Consulting Edition

Getting Started Guide

April 29, 2019

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

Table of Contents

Welcome to the Qualys Consulting Edition

Qualys Consulting Edition provides consultants, auditors, and managed service providers (MSPs) with the ease of use, scalability, precision and centralized management of the Qualys Cloud Platform. This guide is intended to highlight the unique features of the Qualys Consulting Edition and walk you through the initial set up steps.

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 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/.

Get Started

The main addition to the Qualys Consulting Edition is the Networks feature, which is the cornerstone of multi-tenancy within the platform. Because of this, the first step when starting with Consulting Edition is to add a network for your clients. This feature silos network space for your individual clients and prevents the overlapping of data for assets which share the same IP address. Generally, this is only necessary for client engagements in which you are performing an ongoing assessment.

The Clients Tab associates individual scan instances with the applicable client. This will aid in keeping data organized between all your clients and is especially useful for clients who require ad hoc or periodic scans.

Here's the starting workflow of the platform:

Define networks

Add assets

Create asset groups (manage networks from here)

Add a Virtual Scanner Appliance

Configure scan settings

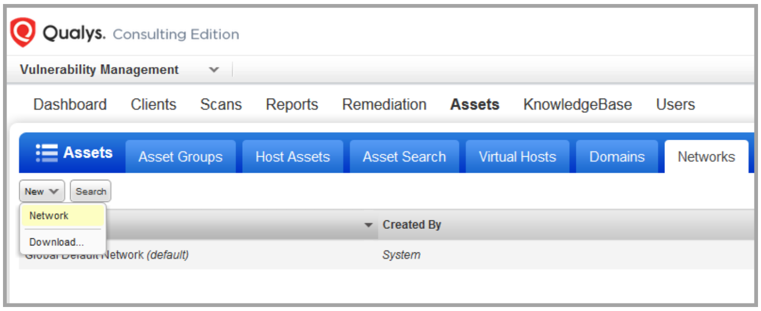
Setup host authentication

Run/Schedule scans

Define networks

Consultants can manage overlapping IP ranges within a single Qualys subscription. Define discrete private networks for each client to keep overlapping blocks isolated from each other. This allows you to easily manage ongoing engagements with clients and track trending information without confusion between environments.

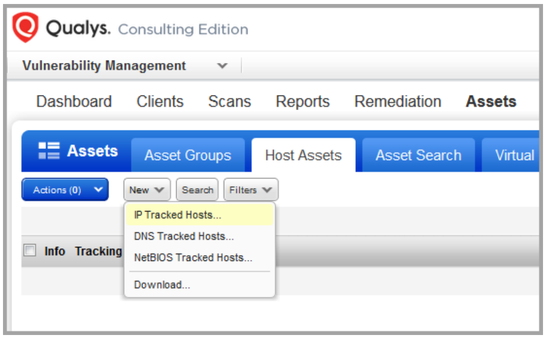
Go to Assets > Networks > New > Network (Manager only), and give your network a friendly name. Save the network. We'll add appliances to it later.



The Global Default Network is used to scan assets that do not belong to custom networks. Want to scan your network perimeter? You'll need to choose the Global Default Network.

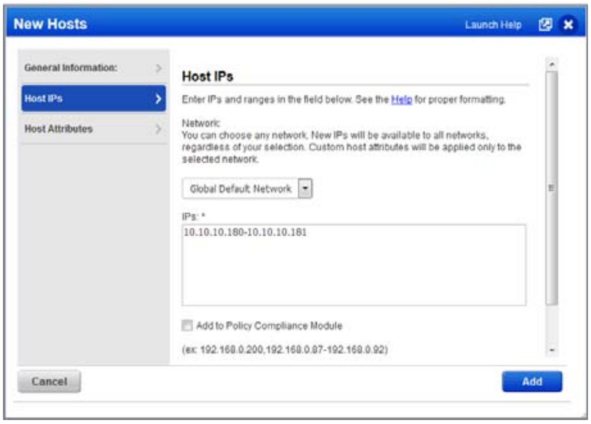
Add assets

You'll need to tell us the IPs/ranges you want to scan and report on. Go to Assets > Host Assets. From the New menu, select IP Tracked Hosts, DNS Tracked Hosts or NetBIOS Tracked Hosts. The tracking method you choose will be assigned to the hosts being added.



Tip - By default we track hosts by IP address. You may want to use DNS or NetBIOS tracking if the hosts on the network are assigned IP addresses dynamically through DHCP.

Jump to the Host IPs tab. Enter the IPs you're adding, and click Add. That's it! The new IPs will appear on your Host Assets list and they'll be available for scanning.



Host IPs

Enter IPs and ranges in the field below. See the Help for proper formatting.

Network:
You can choose any network. New IPs will be available to all networks, regardless of your selection. Custom host attributes will be applied only to the selected network.

Global Default Network

IPs: *
10.10.10.180-10.10.10.181

□ Add to Policy Compliance Module

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Tip - You can keep the Global Default Network selection. New IPs will be available to all networks regardless of your selection.

Which users can add assets?

Unit Managers can be granted the Add Asset permission. In some subscriptions, including consultant subscriptions, Scanner users can also be granted this permission.

The asset being added to an asset group should be a part of the Unit Manager's business unit or assigned to the Scanner user.

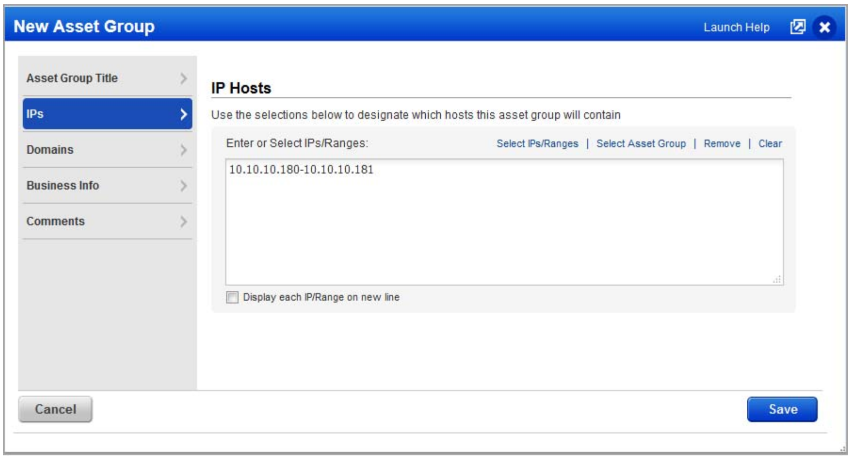
Not sure which IPs to add?

Launch a map to discover live devices on your client's network and add those IPs to your account from the map results. Go here to learn how.

Create asset groups (manage networks from here)

Create asset groups and associate them with your network. Go to Assets > Asset Groups > New > Asset Group. Give your group a name, select a network, and then add assets to it. We recommend you create an asset group for each client, such as Client A, Client B, etc.

Tip - Each asset group can be associated with only one network. Once the asset group is saved, you cannot change its network assignment.



New Asset Group

IP Hosts

Use the selections below to designate which hosts this asset group will contain

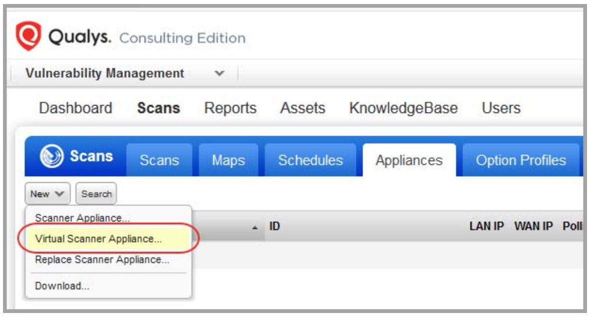
Enter or Select IPs/Ranges: 10.10.10.180-10.10.10.181

Launch Help
Asset Group Title
IPs
Domains
Business Info
Comments
Select IPs/Ranges | Select Asset Group | Remove | Clear
☐ Display each IP/Range on new line
Cancel
Save

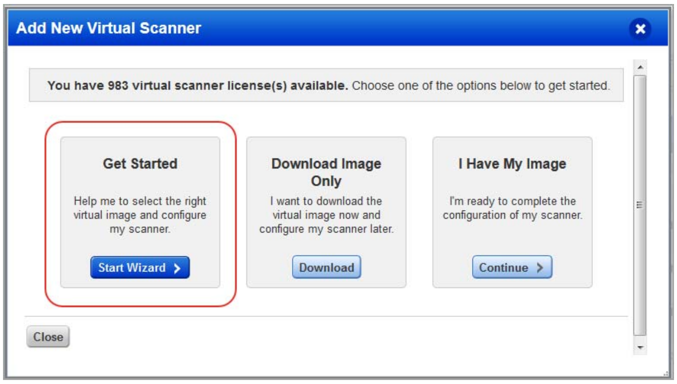
Add a Virtual Scanner Appliance

Add virtual scanners for internal scanning. Then go back to the networks you already created and add appliances to them.

Go to Scans > Appliances and select New > Virtual Scanner Appliance.



Click Start Wizard and we'll walk you through the steps.



Add New Virtual Scanner

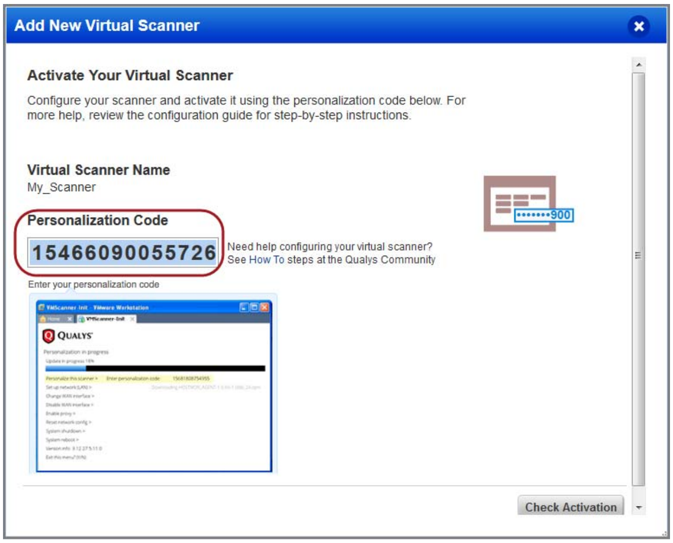
You have 983 virtual scanner license(s) available. Choose one of the options below to get started.

Get Started
Help me to select the right virtual image and configure my scanner.

Download Image Only
I want to download the virtual image now and configure my scanner later.

I Have My Image
I'm ready to complete the configuration of my scanner.

Give your scanner a name, choose a virtualization platform, get your personalization code.



Activate Your Virtual Scanner

Configure your scanner and activate it using the personalization code below. For more help, review the configuration guide for step-by-step instructions.

Virtual Scanner Name
My_Scanner

Personalization Code
15466090055726

Need help configuring your virtual scanner?
See How To steps at the Qualys Community

Enter your personalization code

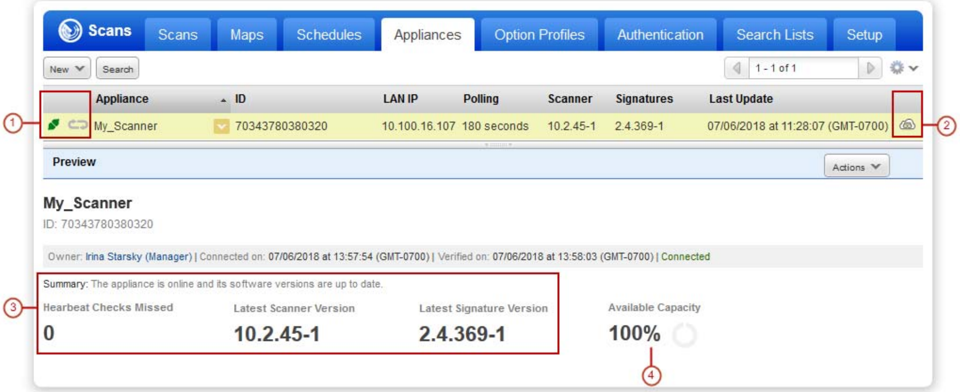
Complete the configuration using the virtual scanner console or cloud platform (this is when you'll need the personalization code).

Be sure activation is successful

Your appliance needs to make a connection to our cloud platform. You'll see the friendly name and IP address when the activation is complete. It may take a few minutes for the appliance activation to occur.

Check your virtual scanner status

Your appliance must be connected to our cloud platform. Go to Scans > Appliances to check your appliance status. Select your scanner and you'll see the preview pane.



	Appliance	ID	LAN IP	Polling	Scanner	Signatures	Last Update	
	My_Scanner	70343780380320	10.100.16.107	180 seconds	10.2.45-1	2.4.369-1	07/06/2018 at 11:28:07 (GMT-0700)	

My_Scanner
ID: 70343780380320

Owner: Irina Starsky (Manager) | Connected on: 07/06/2018 at 13:57:54 (GMT-0700) | Verified on: 07/06/2018 at 13:58:03 (GMT-0700) | Connected

Summary: The appliance is online and its software versions are up to date.

Hearbeat Checks Missed	Latest Scanner Version	Latest Signature Version	Available Capacity
0	10.2.45-1	2.4.369-1	100%

1 - tells you the virtual scanner is ready. Now you can start internal scans! Next to this you'll see the busy icon is grayed out until you launch a scan using this scanner.

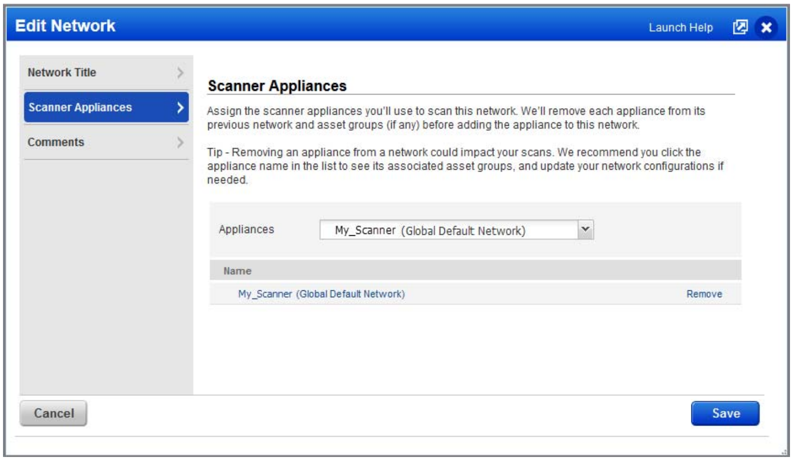
2 - This shows you it's a virtual appliance.

3 - Latest software versions - these are installed as part of the activation.

4 - The available capacity will be 100% until you launch a scan.

Add the scanner to a network

Go to Assets > Networks, identify the network you're interested in and choose Edit from the Quick Actions menu. Then go to the Scanner Appliances tab to add your appliance to the network.



Scanner Appliances

Assign the scanner appliances you'll use to scan this network. We'll remove each appliance from its previous network and asset groups (if any) before adding the appliance to this network.

Tip - Removing an appliance from a network could impact your scans. We recommend you click the appliance name in the list to see its associated asset groups, and update your network configurations if needed.

Appliances: My_Scanner (Global Default Network)

Name	
My_Scanner (Global Default Network)	Remove

Good to Know

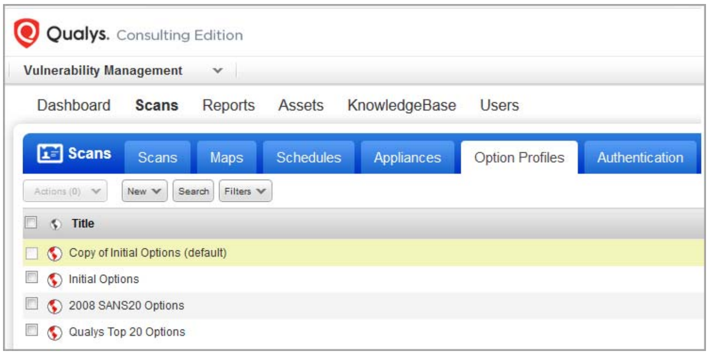
- The scanner appliances you assign to the network will be used to scan the IP addresses in the network.

- Each scanner appliance can be included in only one network. That means when you add a scanner appliance to a network, it will be removed from its previous network and any asset groups that it belonged to, if applicable.

- Be sure the scanner appliances you add to the network will be able to phone home to the Qualys Cloud Platform and can access the IP addresses that you will be scanning.

Configure scan settings

An option profile includes scan settings that you'll choose at scan time. We provide the "Initial Options" profile to get you started but you can also create your own. Go to Scans > Option Profiles. Create a profile from the New menu or edit a default profile to save a copy with customized settings.



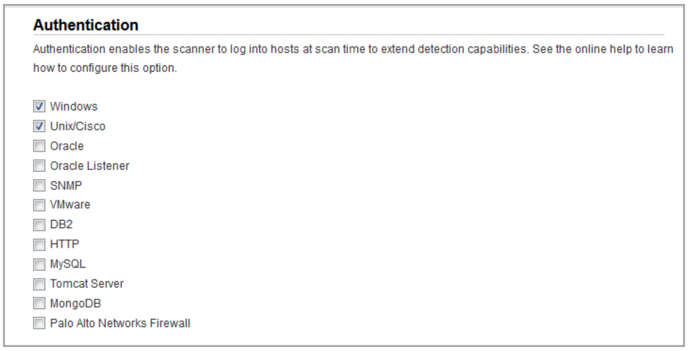
Title
□ Copy of Initial Options (default)
□ Initial Options
□ 2008 SANS20 Options
□ Qualys Top 20 Options

Setup host authentication

Using host authentication (trusted scanning) allows our service to log in to each target system during scanning. For this reason we can perform in depth security assessment and get better visibility into each system's security posture. Running authenticated scans gives you the most accurate results with fewer false positives. How to setup authentication:

Enable authentication in the option profile

In the option profile, go to the Scan tab, scroll down to Authentication, and select each type of authentication you want to use. We're always adding new technologies.



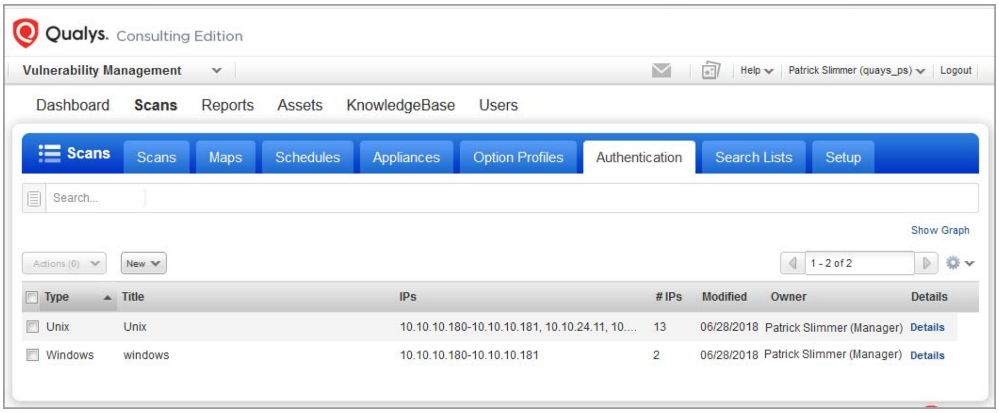
Authentication

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.

☑ Windows
☑ Unix/Cisco
□ Oracle
□ Oracle Listener
□ SNMP
□ VMware
□ DB2
□ HTTP
□ MySQL
□ Tomcat Server
□ MongoDB
□ Palo Alto Networks Firewall

Add authentication records

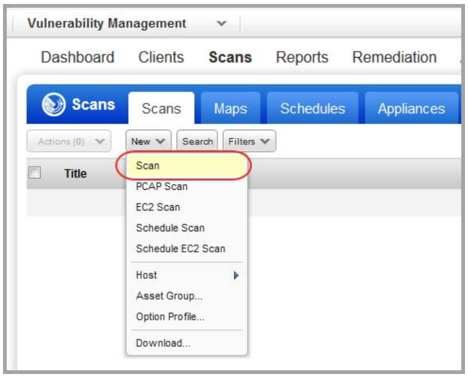
Add authentication records for the host technologies you're interested in. Go to Scans > Authentication and create new records from the New menu. For each record you'll provide login credentials that our service will use to log in to each host at scan time.



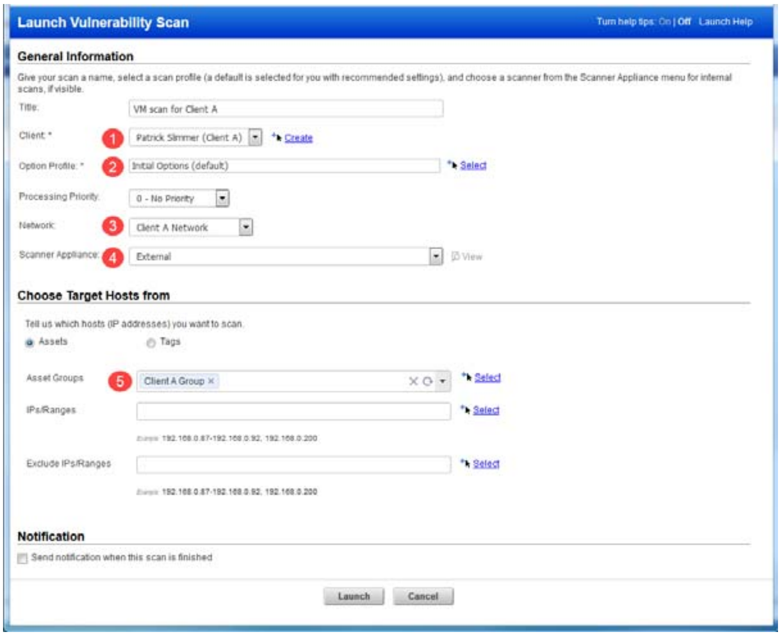
Type	Title	IPs	# IPs	Modified	Owner	Details
Unix	Unix	10.10.10.180-10.10.10.181, 10.10.24.11, 10....	13	06/28/2018	Patrick Slimmer (Manager)	Details
Windows	windows	10.10.10.180-10.10.10.181	2	06/28/2018	Patrick Slimmer (Manager)	Details

Run/Schedule scans

Go to Scans > Scans > New Scan. (Want to schedule your scan?)



Choose your scan settings.



Launch Vulnerability Scan

General Information

Give your scan 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: VM scan for Client A

Client: * (1) Patrick Slimmer (Client A) Create

Option Profile: * (2) Initial Options (default) Select

Processing Priority: 0 - No Priority

Network: (3) Client A Network

Scanner Appliance: (4) External View

Choose Target Hosts from

Tell us which hosts (IP addresses) you want to scan.

● Assets ○ Tags

Asset Groups (5) Client A Group × Select

IPs/Ranges Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Notification

□ Send notification when this scan is finished

(1) Client - Choose the client you want to scan. Click Create to add a client at this time. You'll provide client information like name, email and company address.

(2) Option Profile - You can select one of the default profiles provided or a custom profile that you previously saved.

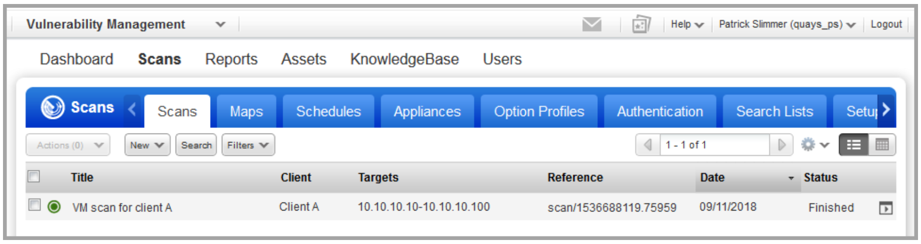
(3) Network - Choose the network you want to scan. You can scan one network at a time. If you didn't set up networks then you won't see this option.

(4) Scanner Appliance - If you added a virtual scanner then you can choose the scanner for an internal scan. If you don't have a scanner, we'll use external scanners for a perimeter scan.

(5) Scan Target - Click Assets to select a combination of asset groups and IP addresses to scan. Or Click Tags to select one or more asset tags to scan.

That's it - just click Launch and you're done.

You'll see your scan in the scans list where you can track its progress.



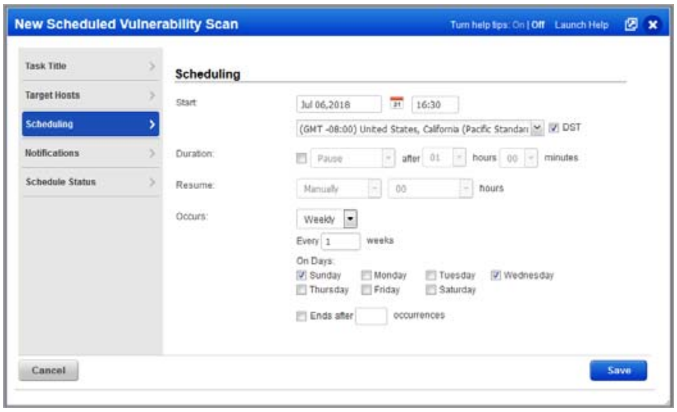
□	Title	Client	Targets	Reference	Date	Status
□ ●	VM scan for client A	Client A	10.10.10.10-10.10.10.100	scan/1536688119.75959	09/11/2018	Finished

● means results are processed and available in your account.

○ means the scan is finished but the results are not processed. Go to Filters > Processing Tasks to see the status.

Want to schedule your scan?

You can schedule the scan to run Daily, Weekly or Monthly. Just choose New > Schedule Scan. Like with an on demand scan, you'll select the client, an option profile, scanner appliance and target hosts. You'll also need to tell us when you want the scan to start and how often it should run. Make these settings on the Scheduling tab.



Scheduling

Start: Jul 06,2018 16:30
(GMT -08:00) United States, California (Pacific Standard ☑ DST

Duration: □ Pause after 01 hours 00 minutes

Resume: Manually 00 hours

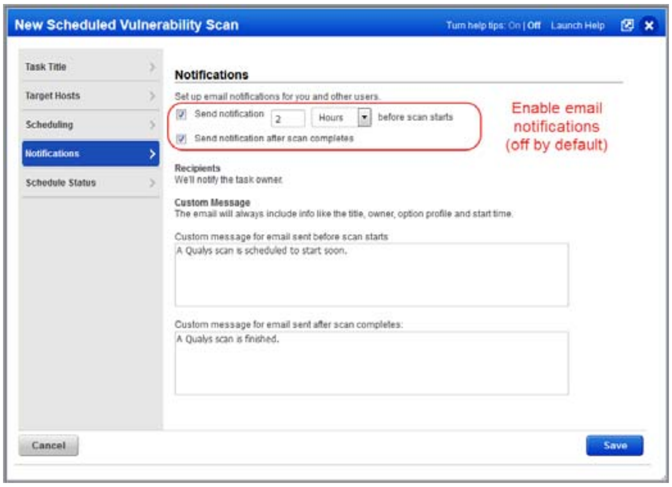
Occurs: Weekly

Every 1 weeks

On Days:
☑ Sunday □ Monday □ Tuesday ☑ Wednesday
□ Thursday □ Friday □ Saturday

□ Ends after occurrences

Go to the Notifications tab if you want to be notified by email before the scan starts or when it's finished. You can even customize the message included in the email body.



Notifications

Set up email notifications for you and other users.

☑ Send notification 2 Hours before scan starts

☑ Send notification after scan completes

Enable email notifications (off by default)

Recipients
We'll notify the task owner.

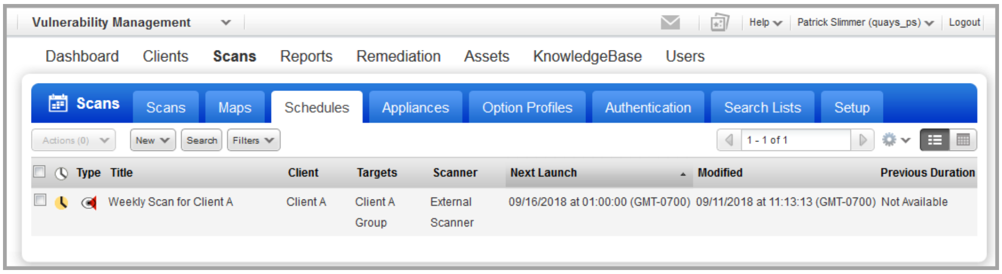
Custom Message
The email will always include info like the title, owner, option profile and start time.

Custom message for email sent before scan starts
A Qualys scan is scheduled to start soon.

Custom message for email sent after scan completes:
A Qualys scan is finished.

Note - You are the task owner. Notifications will be sent to the email address saved in your account.

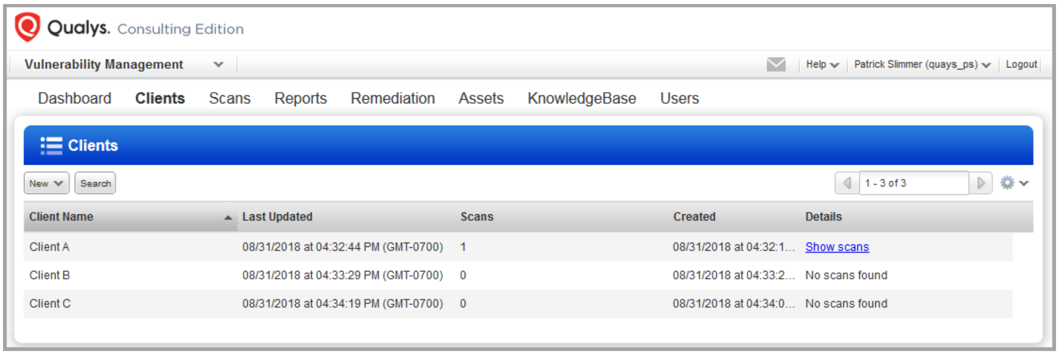
Hit Save to save your scheduled scan. It will appear on the Schedules list. When the scan starts running (at its next scheduled launch time) you'll see it on the Scans list where you can track the status and view results when it's finished.



Type	Title	Client	Targets	Scanner	Next Launch	Modified	Previous Duration
	Weekly Scan for Client A	Client A	Client A Group	External Scanner	09/16/2018 at 01:00:00 (GMT-0700)	09/11/2018 at 11:13:13 (GMT-0700)	Not Available

View scan results by client

Go to your Clients list to see all scan instances conducted for all of your clients in one location. Quickly view scan results for any client by clicking the "Show scans" link.



Client Name	Last Updated	Scans	Created	Details
Client A	08/31/2018 at 04:32:44 PM (GMT-0700)	1	08/31/2018 at 04:32:1...	Show scans
Client B	08/31/2018 at 04:33:29 PM (GMT-0700)	0	08/31/2018 at 04:33:2...	No scans found
Client C	08/31/2018 at 04:34:19 PM (GMT-0700)	0	08/31/2018 at 04:34:0...	No scans found

PCAP Scans

With a PCAP Scan you'll get vulnerability scan results plus a PCAP (Packet Capture) file that contains all TCP network traffic captured between the scanner and the target host.

Good to Know

- The PCAP Scanning feature must be enabled for your account. Please contact your Technical Account Manager or Support to get it.

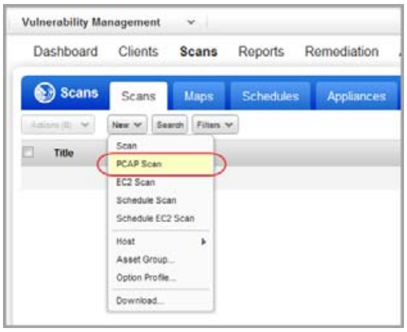
- A scanner appliance (physical or virtual) is required.

- You can scan one IP address at a time.

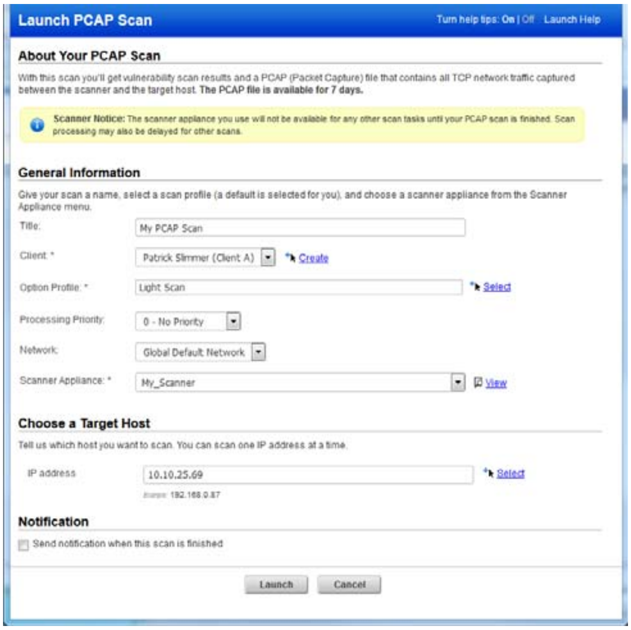
- The PCAP file will be available for 7 days. You'll need a PCAP Viewer to read file contents.

Start a PCAP Scan

Go to Scans > New > PCAP Scan.



Give your scan a name, select a client, select an option profile, and choose a scanner appliance. Then tell us the host you want to scan (a single IP) and click Launch.



Launch PCAP Scan

About Your PCAP Scan

With this scan you'll get vulnerability scan results and a PCAP (Packet Capture) file that contains all TCP network traffic captured between the scanner and the target host. **The PCAP file is available for 7 days.**

Scanner Notice: The scanner appliance you use will not be available for any other scan tasks until your PCAP scan is finished. Scan processing may also be delayed for other scans.

General Information

Give your scan a name, select a scan profile (a default is selected for you), and choose a scanner appliance from the Scanner Appliance menu.

Title: My PCAP Scan

Client: * Patrick Slimmer (Client A) Create

Option Profile: * Light Scan Select

Processing Priority: 0 - No Priority

Network: Global Default Network

Scanner Appliance: * My_Scanner View

Choose a Target Host

Tell us which host you want to scan. You can scan one IP address at a time.

IP address 10.10.25.69 Select

192.168.0.87

Notification

□ Send notification when this scan is finished

Launch Cancel

Important - The scanner appliance you use will not be available for any other scan tasks until your PCAP scan is finished. Scan processing may be delayed for other scans.

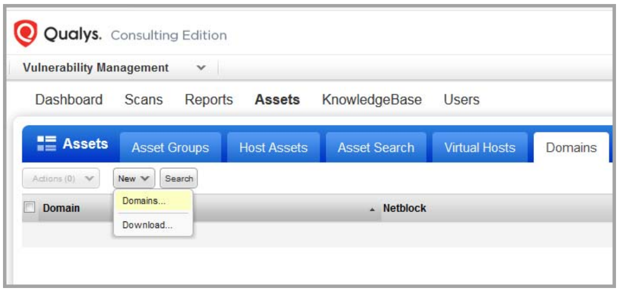
When the scan is finished, you can view scan results and download the PCAP file. Choose PCAP File from the Quick Actions menu. After 7 days the file is no longer available for download.

Discover Your Network

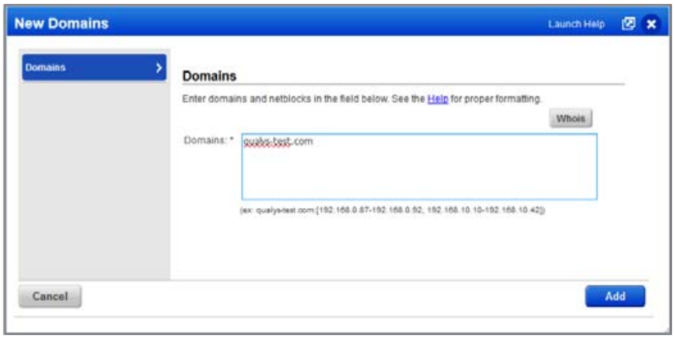
Launch maps to discover network devices and report comprehensive information about them. After discovering live devices on a network you can add them to your account and start scanning them for vulnerabilities.

Add domains for mapping

Qualys uses a domains concept for its network mapping process. "Domain" in this context is our name for a DNS entry, for a netblock, or for a combination. Go to Assets > Domains and select New > Domain.



Enter one or more domains and netblocks (see the help for proper formatting). Click Add.



Domains

Enter domains and netblocks in the field below. See the Help for proper formatting.

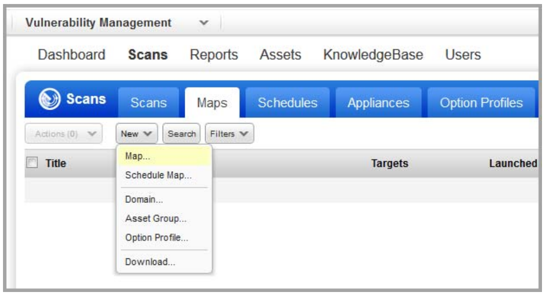
Domains: * qualys-test.com

(ex: qualys-test.com:[192.168.0.87-192.168.0.92, 192.168.10.10-192.168.10.42])

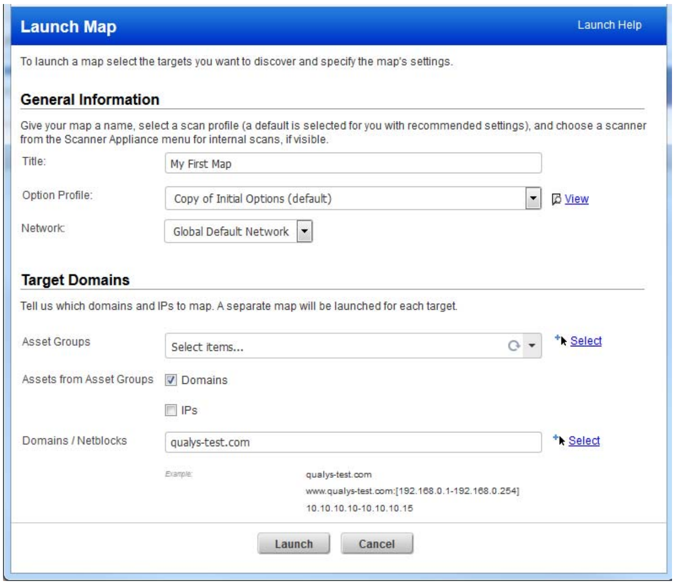
Qualys provides a demo domain called "qualys-test.com" for network mapping. This domain may already be in your account. If not you can add it yourself. Note that the devices in the demo domain reside in Qualys Security Operations Centers, so the Qualys Internet scanners can be used for mapping this domain.

Start your map

Go to Scans > Maps, then select New > Map (or Schedule Map).



Choose your map options.



Launch Map

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: My First Map

Option Profile: Copy of Initial Options (default)

Network: Global Default Network

Target Domains

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

Asset Groups: Select items...

Assets from Asset Groups: ☑ Domains ☐ IPs

Domains / Netblocks: qualys-test.com

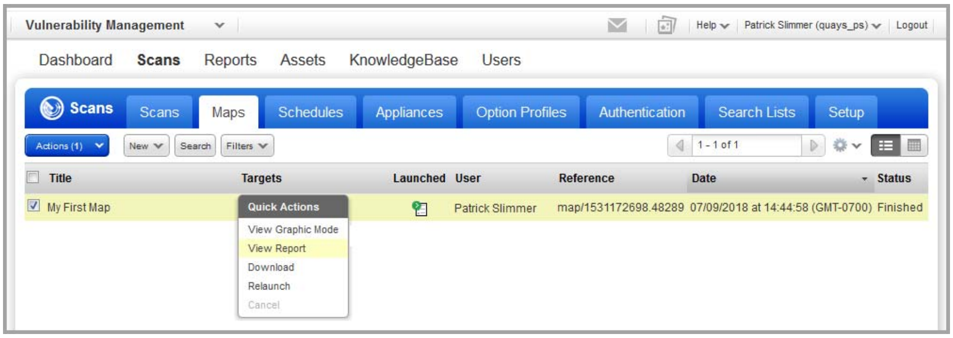
Example:
qualys-test.com
www.qualys-test.com:[192.168.0.1-192.168.0.254]
10.10.10.10-10.10.10.15

Option Profile - Choose an option profile with the map settings you want to use. Tip - For mapping IPs/ranges without a domain, be sure to enable the map option “Perform live host sweep” in the option profile applied to the task.

Target Domains - Specify any combination of asset groups, domains and IPs/ranges for your map target. Enter asset groups in the Asset Groups field, and enter domains and IPs in the Domains/Netblocks field.

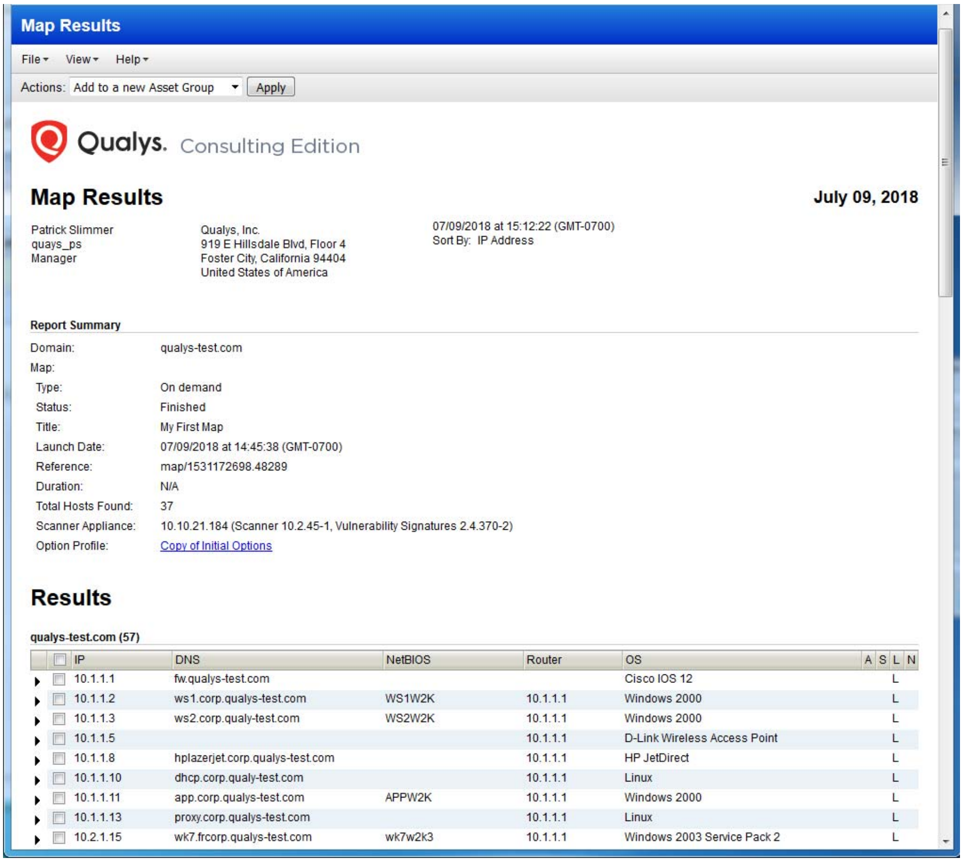
We’ll create a separate map report for each target. That means we’ll create a separate map for each domain plus a map for any IPs entered. These maps will run sequentially - one at a time - and each map will use a single scanner appliance.

When the map status is Finished, choose View Report from the Quick Actions menu.



Title	Targets	Launched	User	Reference	Date	Status
☑ My First Map			Patrick Slimmer	map/1531172698.48289	07/09/2018 at 14:44:58 (GMT-0700)	Finished

In the Results section you'll see a list of the hosts detected on the mapped domain. For each host, you'll see the IP address, DNS and NetBIOS hostnames, the router being used by the host and the operating system.


Map Results
File ▾ View ▾ Help ▾
Actions: Add to a new Asset Group ▾ Apply
Qualys. Consulting Edition

Map Results **July 09, 2018**

Patrick Slimmer
quays_ps
Manager

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

07/09/2018 at 15:12:22 (GMT-0700)
Sort By: IP Address

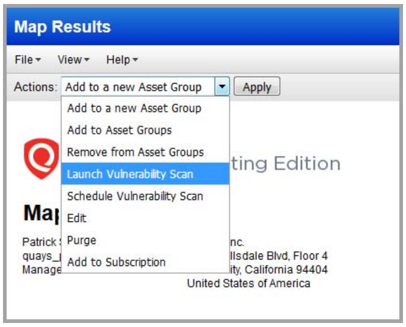
Report Summary

Domain:	qualys-test.com
Map:	
Type:	On demand
Status:	Finished
Title:	My First Map
Launch Date:	07/09/2018 at 14:45:38 (GMT-0700)
Reference:	map/1531172698.48289
Duration:	N/A
Total Hosts Found:	37
Scanner Appliance:	10.10.21.184 (Scanner 10.2.45-1, Vulnerability Signatures 2.4.370-2)
Option Profile:	Copy of Initial Options

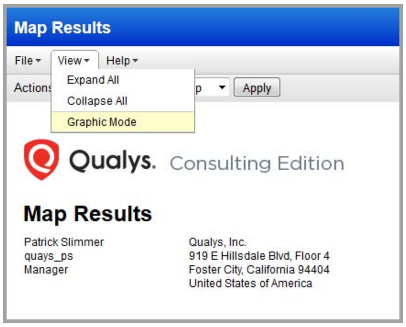
Results

qualys-test.com (57)

	☐	IP	DNS	NetBIOS	Router	OS	A	S	L	N
▸	☐	10.1.1.1	fw.qualys-test.com			Cisco IOS 12			L	
▸	☐	10.1.1.2	ws1.corp.qualys-test.com	WS1W2K	10.1.1.1	Windows 2000			L	
▸	☐	10.1.1.3	ws2.corp.qualy-test.com	WS2W2K	10.1.1.1	Windows 2000			L	
▸	☐	10.1.1.5			10.1.1.1	D-Link Wireless Access Point			L	
▸	☐	10.1.1.8	hplazerjet.corp.qualys-test.com		10.1.1.1	HP JetDirect			L	
▸	☐	10.1.1.10	dhcp.corp.qualy-test.com		10.1.1.1	Linux			L	
▸	☐	10.1.1.11	app.corp.qualys-test.com	APPW2K	10.1.1.1	Windows 2000			L	
▸	☐	10.1.1.13	proxy.corp.qualys-test.com		10.1.1.1	Linux			L	
▸	☐	10.2.1.15	wk7.frcorp.qualys-test.com	wk7w2k3	10.1.1.1	Windows 2003 Service Pack 2			L	



Map results are closely integrated with scan capabilities. There are several actions you can perform on the hosts listed in your map results. For example, you can scan hosts right away, you can add newly discovered hosts to your account. Select the check box next to each host to include in the action, select an action from the Actions drop-down menu (at the top of the report), and then click Apply.



Map Results

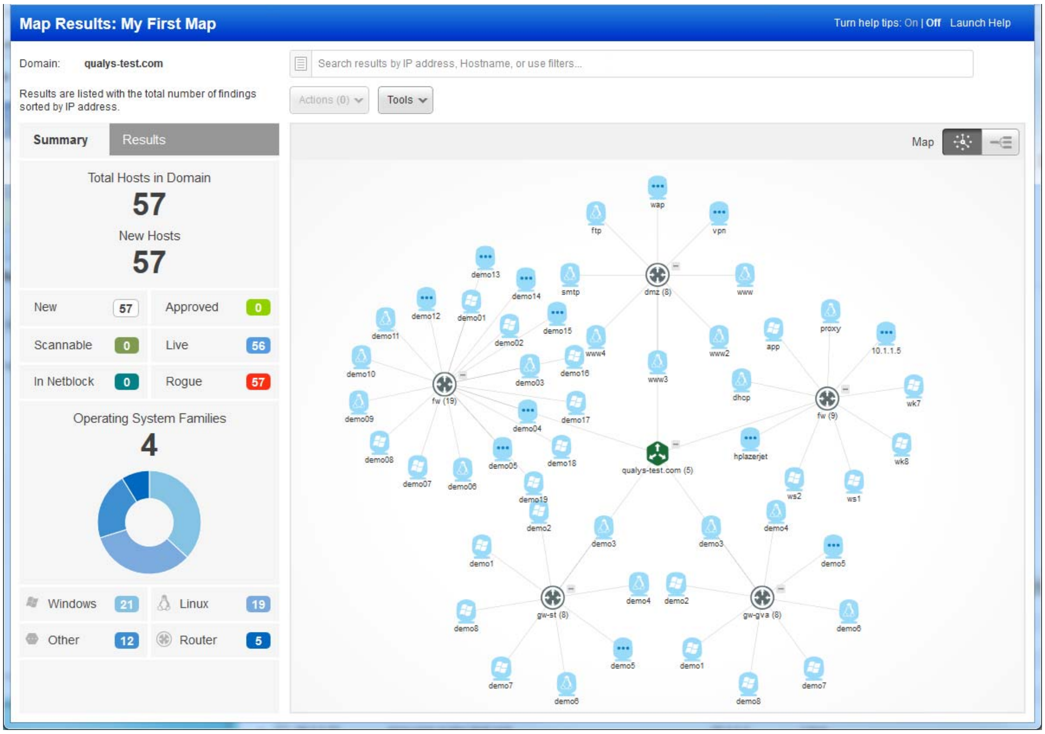
Map Results

Patrick Slimmer
quays_ps
Manager

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

Go to View > Graphic Mode to change the format of your map results to graphic mode.

Your map results will appear in a graphical view like shown below. Use the Summary on the left to drill-down into results or enter a search query at the top of the page.



Map Results: My First Map

Domain: qualys-test.com

Results are listed with the total number of findings sorted by IP address.

Total Hosts in Domain
57

New Hosts
57

New	57	Approved	0
Scannable	0	Live	56
In Netblock	0	Rogue	57

Operating System Families
4

Windows	21	Linux	19
Other	12	Router	5

Deploy Cloud Agents

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents for continuous security and compliance assessments. Group agents using asset tags that are based on the asset groups you created for your clients earlier.

Overview

With Qualys Cloud Agent you'll get continuous network security updates through the cloud. As soon as changes are discovered on your hosts they'll be assessed and you'll know about new security threats right away. All you have to do is install lightweight agents on your hosts - we'll help you do this quickly!

Install lightweight agents in minutes on your IT assets. These can be installed on your on-premise systems, dynamic cloud environments and mobile endpoints. Agents are centrally managed by the cloud agent platform and are self-updating (no reboot needed).

Scanning in the Cloud We'll start syncing asset data to the cloud agent platform once agents are installed. Agents continuously collect metadata, beam it to the cloud agent platform where full assessments occur right away. Since the heavy lifting is done in the cloud the agent needs minimal footprint and processing on target systems.

Stay updated with network security Scanning in the cloud uses the same signatures (vulnerabilities, compliance datapoints) as traditional scanning with Qualys scanners. You'll get informed right away about new security threats using your Qualys Cloud Platform applications - Vulnerability Management (VM), Policy Compliance (PC), Continuous Monitoring (CM), AssetView (AV) and more!

What do I need to know?

There are a few things to know before you install agents on hosts within your network.

We recommend these resources

Cloud Agent Platform Introduction (2m 10 s)

Getting Started Tutorial (4m 58s)

Qualys Cloud Platform

Qualys Cloud Agent Getting Started Guide

Cloud Agent requirements

- We support: Windows, Linux/Unix (.rpm), Linux (.deb), Apple Mac OSX (.pkg)

- Your hosts must be able to reach the Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Go to Help > About for the URL your hosts need to access.

- To install Windows Agent you must have local administrator privileges on your hosts. Proxy configuration is supported

- To install Linux Agent, Unix Agent, Mac Agent you must have root privileges, non-root with Sudo root delegation, or non-root with sufficient privileges (VM scan only). Proxy configuration is supported.

Steps to install agents

- Create an activation key. This lets you group agents and bind them to your account.

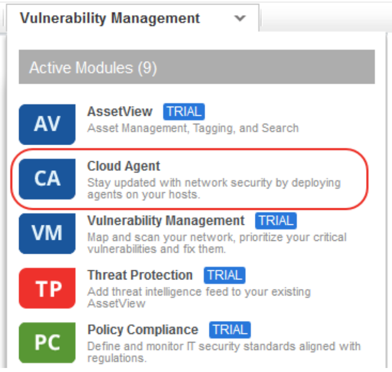
- Download the agent installer to your local machine.

- Run the installer on each host from an elevated command prompt, or use group policy or a systems management tool.

- Activate agents for modules in your subscription (i.e. VM, PC, etc). A license will be consumed for each agent activated.

Get Started

Select the Cloud Agent app from the app picker.



Asset Management, Tagging, and Search

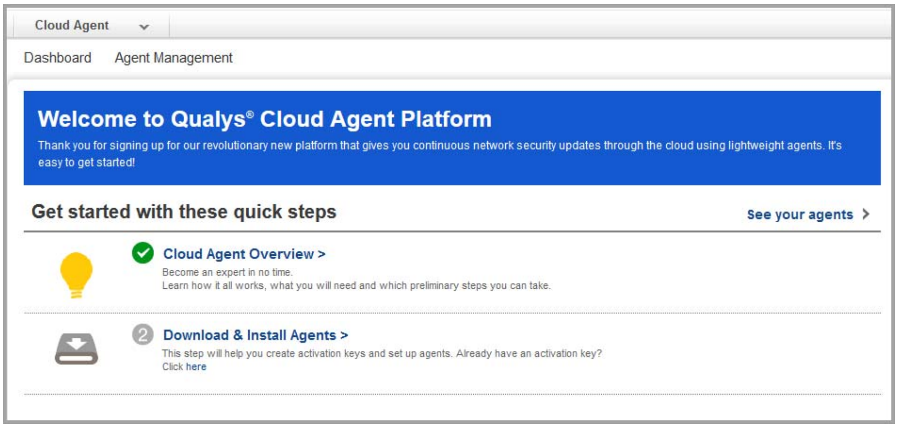
Stay updated with network security by deploying agents on your hosts.

Map and scan your network, prioritize your critical vulnerabilities and fix them.

Add threat intelligence feed to your existing AssetView

Define and monitor IT security standards aligned with regulations.

Check out the Quick Start Guide (you can go to user name menu and select this option anytime). You'll see step by step instructions with links to the right places to take actions.



Welcome to Qualys® Cloud Agent Platform

Thank you for signing up for our revolutionary new platform that gives you continuous network security updates through the cloud using lightweight agents. It's easy to get started!

Get started with these quick steps

Cloud Agent Overview >

Become an expert in no time.
Learn how it all works, what you will need and which preliminary steps you can take.

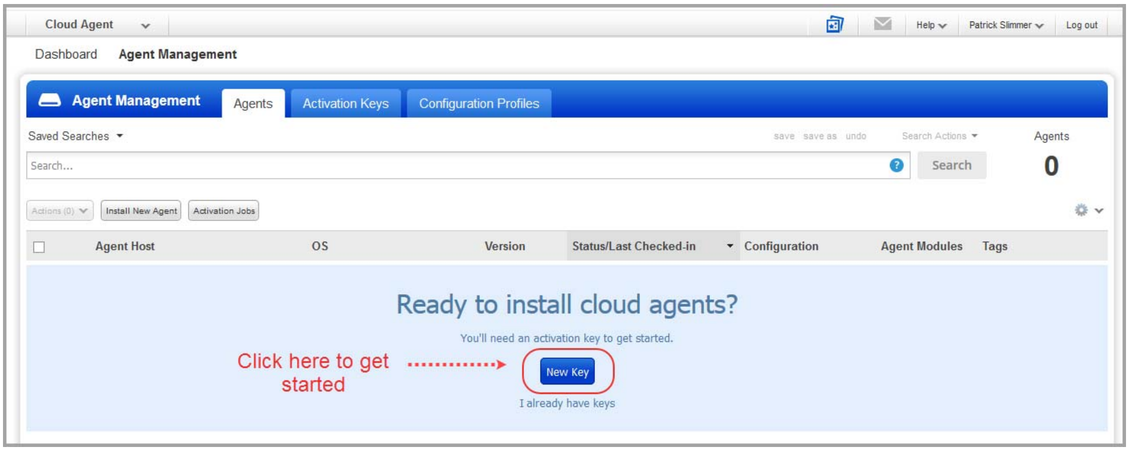
2 Download & Install Agents >

This step will help you create activation keys and set up agents. Already have an activation key? Click here

It’s easy to install agents

It just takes a few minutes to install an agent. Our wizard will help you do it quickly.

You’ll need an activation key. Select New Key to create one.This key provides a way to group agents and bind them to your account.



Ready to install cloud agents?

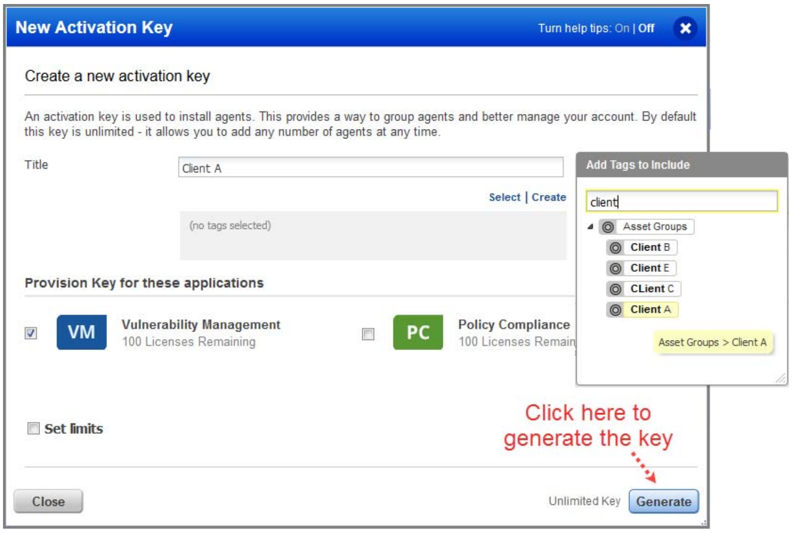
You'll need an activation key to get started.

Click here to get started

We recommend you create different keys for different clients. Give your key a name (e.g. Client A) and assign the key an asset tag (e.g. Client A). We’ll automatically add the same tag to the agents installed using that key.

Did you know? We’ve defined certain tags for you. You’ll have one asset tag for each asset group in your account. That means if you created asset groups for your clients (Client A, Client B, etc.) then you already have asset tags for your clients.

Next, provision the key for the VM application. If you have additional apps like PC, FIM and IOC then you’ll see them listed as well. Click Generate.



Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Client A

Add Tags to Include: client

Provision Key for these applications

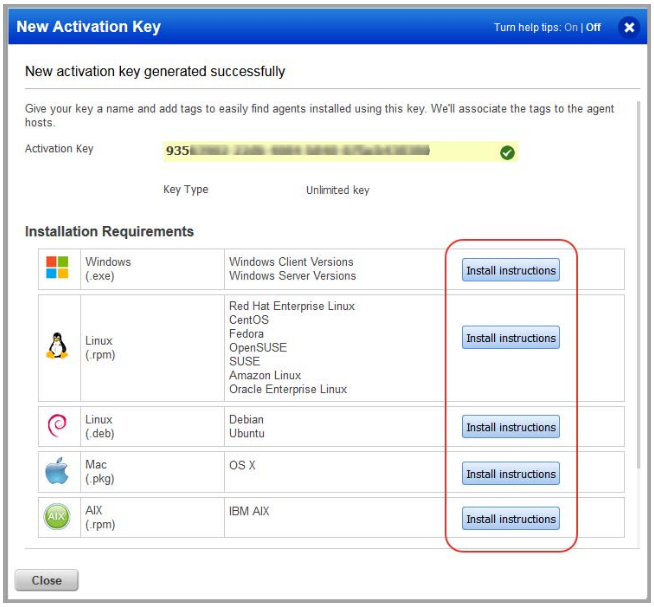
☑ Vulnerability Management
100 Licenses Remaining

☐ Policy Compliance
100 Licenses Remain

☐ Set limits

Click here to generate the key

Review requirements and click Install Instructions for the target agent host.



New activation key generated successfully

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

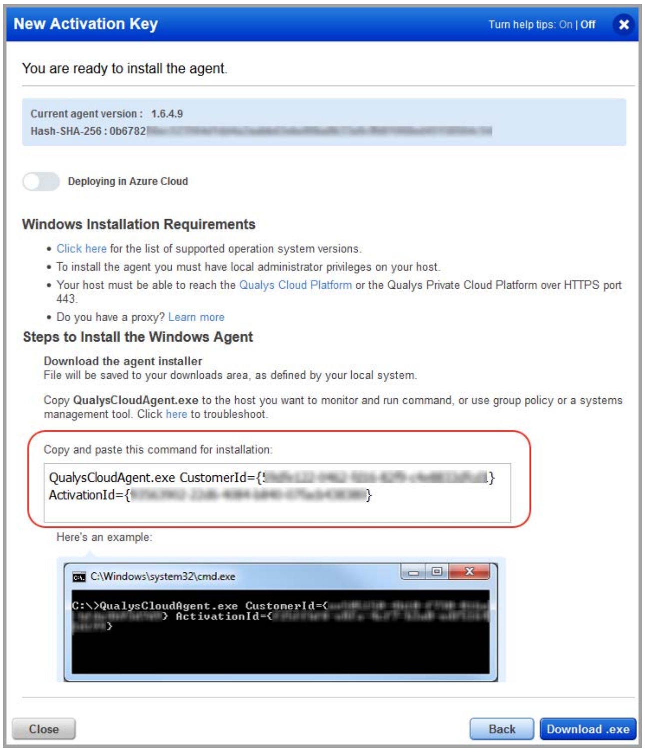
Activation Key 935[redacted] ✓

Key Type Unlimited key

Installation Requirements

Windows (.exe)	Windows Client Versions Windows Server Versions	Install instructions
Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux	Install instructions
Linux (.deb)	Debian Ubuntu	Install instructions
Mac (.pkg)	OS X	Install instructions
AIX (.rpm)	IBM AIX	Install instructions

You'll download the agent installer and run it on your hosts. To run the installer you just copy and paste the command shown - it's that simple.



You are ready to install the agent.

Current agent version : 1.6.4.9
Hash-SHA-256 : 0b6782[redacted]

Deploying in Azure Cloud

Windows Installation Requirements

- Click here for the list of supported operation system versions.
- To install the agent you must have local administrator privileges on your host.
- Your host must be able to reach the Qualys Cloud Platform or the Qualys Private Cloud Platform over HTTPS port 443.
- Do you have a proxy? Learn more

Steps to Install the Windows Agent

Download the agent installer
File will be saved to your downloads area, as defined by your local system.

Copy **QualysCloudAgent.exe** to the host you want to monitor and run command, or use group policy or a systems management tool. Click here to troubleshoot.

Copy and paste this command for installation:

```
QualysCloudAgent.exe CustomerId={[redacted]}
ActivationId={[redacted]}
```

Here's an example:

```
C:\Windows\system32\cmd.exe
C:\>QualysCloudAgent.exe CustomerId={[redacted]} ActivationId={[redacted]}
```

Run the installer on each host from an elevated command prompt, or use group policy or a systems management tool.

Our installation guides will help you with additional options like setting up proxy support, and more.

Installation Guides:

Windows Agent

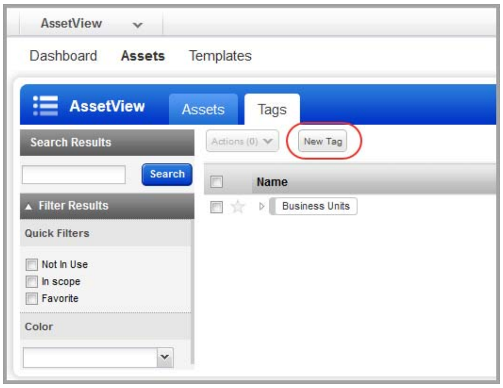
Linux Agent

Unix Agent

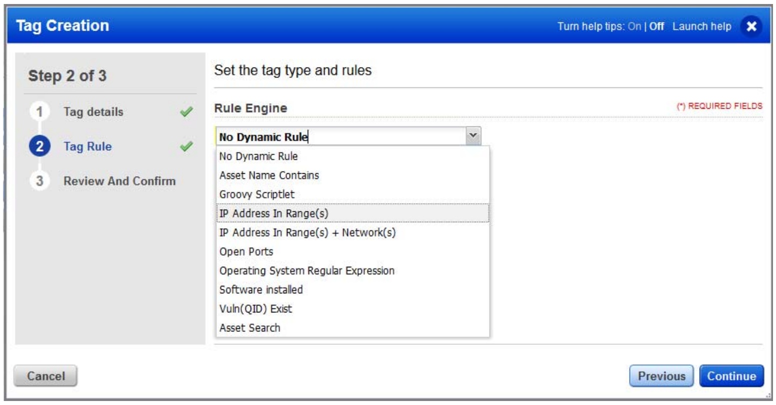
Mac Agent

Want to create more tags?

As previously mentioned we've defined certain tags for you like tags that correspond to your asset groups. You can also create your own custom tags. To get started, choose the AssetView app from the app picker. Then go to the Tags section and click New Tag.



In the Tag Creation wizard, enter the settings for your tag. You'll give the tag a name and configure a tag rule. The rule is used to evaluate asset data returned by scans. When asset data matches a tag rule we'll automatically add the tag to the asset.



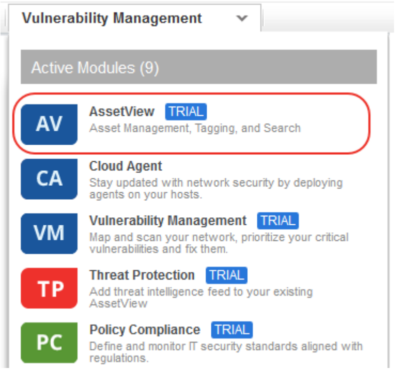
Tip - Turn help tips on (in the wizard title bar) and we'll show you help as you hover over the settings.

Analyze, Query & Report

In this section we'll cover how to query assets, build widgets and dashboards in AssetView and how to create reports in VM.

How to Query Assets

Select the AssetView app from the app picker.



AssetView TRIAL
Asset Management, Tagging, and Search

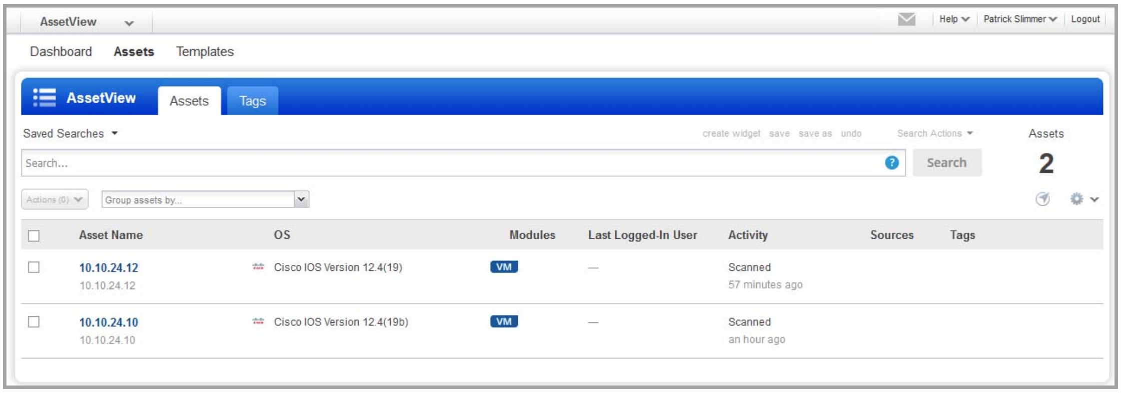
Cloud Agent
Stay updated with network security by deploying agents on your hosts.

Vulnerability Management TRIAL
Map and scan your network, prioritize your critical vulnerabilities and fix them.

Threat Protection TRIAL
Add threat intelligence feed to your existing AssetView

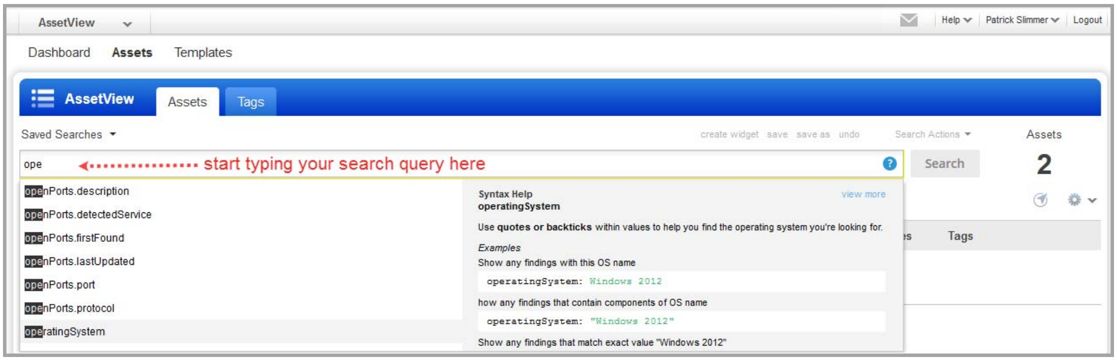
Policy Compliance TRIAL
Define and monitor IT security standards aligned with regulations.

Go to the Assets tab. This is where you'll see an inventory of all your scanned assets.



□	Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
□	10.10.24.12 10.10.24.12	Cisco IOS Version 12.4(19)	VM	—	Scanned 57 minutes ago		
□	10.10.24.10 10.10.24.10	Cisco IOS Version 12.4(19b)	VM	—	Scanned an hour ago		

Start typing in the search field and you'll see a list of asset properties (tokens) you can use to search. Hover over the token name to see syntax help to the right.



ope ◄·················· start typing your search query here

openPorts.description
openPorts.detectedService
openPorts.firstFound
openPorts.lastUpdated
openPorts.port
openPorts.protocol
operatingSystem

Syntax Help
operatingSystem
view more

Use **quotes or backticks** within values to help you find the operating system you're looking for.

Examples
Show any findings with this OS name

```
operatingSystem: Windows 2012
```

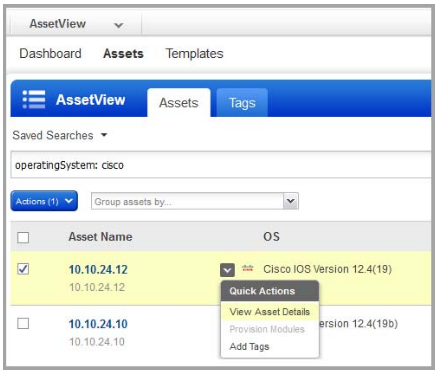
how any findings that contain components of OS name

```
operatingSystem: "Windows 2012"
```

Show any findings that match exact value "Windows 2012"

View Asset Details anytime

The latest vulnerability data is always available in your assets inventory. Just select the asset name and choose View Asset Details from the quick actions menu.

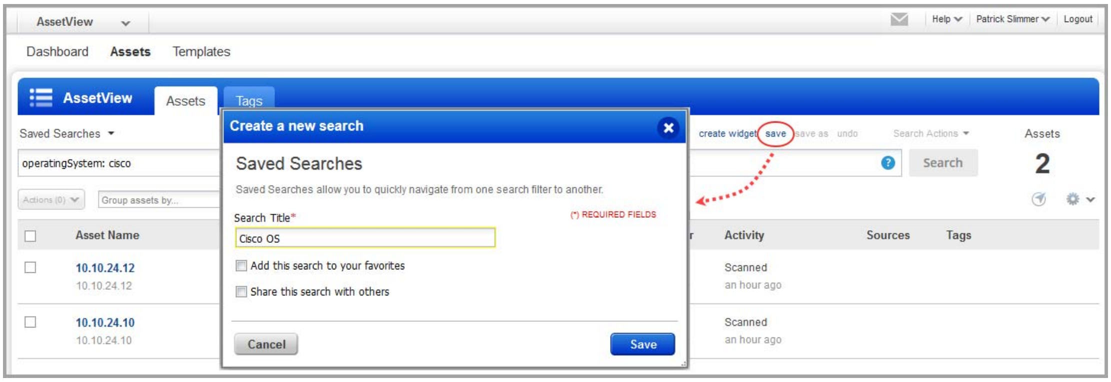


operatingSystem: cisco

☐	Asset Name	OS
☑	10.10.24.12 10.10.24.12	Cisco IOS Version 12.4(19)
☐	10.10.24.10 10.10.24.10	ersion 12.4(19b)

Save Query

Easily save your searches for reuse and share them with others.



operatingSystem: cisco

Create a new search

Saved Searches

Saved Searches allow you to quickly navigate from one search filter to another.

Search Title* (*) REQUIRED FIELDS

Cisco OS

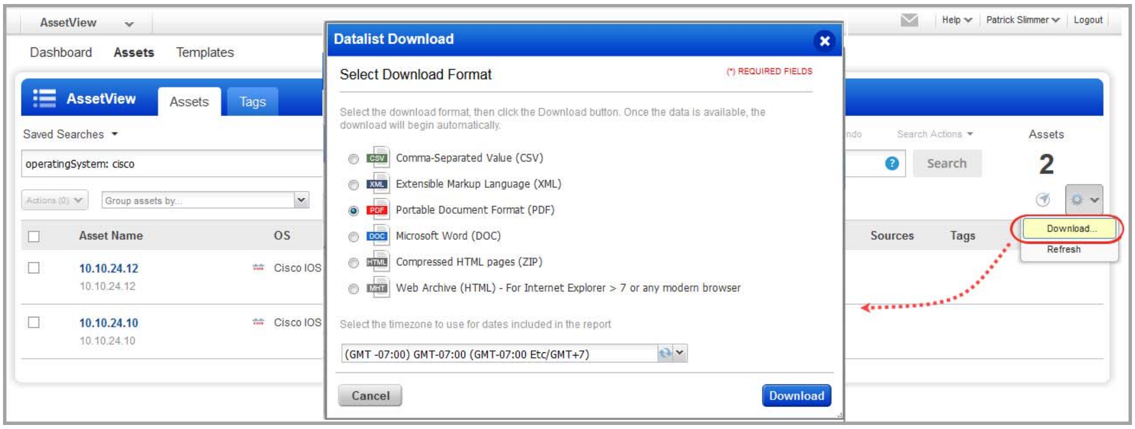
☐ Add this search to your favorites

☐ Share this search with others

☐	Asset Name	Activity	Sources	Tags
☐	10.10.24.12 10.10.24.12	Scanned an hour ago		
☐	10.10.24.10 10.10.24.10	Scanned an hour ago		

Download and export results

It just takes a minute to export search results. Select Download from the Tools menu. Next choose an export format and click Download.



operatingSystem: cisco

Datalist Download

Select Download Format (*) REQUIRED FIELDS

Select the download format, then click the Download button. Once the data is available, the download will begin automatically.

○ CSV Comma-Separated Value (CSV)
○ XML Extensible Markup Language (XML)
● PDF Portable Document Format (PDF)
○ DOC Microsoft Word (DOC)
○ HTML Compressed HTML pages (ZIP)
○ MHT Web Archive (HTML) - For Internet Explorer > 7 or any modern browser

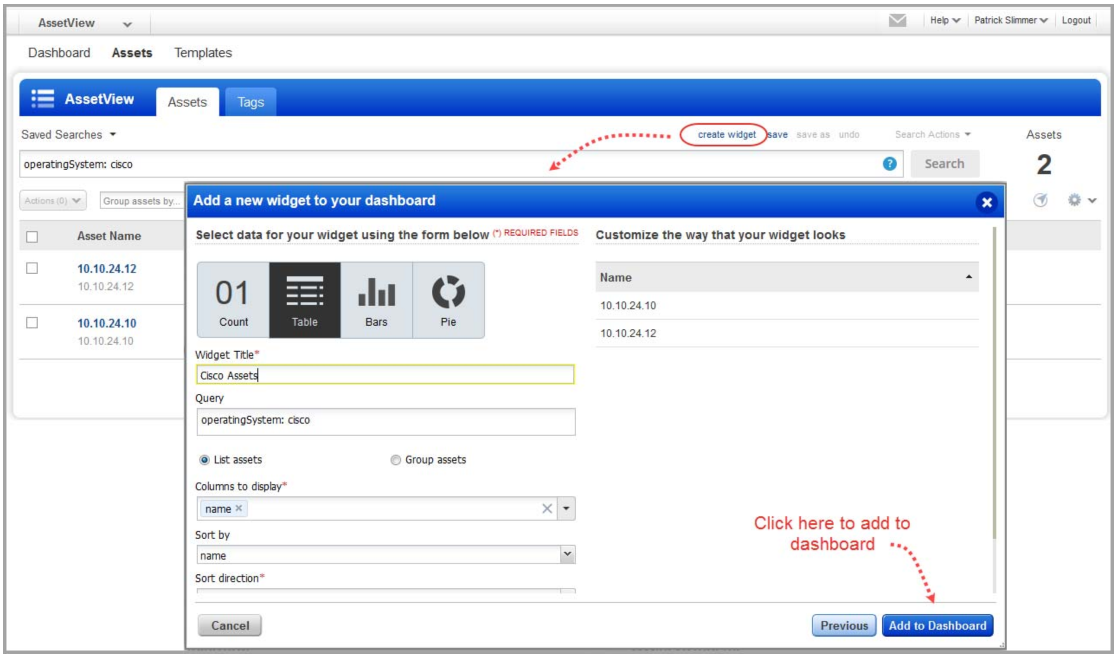
Select the timezone to use for dates included in the report

(GMT -07:00) GMT-07:00 (GMT-07:00 Etc/GMT+7)

☐	Asset Name	OS	Sources	Tags
☐	10.10.24.12 10.10.24.12	Cisco IOS		
☐	10.10.24.10 10.10.24.10	Cisco IOS		

Create widget

You can create a widget based on your query and add it to your dashboard. First search for assets and then choose Create widget. Add a title, you'll see your query is populated for you, just one click to add to your dashboard.



operatingSystem: cisco

Widget Title*: Cisco Assets

Query: operatingSystem: cisco

● List assets ○ Group assets

Columns to display*: name

Sort by: name

Sort direction*

Click here to add to dashboard

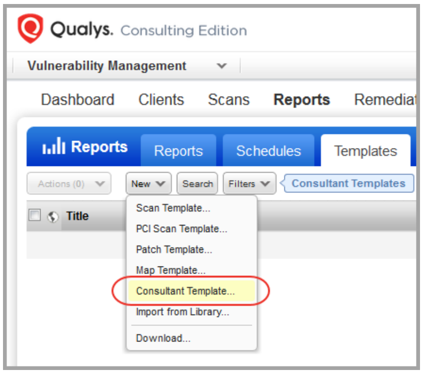
Create Reports

There are several reporting options available. Different reports provide different views of client data.

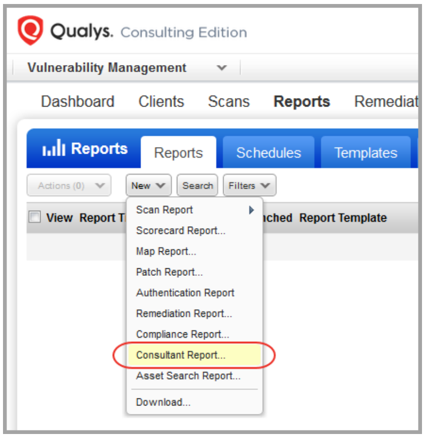
Consultant Reports

Create reports specific to your clients' needs. You can add a custom cover page to your report to include client and consultant contact information plus a summary.

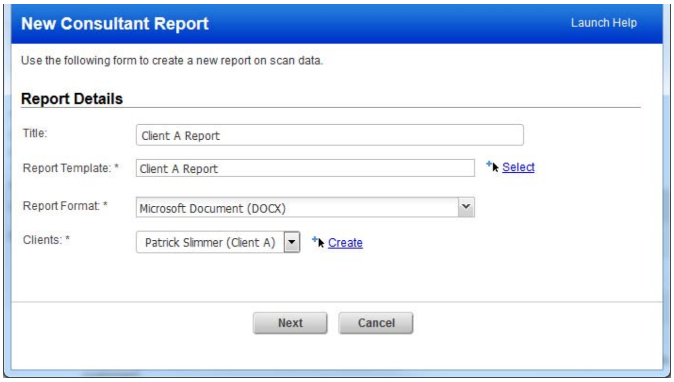
To get started, you'll need to create a consultant report template. Go to Reports > Templates > New > Consultant Template. See the help for help with template settings.



Now go to Reports > Reports > New > Consultant Report.



Choose the report template you created, a report format, and the client.



New Consultant Report

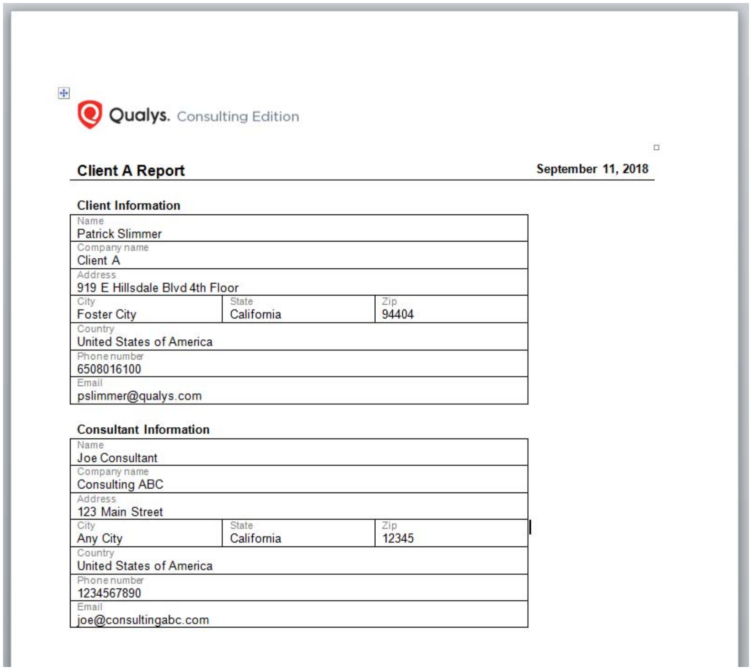
Use the following form to create a new report on scan data.

Report Details

Title:	Client A Report
Report Template: *	Client A Report
Report Format: *	Microsoft Document (DOCX)
Clients: *	Patrick Slimmer (Client A)

Tip - By running the report in DOCX format you can edit the report to focus on the details most important to each of your clients.

Click Next. You'll be prompted to choose client scan results to include in the report, then click Run. Your report will run in a new window.



Client A Report September 11, 2018

Client Information

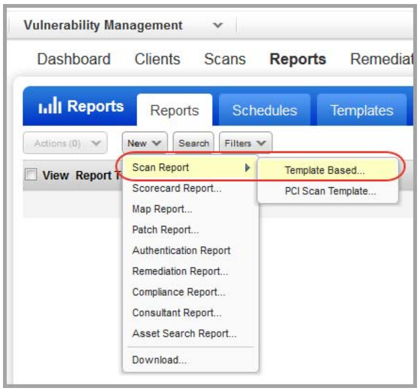
Name Patrick Slimmer		
Company name Client A		
Address 919 E Hillsdale Blvd 4th Floor		
City Foster City	State California	Zip 94404
Country United States of America		
Phone number 6508016100		
Email pslimmer@qualys.com		

Consultant Information

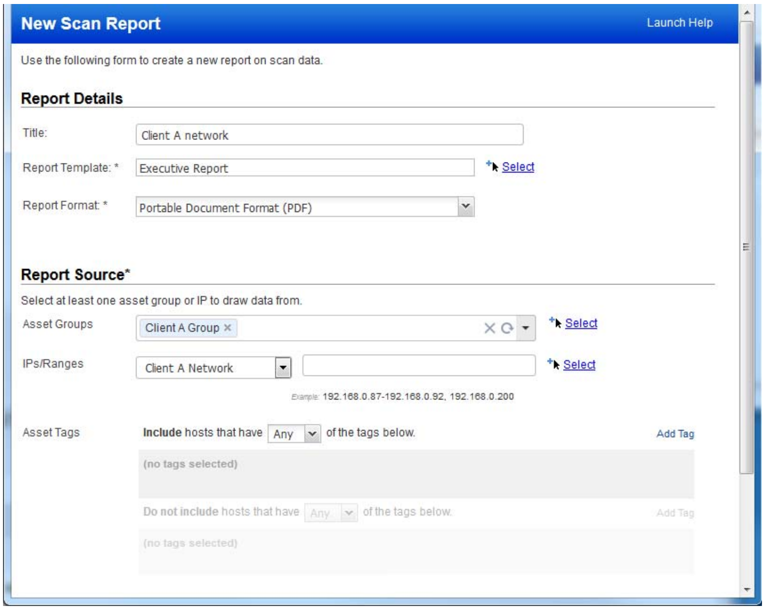
Name Joe Consultant		
Company name Consulting ABC		
Address 123 Main Street		
City Any City	State California	Zip 12345
Country United States of America		
Phone number 1234567890		
Email joe@consultingabc.com		

Template Based Scan Reports

Go to Reports > New > Scan Report > Template Based...



Choose a report template and pick a report format. If you configured client networks then choose the network you want to report on and your report target. Then click Run.



New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title: Client A network

Report Template: * Executive Report Select

Report Format: * Portable Document Format (PDF)

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups: Client A Group × Select

IPs/Ranges: Client A Network Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags: **Include** hosts that have Any of the tags below. Add Tag

(no tags selected)

Do not include hosts that have Any of the tags below. Add Tag

(no tags selected)

There are many report templates to choose from. For example:

The Executive Report provides a global view of your network security. This report is ideal for CIO or executive level managers. This report does not include detailed scan results or details like vulnerability descriptions and verified fixes.

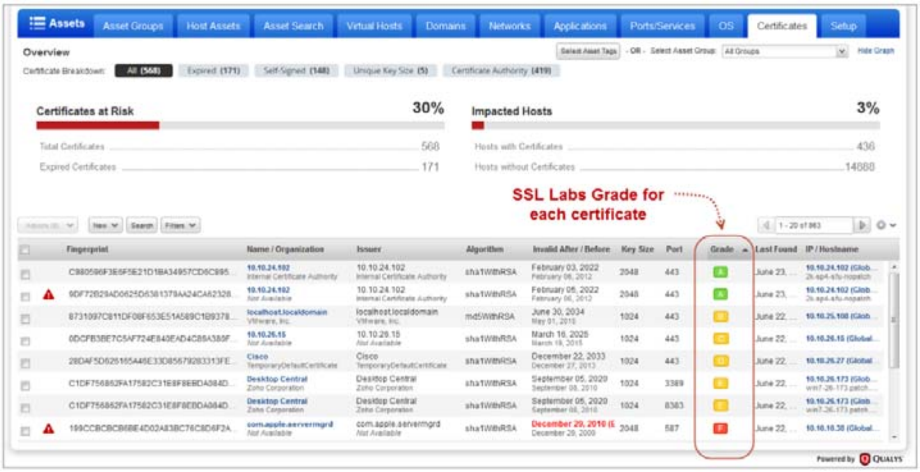
The Technical Report provides detailed scan results including the most current vulnerability information for each host. This report does not show vulnerability trends over time.

You can use a template provided by Qualys or create your own custom templates.

Review Certificates and SSL Grade

Did you know there's a lot of information you can see in Qualys VM without running reports? Under Assets, go to the Certificates, Applications and Ports/Services tabs for easy to search inventories based on your vulnerability scan data.

Let's take a closer look at certificates. Go to VM > Assets > Certificates. You'll see a list of certificates installed on hosts. Newly discovered certificates are added automatically to the inventory as new scan results become available in your account.



Overview

Certificate Breakdown: All (568) Expired (171) Self-Signed (148) Unique Key Size (5) Certificate Authority (419)

Certificates at Risk 30%

Total Certificates 568
Expired Certificates 171

Impacted Hosts 3%

Hosts with Certificates 436
Hosts without Certificates 14880

SSL Labs Grade for each certificate

Fingerprint	Name / Organization	Issuer	Algorithm	Invalid After / Before	Key Size	Port	Grade	Last Found	IP / Hostname
C880596F3E6F5E21D1BA34957CD6C895...	10.10.24.102 Internal Certificate Authority	10.10.24.102 Internal Certificate Authority	sha1WithRSA	February 03, 2022 February 06, 2012	2048	443	A	June 23, ...	10.10.24.102 (Glob... 2k-sp4-sfu-nopatch
⚠ 9DF72B29AD0625D6381379AA24CA62328...	10.10.24.102 Not Available	10.10.24.102 Internal Certificate Authority	sha1WithRSA	February 06, 2022 February 06, 2012	2048	443	A	June 23, ...	10.10.24.102 (Glob... 2k-sp4-sfu-nopatch
8731097C811DF08F653E51A589C1B9378...	localhost.localdomain VMware, Inc.	localhost.localdomain VMware, Inc.	md5WithRSA	June 30, 2034 May 01, 2015	1024	443	[illegible]	June 22, ...	10.10.25.108 (Glob...
0DCFB3BE7C5AF724E840EAD4C86A385F...	10.10.26.15 Not Available	10.10.26.15 Not Available	sha1WithRSA	March 16, 2026 March 19, 2016	1024	443	[illegible]	June 22, ...	10.10.26.15 (Global...
28DAF5D625165A46E33D8567928313FE...	Cisco TemporaryDefaultCertificate	Cisco TemporaryDefaultCertificate	sha1WithRSA	December 22, 2033 December 27, 2013	1024	443	[illegible]	June 22, ...	10.10.26.27 (Global...
C1DF756862FA17582C31E8F8EBDA084D...	Desktop Central Zoho Corporation	Desktop Central Zoho Corporation	sha1WithRSA	September 05, 2020 September 08, 2010	1024	3389	[illegible]	June 22, ...	10.10.26.173 (Glob... win7-26-173 patch...
C1DF756862FA17582C31E8F8EBDA084D...	Desktop Central Zoho Corporation	Desktop Central Zoho Corporation	sha1WithRSA	September 05, 2020 September 08, 2010	1024	8383	[illegible]	June 22, ...	10.10.26.173 (Glob... win7-26-173 patch...
⚠ 199CCBCBCB6BE4D02A83BC76C8D6F2A...	com.apple.servermgrd Not Available	com.apple.servermgrd Not Available	sha1WithRSA	December 29, 2010 (E December 29, 2000	2048	587	F	June 22, ...	10.10.18.38 (Global...

When the SSL Labs Grade feature is enabled for your subscription, you'll see a grade (A+, A, A-, B, C, D, E, F, T, M, NA) for each certificate on your certificates list. Grades are updated automatically each time new vulnerability scan results are processed for your hosts.

How do I get this feature?

Please contact your Technical Account Manager or Support to have the SSL Labs Grade feature enabled for your subscription.

Not seeing a grade?

Make sure the Grade column is shown by selecting it from the Tools menu above the list. If this feature was recently enabled, be sure to run new vulnerability scans on your hosts in order for grades to be calculated.

How are grades calculated?

We first look at the certificate to verify that it is valid and trusted. Then we inspect SSL configuration in three categories: 1) Protocol Support, 2) Key Exchange and 3) Cipher Strength. Each category is given a score and we combine these scores for an overall score of 0-100. (A zero in any category results in an overall score of zero.) The overall numerical score is translated into a letter grade (A-F) using a look-up table. Your A grade will be upgraded to A+ for exceptional configurations, and downgraded to A- when there are one or more warnings. Other grades you might see: T (certificate is not trusted), M (certificate name mismatch), and NA (not applicable, SSL server information not retrieved).

Want to learn more? Check out the SSL Server Rating Guide here:
https://www.ssllabs.com/projects/rating-guide/index.html

PCI Compliance

PCI Scan Requirements

Qualys is certified to help merchants and their consultants achieve compliance with the PCI Data Security Standard (DSS) including these scan requirements:

Per PCI DSS v3.0 requirement 11.2.2, the PCI Council requires merchants to perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the PCI Security Standards Council (PCI SSC). Qualys is a certified ASV. Every part of cardholder data system components needs to be scanned.

What systems should I scan?

Hosts that store cardholder data must be scanned. Also every part of cardholder data system components must be scanned. We recommend you refer to the PCI Data Security Standard (DSS) for details. Check to see these hosts are in your account by going to Assets > Host Assets.

Do I need to whitelist the scanners?

Our scanners must be able to reach the hosts being scanned. You may need to whitelist our scanners to allow access. Go to Help > About to see the IP addresses for our external scanners. You'll also see URLs that your scanner appliance must be able to contact.

Avoid scanning through a firewall from the inside out

Problems can arise when scan traffic is routed through the firewall from the inside out, i.e. when the scanner appliance is sitting in the protected network area and scans a target which is located on the other side of the firewall. See Scanning and Firewalls.

PCI Readiness Reports

Prepare customers of all sizes for ASV certifications and QSA audits by running PCI readiness reports.

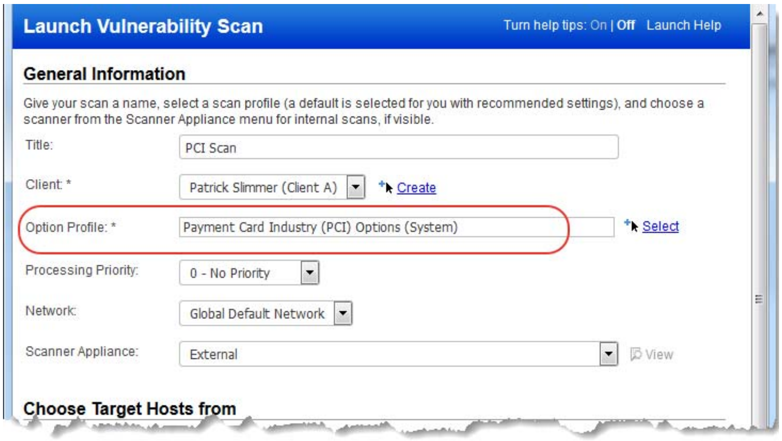
Commonly integrates with:

- PCI Readiness Assessments
- PCI Compliance Road Mapping
- Payment Infrastructure Assessments
- Payment Infrastructure Strategy

What are the steps?

Step 1: Run a Scan

Under VM, go to Scans > New > Scan. Tell us the IPs you want to scan, and select a PCI option profile like “Payment Card Industry (PCI) Options”. This profile has scan settings required according to the PCI DSS standard.



Launch Vulnerability Scan

General Information

Give your scan 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: PCI Scan

Client: * Patrick Slimmer (Client A)

Option Profile: * Payment Card Industry (PCI) Options (System)

Processing Priority: 0 - No Priority

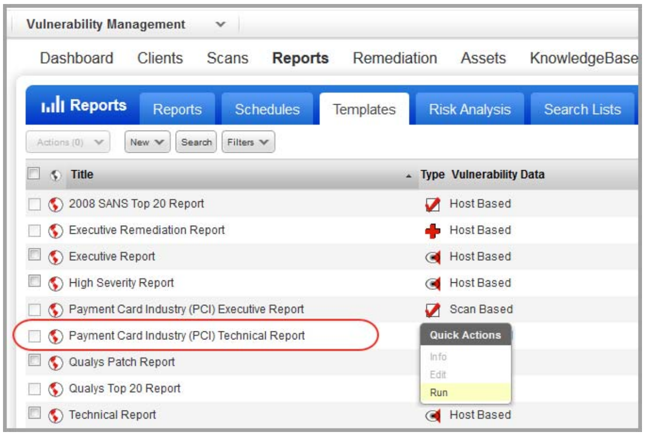
Network: Global Default Network

Scanner Appliance: External

Choose Target Hosts from

Step 2: Fix Vulnerabilities and Re-Scan

Run the PCI Technical Report to see whether your scan is compliant. Go to Reports > Templates, find the “Payment Card Industry (PCI) Technical Report” and select Run from the Quick Actions menu.



Title	Type	Vulnerability Data
2008 SANS Top 20 Report		Host Based
Executive Remediation Report		Host Based
Executive Report		Host Based
High Severity Report		Host Based
Payment Card Industry (PCI) Executive Report		Scan Based
Payment Card Industry (PCI) Technical Report		
Qualys Patch Report		
Qualys Top 20 Report		
Technical Report		Host Based

In your report you’ll see the PCI compliance status (PASS or FAIL) for the overall report, for each host and each vulnerability detected. Vulnerabilities with the FAIL status must be fixed to pass the PCI compliance requirements. (Vulnerabilities with no PCI status are not required for compliance, however we do recommend you fix them in severity order.) See the online help to better understand the Qualys KnowledgeBase and severity levels.

After fixing vulnerabilities, be sure to re-scan to verify that all PCI vulnerabilities are fixed and the overall status is PASS.

Wait, there's more!

Policy Compliance

Use Qualys Policy Compliance (PC) to reduce the risk of internal and external threats while providing proof of compliance demanded by auditors and government regulations.

Qualys Policy Compliance Getting Started Guide

Web Application Scanning

Qualys Web Application Scanning (WAS) is the most powerful web application scanner available. Set up your web application and run discovery and vulnerability scans.

Qualys Web Application Scanning Getting Started Guide

Self Assessment Questionnaire

Qualys Self Assessment Questionnaire (SAQ) is our automated questionnaire service. SAQ helps you automate your risk and compliance through campaigns. Collect risk data and compliance evidence from all the right people, then analyze and report on compliance and vendor risk.

Qualys API

You'll get the Qualys API with your Consultant subscription. Run up to 25 API calls per day (additional packages available).

Check out these API user guides

Qualys API (VM, SCA, PC) User Guide

Qualys API (VM, SCA, PC) XML/DTD Reference