Scan ESXi Hosts on vCenter

User Guide

July 30, 2019

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

Table of Contents

About this Guide

This guide will help you to run Qualys Vulnerability Management and Policy Compliance scans on your ESXi hosts through vCenter. We'll help you get started quickly!

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses 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, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also 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/

Get Started

We now have the ability to run vulnerability and compliance scans on your ESXi hosts through vCenter.

Before you begin, one consideration is that you will need to understand your VMware environment. If your organization has multiple deployments of vCenter in the environment managed by different authentication mechanisms (e.g. different Active Directory Domains, or some domains connected by Active Directory vs others are not) you will need to setup multiple vCenter and ESXi records.

There are two ways to gather map vCenter map data:

1. Using the Qualys map feature.
2. Using a map file provided by your VMware administrator. If you are using a map file provided from your VMware administrator, please skip to Appendix A - Using a map from a VMware administrator

Requirements:

- This feature is supported in Qualys 8.14 and beyond. If you are running on a private cloud platform (PCP), please make sure that your Qualys Cloud Platform is updated to version 8.14 or later.
- An account setup to access vCenter with the proper credentials.
- A list of the vCenter IPs.

Caveat:

We have a single control that's currently not supported using the scanning method described in this document:

8972 Status of the users with shell access on the host

Setting up Qualys to map using vCenter

To create a vCenter map using the Qualys map feature, you will need to obtain an account with the proper rights to perform ESX/ESXi host discovery. In order to perform the discovery using the Qualys map feature, authentication will need to be performed.

1. Request vCenter credentials

To successfully authenticate and scan each ESXi host, we'll need a vCenter account with:

- Read only access to the ESXi host
- In addition to read-only access permissions to

Global.Settings	Expand Global and select "Settings"
Host.Config.Change.Settings	Expand Host > Configuration and select "Change settings"

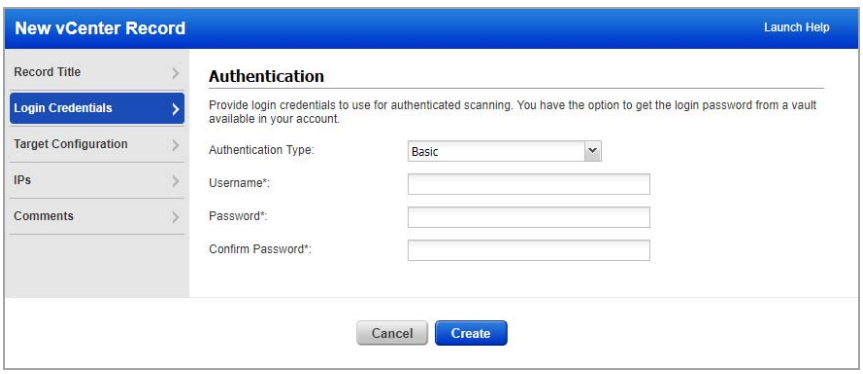
2. Request a list of vCenter IP Addresses

Request a list of vCenter IP addresses from your VMware Administrator.

3. Create a vCenter authentication record

a. Simply go to Scan > Authentication> New > VMware ESXi Record > vCenter Record.

b. In the Login Credentials select the authentication type and enter the credentials that you were provided.



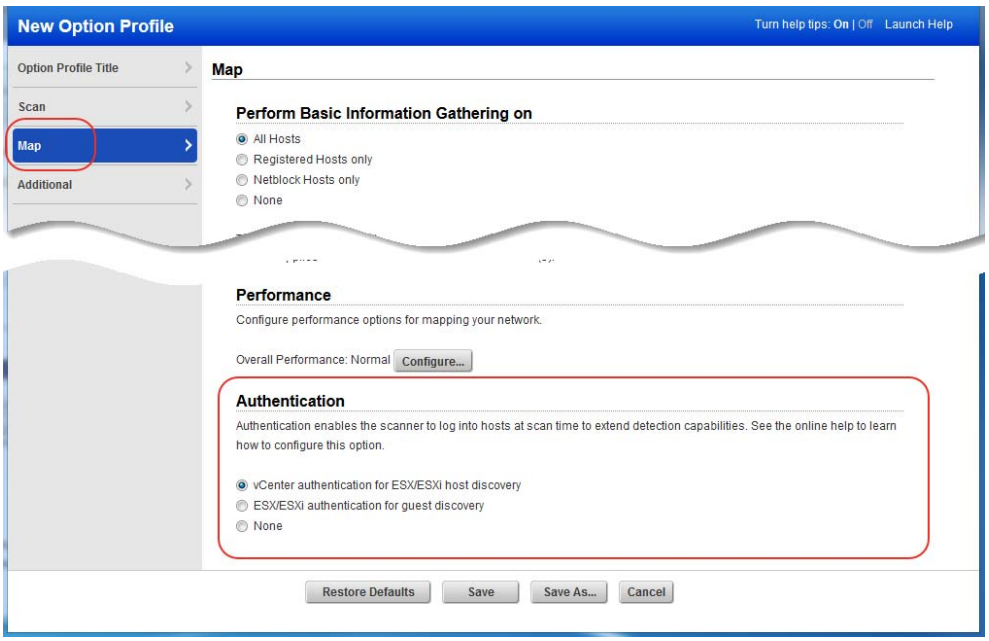
c. In the Target Configuration section, update the settings to match your environment.

d. In the IPs section, input the target list of vCenter IPs/IP Ranges.

Create a Map

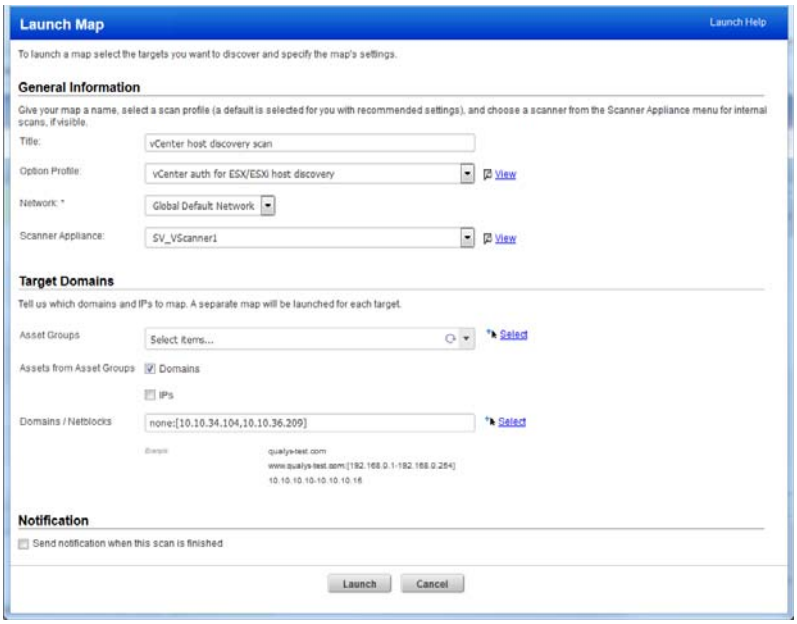
In order to create a map using Qualys we will use the Map feature located in Qualys Vulnerability Management. The steps to perform the automated map discovery scan are below:

1. Create a map Option Profile and define the authentication method respectively to launch map for guest and host discovery.
    a. Go to Scan > Option Profiles > New > Option Profile.
    b. Provide an appropriate title for the Option Profile.
    c. Choose the Map section:
        - Under the Perform Basic Information Gathering on: select All Hosts
        - Under the authentication section of the option profile, select vCenter authentication



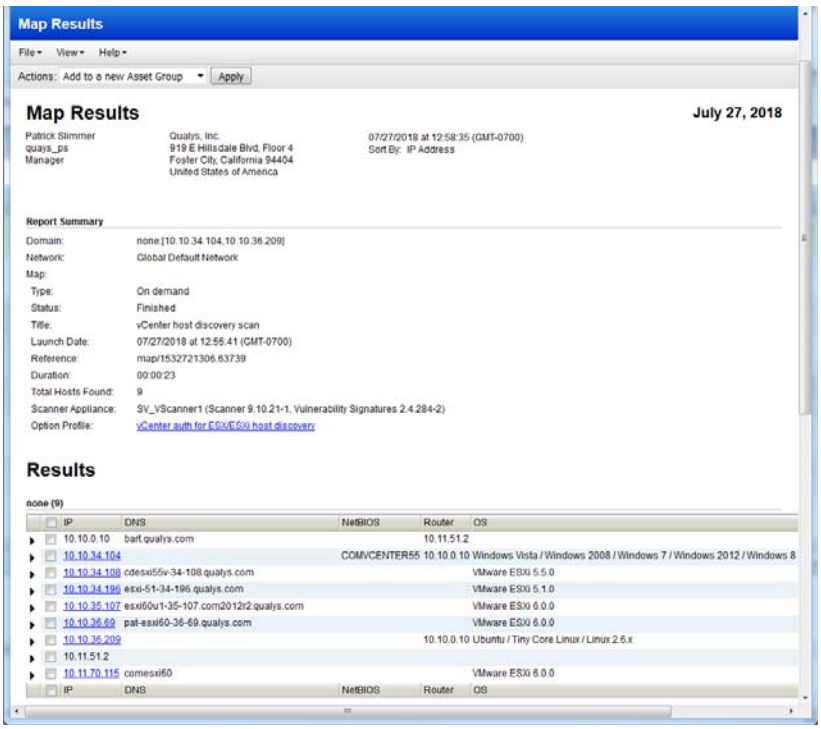
    d. Click Save

2. Launch the discovery map by going to Scans > Maps > New > Map.
    a. Select the options profile you created.
    b. The Domains option will need to be selected and Domains/Netblocks section completed prior to selecting Launch.

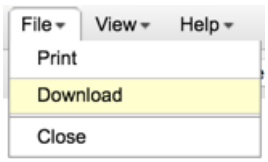


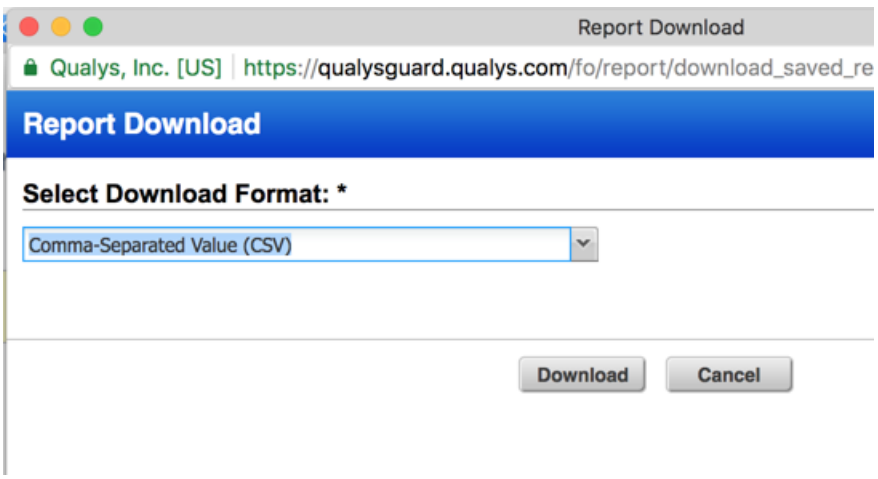
3. View and download map results

   a. To view your map results go to Scans > Map and from the Quick Actions menu select View Report for the map you created.



b. Download Map results as CSV. We will use the downloaded file in several upcoming steps.
   - In the map results: File > Download > select CSV format.



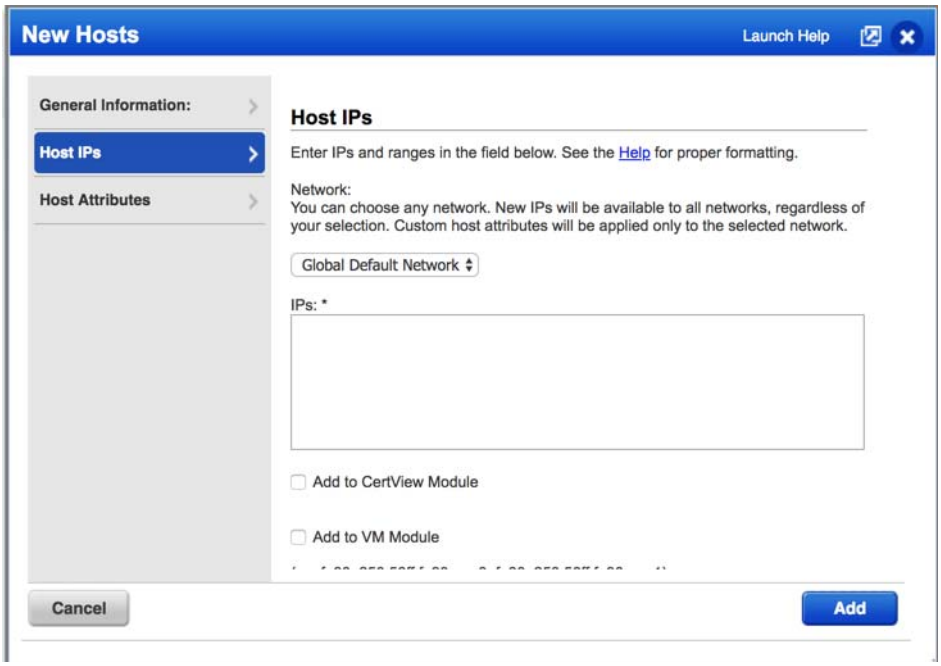


Register and organize vCenter and ESXi Assets

In this step we will be registering the IPs in your subscription and creating an Asset Group.

***Please note: If your subscription has the Networks feature enabled, you will need to repeat this step to register the IPs in the proper Network.

1. Make sure that you have the IP Addresses of vCenters and ESXi hosts available.
2. Go to Assets > Host Assets > New > IP Tracked Hosts.
3. Click the Host IPs tab.
4. Paste the list of vCenter and ESXi IPs in the Host IPs tab (if applicable under the proper network).
5. Click Add, then Apply.

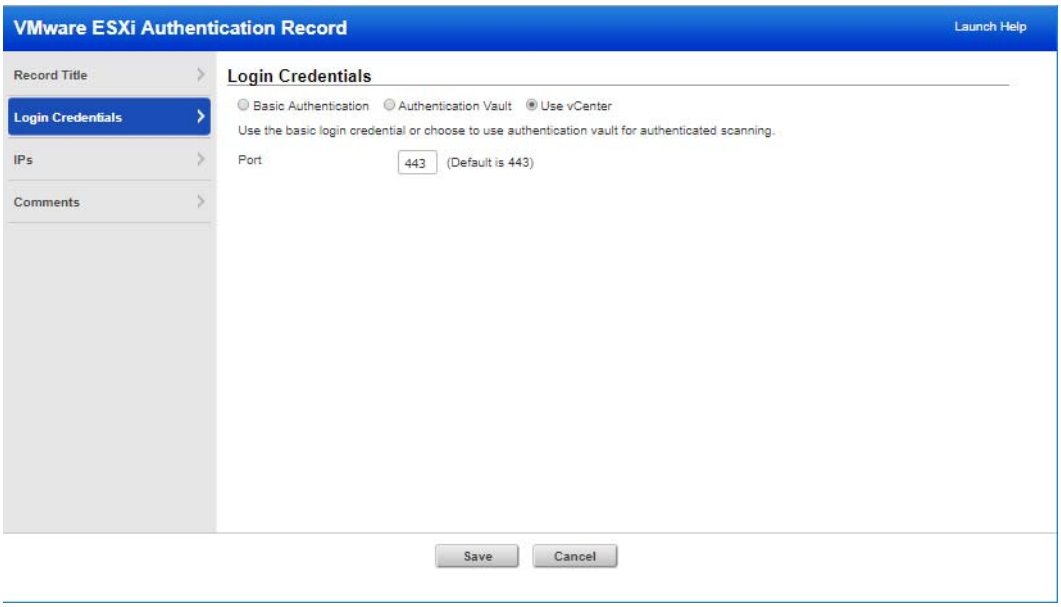


6. Then, go to Assets > Asset Groups > New Asset Group.
7. Provide an appropriate title (and network if applicable) for the Asset Group.
8. Under IPs paste the ESXi host IPs in the group.
9. Click Save.

Create a VMware ESXi Record

Whether you have used a vCenter Map from a VMware Administrator or used the Qualys Map, the list of ESXi IPs will need to be copied from the map file.

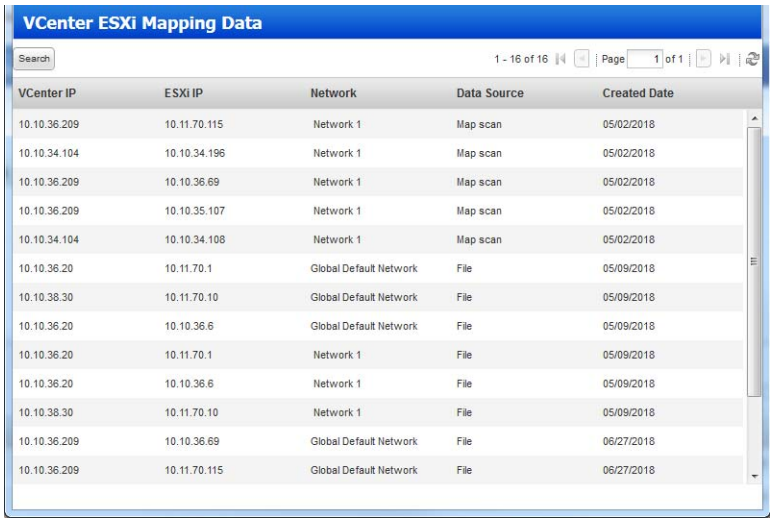
1. Open the file that contains the ESXi IP addresses.
2. Copy all of the IP addresses in the list.
3. Create a new VMware ESXi Record. Go to Scans > Authentication > New > VMware ESXi Record > VMware ESXi Record.
4. Complete the following information in the record:
    a. Record title
    b. Under Login Credentials select: Use vCenter



    c. Under IPs, paste the list of IPs that you have just copied.

View vCenter and ESXi Mapping Data

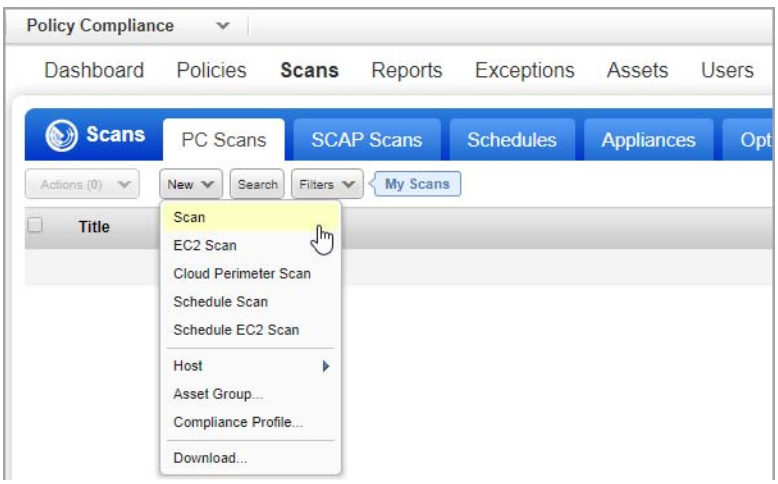
To view your mapping data, go to Scans > Authentication > New > vCenter Mapping. In the data list the Data Source column shows if your mapping is done via file or a discovery map scan.



Launch scans

Now you are ready to launch a scan on your ESXi hosts through vCenter.

Launch a scan like any other scan and for your target hosts choose your ESXi assets by selecting IP addresses, asset groups, asset tags. The authenticated scanning occurs for the ESXi IP addresses defined in your authentication record defined by you.



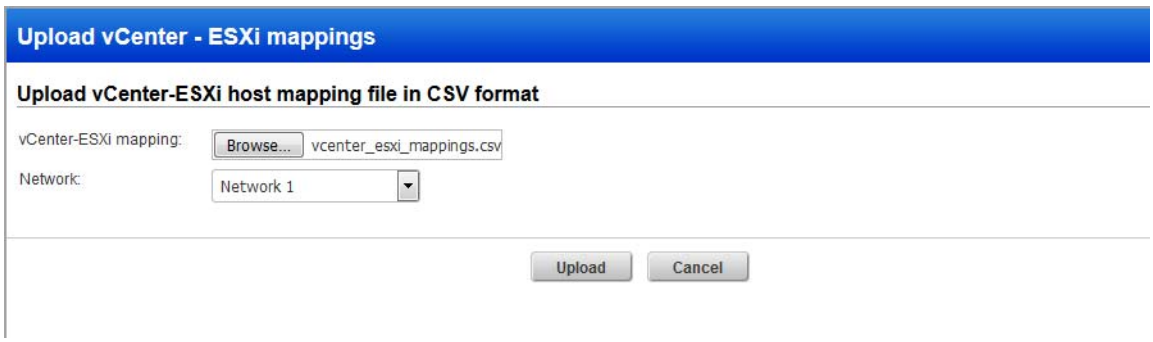
Appendix A - Using a map from a VMware administrator

1. Obtain a vCenter map generated from your VMware administrator in CSV format. Requirements for map file
2. Open the file and verify the file only contains the columns: vCenter Name, vCenter IP, ESXI System Name, Department, Location, LOB, System Type, ESXi IP, OS Long, OS Short, Port.

	A	B	C	D	E	F	G	H
1	Vcenter Name	Vcenter IP	ESXi System Name	Department	Location	LOB	System Type	ESXi IP
2	VMware vCenter 6.5	10.10.1.100	VmWare ESXi 6.5	IT	CA	CHANNELS	symc-csm-AssetSystem-Asset-VMWare-Machine	10.11.70.100

3. Upload Map Results.

To create the ESXi record, go to Scan > Authentication > New > VMware ESXi Record > Upload vCenter Mapping, and upload your vCenter map file.



4. Reference section Register and organize vCenter and ESXi Assets for the remaining steps.

Requirements for map file

1. The vCenter map file has 2 required columns that can be in any order
   - vCenter IP
   - ESXi IP
2. Additional columns are optional and can be in any order: vCenter Name, ESXi System Name, Department, Location, LOB, System Type, OS Long, OS Short, Port
3. Column name are case sensitive

Appendix B - API Support

We provide API support for running scans through vCenter.

API: vCenter Authentication Record | Option Profile | Discovery Scan | Compliance Scan

Looking for the latest Qualys API documentation? Click here

vCenter Authentication Record

To create a vCenter record using API, you need to first define the vCenter - ESXi mappings using the UI. Currently defining the mappings using API is not supported.

Sample - Create VMware Authentication Record with Use vCenter option

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=create&title=VmWare-VCenter-Auth-
API&ips=10.10.10.110&login_type=vcenter&port=80"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2018-06-28T07:43:58Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>179933</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List VMware Authentication Record with Use vCenter option

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&ids=179933"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VMWARE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/auth_vmware_l
ist_output.dtd">
<AUTH_VMWARE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-28T07:44:32Z</DATETIME>
    <AUTH_VMWARE_LIST>
      <AUTH_VMWARE>
        <ID>179933</ID>
        <TITLE><![CDATA[VmWare-VCenter-Auth-API]]></TITLE>
        <PORT>80</PORT>
        <SSL_VERIFY><![CDATA[all]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.110</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-06-28T07:43:58Z</DATETIME>
          <BY>user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-06-28T07:43:58Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_VMWARE>
    </AUTH_VMWARE_LIST>
  </RESPONSE>
</AUTH_VMWARE_LIST_OUTPUT>
```

Sample - Create vCenter Authentication Record with Basic Authentication option

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=create&title=VCenter-Auth-Create
API&ips=10.10.10.110&login_type=basic&port=80&username=username&pa
ssword=password"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

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

```
    <DATETIME>2018-06-28T07:47:47Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>179973</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List vCenter Authentication Record with Basic Authentication option

API request:

```
curl -H "X-Requested-With:curl demo2" -u "user:password" -d
"action=list&ids=179973"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VCENTER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/auth_vcenter
_list_output.dtd">
<AUTH_VCENTER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2018-06-28T07:48:13Z</DATETIME>
    <AUTH_VCENTER_LIST>
      <AUTH_VCENTER>
        <ID>179973</ID>
        <TITLE><![CDATA[VCenter-Auth-Create API]]></TITLE>
        <USERNAME><![CDATA[username]]></USERNAME>
        <PORT>80</PORT>
        <SSL_VERIFY><![CDATA[none]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.110</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2018-06-28T07:47:47Z</DATETIME>
          <BY>user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2018-06-28T07:47:47Z</DATETIME>
        </LAST_MODIFIED>
```

```
      </AUTH_VCENTER>
    </AUTH_VCENTER_LIST>
  </RESPONSE>
</AUTH_VCENTER_LIST_OUTPUT>
```

Option Profile

The vCenter map authentication option in the option profile, required to run an automated discovery scan (map) of ESXi hosts, can be set using the option profile API (import/export). (This automated discovery scan is supported using Qualys (VM, PC) version 8.14 and later.)

Option Profile API (import/export)

URL:

<platformURL>/api/2.0/api/2.0/fo/subscription/option_profile/

DTD for import/export data:

<platformURL>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

The <MAP_AUTHENTICATION> tag can be set to: VMware-ESXi (i.e. ESX/ESXi authentication for guest discovery), vCenter (i.e. vCenter authentication for ESX/ESXi host discovery) or none.

Sample - Map Authentication - vCenter authentication for ESX/ESXi host discovery

API request:

```
curl -H "X-Requested-With:curl demo2" -u "USERNAME:PASSWORD" -H
Content-Type:text/xml --data-binary "@/root/myfile.xml"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/?action=import
```

Note - "myfile.xml" contains the request POST data.

Request POST data:

```
...
 </VULNERABILITY_DETECTION>
    <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
    <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENA
BLE>
    </DISSOLVABLE_AGENT>
</SCAN>
<MAP>
    <BASIC_INFO_GATHERING_ON>all</BASIC_INFO_GATHERING_ON>
```

```
        <TCP_PORTS>
            <TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
            <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
        </UDP_PORTS>
        <MAP_OPTIONS>
            <PERFORM_LIVE_HOST_SWEEP>1</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
        </MAP_OPTIONS>
        <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
                <EXTERNAL_SCANNERS>4</EXTERNAL_SCANNERS>
                <SCANNER_APPLIANCES>4</SCANNER_APPLIANCES>
                <NETBLOCK_SIZE>65536 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Long</PACKET_DELAY>
        </MAP_PERFORMANCE>
        <MAP_AUTHENTICATION>vCenter</MAP_AUTHENTICATION>
    </MAP>
    <ADDITIONAL>
        <HOST_DISCOVERY>
            <TCP_PORTS>
                <STANDARD_SCAN>1</STANDARD_SCAN>
    ...
```

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>2018-05-03T08:33:58Z</DATETIME>
   <TEXT>Successfully imported Option profile for the subscription
Id nnnnnn</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>329725</KEY>
        <VALUE>OP for_vCenter authentication for ESX/ESXi host
discovery</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Discovery Scan

You can launch, list, cancel and delete discovery scans (map) using the Map API as described in Qualys API documentation.

Sample - Launch map

API request:

```
https://qualysapi.qualys.com/msp/map-
2.php?domain=none:[10.10.34.104,10.10.36.209]&option=vCenter+auth+
for+ESX/ESXi_host discovery&iscanner_name=hq2&save_report=yes
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE MAPREPORT SYSTEM
"https://qualysapi.qualys.com/map_report.dtd">
<MAPREPORT>
  <HEADER>
    <DOMAIN>none:[10.10.34.104,10.10.36.209]</DOMAIN>
    <NETWORK>Global Default Network</NETWORK>
    <USERNAME>acme_bb2</USERNAME>
    <REPORT_TEMPLATE><![CDATA[Map Results]]></REPORT_TEMPLATE>
    <REPORT_TITLE><![CDATA[Map Results]]></REPORT_TITLE>
    <MAP_RESULT_LIST>
      <MAP_RESULT>
        <MAP_RESULT_TITLE><![CDATA[vCenter host discovery
scan]]></MAP_RESULT_TITLE>
        <MAP_DATE>2018-07-27T19:55:41Z</MAP_DATE>
        <OPTION_PROFILE><![CDATA[vCenter auth for ESX/ESXi host
discovery]]></OPTION_PROFILE>
        <MAP_REFERENCE>map/1532721306.63739</MAP_REFERENCE>
      </MAP_RESULT>
    </MAP_RESULT_LIST>
  </HEADER>
  <HOST_LIST>
<HOST>
      <IP network_id="0">10.10.34.104</IP>
      <HOSTNAME><![CDATA[]]></HOSTNAME>
      <NETBIOS><![CDATA[COMVCENTER55]]></NETBIOS>
      <ROUTER>10.10.0.10</ROUTER>
     <OS>Windows Vista / Windows 2008 / Windows 7 / Windows 2012 /
Windows 8 / Windows 10</OS>
      <APPROVED>0</APPROVED>
      <SCANNABLE>1</SCANNABLE>
      <IN_NETBLOCK>1</IN_NETBLOCK>
      <LIVE>1</LIVE>
```

```
<DISCOVERY_LIST>
  <DISCOVERY>
    <DISCOVERY_NAME>ICMP</DISCOVERY_NAME>
    <PORT></PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>80</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>88</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>135</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>139</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>443</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>445</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP</DISCOVERY_NAME>
    <PORT>1433</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>UDP</DISCOVERY_NAME>
    <PORT>137</PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>TCP RST</DISCOVERY_NAME>
    <PORT></PORT>
  </DISCOVERY>
  <DISCOVERY>
    <DISCOVERY_NAME>https</DISCOVERY_NAME>
    <PORT></PORT>
  </DISCOVERY>
```

```
      </DISCOVERY_LIST>
      <ESXI_LIST>
        <ESXI>10.10.34.196</ESXI>
        <ESXI>10.10.34.108</ESXI>
      </ESXI_LIST>
    </HOST>
...
```

Compliance Scan

You can launch, list, cancel and delete compliance scans using the Compliance Scan API as described in Qualys API documentation.

Sample - Launch compliance scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=launch&asset_group_ids=1234&iscanner_name=iscan5&option_ti
tle=My+Option+Profile&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

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>2018-07-15T21:55:36Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>18198</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1443996555.12121</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```