Learn more

3) Launch Scans and Reports - You can launch a scan on a single network. Launching a report does not have this restriction. You can launch a report on multiple networks. Learn more

New APIs and updates to existing ones

The new Network Support API consists of new Qualys APIs (for creating networks and assigning scanner appliances to them), and updates to existing APIs (for managing asset groups, host assets and launching scans and reports).

Important! This document describes features and functionality available when the Network Support feature is turned on for your account. There are several changes to XML output and existing DTDs as indicated. These changes are visible when you have Network Support turned on.

In this guide you'll find Network API documentation for new and existing APIs. You'll want to refer to these user guides for all the details on existing APIs: Qualys API User Guide v1 and Qualys API User Guide v2.

Looking for the latest API user guides? You can find them at our Community here (https://community.qualys.com/community/developer)

Samples in this guide

Qualys maintains multiple Qualys Cloud Platforms. This guide includes many samples assuming your account is on Qualys US Platform 1 (https://qualysapi.qualys.com). If your account is located on another platform, please replace the server URL with the one for your account.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys EU Platform	https://qualysapi.qualys.eu
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

Get API notifications

We recommend you join our Community and subscribe to our API notifications so you'll get email notifications telling you about important upcoming API enhancements and changes.

From the Qualys Community

Join our Community

Subscribe to API Notifications (select Receive email notifications)

2

Set Up Networks

Using the Qualys API you can set up custom networks and assign scanner appliances to them. Each network must have at least 1 scanner appliance assigned. This appliance will be used to scan the IP addresses in the network.

Tip - As always be sure the scanner appliances will be able to phone home to the Qualys Cloud Platform and also will be able to access the IP addresses that you will be scanning.

Good to know

Once you've added a custom network you can start scanning right away - all IPs are available for scanning. We recommend you take a moment to associate assets with your network by creating asset groups.

Learn more

Create Network API v2

Update Network API v2

Network List API v2

Scanner Appliance - Assign to Network API v2

Scanner Appliance List API v2

Create Network API v2

Tell me about this API

The new Create Network API v2 (resource /api/2.0/fo/network/ with parameter action=create) is used to create a new network. The input parameter "name" (required) is a user-defined friendly name. A successful request will return a unique network ID and this is used to manage your network using the API.

Supported methods	POST
Permissions	This API is available to Managers only

Next steps

Before you're ready to start scanning, you'll need to 1) assign scanner appliance(s) to your network, and 2) add host assets to your network (assign asset groups to it).

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&name=My+Network"
"https://qualysapi.qualys.com/api/2.0/fo/network/"
```

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>2014-01-14T04:37:24Z</DATETIME>
    <TEXT>Network created with ID</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>id</KEY>
        <VALUE>1103</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update Network API v2

Tell me about this API

The new Update Network API v2 (resource /api/2.0/fo/network/ with parameter action=update) is used to change the name for a network. Use the "name" parameter to specify a new network name. (The network ID is assigned by our service and it can't be changed.)

Supported methods	POST
Permissions	This API is available to Managers only

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"id=1130&action=update&name=Network+123"
"https://qualysapi.qualys.com/api/2.0/fo/network/"
```

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>2014-01-20T06:17:06Z</DATETIME>
    <TEXT>Network updated</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>id</KEY>
        <VALUE>1103</VALUE>
      </ITEM>
      <ITEM>
        <KEY>name</KEY>
        <VALUE>Network 123</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Network List API v2

Tell me about this API

Use the new Network List API v2 (resource /api/2.0/fo/network/ with parameter action=list) to list custom networks in your account. The optional "ids" input parameter can be used to filter the list.

Supported methods	GET and POST
Permissions	This API is available to all users with the API access permission. A Manager will view all custom networks in the subscription, a Unit Manager will view custom networks in their business unit's assigned asset groups, and a Scanner/Reader will view custom networks in their account's assigned asset groups.

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/network/?action=list&ids=
7343,7345,7350"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NETWORK_LIST SYSTEM
"https://qualysapi.qualys.com/network_list_output.dtd">
<RESPONSE>
  <DATETIME>2013-07-28T01:06:45Z</DATETIME>
  <NETWORK_LIST>
    <NETWORK>
      <ID>7343</ID>
      <NAME><![CDATA[My New Network]]></TITLE>
      <SCANNER_APPLIANCE_LIST>
        <SCANNER_APPLIANCE>
          <ID>1234</ID>
          <FRIENDLY_NAME><![[CDATA[abc123]]></FRIENDLY_NAME>
        </SCANNER_APPLIANCE>
      </SCANNER_APPLIANCE_LIST>
    </NETWORK>
    ...
  </NETWORK_LIST>
```

```
</RESPONSE>
```

New DTD:

```
<!-- QUALYS NETWORK_LIST_OUTPUT DTD -->
<!ELEMENT NETWORK_LIST_OUTPUT (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
                   POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, NETWORK_LIST?)>
<!ELEMENT NETWORK_LIST (NETWORK+)>
<!ELEMENT NETWORK (ID, NAME, SCANNER_APPLIANCE_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME  (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCE_LIST (SCANNER_APPLIANCE+)>
<!ELEMENT SCANNER_APPLIANCE (ID, FRIENDLY_NAME)>
<!ELEMENT FRIENDLY_NAME (#PCDATA)>
<!-- EOF -->
```

Scanner Appliance - Assign to Network API v2

Tell me about this API

The new Assign Scanner Appliance to Network API v2 (resource /api/2.0/fo/appliance/ with parameter action=assign_network_id) is used to assign a scanner appliance to a network. When the network support feature is enabled for your subscription, scanner appliances are assigned to networks. Each appliance can be assigned to 1 network only.

Supported methods	POST
Permissions	This API is available to Managers only
Required input parameters	action=assign_network_id appliance_id={id} network_id={id}

Sample

API request:

```
curl -k -u "USERNAME:PASSWORD" -H "X-Requested-With: test" -d
action=assign_network_id&appliance_id=506&network_id=1002"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

The response will look like this, if successful:

```
<?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>2013-12-16T22:50:49Z</DATETIME>
    <TEXT>Success: Network ID=[1103] assigned to Appliance with
ID=[506]</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Or, if unsuccessful, the response might look like this:

```
<?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>2013-12-16T22:53:41Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT>parameter network_id has invalid value: 1103 (No such
network ID)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Scanner Appliance List API v2

Tell me about this API

The Scanner Appliance List API v2 (resource /api/2.0/fo/appliance/ with action=list) returns scanner appliances in your account. For details on this API, see the Qualys API User Guide v2.

With network support

Use the new optional input parameter "network_id" to return a list of scanner appliances for a certain network. Specify 0 for the Global Default Network or a custom network ID.

The XML output now identifies the network ID for each scanner appliance when the subscription has at least 1 network defined. A new NETWORK_ID element was added to the appliances list XML output (appliance_list_output.dtd). This identifies the appliance's network (an appliance can be assigned to 1 network).

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/?action=list&ne
twork_id=1002"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_list_
output.dtd">
<APPLIANCE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2013-12-16T20:40:58Z</DATETIME>
    <APPLIANCE_LIST>
      <APPLIANCE>
        <ID>506</ID>
        <NAME>vs_acme_123</NAME>
        <NETWORK_ID>1002</NETWORK_ID>
        <SOFTWARE_VERSION>2.6</SOFTWARE_VERSION>
        <RUNNING_SCAN_COUNT>0</RUNNING_SCAN_COUNT>
        <STATUS>Offline</STATUS>
      </APPLIANCE>
      ...
```

```
    </APPLIANCE_LIST>
  </RESPONSE>
</APPLIANCE_LIST_OUTPUT>
```

DTD update:

New NETWORK_ID subelement for each APPLIANCE element.

```
<!ELEMENT APPLIANCE (ID, NAME, NETWORK_ID?, SOFTWARE_VERSION,
                     RUNNING_SCAN_COUNT, STATUS, MODEL_NUMBER?,
                    SERIAL_NUMBER?, ACTIVATION_CODE?,
                    INTERFACE_SETTINGS*, PROXY_SETTINGS?, VLANS?,
                    STATIC_ROUTES?, ML_LATEST?, ML_VERSION?,
                    VULNSIGS_LATEST?, VULNSIGS_VERSION?,
                    ASSET_GROUP_COUNT?, ASSET_GROUP_LIST?,
                    LAST_UPDATED_DATE?, POLLING_INTERVAL?,
                    USER_LOGIN?, HEARTBEATS_MISSED?,
                    SS_CONNECTION?, SS_LAST_CONNECTED?,
                    FDCC_ENABLED?, USER_LIST?, UPDATED?,
                    COMMENTS?, RUNNING_SCANS?)>
...
<!ELEMENT NETWORK_ID  (#PCDATA)>
...
```

3

Organize Assets by Network

The Qualys API allows you to organize assets by network by creating asset group(s) and assigning them to your network using 1 API call. The IP addresses and domains you assign to each asset group should belong to 1 network.

Tip - The IPs/domains in your account can still be assigned to multiple asset groups.

Good to know

- Each asset group can be assigned to only 1 network.

- Once you've created an asset group, you can't change its network assignment.

Learn more

Add Asset Group API v1

Asset Group List API v1

Add Asset Group API v1

Tell me about this API

The Add Asset Group API v2 (/msp/asset_group.php/?action=add) is used to add new asset groups to your account. For details on this API, see the Qualys API User Guide v1.

With network support

The new “network_id” parameter is used to assign a new asset group to a custom network. By default the Global Default Network is assigned. This parameter can be specified only when creating a new asset group (action=add), and it is invalid when editing an existing group (action=edit).

Sample

API request:

```
curl -u “USERNAME:PASSWORD” -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/msp/asset_group.php?action=add&title
=My_Assets&network_id=1001"
```

XML output:

Uses the simple return XML (simple_return.dtd). There were no changes made to the XML output.

Asset Group List API v1

Tell me about this API

The Asset Group List API v1 (/msp/asset_group_list.php) is used to retrieve a list of asset groups in your account. For details on this API, see the Qualys API User Guide v1.

With network support

We updated the XML output (asset_group_list.dtd). There's new elements and a new attribute.

/ASSET_GROUP_LIST/ASSET_GROUP/NETWORK_ID	
	(New element) A user-configured asset group can be assigned to 1 network. For this type of asset group, you'll see the <NETWORK_ID> element set to a single custom network ID or 0 for the Global Default Network.
/ASSET_GROUP_LIST/ASSET_GROUP/NETWORK_IDS	
	(New element) The All asset group can be assigned to multiple custom networks. For the asset group All you'll see the <NETWORK_IDS> element showing a comma separated list of custom network IDs in your account. (This element does not appear in a case where there are no custom networks with assigned assets.)
/ASSET_GROUP_LIST/ASSET_GROUP/SCANIPS/IP attribute=network_id	
	(New attribute) The new attribute "network_id" appears for an All asset group that is not the same as the subscription's All asset group.
/ASSET_GROUP_LIST/ASSET_GROUP/MAPDOMAINS/DOMAIN attribute=network_id	
	(New attribute) The new attribute "network_id" appears for an All asset group that is not the same as the subscription's All asset group.

Have multiple All asset groups? Yes you might. There is always 1 All asset group for the subscription - this includes all assets, visible to Managers. If you have business units, there is 1 unique All asset group for each business unit. If you have Scanners and/or Readers, there is 1 unique All asset group for each Scanner/Reader account. (There is no All asset group for a network.)

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/msp/asset_group_list.php"
```

XML output 1:

This shows XML output returned in a case where the All asset group is the All asset group for the subscription.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_GROUP_LIST SYSTEM
"https://qualysapi.qualys.com/asset_group_list.dtd">
<ASSET_GROUP_LIST>
  <ASSET_GROUP>
    <ID>7343</ID>
    <TITLE><![CDATA[New shiny group]]></TITLE>
    <SCANIPS>
      <IP>5.5.5.7</IP>
      <IP>10.10.10.1-10.10.10.254</IP>
    </SCANIPS>
    <MAPDOMAINS>
      <DOMAIN netblock="">qualys-test.com</DOMAIN>
    </MAPDOMAINS>
    <NETWORK_ID>123</NETWORK_ID>
    <BUSINESS_IMPACT>
      <RANK>3</RANK>
      <IMPACT_TITLE><![CDATA[Medium]]></IMPACT_TITLE>
    </BUSINESS_IMPACT>
    <CVSS_ENVIRO_CDP><![CDATA[None]]></CVSS_ENVIRO_CDP>
    <CVSS_ENVIRO_TD><![CDATA[None]]></CVSS_ENVIRO_TD>
    <CVSS_ENVIRO_CR><![CDATA[Invalid Data]]></CVSS_ENVIRO_CR>
    <CVSS_ENVIRO_IR><![CDATA[Invalid Data]]></CVSS_ENVIRO_IR>
    <CVSS_ENVIRO_AR><![CDATA[Invalid Data]]></CVSS_ENVIRO_AR>
    <ASSIGNED_USERS>
      <ASSIGNED_USER>
        <LOGIN><![CDATA[acme_er]]></LOGIN>
        <FIRSTNAME><![CDATA[Joe]]></FIRSTNAME>
        <LASTNAME><![CDATA[Smith]]></LASTNAME>
        <ROLE><![CDATA[Unit Manager]]></ROLE>
      </ASSIGNED_USER>
    </ASSIGNED_USERS>
```

```
  </ASSET_GROUP>
  ...
  <ASSET_GROUP>
    <ID>3107</ID>
    <TITLE><![CDATA[All]]></TITLE>
    <SCANIPS>
      <IP>5.5.5.6-5.5.5.9</IP>
      <IP>6.6.6.6-6.6.6.7</IP>
      <IP>6.6.6.10</IP>
      <IP>6.6.6.20-6.6.6.30</IP>
      <IP>10.0.0.0-10.255.255.255</IP>
    </SCANIPS>
    <MAPDOMAINS>
      <DOMAIN netblock="">qualys-test.com</DOMAIN>
      <DOMAIN netblock="10.0.0.1-10.0.0.255">none</DOMAIN>
      <DOMAIN netblock="10.1.0.0-10.1.0.255">none.com</DOMAIN>
      <DOMAIN netblock="10.1.1.0-10.1.1.255">none1.com</DOMAIN>
    </MAPDOMAINS>
    <NETWORK_IDS>0,7343</NETWORK_IDS>
    <BUSINESS_IMPACT>
      <RANK>4</RANK>
      <IMPACT_TITLE><![CDATA[High]]></IMPACT_TITLE>
    </BUSINESS_IMPACT>
    <CVSS_ENVIRO_CDP><![CDATA[None]]></CVSS_ENVIRO_CDP>
    <CVSS_ENVIRO_TD><![CDATA[None]]></CVSS_ENVIRO_TD>
    <CVSS_ENVIRO_CR><![CDATA[Invalid Data]]></CVSS_ENVIRO_CR>
    <CVSS_ENVIRO_IR><![CDATA[Invalid Data]]></CVSS_ENVIRO_IR>
    <CVSS_ENVIRO_AR><![CDATA[Invalid Data]]></CVSS_ENVIRO_AR>
  </ASSET_GROUP>
</ASSET_GROUP_LIST>
```

XML output 2:

Sample XML output showing an All asset group that is not the subscription's All asset group. You'll see the "network_id" parameter for the subelementS /SCANIPS/IP and /MAPDOMAINS/DOMAIN.

```
...
<ASSET_GROUP>
  <ID>5010</ID>
  <TITLE><![CDATA[All]]></TITLE>
  <SCANIPS>
    <IP network_id="0"> 10.0.0.0-10.10.10.11</IP>
```

```
    <IP network_id="0"> 10.10.10.13-10.10.10.247</IP>
    <IP network_id="1193"> 10.0.0.0-10.10.10.11</IP>
    <IP network_id="1193"> 10.10.10.13-10.10.10.247</IP>
...
  <MAPDOMAINS>
    <DOMAIN network_id="0">qualys-test.com</DOMAIN>
    <DOMAIN netblock="10.10.10.10, 10.10.10.17"
network_id="0">qualys-test2.com</DOMAIN>
    <DOMAIN network_id="1193">qualys-test.com</DOMAIN>
  </MAPDOMAINS>
...
```

DTD updates:

We added new ASSET_GROUP subelement (NETWORK_ID|NETWORK_IDS) after SCANNER_APPLIANCES. Also we added optional "network_id" attribute to the IP subelement.

```
<!ELEMENT ASSET_GROUP (ID, TITLE, SCANIPS?, SCANDNS?,
                       SCANNETBIOS?, MAPDOMAINS?,
                       SCANNER_APPLIANCES?,
                       (NETWORK_ID|NETWORK_IDS)?, COMMENTS?,
                       BUSINESS_IMPACT, DIVISION?, FUNCTION?,
                       LOCATION?, CVSS_ENVIRO_CDP?,
                       CVSS_ENVIRO_TD?, CVSS_ENVIRO_CR?,
                       CVSS_ENVIRO_IR?, CVSS_ENVIRO_AR?,
                       LAST_UPDATE, ASSIGNED_USERS?)>
...
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA "0">
...
<!ATTLIST DOMAIN
          netblock CDATA #IMPLIED
          network_id CDATA "0"
...
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT NETWORK_IDS (#PCDATA)>
```

4

Scanning and Reporting

Using the Qualys API you can launch a scan on a single network. Unlike a scan, you can launch a report on multiple networks.

Good to know

- For a scan the Global Default Network is selected by default, when “ip_network_id” is not specified as part of the request.

- Target hosts may include a mix of IP addresses and/or asset groups. This applies to scans and reports.

Learn more

Launch Vulnerability Scan API v2

Scan Authentication Records List API v2

Scan IPv6 Mappings List API v2

Scan Authentication Records List API v2

Launch Vulnerability Scan API v2

Tell me about this API

The Launch Vulnerability Scan API v1 (resource /api/2.0/fo/scan/ with parameter action=launch) is used to launch a vulnerability scan on hosts in your account. For details on this API, see the Qualys API User Guide v2.

With network support

You can launch a new scan on 1 network. By default the Global Default Network is selected. Use the new "ip_network_id" parameter to select another network. (You can specify the Global Default Network using "ip_network_id=0".)

Good to know

For the scan target you must select hosts that are accessible to the selected network (the "ip_network_id" value).

- IP addresses in the "ip" parameter must be accessible to the selected network (the "ip_network_id" value).

- Asset groups in "asset_groups" and/or "asset_group_ids" are not filtered based on the selected network (the "ip_network_id" value).

- The scan target cannot include the All asset group (asset_groups=All), if your account has custom network(s).

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=launch&option_id=12345&ip=10.10.10.13-10.10.10.18&ip_netwo
rk_id=1001" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

Uses the simple return XML (simple_return.dtd). No changes made to the XML.

```
<?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>2014-01-18T14:21:08Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
```

```
        <KEY>ID</KEY>
        <VALUE>3382361</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1390054867.82361</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Scan Authentication Records List API v2

The Authentication Record List by Type API v2 (resource /api/2.0/fo/auth/<type>/ with action=list) is used to view a list of authentication records visible to the user for a specific authentication type (Unix, VMware, Windows etc).

The XML output now identifies the network ID for each record when the user's account has more than 1 network. We added a new NETWORK_ID subelement for AUTH_<type> subelements (like AUTH_UNIX, AUTH_WINDOWS, AUTH_VMWARE, etc). 12 DTDs were updated.

XML output (Unix Record List):

```
<AUTH_UNIX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-03-27T13:32:17Z</DATETIME>
    <AUTH_UNIX_LIST>
      <AUTH_UNIX>
        <ID>678</ID>
        <TITLE><![CDATA[My Unix Record]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <ROOT_TOOL>Sudo</ROOT_TOOL>
        <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
        <IP_SET>
          <IP_RANGE>10.10.10.168-10.10.10.195</IP_RANGE>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
            <DATETIME>2014-02-20T01:01:01</DATETIME>
            <BY>username</BY>
        </CREATED>
...
```

1) DTD update - Unix Record List

<baseurl>/api/2.0/fo/auth/unix/auth_unix_list_output.dtd

```
...
<!ELEMENT AUTH_UNIX (ID, TITLE, USERNAME, CLEARTEXT_PASSWORD,
ROOT_TOOL, RSA_PRIVATE_KEY?, DSA_PRIVATE_KEY?, PORT?, IP_SET,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?,
USE_AGENTLESS_TRACKING?, AGENTLESS_TRACKING_PATH?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
```

```
...
```

2) DTD update - Windows Record List

<baseurl>/api/2.0/fo/auth/windows/auth_windows_list_output.dtd

```
...
<!ELEMENT AUTH_WINDOWS (ID, TITLE, USERNAME, NTLM?,
WINDOWS_DOMAIN?, WINDOWS_AD_DOMAIN?, WINDOWS_AD_TRUST?, IP_SET?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?,
USE_AGENTLESS_TRACKING?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

3) DTD update - VMware Record List

<baseurl>/api/2.0/fo/auth/vmware/auth_vmware_list_output.dtd

```
...
<!ELEMENT AUTH_VMWARE (ID, TITLE, USERNAME, PORT, SSL_VERIFY,
HOSTS?, IP_SET, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
..
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

4) DTD update - SNMP Record List

<baseurl>/api/2.0/fo/auth/snmp/auth_snmp_list_output.dtd

```
...
<!ELEMENT AUTH_SNMP (ID, TITLE, USERNAME?, AUTH_ALG?, PRIV_ALG?,
SEC_ENG?, CONTEXT_ENG?, CONTEXT?, COMMUNITY_STRINGS?, VERSION,
IP_SET, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

5) DTD update - Oracle Record List

<baseurl>/api/2.0/fo/auth/oracle/auth_oracle_list_output.dtd

```
...
<!ELEMENT AUTH_ORACLE (ID, TITLE, USERNAME, (SID|SERVICENAME),
PORT, IP_SET, PC_ONLY?, WINDOWS_OS_CHECKS, WINDOWS_OS_OPTIONS?,
UNIX_OPATCH_CHECKS, UNIX_OS_CHECKS, UNIX_OS_OPTIONS?, NETWORK_ID?,
```

```
CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

6) Oracle Listener Record List

<baseurl>/api/2.0/fo/auth/oracle_listener/auth_oracle_listener_list_output.dtd

```
...
<!ELEMENT AUTH_ORACLE_LISTENER (ID, TITLE, IP_SET, NETWORK_ID?,
CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

7) MS SQL Record List

<baseurl>/api/2.0/fo/auth/ms_sql/auth_ms_sql_list_output.dtd

```
...
<!ELEMENT AUTH_MS_SQL (ID, TITLE, USERNAME, (INSTANCE |
AUTO_DISCOVER_INSTANCES), (DATABASE | AUTO_DISCOVER_DATABASES),
(PORT|AUTO_DISCOVER_PORTS), DB_LOCAL, WINDOWS_DOMAIN?, IP_SET,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

8) MS IIS Server Record List

<baseurl>/api/2.0/fo/auth/ms_iis/auth_ms_iis_list_output.dtd

```
...
<!ELEMENT AUTH_MS_IIS (ID, TITLE, IP_SET, NETWORK_ID?, CREATED,
LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

9) IBM WebSphere Record List

<baseurl>/api/2.0/fo/auth/ibm_websphere/auth_ibm_websphere_list_output.dtd

```
...
<!ELEMENT AUTH_IBM_WEBSPHERE (ID, TITLE, IP_SET,
UNIX_INSTLLATION_DIRECTORY, NETWORK_ID?, CREATED, LAST_MODIFIED,
COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

10) IBM DB2 Record List

<baseurl>/api/2.0/fo/auth/ibm_db2/auth_ibm_db2_list_output.dtd

```
...
<!ELEMENT AUTH_IBM_DB2 (ID, TITLE, USERNAME, DATABASE, PORT,
IP_SET, PC_ONLY?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

11) HTTP Record List

<baseurl>/api/2.0/fo/auth/http/auth_http_list_output.dtd

```
...
<!ELEMENT AUTH_HTTP (ID, TITLE, USERNAME, SSL, (REALM|VHOST),
IP_SET?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

12) Apache Web Server Record List

<baseurl>/api/2.0/fo/auth/apache/auth_apache_list_output.dtd

```
...
<!ELEMENT AUTH_APACHE (ID, TITLE, IP_SET, UNIX_CONFIGURATION_FILE,
UNIX_CONTROL_COMMAND, NETWORK_ID?, CREATED, LAST_MODIFIED,
COMMENTS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

Scan IPv6 Mappings List API v2

The IPv6 List API v2 (resource /api/2.0/fo/asset/ip/v4_v6/ with action=list) is used to view a list of IPv6 mapping records in your account. The XML output now identifies the network ID for each IPv6 mapping when the user's account has more than 1 network. We added a new NETWORK_ID element to the XML output (ip_map_list_output.dtd).

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_MAP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/v4_v6/ip_map_lis
t_output.dtd">
<IP_MAP_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2014-03-27T19:42:10Z</DATETIME>
   <IP_MAP_LIST>
     <IP_MAP>
       <ID>46947</ID>
       <V4>0.0.0.7</V4>
       <V6>2001:db8:85a3::8a2e:370:84</V6>
       <NETWORK_ID>1234</NETWORK_ID>
     </IP_MAP>
     <IP_MAP>
       <ID>47036</ID>
       <V4>0.0.0.1</V4>
       <V6>2001:db8:85a3::8a2e:370:77</V6>
       <NETWORK_ID>0</NETWORK_ID>
     </IP_MAP>
   </IP_MAP_LIST>
 </RESPONSE>
</IP_MAP_LIST_OUTPUT>
```

DTD update:

New NETWORK_ID subelement added for the subelement /IP_MAP.

```
...
<!ELEMENT RESPONSE (DATETIME, IP_MAP_LIST?, WARNING?)>

<!ELEMENT IP_MAP_LIST (IP_MAP+)>
<!ELEMENT IP_MAP (ID, V4, V6, NETWORK_ID?)>
<!ELEMENT ID (#PCDATA)>
```

```
<!ELEMENT V4 (#PCDATA)>
<!ELEMENT V6 (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
```

Launch Report API v2

Tell me about this API

The Launch Report API v2 (resource /api/2.0/fo/report/ with parameter action=launch) is used to launch a report. This API is available when the report share feature must be enabled for your subscription. For details on this API, see the Qualys API User Guide v2.

With network support

The optional "ips_network_id" input parameter allows you to restrict the report's target to the IP addresses specified in the "ips" parameter ("ips_network_id" is valid only when "ips" is specified for the same request).

The "ip_restriction" parameter can be used to specify certain IP addresses/ranges to include in scan and map reports. (This option was available in previous releases.)

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=launch&report_type=Scan&ips=10.10.10.10-10.10.10.13&asset_
group_ids=3456,6789&ips_network_id=1001&template_id=1234&output_fo
rmat=csv" "https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

Uses the simple return XML (simple_return.dtd). No changes were made to the XML.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE GENERIC SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2014-01-13T21:45:23Z</DATETIME>
    <TEXT>New report launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1665</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

5

Asset Inventory

Asset API functions return XML output showing the network that each host belongs to. The input parameter “network_ids” can be used to list hosts that are associated with a single network, and to purge hosts that are associated with a network.

Good to know

- Network information is returned once hosts have been scanned.

Learn more

Host Asset List API v2

Host Asset Purge API v2

Host Detection List API v2

IP List API v2

Excluded IP List API v2

Excluded IP Change History API v2

Host Asset List API v2

Tell me about this API

The Host Asset List API v2 (/api/2.0/fo/asset/host/) is used to retrieve a list of host assets in your account. For details on this API, see the Qualys API User Guide v2.

With network support

The new "network_ids" parameter is used to restrict the action of the request to selected custom network IDs.

The XML output now identifies the network ID for each host. A new NETWORK_ID element was added to the host list XML output (host_list_output.dtd).

Sample

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/host_list_outp
ut.dtd">
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-01-06T19:43:46Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>33601</ID>
        <IP>10.10.10.161</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <NETWORK_ID>0</NETWORK_ID>
      </HOST>
...
      <HOST>
        <ID>942553</ID>
        <IP>10.10.10.24</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <NETWORK_ID>123</NETWORK_ID>
        <NETBIOS><![CDATA[MACBOOKPRO-E9B6]]></NETBIOS>
        <OS><![CDATA[MacOS X]]></OS>
```

```
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

DTD update:

New NETWORK_ID subelement for each HOST element.

```
<!ELEMENT HOST (ID, IP?, TRACKING_METHOD?, NETWORK_ID?,
                DNS?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?,
                TAGS?, LAST_VULN_SCAN_DATETIME?,
                LAST_COMPLIANCE_SCAN_DATETIME?,
                OWNER?, COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
...
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

Host Asset Purge API v2

Tell me about this API

The Host Asset Purge API v2 (/api/2.0/fo/asset/host/ with action=purge) is used to purge hosts in your account. Purging hosts will remove security assessment data collected from scans (scan results will not be removed). For details on this API, see the Qualys API User Guide v2.

With network support

The new "network_ids" parameter is used to restrict the action of the request to selected custom network IDs. When making a request, one of these input parameters is required: ids (specify host IDs), ips (specify host IP addresses), ag_ids (specify asset group IDs) or ag_titles (specify asset group titles).

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=purge&ips=10.10.10.29&network_ids=1082"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

Uses the batch return XML (batch_return.dtd). There were no changes made to the XML output.

Host Detection List API v2

Tell me about this API

The Host Detection List API v2 (/api/2.0/fo/asset/host/vm/detection/ with action=list) returns vulnerability detection data that can be easily imported into a third party solution. For details on this API, see the Qualys API User Guide v2.

With network support

The new "network_ids" input parameter is used to filter the host list to include selected custom network IDs. When unspecified, no network filters are applied.

The XML output now identifies the network ID for each host. A new NETWORK_ID element was added to the host detection list XML output (host_detection_list_vm_detection_output.dtd).

Sample

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?
action=list&network_ids=1234"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/h
ost_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-01-09T22:58:14Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>33645</ID>
        <IP>10.10.10.40</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <NETWORK_ID>1234</NETWORK_ID>
        <OS><![CDATA[Linux 2.4-2.6]]></OS>
        <DNS><![CDATA[dhcp-40.vuln.qa.qualys.com]]></DNS>
        <LAST_SCAN_DATETIME>2014-01-
08T12:40:01Z</LAST_SCAN_DATETIME>
        <DETECTION_LIST>
          <DETECTION>
```

```
            <QID>82054</QID>
            <TYPE>Confirmed</TYPE>
            <SSL>0</SSL>
           <RESULTS><![CDATA[Tested on port 2222 with an injected
SYN/RST offset by 16 bytes.]]></RESULTS>
            <STATUS>New</STATUS>
            <FIRST_FOUND_DATETIME>2013-08-
09T18:48:51Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2014-01-
08T12:40:01Z</LAST_FOUND_DATETIME>
            <LAST_TEST_DATETIME>2014-01-
08T12:40:01Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2014-01-
08T12:40:01Z</LAST_UPDATE_DATETIME>
          </DETECTION>
        </DETECTION_LIST>
      </HOST>
...
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
...
```

DTD update:

New NETWORK_ID subelement for each HOST element.

```
<!ELEMENT HOST (ID, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?,
                OS?, OS_CPE?, DNS?, NETBIOS?, QG_HOSTID?,
                LAST_SCAN_DATETIME?, TAGS?, DETECTION_LIST)>
...
<!ELEMENT NETWORK_ID  (#PCDATA)>
...
```

IP List API v2

Tell me about this API

The IP List API v2 (resource /api/2.0/fo/asset/ip/ with action=list) is used to retrieve a list of IP addresses in your account. For details on this API, see the Qualys API User Guide v2.

With network support

Use the new input parameter "network_id" (optional) to return a list of IPs for a certain network.

The XML output now lists the network ID for each IP address/range when the request is made by a sub-user with access to multiple networks. We added a new attribute "network_id" to the subelements /IP_SET/IP and /IP_SET/IP_RANGE in the XML output (ip_list_output.dtd).

Good to know

- Managers will not see the "network_id" attribute for any IP or IP_RANGE elements in the output since Managers can see all IPs for all networks.

- Any sub-user with access to only a single network (the Global Default Network or a custom network) will not see the "network_id" attribute either. This is for consistency with the UI, where these users do not see the network workflows.

Sample

Sample API request made by a Scanner user with access to multiple networks. XML output includes the "network_id" attribute.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/ip/ip_list_output.d
td">
<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-02-14T22:47:32Z</DATETIME>
    <IP_SET>
      <IP_RANGE network_id="0">1.0.0.0-10.10.10.14</IP_RANGE>
      <IP_RANGE network_id="0">10.10.10.17-10.10.10.29</IP_RANGE>
```

```
      <IP network_id="0">10.10.10.32</IP>
      <IP_RANGE network_id="0">10.10.10.36-10.10.10.37</IP_RANGE>
      <IP_RANGE network_id="0">10.10.10.39-10.10.10.193</IP_RANGE>
      <IP_RANGE network_id="0">10.10.10.196-10.10.25.80</IP_RANGE>
      <IP_RANGE network_id="0">10.10.25.82-10.10.30.245</IP_RANGE>
      <IP_RANGE network_id="0">10.10.30.247-
126.255.255.255</IP_RANGE>
      <IP_RANGE network_id="0">172.16.1.42-172.16.1.43</IP_RANGE>
      <IP_RANGE network_id="1002">1.0.0.0-
126.255.255.255</IP_RANGE>
      <IP_RANGE network_id="1002">172.16.1.42-
172.16.1.43</IP_RANGE>
      <IP_RANGE network_id="1100">1.0.0.0-
126.255.255.255</IP_RANGE>
      <IP_RANGE network_id="1100">172.16.1.42-
172.16.1.43</IP_RANGE>
    </IP_SET>
  </RESPONSE>
</IP_LIST_OUTPUT>
```

DTD update:

We added a new "network_id" attribute to the subelements /IP_SET/IP and /IP_SET/IP_RANGE.

```
...
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id  CDATA  "0"
>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE
  network_id  CDATA  "0"
>
...
```

Excluded IP List API v2

Tell me about this API

The Excluded IP List API v2 (/api/2.0/fo/asset/excluded_ip/ with action=list) returns a list of excluded hosts. These are hosts in your account that will not be scanned. For details on this API, see the Qualys API User Guide v2.

With network support

Use the new input parameter "network_id" (optional) to return a list of excluded IPs for a certain network.

The XML output now identifies the network ID for each IP address/range when your subscription has at least 1 network defined. We added a new attribute "network_id" to the subelements /IP_SET/IP and /IP_SET/IP_RANGE in the XML output (ip_list_output.dtd).

Sample

API request:

List the excluded IPs for all networks.

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IP_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/ip_list
_output.dtd">
<IP_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-03-20T20:49:19Z</DATETIME>
    <IP_SET>
      <IP network_id="0">10.10.10.19</IP>
      <IP_RANGE network_id="1275">10.10.50.6-
10.10.50.10</IP_RANGE>
    </IP_SET>
  </RESPONSE>
</IP_LIST_OUTPUT>
```

DTD update:

New “network_id” attribute added to the subelements /IP_SET/IP and /IP_SET/IP_RANGE.

```
...
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id  CDATA  "0"
>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE
  network_id  CDATA  "0"
>
...
```

Excluded IP Change History API v2

Tell me about this API

The excluded IP change history V2 API (/api/2.0/fo/asset/excluded_ip/history/ with action=list) returns a change history for excluded hosts. For details on this API, see the Qualys API User Guide v2.

With network support

Use the new input parameter "network_id" (optional) to return a list of change history for excluded hosts for a certain network.

The XML output now identifies the network ID for each IP address/range when your subscription has at least 1 network defined. We added a new attribute "network_id" to the subelements /IP_SET/IP and /IP_SET/IP_RANGE in the XML output (history_list_output.dtd).

Sample

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HISTORY_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/excluded_ip/history
/history_list_output.dtd">
<HISTORY_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2014-04-03T20:43:33Z</DATETIME>
 <HISTORY_LIST>
      <HISTORY>
        <ID>1441</ID>
        <IP_SET>
          <IP_RANGE network_id="0">10.10.10.234-
10.10.10.235</IP_RANGE>
        </IP_SET>
        <ACTION>Added</ACTION>
        <DATETIME>2014-04-02T16:16:19Z</DATETIME>
...
```

DTD update:

New “network_id” attribute added to the subelements /IP_SET/IP and /IP_SET/IP_RANGE.

```
...
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
    network_id  CDATA  "0"
...
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE
    network_id  CDATA  "0"
...
```

APPENDIX A

Tell me about the latest updates

Qualys API 8.1 and later includes enhancements to support the Networks feature. We made updates to API operations and DTD output. (Updates are not visible to users who do not not have the Networks feature turned on in their accounts.)

VM Updates	
1) Scan Report API	10) Ticket Edit API
2) Asset Search API	11) Ticket Delete API
3) Scan Target History API	12) Patch Scorecard Report
4) Scheduled Scans API	13) Most Vulnerable Hosts Scorecard Report
5) Get Host Info API	14) Risk Analysis Report
6) Asset Data Report API	15) Ignored Vulnerabilities Scorecard Report
7) Asset Range Info API	16) Map Report API
8) Ticket List API	17) Map API
9) Ignore Vulnerabilities API	18) Map Report Output

VM and PC Updates	
1) IP List API	2) Authentication Report DTD
PC Updates	
1) Compliance Policy List API	3) Compliance Individual Host Report
2) Compliance Posture List API	4) Compliance Control Pass/Fail Report

VM Updates

1) Scan Report API

API endpoint: msp/scan_report.php

XML output:

```
...
<KEY value="STATUS">ERROR</KEY>
<KEY value="NETWORK_TITLE">Network 2</KEY>
<KEY value="NETWORK_ID">1364</KEY>
<ASSET_GROUPS>
...
</ASSET_GROUPS>...
```

DTD update: No update to DTD (scan-1.dtd)

2) Asset Search API

API endpoint: msp/asset_search.php

XML output:

```
...
<ASSET_SEARCH_REPORT>
    ...
    <HOST_LIST>
        <HOST>
            <IP>10.0.0.7</IP>
            <TRACKING_METHOD>IP</TRACKING_METHOD>
            <NETBIOS><![CDATA[STORE]]></NETBIOS>
            <OPERATING_SYSTEM><![CDATA[Linux 2.2-2.6]]></OPERATING_SYSTEM>
            <NETWORK><![CDATA[Qualys Default Network]]></NETWORK>
            <LAST_SCAN_DATE>2014-04-18T21:23:04Z</LAST_SCAN_DATE>
        </HOST>
    </HOST_LIST>
</ASSET_SEARCH_REPORT>
...
```

DTD update: Added NETWORK tag to DTD (asset_search_report.dtd).

```
<!ELEMENT HOST (ERROR | (IP, HOST_TAGS?,TRACKING_METHOD,
DNS?, NETBIOS?, OPERATING_SYSTEM?, OS_CPE?, QID_LIST?,
PORT_SERVICE_LIST?,ASSET_GROUPS?, LAST_SCAN_DATE?, NETWORK?))>
...
<!ELEMENT LAST_SCAN_DATE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)
...
```

3) Scan Target History API

API endpoint: msp/scan_target_history.php

XML output:

```
...
<IP_TARGETED_LIST>
    <IP_TARGETED network_id="1364">
        <IP>10.10.10.1</IP>
        <NB_SCANS>11</NB_SCANS>
    </IP_TARGETED>
    <IP_TARGETED network_id="0">
        <IP>10.10.10.1</IP>
        <NB_SCANS>18</NB_SCANS>
    </IP_TARGETED>
</IP_TARGETED_LIST>...
```

DTD update: Added network_id attribute to DTD (scan_target_history_output.dtd).

```
...
<!-- TARGETED LIST -->
<!ELEMENT IP_TARGETED_LIST (IP_TARGETED*)>
<!ELEMENT IP_TARGETED (IP, NB_SCANS, IP_DETAILED_HISTORY?)>
<!ATTLIST IP_TARGETED
  network_id CDATA #IMPLIED>
<!ELEMENT IP (#PCDATA)>
...
```

4) Scheduled Scans API

API endpoint: msp/scheduled_scans.php

Input parameter (optional): network_id

XML output:

```
...
<USER_ENTERED_IPS network_id="0">
    <RANGE>
  <START>192.169.1.12</START>
  <END>192.169.1.12</END>
  </RANGE>
</USER_ENTERED_IPS>

<EXCLUDE_IP_PER_SCAN network_id="0">10.10.1.61, 10.10.2.3-
10.10.2.63
</EXCLUDE_IP_PER_SCAN>

<ASSET_GROUP>
  <ASSET_GROUP_TITLE><![CDATA[My Asset Group]]></ASSET_GROUP_TITLE>
```

```
    <NETWORK_ID>0</NETWORK_ID>
</ASSET_GROUP>
<DOMAIN_NAME network_id="0">domain.com</DOMAIN_NAME>
...
```

DTD update: Added network_id attribute and NETWORK_ID tag to DTD (scheduled_scans.dtd).

```
...
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE, NETWORK_ID?)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ATTLIST EXCLUDE_IP_PER_SCAN
network_id  CDATA  #IMPLIED
>
<!ELEMENT USER_ENTERED_DOMAINS (DOMAIN*)>
<!ELEMENT DOMAIN (DOMAIN_NAME+, NETBLOCK*)>
<!ELEMENT DOMAIN_NAME (#PCDATA)>
<!ATTLIST DOMAIN_NAME
network_id  CDATA  #IMPLIED

>
...
<!ELEMENT USER_ENTERED_IPS (RANGE*)>
<!ATTLIST USER_ENTERED_IPS
network_id  CDATA  #IMPLIED
>
...
```

5) Get Host Info API

API endpoint: msp/get_host_info.php

XML output:

```
...
<HOST>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
    <SECURITY_RISK>0</SECURITY_RISK>
    <IP network_id="0">10.10.10.25</IP>
    <OPERATING_SYSTEM>
        <![CDATA[]]>
    </OPERATING_SYSTEM>
...
</HOST>
...
```

DTD update: Added network_id attribute to DTD (get_host_info.dtd).

```
...
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id CDATA #IMPLIED>
...
```

6) Asset Data Report API

API endpoint: msp/asset_data_report.php

XML output:

```
<ASSET_DATA_REPORT>
    <HEADER>
        ...
        <TARGET>
            <USER_ASSET_GROUPS>
                ...
            </USER_ASSET_GROUPS>
            <USER_IP_LIST>
                <RANGE network_id="0">
                    <START>10.10.10.1</START>
                    <END>10.10.10.9</END>
                </RANGE>
            </USER_IP_LIST>
            <COMBINED_IP_LIST>
                <RANGE network_id="0">
                    <START>10.10.10.1</START>
                    <END>10.10.10.9</END>
                </RANGE>
                ...
            </COMBINED_IP_LIST>
        </TARGET>
        ...
    </HEADER>
    <RISK_SCORE_PER_HOST>
        <HOSTS>
            <IP_ADDRESS network_id="0">10.10.10.1</IP_ADDRESS>
            <TOTAL_VULNERABILITIES>6</TOTAL_VULNERABILITIES>
            <SECURITY_RISK>3.3</SECURITY_RISK>
        </HOSTS>
        ...
    </RISK_SCORE_PER_HOST>
    <HOST_LIST>
        <HOST>
            <IP network_id="0">10.10.10.1</IP>
            <TRACKING_METHOD>IP</TRACKING_METHOD>
            <DNS>
```

```
                <![CDATA[server.corp.com]]>
            </DNS>
            ...
        </HOST>
    </HOST_LIST>
    <GLOSSARY>
        ...
    </GLOSSARY>
    <APPENDICES>
        <NO_RESULTS>
            <IP_LIST>
                <RANGE network_id="0">
                    <START>10.10.10.4</START>
                    <END>10.10.10.6</END>
...
</ASSET_DATA_REPORT>
```

DTD update: Added network_id attribute to DTD (asset_data_report.dtd).

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

7) Asset Range Info API

API endpoint: msp/asset_range_info.php

XML output:

```
...
<HOST>
    <IP network_id="0">10.10.25.143</IP>
    <TRACKING_METHOD>IP</TRACKING_METHOD>
    ...
</HOST>
...
```

DTD update: Added network_id attribute to DTD (asset_range_info.dtd).

```
...
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id  CDATA  "0"
>
...
```

8) Ticket List API

API endpoint: msp/ticket_list.php

XML output:

```
...
<TICKET_LIST>
  <TICKET>
      <NUMBER>450</NUMBER>
    ...
    <LOGIN>username</LOGIN>
    <DETECTION>
      <IP network_id="1365">10.10.30.47</IP>
    ...
      </DETECTION>
    ...
</TICKET_LIST>
...
```

DTD update: Added network_id attribute to DTD (ticket_list_output.dtd).

```
...
<!ELEMENT IP (#PCDATA) >
<!ATTLIST IP
  network_id  CDATA  #IMPLIED
>
...
```

9) Ignore Vulnerabilities API

API endpoint: msp/ticket_list.php

Input parameter (optional): network_id

XML output:

```
...
<IGNORED>
    ...
    <IP network_id="1365">10.10.24.7</IP>
    ...
</IGNORED>

<RESTORED>
    ...
    <IP network_id="1365">10.10.24.7</IP>
    ...
```

```
</RESTORED>
...
```

DTD update: Added network_id attribute to DTD (ignore_vuln_output.dtd).

```
...
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
...
```

10) Ticket Edit API

API endpoint: msp/ticket_edit.php

Input parameter (optional): network_id (network_id or asset_groups may be specified)

XML output:

```
...
<TICKET_EDIT_OUTPUT>
    <HEADER>
        <USER_LOGIN>username</USER_LOGIN>
    ...
    <WHERE>
            <NETWORK_ID>1365</NETWORK_ID>
    </WHERE>...
```

DTD update: Added NETWORK_ID to WHERE section in DTD (ticket_edit_output.dtd).

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

11) Ticket Delete API

API endpoint: msp/ticket_delete.php

Input parameter (optional): network_id

XML output:

```
...
<TICKET_DELETE_OUTPUT>
    <HEADER>
  ...
  <WHERE>
      <TICKET_NUMBERS>20</TICKET_NUMBERS>
      <NETWORK_ID>1365</NETWORK_ID>
    </WHERE>
  </HEADER>
    ...
</TICKET_DELETE_OUTPUT>
```

DTD update: Added NETWORK_ID to WHERE section in DTD (ticket_delete_output.dtd).

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

12) Patch Scorecard Report

API endpoint: php/patch_scorecard_report.dtd

XML output:

```
...
<DETECTION_LIST>
   <DETECTION>
      <HOST>
         <IP><![CDATA[ 10.10.10.2 ]]></IP>
         <DNS><![CDATA[ ns1.corp.corp2.com ]]></DNS>
         <NETBIOS><![CDATA[ ]]></NETBIOS>
         <OS><![CDATA[ Linux 2.2-2.6 ]]></OS>
         <OWNER><![CDATA[ ]]></OWNER>
         <NETWORK><![CDATA[ Global Default Network ]]></NETWORK>
         </HOST>
      <VULN>
         <QID><![CDATA[ 15077 ]]></QID>
...
```

DTD update: Added NETWORK tag to DTD (patch_report_scorecard.dtd).

```
...
<!ELEMENT DETECTION_LIST (DETECTION*)>
<!ELEMENT DETECTION (HOST, VULN)>
...
<!ELEMENT HOST (IP, DNS?, NETBIOS?, OS?, OS_CPE?, OWNER?, NETWORK?)>
```

13) Most Vulnerable Hosts Scorecard Report

API endpoint: php/most_vulnerable_hosts_scorecard_report.dtd

XML output:

```
...
<MOST_VULNERABLE_HOSTS_SCORECARD>
   <HEADER>...</HEADER>
   <SUMMARY>...</SUMMARY>
   <RESULTS>
     <HOST_LIST>
       <HOST>
         <RANK>...</RANK>
         <IP>
         <![CDATA[ 10.10.10.10 ]]>
       </IP>
         <DNS>...</DNS>
         <NETBIOS>...</NETBIOS>
         <LAST_SCAN_DATE>...</LAST_SCAN_DATE>
         <NUM_SEV_5>...</NUM_SEV_5>
       <NUM_SEV_4>...</NUM_SEV_4>
       <BUSINESS_RISK>...</BUSINESS_RISK>
       <SECURITY_RISK>...</SECURITY_RISK>
       <ASSET_GROUPS>...</ASSET_GROUPS>
       <NETWORK>
       <![CDATA[ NET1 ]]>
     </NETWORK>
   </HOST>
...
```

DTD update: Added NETWORK tag to the DTD (most_vulnerable_hosts_scorecard.dtd).

```
...
<!ELEMENT IP_LIST (RANGE*, NETWORK?)>
...
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (IP, DNS?, NETBIOS?, ASSET_GROUPS?, IMPACT?, SCORE?, QID?,
OS?, SERVICE?, PORT?, RESULTS?, NETWORK?)>
<!ELEMENT RESULTS (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
```

```
...
```

14) Risk Analysis Report

API endpoint: php/risk_analysis_report.dtd

XML output:

```
...
<HOST_LIST>
<HOST>
<IP>10.10.10.28</IP>
<DNS>
<![CDATA[xpsp3-10-28.qualys.com]]>
</DNS>
<NETBIOS>
<![CDATA[XPSP3-10-28]]>
</NETBIOS>
<ASSET_GROUPS/>
<IMPACT>
<![CDATA[High]]>
</IMPACT>
<QID>Check</QID>
<OS>Check</OS>
<SERVICE>Check</SERVICE>
<PORT>Check</PORT>
<RESULTS>Check</RESULTS>
<NETWORK>NET1</NETWORK>
</HOST>
...
```

DTD update: Added NETWORK tag to DTD (risk_analysis_report.dtd)

```
...
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (RANK, IP, DNS?, NETBIOS?, LAST_SCAN_DATE?,
                NUM_SEV_5, NUM_SEV_4, BUSINESS_RISK, SECURITY_RISK,
ASSET_GROUPS?, NETWORK?)>
...
```

15) Ignored Vulnerabilities Scorecard Report

API endpoint: php/ignored_vulns_scorecard.dtd

XML output:

```
...
<IGNORED_VULNS_SCORECARD>
  <HEADER>...</HEADER>
  <SUMMARY>...</SUMMARY>
  <RESULTS>
```

```
    <ASSET_GROUP_LIST>
      <ASSET_GROUP>
        <TITLE>
        <![CDATA[ 10.10.10.7-10.10.10.10 ]]>
      </TITLE>
        <DETECTION_LIST>
          <DETECTION>
            <HOST>
              <IP>
              <![CDATA[ 10.10.10.7 ]]>
            </IP>
             <DNS>...</DNS>
             <NETBIOS>...</NETBIOS>
             <OS>...</OS>
             <NETWORK>
             <![CDATA[ NET2 ]]>
            </NETWORK>
          </HOST>
           <VULN>...</VULN>
           <TICKET>...</TICKET>
        </DETECTION>
...
```

DTD update: We added we add the attributes network_id and network to the DTD (ignored_vulns_scorecard.dtd).

```
...
<!ELEMENT HOST (IP, DNS?, NETBIOS?, OS?, OS_CPE?, OWNER?, NETWORK?)>
...
```

16) Map Report API

API endpoint: php/map_report.php

XML output:

```
...
    <KEY value="NETWORK_ID">0</KEY>
    <KEY value="OPTIONS">Information gathering: Registered Hosts Only,
Perform live host sweep, Standard TCP port list, Standard UDP port list,
ICMP Host Discovery</KEY>
    ...
    </USER_ENTERED_DOMAINS>
    <OPTION_PROFILE>
      ...
    </OPTION_PROFILE>
</HEADER>
<IP value="192.168.0.1" name="server2.qualys-test.com" os="Cisco IOS"
type="router" network="Global Default Network" network_id="0">
  <DISCOVERY method="traceroute" />
```

```
...
```

DTD update: Added a NETWORK tag to the DTD (map_report.dtd).

```
...
<!ELEMENT HEADER (DOMAIN, NETWORK?, USERNAME, REPORT_TEMPLATE,
REPORT_TITLE, RESTRICTED_IPS?, MAP_RESULT_LIST, NETWORK?)>
...
<!ELEMENT NETWORK (#PCDATA)>
...
```

17) Map API

API endpoint: php/map.php

Input parameter (optional): network_id

XML output:

```
...
<HEADER>
  ...
    <KEY value="NETWORK_ID">1340</KEY>
</HEADER>

<IP value="192.168.0.1" name="server2.qualys-test.com" os="Cisco IOS"
type="router" network_id="1340">
<DISCOVERY method="traceroute" />
...
```

DTD update: Added a NETWORK tag to the DTD (map_report.dtd).

18) Map Report Output

API endpoint: php/map-2.dtd

XML output:

```
...
<AUTH_SCAN_ISSUES>
   <AUTH_SCAN_FAILED>
   <HOST_INFO>
   <DNS><![CDATA[server.qualys.com]]></DNS>
   <IP><![CDATA[10.10.10.7]]></IP>
   <NETBIOS><![CDATA[STORE]]></NETBIOS>
   <INSTANCE><![CDATA[os]]></INSTANCE>
   <CAUSE><![CDATA[Unable to complete login for host=10.0.0.7,
user=root]]></CAUSE>
   <NETWORK><![CDATA[Global Default Network]]></NETWORK>
   </HOST_INFO>
   </AUTH_SCAN_FAILED>
```

```
</AUTH_SCAN_ISSUES>
...
```

DTD update: Added network attribute to the DTD (map-2.dtd).

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

VM and PC Updates

1) IP List API

API endpoint: msp/asset_ip_list.php

XML output:

```
...
   <HOST>
      <IP network_id="0">
         <![CDATA[10.10.24.58]]>
      </IP>
...
   </HOST>
...
```

DTD update: Added network_id attribute to DTD (ip_list_output.dtd).

```
...
<!ELEMENT IP_SET ((IP|IP_RANGE)+)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP
  network_id  CDATA  #IMPLIED
>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ATTLIST IP_RANGE
  network_id  CDATA  #IMPLIED
>
...
```

2) Authentication Report DTD

API endpoint: php/compliance_authentication_report.dtd

XML output:

```
...
<HOST_LIST>
   <HOST>
     <TRACKING_METHOD>...</TRACKING_METHOD>
     <IP>
     <![CDATA[ 10.10.10.28 ]]>
   </IP>
    <DNS>...</DNS>
    <NETBIOS>...</NETBIOS>
    <HOST_TECHNOLOGY>...</HOST_TECHNOLOGY>
    <STATUS>...</STATUS>
    <CAUSE>...</CAUSE>
    <NETWORK>
```

```
    <![CDATA[ Global Default Network ]]>
   </NETWORK>
...
```

DTD update: Added NETWORK tag to DTD (compliance_authentication_report.dtd).

```
...
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, HOST_TECHNOLOGY?,
INSTANCE?, STATUS, CAUSE?, NETWORK?)>
...
```

PC Updates

1) Compliance Policy List API

API endpoint: api/2.0/fo/compliance/policy/?action=list

XML output:

```
...
<GLOSSARY>
<ASSET_GROUP_LIST>
<ASSET_GROUP>
<ID>621387</ID>
<TITLE><![CDATA[10.10.10.2 and 10 -GlobalDefNet]]></TITLE>
<NETWORK_ID>0</NETWORK_ID>
<IP_SET>
<IP>10.10.10.10</IP>
</IP_SET>
</ASSET_GROUP>
<ASSET_GROUP>
<ID>616482</ID>
<TITLE><![CDATA[ForNET1_AG1-2-10]]></TITLE>
<NETWORK_ID>1048</NETWORK_ID>
<IP_SET>
<IP_RANGE>10.10.10.3-10.10.10.10</IP_RANGE>
</IP_SET>
</ASSET_GROUP>
<ASSET_GROUP>
<ID>616487</ID>
<TITLE><![CDATA[ForNet2_2-10+ From Map 52-63]]></TITLE>
<NETWORK_ID>1049</NETWORK_ID>
<IP_SET>
<IP_RANGE>10.10.10.3-10.10.10.10</IP_RANGE>
<IP_RANGE>10.10.10.28-10.10.10.29</IP_RANGE>
<IP_RANGE>10.10.10.52-10.10.10.58</IP_RANGE>
<IP>10.10.10.63</IP>
```

```
</IP_SET>
</ASSET_GROUP>
</ASSET_GROUP_LIST>
</GLOSSARY>
...
```

DTD update: Added NETWORK_ID tag to DTD (policy_list_output.dtd).

```
...
<!ELEMENT GLOSSARY (ASSET_GROUP_LIST?, USER_LIST?)>
<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, TITLE, NETWORK_ID?, IP_SET?)>
<!ELEMENT NETWORK_ID (#PCDATA)>
...
```

2) Compliance Posture List API

API endpoint: api/2.0/fo/compliance/posture/?action=list

XML output:

```
...
<HOST>
   <ID>942957</ID>
   <IP network_id="0">10.10.24.245</IP>
   <TRACKING_METHOD>IP
   </TRACKING_METHOD>
.........
</HOST>
```

DTD update: Added network_id attribute to DTD (posture_info_list_output.dtd).

```
...
<!ELEMENT HOST (ID, IP, TRACKING_METHOD, DNS?, NETBIOS?, OS?, OS_CPE?,
                LAST_VULN_SCAN_DATETIME?, LAST_COMPLIANCE_SCAN_DATETIME?,
                PERCENTAGE?)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id  CDATA  #IMPLIED>
...
```

3) Compliance Individual Host Report

API endpoint: php/individual_host_compliance_report.dtd

DTD update: Added NETWORK tag to DTD (individual_host_compliance_report.dtd).

```
...
<!ELEMENT IP_LIST (RANGE*, NETWORK?)>
...
```

4) Compliance Control Pass/Fail Report

API endpoint: php/control_pass_fail_report.dtd.dtd

XML output:

```
<HOST_LIST>
   <HOST>
      <TRACKING_METHOD><![CDATA[ IP ]]></TRACKING_METHOD>
      <IP><![CDATA[ 10.10.10.29 ]]></IP>
      <DNS><![CDATA[ xpsp3-10-29-1.patch.abc.corp.com ]]></DNS>
      <NETBIOS><![CDATA[ XPSP3-10-29-1 ]]></NETBIOS>
      <OPERATING_SYSTEM><![CDATA[ Windows XP Service Pack 3 ]]>
</OPERATING_SYSTEM>
      <POSTURE><![CDATA[ Failed ]]></POSTURE>
      <NETWORK><![CDATA[ ]]></NETWORK>
   </HOST>
</HOST_LIST>
```

DTD update: Added NETWORK tag to DTD (control_pass_fail_report.dtd).

```
...
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, INSTANCE?,
OPERATING_SYSTEM, OS_CPE?, POSTURE, NETWORK?)>

<!ELEMENT TRACKING_METHOD (#PCDATA)>
...
<!ELEMENT NETWORK (#PCDATA)>
...
```

5) SCAP ARF Report

API endpoint: /api/2.0/fo/report/

Input parameter (optional): ips_network_id

Optional and valid only when the policy has SCAP 1.2 content) Use this parameter to restrict the report's target to the IPs specified in the "ips" parameter ("ips_network_id" is valid only when "ips" is specified in the same request).

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -d
"scan_id=3362251&ips=10.10.10.1-10.10.10.10&ips_network_id=1001"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/scap/arf/"
```

XML Output:

The XML output is compliant with the ARF 1.1 Schema. Show me this schema