



Scan ESXi Hosts on vCenter

User Guide

March 22, 2022

Copyright 2018-2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



Table of Contents

About this Guide	4
About Qualys	4
Contact Qualys Support	4
Get Started	5
Setting up Qualys to map using vCenter	6
Create a Map	7
Register and organize vCenter and ESXi Assets	10
Create a VMware ESXi Record	11
Manage vCenter and ESXi Mapping Data	12
Launch scans	14
Appendix A - Using a map from a VMware administrator.....	15
Appendix B - API Support	16
VMware Authentication Record	16
List VMware Authentication Records	20
Option Profile	22
Discovery Scan	24
Compliance Scan	26

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 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 later. 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

- Go to Scan > Authentication> New > VMware > VMware ESXi Record > vCenter Record.
- In the Login Credentials section, select the authentication type and enter the credentials that you were provided.

- In the Target Configuration section, update the settings to match your environment.
- 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. Go to the Map section:
 - Under the Perform Basic Information Gathering on: select All Hosts
 - Under the authentication section of the option profile, select vCenter authentication for ESX/ESXi host discovery.

New Option Profile Turn help tips: On | Off Launch Help

Option Profile Title > **Map**

Scan >

Map >

Additional >

Perform Basic Information Gathering on

- ☒ All Hosts
- ☐ Registered Hosts only
- ☐ Netblock Hosts only
- ☐ None

Performance

Configure performance options for mapping your network.

Overall Performance: Normal [Configure...](#)

Authentication

Authentication enables the scanner to log into hosts at scan time to extend detection capabilities. See the online help to learn how to configure this option.

- ☒ vCenter authentication for ESX/ESXi host discovery
- ☐ ESX/ESXi authentication for guest discovery
- ☐ None

[Restore Defaults](#) [Save](#) [Save As...](#) [Cancel](#)

- d. Click Save
2. Launch the discovery map by going to Scans > Maps > New > Map. Provide the following map settings and then click Launch.
 - a. Select the option profile you created in the previous step for the map.
 - b. In the Target Domains section, you'll need to provide the vCenter host IP addresses as the target of the map.

Launch Map Launch Help

To launch a map select the targets you want to discover and specify the map's settings.

General Information

Give your map a name, select a scan profile (a default is selected for you with recommended settings), and choose a scanner from the Scanner Appliance menu for internal scans, if visible.

Title:

Option Profile: [View](#)

Network:

Scanner Appliance: [View](#)

Target Domains

Tell us which domains and IPs to map. A separate map will be launched for each target.

Asset Groups: [Select](#)

Assets from Asset Groups: ☒ Domains ☐ IPs

Domains / Netblocks: [Select](#)

Example:
 qualys-test.com
 www.qualys-test.com [192.168.0.1-192.168.0.254]
 10.10.10.10-10.10.10.15

Notification

☐ Send notification when this scan is finished

3. View and download your 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.

Map Results File View Help

Actions: Add to a new Asset Group

Map Results July 27, 2018

Patrick Slimmer
qualys_js
Manager

Qualys, Inc.
919 E Hillside Blvd, Floor 4
Foster City, California 94404
United States of America

07/27/2018 at 12:58:35 (GMT-0700)
Sort By: IP Address

Report Summary

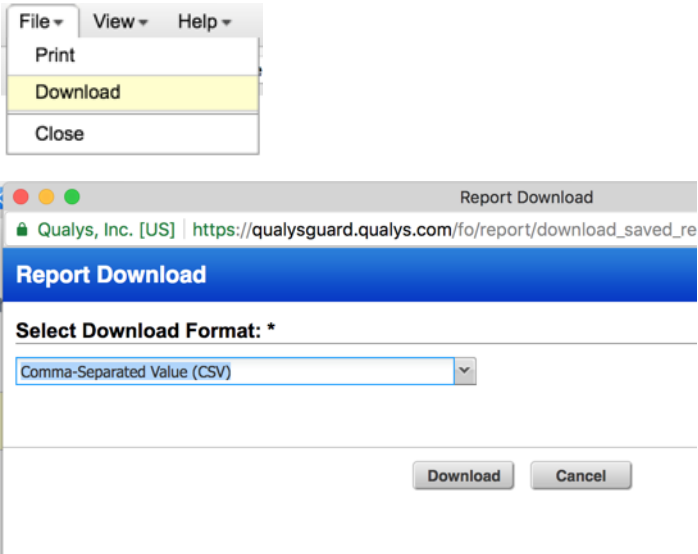
Domain: none[10.10.34.104,10.10.36.209]
 Network: Global Default Network
 Map:
 Type: On demand
 Status: Finished
 Title: vCenter host discovery scan
 Launch Date: 07/27/2018 at 12:55:41 (GMT-0700)
 Reference: map/1532721306.63739
 Duration: 00:00:23
 Total Hosts Found: 9
 Scanner Appliance: SV_VScanner1 (Scanner 9.10.21-1, Vulnerability Signatures 2.4.284-2)
 Option Profile: [vCenter auth for ESX/ESXi host discovery](#)

Results

none (9)

IP	DNS	NetBIOS	Router	OS
10.10.0.10	bart.qualys.com			10.11.51.2
10.10.34.104		COMVCENTER55	10.10.0.10	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8
10.10.34.108	cdexi55v-34-108.qualys.com			VMware ESXi 5.5.0
10.10.34.196	esxi-51-34-196.qualys.com			VMware ESXi 5.1.0
10.10.35.107	esxi60u1-35-107.com2012r2.qualys.com			VMware ESXi 6.0.0
10.10.36.69	pat-esxi60-36-69.qualys.com			VMware ESXi 6.0.0
10.10.36.209			10.10.0.10	Ubuntu / Tiny Core Linux / Linux 2.6.x
10.11.51.2				
10.11.70.115	comexi60			VMware ESXi 6.0.0
IP	DNS	NetBIOS	Router	OS

- b. Download Map results as CSV. We will use the downloaded file in upcoming steps. In the map results, go to File > Download, and select CSV format. Click Download.



4. The vCenter and ESXi mapping data is auto populated as a result of your discovery map scan. To see the mapping data, go to Scans > Authentication > New > VMware... > vCenter Mapping List. For each mapping record in the list, the Data Source column indicates whether the record is the result of an uploaded CSV file ("File") or the result of a discovery map scan ("Map Scan").

The image shows a web application interface titled 'vCenter ESXi Mapping Data'. It includes a toolbar with 'Actions', 'Search', 'Download CSV', and 'Purge' buttons. Below the toolbar is a table with columns: 'ESXi IP', 'Network', 'Data Source', and 'Created Date'. The table contains 13 rows of data. The 10th row is highlighted in yellow and has a checkmark in the first column. The 'Data Source' column for all rows is 'File'. The 'Created Date' for all rows is '12/11/2020'.

	ESXi IP	Network	Data Source	Created Date
<input type="checkbox"/>	10.9.134.71	Global Default Network	File	12/11/2020
<input type="checkbox"/>	10.10.34.104	Global Default Network	File	12/11/2020
<input type="checkbox"/>	10.10.36.209	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input checked="" type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020

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 vCenter and ESXi hosts available.
2. Go to **Assets > Host Assets > New > IP Tracked Hosts**.

Note: If Asset Group Management Service (AGMS) is enabled for your subscription, you will see the **Address Management** tab instead of **Host Assets**. To understand the changes that happen when AGMS is enabled for your subscription, refer to [AGMS Online Help](#).

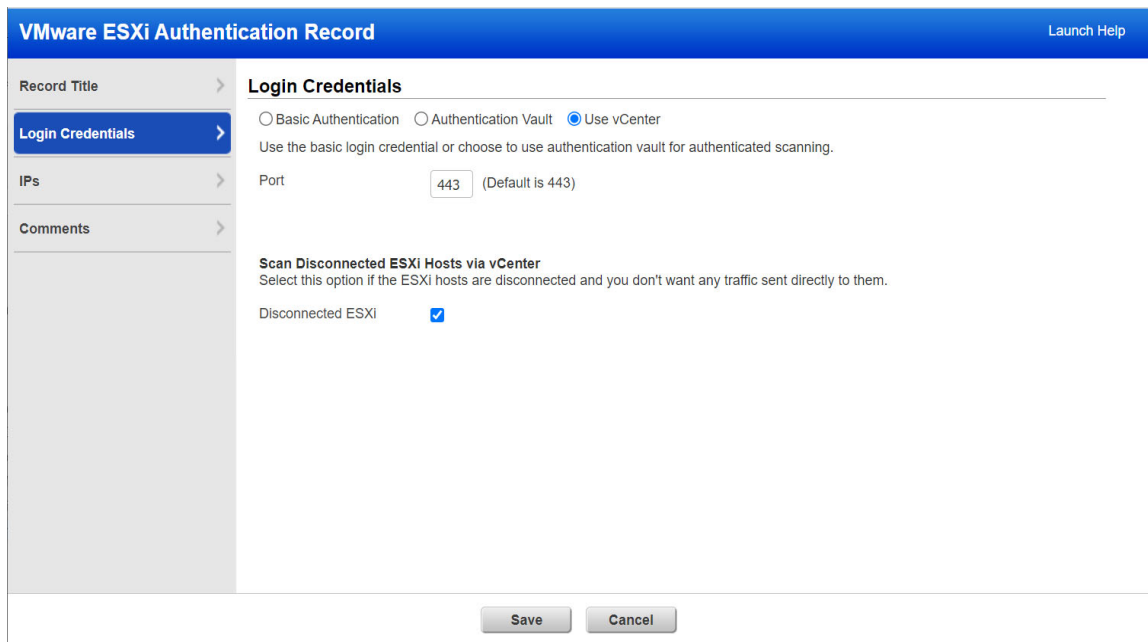
3. Click the **Host IPs** tab.
4. Paste the list of vCenter and ESXi IPs in the Host IPs tab (if applicable under the proper network).
5. Click Add, then Apply.

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



The screenshot shows the 'VMware ESXi Authentication Record' form. The left sidebar contains a 'Record Title' section with a dropdown arrow, and a 'Login Credentials' section with a blue button and a dropdown arrow. Below this are 'IPs' and 'Comments' sections, each with a dropdown arrow. The main content area is titled 'Login Credentials' and contains three radio buttons: 'Basic Authentication', 'Authentication Vault', and 'Use vCenter' (which is selected). Below the radio buttons is a text input field for 'Port' with the value '443' and a note '(Default is 443)'. Further down is a section titled 'Scan Disconnected ESXi Hosts via vCenter' with a subtext 'Select this option if the ESXi hosts are disconnected and you don't want any traffic sent directly to them.' and a checkbox labeled 'Disconnected ESXi' which is checked. At the bottom of the form are 'Save' and 'Cancel' buttons.

- c. Under IPs, paste the list of IPs that you have just copied.
- d. Under Scan Disconnected ESXi Hosts via vCenter, select the Disconnected ESXi option to scan ESXi hosts without sending any data to the host. By default, this option is clear (un-selected).

Manage vCenter and ESXi Mapping Data

You can search, download, delete, and, purge the vCenter and ESXi Mapping Data.

Go to Scans > Authentication > New > VMware... > vCenter Mapping List. The Data Source column in vCenter and ESXi Mapping Data screen shows if your mapping is done via file or a discovery map scan.

vCenter ESXi Mapping Data				
Actions	Search	Download CSV	Purge	1 - 18 of 18
<div> <div>Delete</div> <div>Clear Selections</div> </div>	ESXi IP	Network	Data Source	Created Date
<input type="checkbox"/>	10.9.134.71	Global Default Network	File	12/11/2020
<input type="checkbox"/>	10.10.34.104	Global Default Network	File	12/11/2020
<input type="checkbox"/>	10.10.36.209	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input checked="" type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020
<input type="checkbox"/>	128.0.0.0	Global Default Network	File	12/11/2020

Search: This option allows you to search for a specific vCenter IP Address or ESXi IP Address. You can further filter the data under file or discovery map scan.

vCenter ESXi Mapping Data

Actions

Search

Download CSV

Purge

Page 1 of 1

1 - 8 of 8

vCenter IP

☐ 1.1.1.1
 ☐ 1.1.1.2
 ☐ 10.10.34.104
 ☐ 10.10.34.104
 ☐ 10.10.36.209
 ☐ 10.10.36.209
 ☐ 10.10.36.209
 ☐ 10.10.36.209

Search

vCenter IP Address:

ESXi IP Address:

Data Source:

All

File

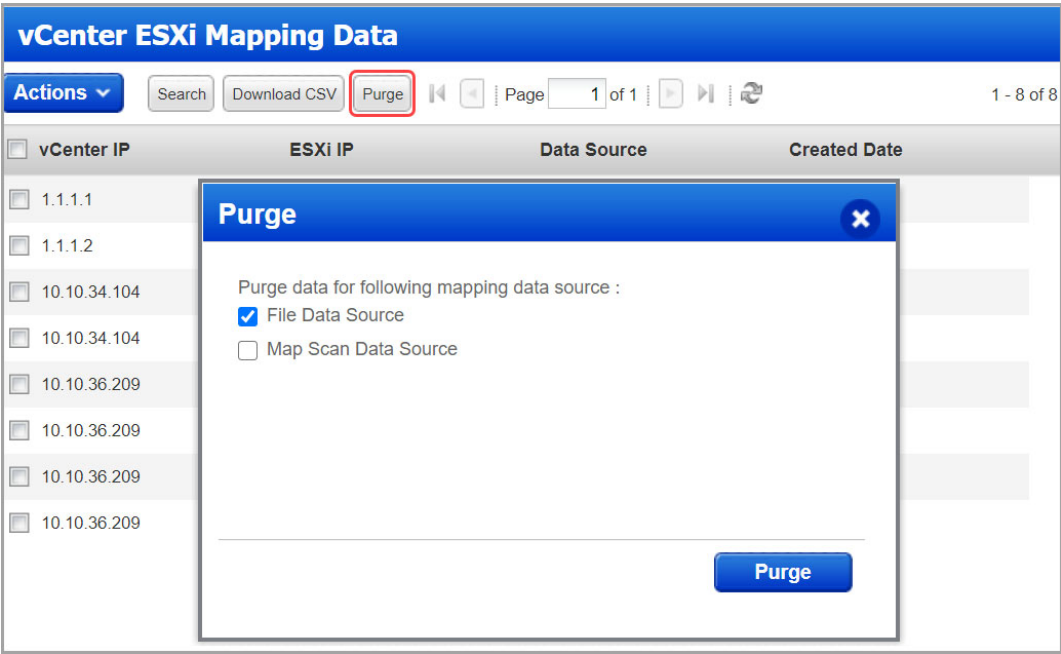
Map Scan

Search

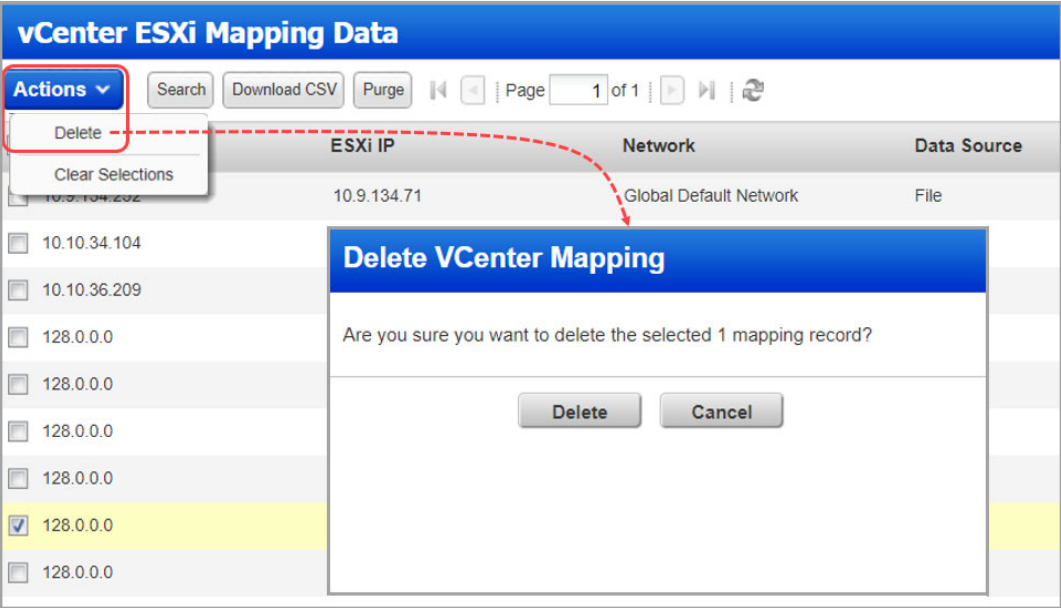
Download CSV: Download the vCenter and ESXi Mapping data in CSV format. If you have searched for certain IP using the Search option all the records related to the searched IP will be downloaded.

Purge: This option allows you to delete the vCenter and ESXi Mapping Data. You can delete the data from the following sources:

- File Data Source
- Map Scan Data Source



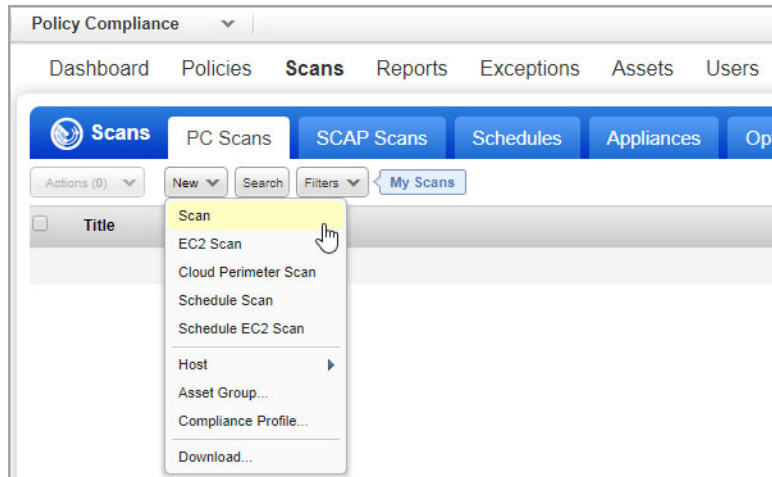
Delete: This option allows you to delete the selected mapping records from vCenter and ESXi Mapping Data. Select the records to be deleted and click Delete from Actions drop down.



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-	10.11.70.100

3. Upload the map file. To upload the file, go to Scans > Authentication > New > VMware... > vCenter Mapping Upload. Select the map file in CSV format, and click Upload.

Upload vCenter - ESXi mappings

Upload vCenter-ESXi host mapping file in CSV format

vCenter-ESXi mapping: vcenter_esxi_mappings.csv

Network:

4. Refer to the 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 names are case sensitive

Appendix B - API Support

We provide API support for running scans through vCenter.

API: [VMware Authentication Record](#) | [Option Profile](#) | [Discovery Scan](#) | [Compliance Scan](#)

Looking for the latest Qualys API documentation? [Click here](#)

VMware 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
"http://qualysapi.qualys.com/api/2.0/fo/auth/vmware/auth_vmware_list_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&password=password"
"http://qualysapi.qualys.com/api/2.0/fo/auth/vcenter/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://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>
```

Sample Create VMware Authentication Record with Disconnected ESXi Hosts

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=create&title=NewVMwareRecordWithAPI&login_type=vcenter&ips=10.11.
12.13&is_disconnect=1"
"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>2021-11-03T12:09:53Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1344231</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Update VMware Authentication Record with Disconnected ESXi Hosts

In this sample, we are updating an existing VMware authentication record to specify that ESXi hosts are disconnected.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=update&ids=1344232&is_disconnect=1"
"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>2021-11-03T12:19:41Z</DATETIME>
```

```
<BATCH_LIST>
  <BATCH>
    <TEXT>Successfully Updated</TEXT>
    <ID_SET>
      <ID>1344232</ID>
    </ID_SET>
  </BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

List VMware Authentication Records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X "POST" -d
"action=list&details=All"
"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_list_out
put.dtd">
<AUTH_VMWARE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-11-22T07:32:21Z</DATETIME>
    <AUTH_VMWARE_LIST>
      <AUTH_VMWARE>
        <ID>409187</ID>
        <TITLE><![CDATA[VMware_Basic]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <PORT>443</PORT>
        <SSL_VERIFY><![CDATA[skip]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-01-23T07:55:13Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-01-23T07:55:13Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_VMWARE>
      <AUTH_VMWARE>
        <ID>1344231</ID>
        <TITLE><![CDATA[VMware_Disconnected_Disabled]]></TITLE>
        <PORT>443</PORT>
        <IP_SET>
```

```

        <IP>10.11.12.13</IP>
    </IP_SET>
    <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
    <DISCONNECTED_ESXI>0</DISCONNECTED_ESXI>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
        <DATETIME>2021-11-03T12:09:53Z</DATETIME>
        <BY>joe_user</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2021-11-10T13:11:23Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_VMWARE>
<AUTH_VMWARE>
    <ID>1344232</ID>
    <TITLE><![CDATA[VMware_Disconnected_Enabled]]></TITLE>
    <PORT>443</PORT>
    <IP_SET>
        <IP>8.9.10.11</IP>
    </IP_SET>
    <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
    <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
    <NETWORK_ID>0</NETWORK_ID>
    <CREATED>
        <DATETIME>2021-11-03T12:16:36Z</DATETIME>
        <BY>joe_user</BY>
    </CREATED>
    <LAST_MODIFIED>
        <DATETIME>2021-11-10T13:10:17Z</DATETIME>
    </LAST_MODIFIED>
</AUTH_VMWARE>
</AUTH_VMWARE_LIST>
<GLOSSARY>
    <USER_LIST>
        <USER>
            <USER_LOGIN>joe_user</USER_LOGIN>
            <FIRST_NAME>Joe</FIRST_NAME>
            <LAST_NAME>User</LAST_NAME>
        </USER>
    </USER_LIST>
</GLOSSARY>
</RESPONSE>
</AUTH_VMWARE_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>
    </TCP_PORTS>
  </HOST_DISCOVERY>
</ADDITIONAL>
...

```

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 nnnnnnn</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
"http://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_title=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>

```