



Community Edition

Getting Started Guide

July 25, 2018

Copyright 2018 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

Welcome to the Qualys Community Edition.....	4
Get Started	5
Add and organize your assets	5
Add IP addresses for scanning.....	5
Add domains for mapping	6
Discover your network	7
Organize assets into asset groups (optional)	10
Add a Virtual Scanner Appliance	11
Configure scan settings	12
Start your first scan!	14
Deploy cloud agents for continuous assessments.....	17
Overview	17
What do I need to know?	17
Get Started	18
Analyze, Query & Report	21
How to Query Assets	21
View Asset Details anytime	22
Save Query	22
Download and export results	22
Create widget.....	23
Organize assets using asset tags (optional)	23
Create Reports	24
Web Application Scanning	25
Add a web application	25
Launch a discovery scan.....	27
Scan for vulnerabilities	30
CloudView Free	34
Activate CloudView Free service	34
Add a connector.....	35
Create AWS connector	35
Create Azure connector.....	36
View Resource Inventory	38
Dashboard.....	38
Resources Details	39
Community Edition vs. Express Lite	40

Welcome to the Qualys Community Edition

Qualys Community Edition provides organizations with the ease of use, scalability, precision and centralized management of the Qualys Cloud Platform, free of charge. This cloud-based offering allows organizations to protect themselves from threats present in the wild without deploying any hardware or incurring maintenance costs.

Key Features

- Map your entire IT environment and discover all your assets, wherever they are — in the cloud or on premises
- Detect and assess vulnerabilities on internal and external IT assets and infrastructure
- Scan a public-facing or internal web application for vulnerabilities, including the OWASP Top 10
- Customize dynamic dashboards to reflect your organization's critical security information

Qualys Community Edition Includes

- 16 Cloud Agents
- Vulnerability Management for 16 Internal and 3 External IPs
- Web Application Scanning for 1 URL
- 1 Virtual Scanner Appliance
- CloudView for inventorying public cloud workloads and infrastructure

Limited version of Express Lite

Qualys Community Edition is a limited version of Express Lite, but scan functionality, full CVE coverage, and Six Sigma accuracy remain the same. See [Community Edition vs. Express Lite](#).

Get Started

We'll help you become familiar with the Qualys UI and complete your first scan.

Quick Steps

[Add and organize your assets](#)

[Add a Virtual Scanner Appliance](#)

[Configure scan settings](#)

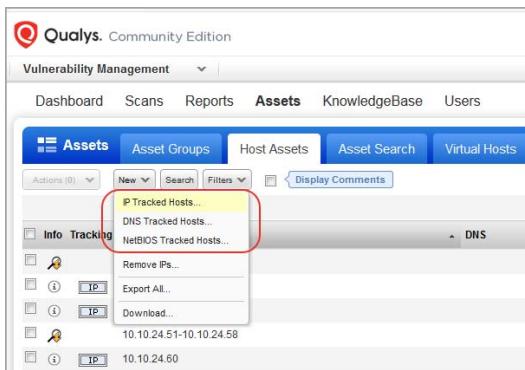
[Start your first scan!](#)

[Deploy cloud agents for continuous assessments](#)

Add and organize your assets

Add IP addresses for scanning

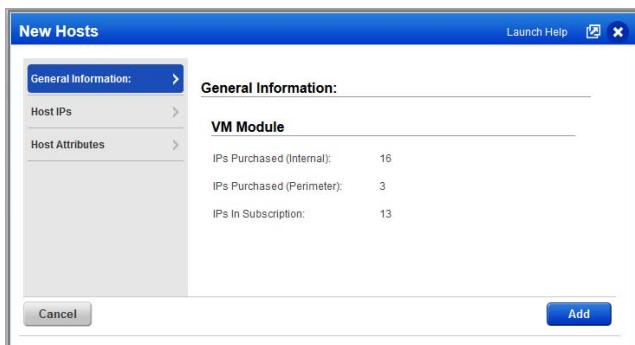
The first thing you'll want to do is tell us the IPs/ranges that you want to scan and report on. In Qualys VM, go to Assets > Host Assets. From the New menu, select IP Tracked Hosts, DNS Tracked Hosts or NetBIOS Tracked Hosts. The tracking method you choose will be assigned to all of the hosts being added.



About the tracking method...

By default we track hosts by IP address. You'll notice that you have the option to add hosts tracked by DNS and NetBIOS hostname, which allows for reporting host scan results in dynamic networking environments. For example, you may want to use DNS or NetBIOS hostname tracking if the hosts on your network are assigned IP addresses dynamically through DHCP.

Review the number of IPs in your account. To start you'll have 16 internal and 3 external (perimeter) IPs. The number of IPs in the subscription is the number of IPs already added.



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

New Hosts

General Information: >

Host IPs > Enter IPs and ranges in the field below. See the [Help](#) for proper formatting.

Host Attributes: >

Host IPs:

IPs: * 10.10.10.180-10.10.10.181

(ex: 192.168.0.200,192.168.0.87-192.168.0.92)

Validate IPs through [Whois](#)

Cancel Add

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.

Qualys. Community Edition

Vulnerability Management

Dashboard Scans Reports **Assets** KnowledgeBase Users

Assets Asset Groups Host Assets Asset Search Virtual Hosts Domains

Actions (0) New Search

Domain Domains... Netblock Download...

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

New Domains

Domains >

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])

Whois

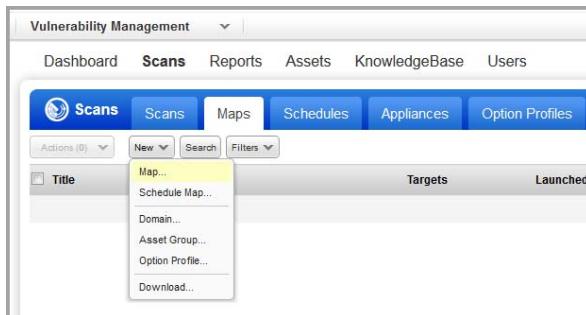
Cancel Add

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.

Discover your network

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

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



Choose your map options.

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](#)

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]
10.10.10.10-10.10.15

[Launch](#) [Cancel](#)

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.

Scanner Appliance - If you have a virtual scanner, then you can use it for mapping private use internal IPs. If not, we’ll use external scanners to map your network perimeter.

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.

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.

	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.qualys-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.qualys-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

File ▾ View ▾ Help ▾

Actions: Add to a new Asset Group ▾ Apply

- Add to a new Asset Group
- Add to Asset Groups
- Remove from Asset Groups
- Launch Vulnerability Scan**
- Schedule Vulnerability Scan

Map Edit

Patrick Slimmer
quays_ps
Manager

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

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

File ▾ View ▾ Help ▾

Actions: Expand All ▾ Collapse All ▾ Graphic Mode ▾ Apply

Qualys. Community Edition

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

Turn help tips: On | Off | Launch Help

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

Actions (0) Tools

Summary Results

Total Hosts in Domain **57**

New Hosts **57**

New Scannable Live In Netblock Approved Rogue

Operating System Families **4**

Windows 21 Linux 19 Other 12 Router 5

Map

The screenshot shows a network graph with 57 nodes. Nodes are categorized by icon: Windows (blue square with white 'W'), Linux (green square with white 'L'), Router (grey square with white 'R'), and Other (grey square with white 'O'). Some nodes have labels like 'fw (19)', 'qualys-test.com (5)', 'gw-gw (8)', 'gw-si (8)', 'demo1' through 'demo19', 'www1' through 'www4', 'ftp', 'smtp', 'proxy', 'dhop', 'ws1', 'ws2', 'wk7', '10.1.1.5', and '10.1.1.6'. A legend on the left indicates the counts for each category: Windows (21), Linux (19), Other (12), and Router (5).

Organize assets into asset groups (optional)

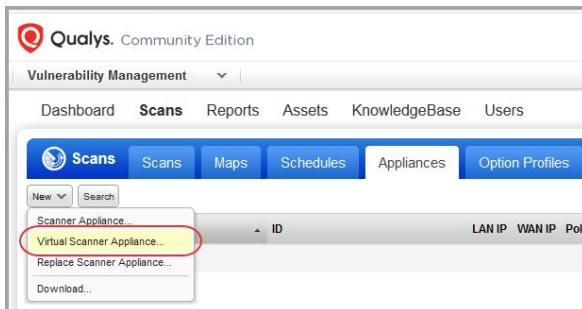
Asset groups give you a convenient way to make logical groupings of the assets you want to scan and report on. The same assets can appear in multiple groups as needed.

Go to Assets > Asset Groups and select New > Asset Group. Give the group a name, then go to the IPs section to add IPs to the group and go to the Domains section to add domains to the group. Hit Save when you're done.

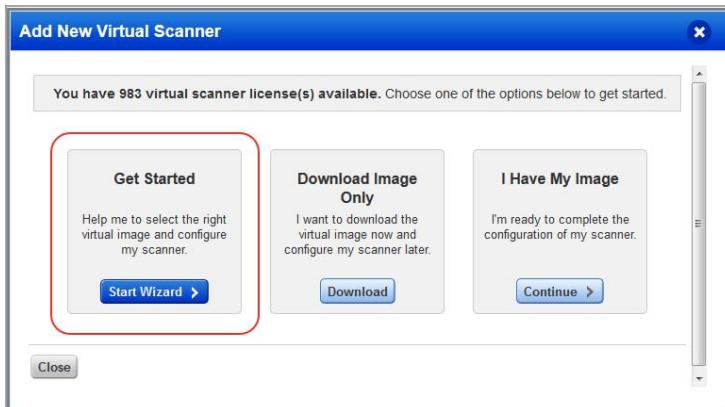
The screenshot shows the 'New Asset Group' dialog box. On the left, there's a sidebar with tabs: 'Asset Group Title' (disabled), 'IPs' (selected and highlighted in blue), 'Domains', 'Business Info', and 'Comments'. The main area is titled 'IP Hosts' with the sub-instruction 'Use the selections below to designate which hosts this asset group will contain'. It contains a text input field with the value '10.10.10.180-10.10.10.181' and several control buttons: 'Select IPs/Ranges', 'Select Asset Group', 'Remove', and 'Clear'. Below the input field is a checkbox labeled 'Display each IP/Range on new line'. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Add a Virtual Scanner Appliance

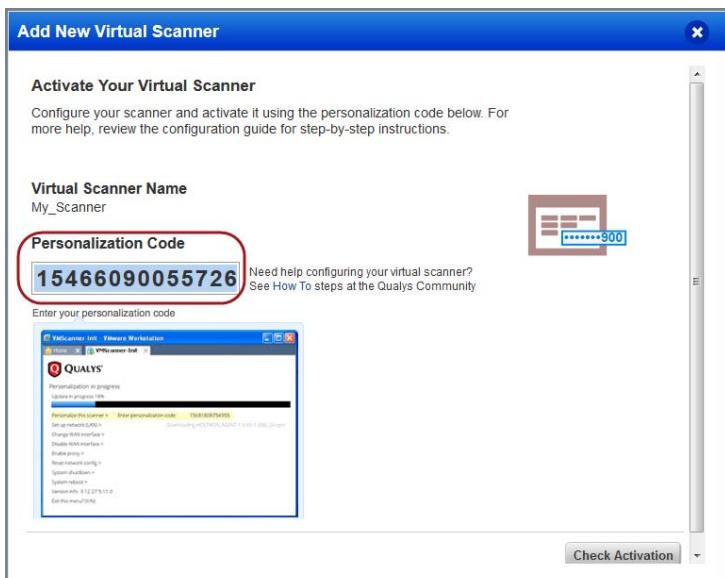
Your Community Edition subscription allows 1 virtual scanner appliance for internal scanning. Go to Scans > Appliances and select New > Virtual Scanner Appliance.



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



Give your scanner a name, choose a virtualization platform, get 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.
Heartbeat Checks Missed: 0 | Latest Scanner Version: 10.2.45-1 | Latest Signature Version: 2.4.369-1 | Available Capacity: 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.

Configure scan settings

An option profile includes scan settings that you'll choose at scan time. With a Community Edition subscription you get 3 profiles to start and you can add 1 custom profile. Create a profile from the New menu or edit a default profile to save a copy.

Go to Scans > Option Profiles to configure scan settings in option profiles.

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

Host Authentication is recommended

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:

- 1) Enable authentication in the option profile that you'll apply to your scan.

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

In the option profile, go to the Scan tab, scroll down to Authentication, and select each type of authentication you want to use.

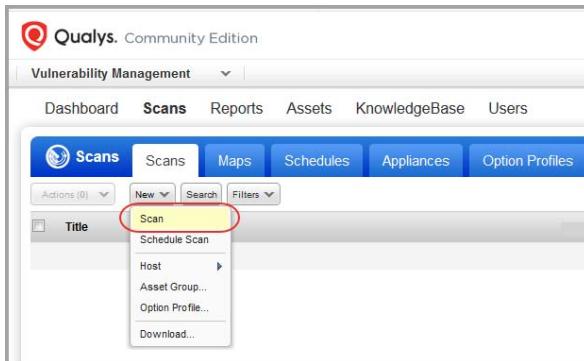
- 2) Add authentication records for your host technologies. Go to Scans > Authentication and create new records from the New menu. For each record you'll provide login credentials that our service will use to log in to each host at scan time.

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

Start your first scan!

You're now ready to start a vulnerability scan.

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



Choose your scan settings.

- (1) Option Profile - You can choose one of the default profiles provided or the custom profile that you previously saved, if applicable.
- (2) 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, then we'll use external scanners for a perimeter scan.
- (3) 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	Targets	User	Reference	Date	Status
My First Scan	10.10.10.180-10.10.181	Patrick Slimmer	scan/1530919178.46164	07/06/2018	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 Weekly or Monthly. Just choose New > Schedule Scan. Like with an on demand scan, you'll choose 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.

New Scheduled Vulnerability Scan

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

Occurs: Weekly Every 1 weeks

On Days:

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Ends after occurrences

Cancel Save

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.

New Scheduled Vulnerability Scan

Task Title: >

Target Hosts: >

Scheduling: >

Notifications > Enable email notifications (off by default)

Recipients: Well 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.

Save

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.

Vulnerability Management

Dashboard Scans Reports Assets KnowledgeBase Users

Scans Scans Maps Schedules Appliances Option Profiles Authentication Search Lists Setup

Actions (0)	New	Search	Filters	1 - 2 of 2	1	2	3	4	
<input type="checkbox"/>		Type	Title	Targets	Scanner	Assigned User	Next Launch	Modified	Previous Duration
<input type="checkbox"/>		My Weekly Scan	Ag1	External Scanner	Patrick Slimmer	07/08/2018 at 16:30:00 (GMT-0700)	07/06/2018 at 16:57:06 (GMT-0700)	Not Available	
<input type="checkbox"/>		schedule scan	10.10.10.180-10.10.10.181, External Scanner	10.10.24.11, 10.10.24.30, 10.10.24.51-10.10.24.58, 10.10.24.60	Patrick Slimmer	07/12/2018 at 15:10:00 (GMT-0700)	06/28/2018 at 15:05:42 (GMT-0700)	00:12:56	

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

Deploy cloud agents for continuous assessments

Using our revolutionary Qualys Cloud Agent platform you can deploy lightweight cloud agents for continuous security and compliance assessments.

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 your Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Go to Help > About to see the URL your hosts need to access.
- To install Windows Agent you must have local administrator privileges on your hosts. Proxy configuration is supported

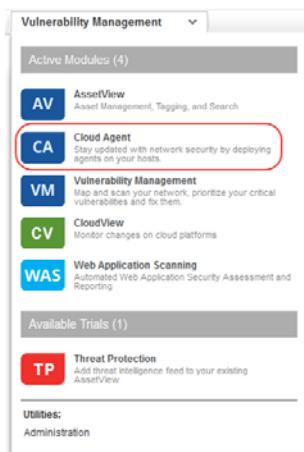
- To install Linux Agent, Unix Agent, Mac Agent you must have root privileges, non-root with Sudo root delegation, or non-root with sufficient privileges (VM scan only). Proxy configuration is supported.

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.



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.

The screenshot shows the 'Welcome to Qualys® Cloud Agent Platform' screen. It features a blue header bar with the welcome message and a note: '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!'. Below this, there is a section titled 'Get started with these quick steps' with two items: 'Cloud Agent Overview >' (with a lightbulb icon) and 'Download & Install Agents >' (with a download icon). Each item has a brief description and a 'See your agents >' link at the top right.

It's easy to install agents

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

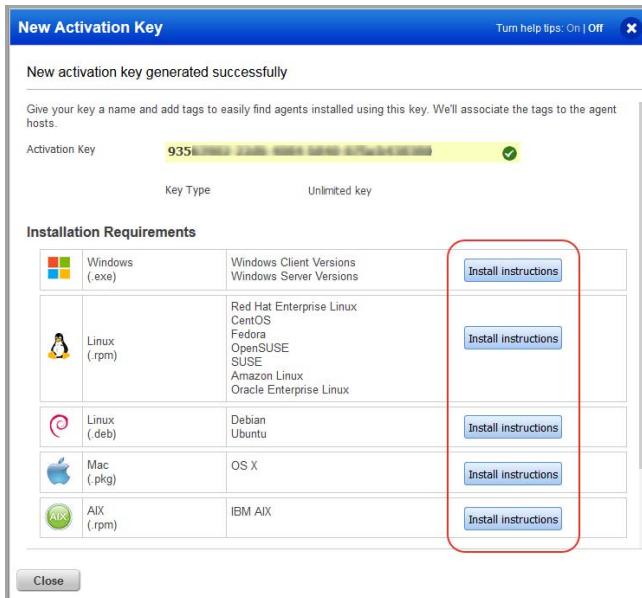
You'll need an activation key. Select New Key to create one. This key provides a way to group agents and bind them to your account. For example, you can create different keys for various business functions and users. (Already have a key? Select a key on the activation keys list and choose Install Agent from the Quick Actions menu.)

The screenshot shows the Qualys Cloud Agent interface. At the top, there's a navigation bar with 'Cloud Agent' and other options like 'Dashboard', 'Agent Management', 'Activation Keys', and 'Configuration Profiles'. Below the navigation is a search bar and a toolbar with buttons for 'Actions (0)', 'Install New Agent', and 'Activation Jobs'. The main area has tabs for 'Agent Host', 'OS', 'Version', 'Status/Last Checked-in', 'Configuration', 'Agent Modules', and 'Tags'. A large blue box in the center says 'Ready to install cloud agents?' with a sub-instruction 'Click here to get started' pointing to a 'New Key' button. The 'New Key' button is highlighted with a red circle. Below it, there's a link 'I already have keys'.

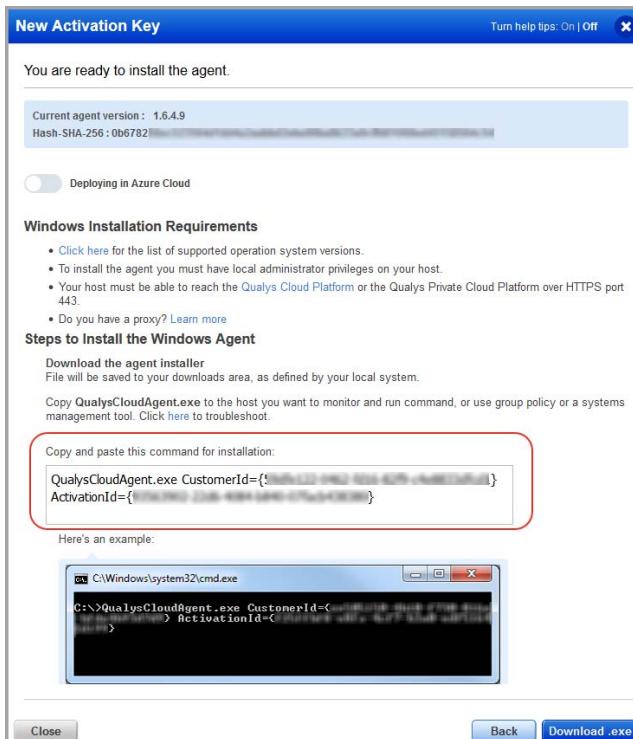
Give your key a name and provision the key for the VM application. If you have additional apps like PC, FIM and IOC then you'll see them listed as well. Click Generate.

The screenshot shows the 'New Activation Key' dialog box. It has a title bar 'New Activation Key' with a 'Turn help tips: On | Off' switch and a close button. The main area starts with 'Create a new activation key' and a note about activation keys. It includes fields for 'Title' (set to 'vm-agents') and 'Select | Create' (with '(no tags selected)'). Below that is a section 'Provision Key for these applications' with a checked checkbox for 'VM' (Vulnerability Management) and '100 Licenses Remaining'. There's also an unchecked checkbox for 'Set limits'. At the bottom are 'Close' and 'Generate' buttons, with a red arrow pointing to the 'Generate' button.

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



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.



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](#)

Analyze, Query & Report

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

How to Query Assets

The screenshot shows the Qualys app picker interface. At the top, there's a dropdown menu labeled "Vulnerability Management". Below it, under "Active Modules (4)", there are four items: "AV AssetView" (highlighted with a red box), "VM Vulnerability Management", "CV CloudView", and "WAS Web Application Scanning". Under "Available Trials (1)", there's a "TP Threat Protection" item. At the bottom, there's a section for "Utilities" with "Administration".

Select the AssetView app from the app picker.

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

The screenshot shows the AssetView interface with the "Assets" tab selected. At the top, there are tabs for "AssetView", "Assets", and "Tags". Below the tabs is a search bar with placeholder text "Search..." and a "Search" button. To the right of the search bar is a summary box showing "Assets" with the number "2". The main area is a table with columns: "Asset Name", "OS", "Modules", "Last Logged-In User", "Activity", "Sources", and "Tags". There are two entries in the table:

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.

The screenshot shows the AssetView interface with the "Assets" tab selected. A search query "ope" is being typed into the search bar. A tooltip appears over the "ope" token, providing syntax help: "Syntax Help operatingSystem" and "Use quotes or backticks within values to help you find the operating system you're looking for." Examples shown include "operatingSystem: Windows 2012" and "operatingSystem: \"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.

A screenshot of the AssetView interface. The top navigation bar shows 'AssetView', 'Dashboard', 'Assets', and 'Templates'. Below this is a search bar with 'operatingSystem: cisco'. A table lists two assets: '10.10.24.12' and '10.10.24.10'. Overlaid on the table is a context menu for the first asset, with 'View Asset Details' highlighted.

Save Query

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

A screenshot of the AssetView interface. A modal dialog box titled 'Create a new search' is open. It contains fields for 'Search Title' (set to 'Cisco OS') and checkboxes for 'Add this search to your favorites' and 'Share this search with others'. At the bottom are 'Cancel' and 'Save' buttons, with 'Save' being circled in red. The background shows a search results table with two assets: '10.10.24.12' and '10.10.24.10'.

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.

A screenshot of the AssetView interface. A modal dialog box titled 'Datalist Download' is open. It asks to 'Select Download Format' with options like CSV, XML, PDF, DOC, etc., and a 'Comma-Separated Value (CSV)' radio button selected. It also asks to 'Select the timezone to use for dates included in the report' with '(GMT -07:00) GMT-07:00 (GMT-07:00 Etc/GMT+7)' in a dropdown. At the bottom are 'Cancel' and 'Download' buttons, with 'Download' being circled in red. The background shows a search results table with two assets: '10.10.24.12' and '10.10.24.10'.

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.

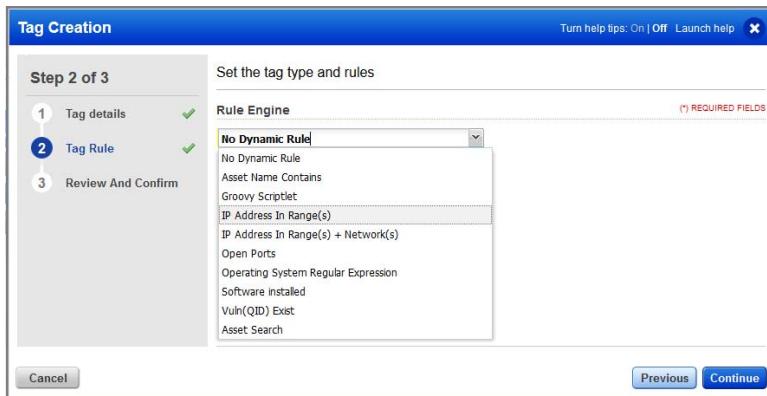
The screenshot shows the AssetView application interface. In the center, a modal window titled "Add a new widget to your dashboard" is open. It contains fields for "Widget Title" (set to "Cisco Assets"), "Query" (set to "operatingSystem: cisco"), and "Columns to display" (set to "name"). On the right side of the modal, there's a "Customize the way that your widget looks" section with a "Name" dropdown containing "10.10.24.10" and "10.10.24.12". At the bottom right of the modal, there are "Previous" and "Add to Dashboard" buttons. A red arrow points from the "create widget" button at the top right of the modal to the "Add to Dashboard" button at the bottom right. The background shows a search results page with a list of assets, including "10.10.24.12" and "10.10.24.10".

Organize assets using asset tags (optional)

While in the AssetView app, jump over to the Tags section to configure tags so you can apply them to assets in your subscription. This helps you to organize your assets. You can apply tags to IP addresses and web applications.

The screenshot shows the AssetView application interface with the "Tags" tab selected. On the left, there's a sidebar with "Search Results" and "Filter Results" sections. The main area shows a list of tags, with "Name" being the first item. A red circle highlights the "New Tag" button located at the top right of the tag list. The interface also includes a "Search" bar and a "Quick Filters" section with options like "Not In Use", "In scope", and "Favorite".

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.

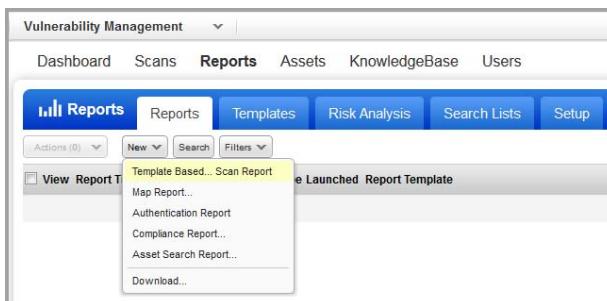


Tip - Turn help tips on (in the wizard title bar) and we'll show you help as you hover over the settings.

Create Reports

There are several reporting options available in Qualys VM. For Community Edition subscriptions, you can run any of these template based scan reports: Technical Report, Executive Report, High Severity Report or a custom scan report. These reports provide different views of your data.

Go to Reports > New > Template Based... Scan Report. Then choose a report template, pick a report format, select your report target and click Run.



Web Application Scanning

Qualys WAS is the most powerful web application scanner available. We'll help you set up your web application and run discovery and vulnerability scans.

Quick Steps

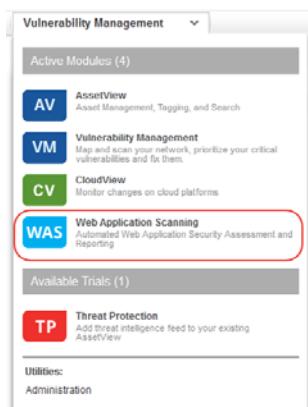
[Add a web application](#)

[Launch a discovery scan](#)

[Scan for vulnerabilities](#)

Add a web application

Select the WAS app from the app picker.

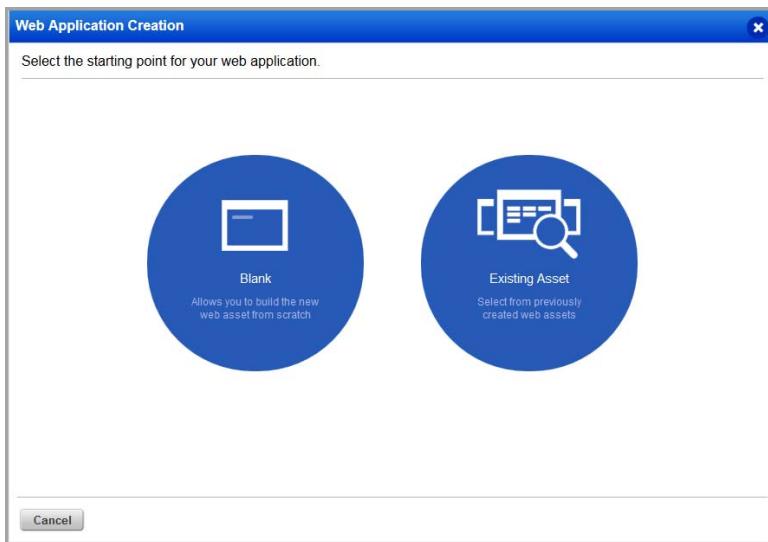


Start by telling us about the web application you want to scan. Click Add Web Application.

The screenshot shows the 'Web Application Scanning' dashboard. At the top, there's a navigation bar with links for Dashboard, Web Applications, Scans, Detections, Reports, Configuration, and KnowledgeBase. The dashboard area displays a message: 'You have no web applications as of today. Please add a web application to get started.' Below this message is a blue button labeled 'Add Web Application', which is also circled in red. A dotted arrow points from the text 'Click here to start' to this button. On the right side of the dashboard, there's a 'CATALOG' section with a message 'No records.' and a 'View All' link. At the bottom right of the dashboard, there's a 'New Scan' button and a 'Add Web Application' link.

Choose the starting point

Select Blank and you'll be able to build the new web asset from scratch.



Add your web app settings

The web application name and URL are required when adding a web app from scratch. Follow the wizard to complete all the steps and then save your web application.

The screenshot shows the 'Web Application Creation' wizard at Step 1 of 11. The left sidebar lists steps 1 through 11. Step 1 is 'Asset Details' (marked with a green checkmark), and step 2 is 'Application Details'. The main form has sections for 'Definition' (with a note about basic information), 'Target Definition' (with a 'Web Application URL' field containing 'http:// myWebapp.com'), 'Custom Attributes' (with a 'Username' field containing 'Jason'), and 'Tags' (with a 'Select' button). A red arrow points to the 'Web Application URL' field. A yellow callout box titled 'Web Application URL' provides help: 'Enter the URL of the target web application. Tip: For a secure URL, click http:// to switch to https:// You can enter a maximum of 2048 characters.' At the bottom are 'Cancel' and 'Continue' buttons. In the title bar, there is a 'Turn help tips: On | Off' button, which is circled in red.

Help Tips - Turn this on (in the title bar) and get help for each setting as you hover over fields.

Your new web application appears in the Web Applications tab, where you can edit the application settings or launch a scan on it.

Name	# Pages	# Vulns	Severity	MDS Severity	Scanned	Updated
Demo Web Application http://10.10.26.238:80/	-	-	-	N/A	-	30 Jun 2017

Why use authentication?

Using authentication allows our service to access to all parts of your web application during the crawling process. This way we can perform more in-depth assessment of your web application. Some web applications require authenticated access to the majority of their functionality. Authenticated scanning can be configured for HTML forms like login pages and server-based authentication (HTTP Basic, Digest, NTLM, or SSL client certificates). Just go to the Authentication tab, select New Record and configure an authentication record with access credentials. Form and server authentication may be combined as needed - we'll monitor the session state to ensure an authenticated scan remains authenticated throughout the crawl.

Warning about scans and their potential impact

Web application scans submit forms with test data. If this is not desired you should add configurations for black lists, POST data black lists, and/or select the GET only method within the option profile. Keep in mind when these configurations are used, testing of certain areas of the web application is not included and any vulnerabilities that exist in these areas may not be detected.

Launch a discovery scan

A discovery scan finds information about your web application without performing vulnerability testing. This is a good way to understand where the scan will go and whether there are URIs you should blacklist for vulnerability scans.

Go to Web Applications (on the top menu) and then select New Scan > Discovery Scan.

New Scan

- Discovery Scan
- Vulnerability Scan

The launch scan wizard walks you through the steps. Tell us the web application you want to scan and select scan settings (* means required). Click Continue to walk through the discovery scan wizard. Then click Finish when you're done.

Launch New WAS Discovery Scan

Step 1 of 3

Name your scan and configure target to be assessed

Scan Name* My Discovery Scan (*) REQUIRED FIELDS

Scan Target

Tell us the web applications you want to scan for security risks.

Names Tags

Select one or more web application names. The list includes all web applications you have access to.

Web Applications* Please select a web application

Demo Web Application

The scan view

Double click the finished scan to see the scan view.

Name	Status	Links	Severity	Scan Date
My Discovery Scan	Finished	228	-	30 Jun 2017

The Overview gives you an overview of the scan findings.

WAS Vulnerability Scan View

View Mode

Overview

Scan findings overview

My Discovery Scan

Target: Demo Web Application

Status: **Finished**

Authentication Status: None

Applications Scanned: 1

Start Date: 04 Jul 2017 3:07PM GMT+0530

Duration: 00:39:33

Crawling Time 00:09:22

Assessment Time 00:30:03

Operating System Linux 2.4.2-6 ...

Links Collected 13000

Links Crawled 299

Requests Performed 85836

Avg. Response Time 0.030212 seconds

Want to view the full scan report? Just click the View Report button.

The full scan report

Each QID is a security check we performed and gathered information on. Just click the row to see details.

QID	Description
45017	Operating System Detected
150152	Forms Crawled
150135	Strict Transport Security Missing Header Analysis
150126	Links With High Resource Consumption
150125	File Upload Form Found
150115	Authentication Form found
150106	Content of crossdomain.xml
150099	Cookies Issued Without User Consent
150087	Web Service Found
150082	Protection against Clickjacking vulnerability
150058	Flash Analysis
150054	Email Addresses Collected
150041	Links Rejected
150028	Cookies Collected
150026	Maximum Number of Links Reached During Crawl
150025	Exception At Scan Launch
150021	Scan Diagnostics
150014	External Form Actions Discovered
150010	External Links Discovered
150009	Links Crawled
45038	Host Scan Time
6	DNS HostName

Be sure to check QID 150009 Links Crawled and QID 150021 Scan Diagnostics to review important data about the scan.

You'll see the results for QID 150009 Links Crawled gives you a listing of the links crawled.

Information Gathered Details

150009 Links Crawled

Field	Value
Group	691830* (37970147)
CWE	-
OWASP	-
WASC	-
Web Application Authentication	Demo Web Application Not Used
Detection Date	27 Jun 2017 5:54PM GMT+0530

Details

Results

Highlight changes from previous scan

- New - this link was not found in the previous scan
- Modified - this result was found by the previous scan but its value was different
- Removed - this link was not found, but was reported in the previous scan

Duration of crawl phase (seconds): 541.00
Number of links: 299
(This number excludes form requests and links re-requested during authentication.)

```

http://10.11.72.37/
http://10.11.72.37/cassandra/AutoExpress/Index.html
http://10.11.72.37/crossdomain.xml
http://10.11.72.37/html/images/logo.png
http://10.11.72.37/randomLink%3Chr%20%3E%0A%3Cb%3ENotice%3C/b%3E%3A%20%20Undefined%20variable%3A%20%20_PHP_SELF%20in%20%3Cb%3E%var/www/html/randomLink/randomLink.php%3C/b%3E%20on%20line%20%3Cb%3E%191%3C/b%3E%3Chr%20%3E%0A
http://10.11.72.37/randomLink/randomLink.php

```

Scan for vulnerabilities

A vulnerability scan performs vulnerability checks and sensitive content checks to tell you about the security posture of your web application.

What vulnerability checks are tested?

We'll scan for all vulnerability checks (QIDs) listed in the KnowledgeBase unless you configure your option profile to limit the scan to certain vulnerabilities (confirmed, potential and/or information gathered). We constantly update the KnowledgeBase as new security information becomes available.

Click KnowledgeBase on the top menu.

QID	Name	Information	Category	Severity
115767	SUSE Security Announcement: krb5 (SUSE-SA:2008:016)		Local	
38688	PAN-OS Management Interface Remote Code Execution Vulnerability (PAN-SA-2017-0027)		General remote services	
86175	Multiple Cross-Site Scripting Vulnerabilities Detected		Web server	
45224	Unofficial OpenJDK Detected		Information gathering	
11837	Java Deserialization Vulnerability Detected		CGI	
91438	Microsoft Windows CredSSP updates for March 2018		Windows	
370946	IBM WebSphere Application Server information exposure vulnerability (swg22013601)		Local	
370951	Mozilla Thunderbird Multiple Vulnerabilities (msfa2018-09)		Local	

What is Severity? Each QID is assigned a severity level by our service: confirmed vulnerability (red), potential vulnerability (yellow) and information gathered (blue).

Start your scan

Go to Scans on the top menu and then select New Scan > Vulnerability Scan.

Actions ▾ New Scan ▾

Discovery Scan

Vulnerability Scan

The launch scan wizard walks you through the steps. You'll tell us the web application you'd like to scan for vulnerabilities and select scan settings. Click Continue to make your settings and then click Finish.

Launch New WAS Vulnerability Scan

Turn help tips: On | Off | Launch help | **X**

Step 1 of 3

Scan Details ✓
Scan Settings
Review And Confirm

Name your scan and configure target to be assessed

(*) REQUIRED FIELDS

Scan Name* My Vulnerability Scan

Scan Target

Tell us the web applications you want to scan for security risks.

Names Tags

Select one or more web application names. The list includes all web applications you have access to.

Web Applications* Please select a web application

Demo Web Application Remove | View

Cancel **Continue**

Check scan progress

The status column tells you the status (in this case Running).

Scan Management

Scan List | Schedules | Option Profiles

Search Results

Actions (1) | New Scan | 1 - 2 of 2

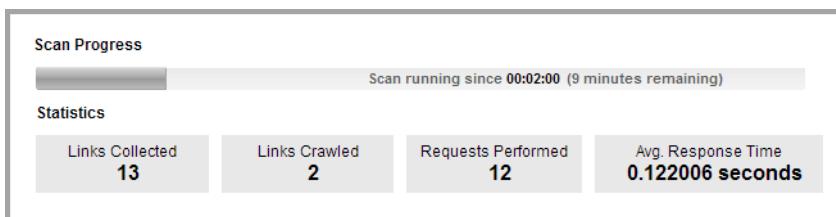
Name	Status	Links	Severity	Scan Date
My Vulnerability Scan http://10.10.26.238:80/	Running	-	-	22 Jul 2014
My Discovery Scan http://10.10.26.238:80/	Finished	228	-	22 Jul 2014

Filter Results

Quick Filters

My Scans

Want more info? Double click the scan row. Then you'll see the Scan Progress bar - this gives you an estimate of when the scan will finish.



Your scan results

Select the finished scan to see a preview of the scan (below the list).

The screenshot shows the Qualys Community Edition interface for web application scanning. At the top, there are tabs for 'Scan List', 'Schedules', 'Option Profiles', and 'Defaults'. Below these are buttons for 'Actions (1)' and 'New Scan'. The main area displays a list of scans. One scan is highlighted in yellow: 'Web App Vulnerability Scan - 2017-07-12' (http://10.11.72.37), which is 'Finished'. To the right of the list is a 'Preview' section for this specific scan. It includes details like 'Scan Launched by' (redacted), 'Scan Launched at' (12 Jul 2017 3:39PM GMT+0530), and 'Status' (Finished). Below this, it shows 'Mode: On-Demand', 'Authentication: None', and 'Scanner: WAS_Scanner_2'. A summary of detections is provided: '# vulnerabilities 120', 'High Severity 40', 'Medium Severity 11', and 'Low Severity 69'. A red box highlights the 'View Report' button, with a red arrow pointing to it labeled 'Full scan report'. Another red arrow points to a thumbnail image of a web page showing a dollar bill, labeled 'Snapshot of web app'. A red arrow also points to the 'Detections' summary.

The scan view

Hover over the scan and select View from the Quick Actions menu. The Overview gives you an overview of the scan findings.

The screenshot shows the 'WAS Vulnerability Scan View' dialog box. On the left is a sidebar with 'View Mode' options: 'Overview' (which is selected and highlighted in blue), 'Scan Details', 'Scan Settings', and 'Action Log'. The main area is titled 'Scan findings overview' and shows details for the 'Web App Vulnerability Scan - 2017-07-12'. It includes fields for Target (Demo Web Application), Status (Finished), Authentication Status (None), Applications Scanned (1), Start Date (12 Jul 2017 3:39PM GMT+0530), Duration (00:08:59), Crawling Time (00:01:38), Assessment Time (00:07:20), Operating System (Linux 2.4-2.6 ...), Links Collected (251), Links Crawled (10), Requests Performed (5342), and Avg. Response Time (0.043402 seconds). At the bottom right of the dialog is a 'View Report' button. A red arrow points to this button from the text below.

Want to see the full scan report? Just click the View Report button.

The full scan report

Vulnerabilities are sorted by group.

The screenshot shows the Qualys Community Edition Web Application Scanning interface. The top navigation bar includes 'Report Management', 'Reports', 'Schedules', 'Templates', 'Scan report', and 'Defaults'. The main content area is titled 'Results (138)'. A tree view on the left lists categories: 'Vulnerabilities (120)', 'Cross-Site Scripting (46)', 'SQL Injection (2)', 'Path Disclosure (50)', 'Information Disclosure (22)', and 'Information Gathered (18)'. An 'Appendix' section contains links to 'Scan Details', 'Web Application Details: Demo Web Application', and 'Severity Levels'. A callout bubble points to the 'Vulnerabilities' section with the text 'Click here to see vulnerability details'. A modal window titled 'Vulnerability Details' is open, showing a specific entry: '150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities' with a URL of 'https://10.11.72.37/?account=business'. The modal includes tabs for 'Details', 'Detection Information', and 'Payloads'. The 'Detection Information' tab shows parameters like 'account' and access path, and provides a preview URL 'http://10.11.72.37/'. The 'Payloads' tab shows a request payload: 'account=business%20%3Cscript%3E_q%3Drandom()%3C%2Fscript%3E' and a corresponding GET request line.

Easily find out what the severity levels mean in the Appendix.

The screenshot shows the Qualys interface with the 'Appendix' section expanded. It contains links to 'Scan Details', 'Web Application Details: Demo Web Application', 'Severity Levels', and 'Confirmed Vulnerabilities'. The 'Severity Levels' section defines five levels: Minimal (basic information disclosure), Medium (intruders collect sensitive info about the platform), Serious (vulnerabilities disclose security-related info that could result in misuse or exploit), Critical (exploit to gain sensitive content or affect other users), and Urgent (exploit to compromise data store, obtain info from accounts, or execute commands). The 'Confirmed Vulnerabilities' section notes that QIDs represent design flaws, errors, or misconfigurations that make the web application susceptible to attacks. A table maps Severity to Level and Description:

Severity	Level	Description
■	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.
■ ■	Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to those versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.
■ ■ ■	Serious	Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.
■ ■ ■ ■	Critical	Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.
■ ■ ■ ■ ■	Urgent	Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.

Other sections shown include 'Potential Vulnerabilities' and 'Sensitive Contents'.

CloudView Free

Qualys CloudView provides visibility and continuous security across all of your cloud environments.

Quick Steps

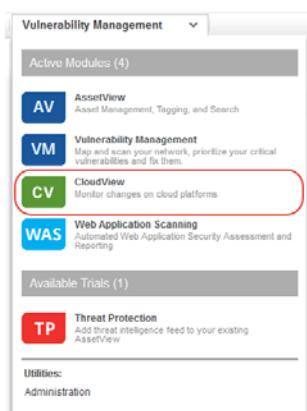
[Activate CloudView Free service](#)

[Add a connector](#)

[View Resource Inventory](#)

Activate CloudView Free service

Select the CV app from the app picker.



Click Activate to get started with the CloudView Free service.

The screenshot shows the CloudView Free Service landing page. At the top, it features the CloudView logo and the tagline "Continuously monitor and secure your public clouds". On the left, there is a section titled "Get unparalleled visibility and continuous security of public cloud infrastructure" with a detailed description of how CloudView helps protect public cloud assets. On the right, there is a section titled "CloudView Free Service" with a description of the service's capabilities and a list of benefits. A prominent red "Activate" button is located at the bottom of this section. Below the main content, there is a note: "Or, start a full 14-day Trial that includes CSA."

The Quick Start Guide appears with 3 quick steps to securing your public clouds. We'll help you with these steps.

The screenshot shows the Qualys CloudView interface. At the top, there's a navigation bar with tabs: DASHBOARD, RESOURCES, MONITOR, POLICIES, and CONFIGURATION. Below the navigation bar, a banner says "Welcome to Qualys® CloudView" and "Continuously monitor and secure your public clouds". On the left, a section titled "Get started with these quick steps" lists three steps: 1. Get Started by creating a new Connector > (with a sub-note about setting up the connector), 2. View Resource Inventory > (with a note about visibility across accounts and platforms), and 3. Monitor Resources and Misconfigurations > (with a note about controlling evaluations and viewing misconfigurations). To the right of this list is a "Video Tutorials" section featuring a thumbnail for "Qualys Company Overview" and a "Related Community Posts" section with a tweet from @qualys.

Add a connector

Once you have your connector, we'll start discovering resources that are present in your cloud account. You can create AWS connectors and Azure connectors.

Create AWS connector

Go to the Configuration tab and select Create Connector > Amazon Web Services.

The screenshot shows the Configuration tab of the Qualys CloudView interface. The top navigation bar has tabs: DASHBOARD, RESOURCES, MONITOR, POLICIES, and CONFIGURATION, with CONFIGURATION being the active tab. Below the navigation bar, there's a search bar and a "Create Connector" dropdown menu. The dropdown menu has two options: "Amazon Web Services" (which is highlighted with a red circle) and "Microsoft Azure".

Provide a name and description (optional) for your connector. Then copy settings from the connector details: Qualys AWS Account ID and External ID. You'll need these for creating your IAM role in the AWS console..

The screenshot shows the "Create AWS Connector" wizard. The first step, "Connector Details", asks for a name (My AWS Connector) and a description. The second step, "Specify cross account ARN", asks for Qualys AWS Account ID (205767712438) and External ID (1532406585030). Both fields have a "Copy" button next to them. A red box highlights the "Enter connector name" field and the "Copy these settings" text at the bottom. To the right, a sidebar provides detailed steps for creating an IAM role in AWS:

- Log in to Amazon Web Services (AWS) Console.
- Go to the IAM service.
- Go to Roles and click **Create Role**.
- Under "Select type of trusted entity" choose **Another AWS account**.
a. Paste in the Qualys AWS Account ID (from connector details).
- Select **Require external ID** and paste in the External ID (from connector details).
- Click **Next: Permissions**.
- Find the policy titled "SecurityAudit" and select the check box next to it. Optionally, create a custom AWS IAM Policy following details in the online help. Click **Next: Review**.
- Enter a role name (e.g. QualysCloudViewRole) and click **Create role**.
- Click on the role you just created to view details. Copy the Role ARN value and paste it into the connector details.

Want to create a role using CloudFormation? +

Follow the detailed steps on the right side of the screen to create an IAM role in AWS and get the Role ARN value.

When you have the Role ARN value, come back to your connector in Qualys CloudView and paste the value into the connector details. Click Create Connector to finish.

Connector Details

Name: My AWS Connector

Description:

Specify cross account ARN

Qualys AWS Account ID: 205767712438

External ID: 1537406585030

Role ARN: arn:aws:iam::111111111111:role/QualysEC2Role

Create Connector

That's it! The connector will establish a connection with AWS to start discovering resources from each region and evaluate them against policies.

Want to create a role using CloudFormation?

Download the CloudFormation template from the Create AWS Connector window.

Create A Role For Cross-Account Access

Want to create a role using CloudFormation ?

1. Download the CloudFormation template.
2. Log in to Amazon Web Services (AWS) and go to CloudFormation.
3. Create stack & upload template.
4. When the stack is complete, copy the Role ARN value from the output and paste it into the connector details.

Follow the steps on the screen to create a stack and upload the template. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

Create Azure connector

Go to the Configuration tab and select Create Connector > Microsoft Azure.

CONNECTOR NAME	ACCOUNT ID	STATE
Microsoft Azure	179064574731	Regions Discovered

Provide a name and description (optional) for your connector.

Connector Details

Give your connector a name and provide a description (optional).

Azure Account Name: Required

Account Description:

Create Application and get Application ID

Create application in Azure Active Directory and you can then note the application ID.

- Log on to the Microsoft Azure console. Go to Azure Active Directory in the left navigation pane, then App Registrations.
- Click New application registration and provide these details:
 - Name: A name for the application (e.g. My_Azure_Connector)
 - Application Type: Select Web app/API
 - Sign-on URL: Enter any valid URL (e.g. https://localhost/azure.com)
- Click Create. The newly created app appears in the list of applications. Copy the Application ID and paste it into the connector details.

Authentication Details

Application ID:

Directory ID: Required

Authentication Key: Required

Subscription ID: Required

Buttons

- Obtain Directory ID
- Generate Authentication Key
- Acquire Subscription ID

Actions

Follow the detailed steps on the right side of the screen (and see the online help) to configure the application ID, directory ID, authentication key and subscription ID from the Microsoft Azure console to paste into your connector details.

View Resource Inventory

Upon setting up your connector, it starts discovering the resources that are present in your cloud account. The resources inventory and the metadata of the resources is pushed to Qualys portal. You can navigate to the Resources tab to view the resources getting collected along with their details.

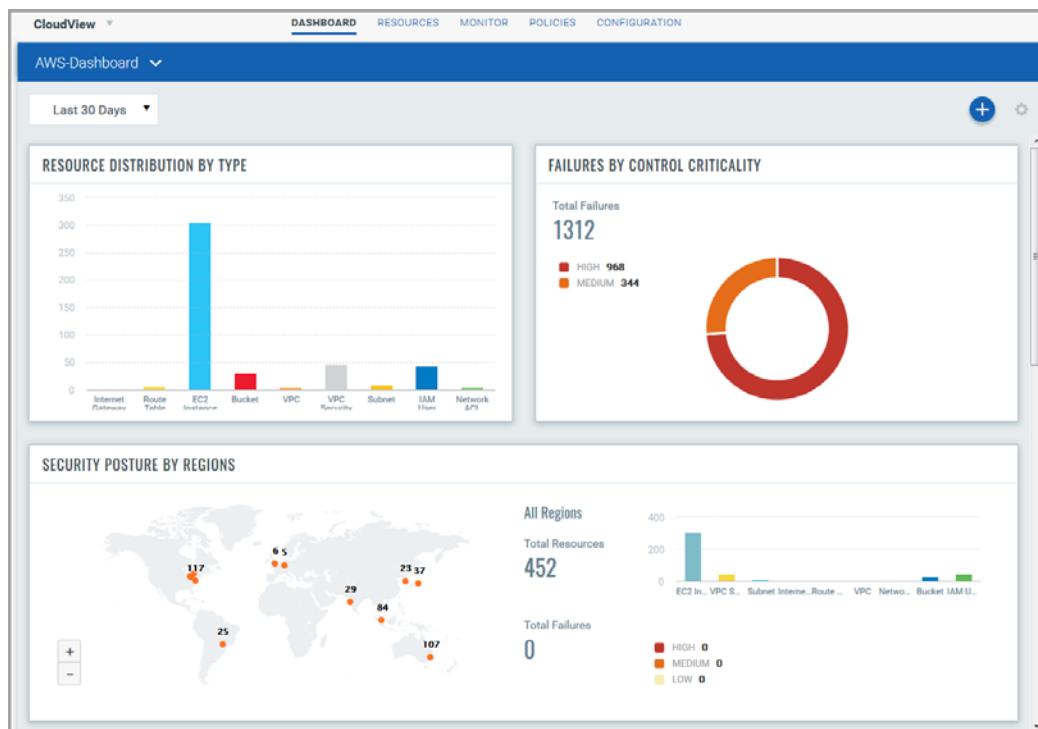
Dashboard

The Qualys CloudView application provides out-of-the box default AWS Security Overview Dashboard providing a summary of inventory and security posture across resources.

The default dashboard provides:

- Resource inventory - Route Tables, EC2 Instances, VPC, Subnets, IAM Users, etc
- Total evaluation failures i.e. the resources misconfigurations by control criticality
- Security posture at each region level showing resources and failures
- Top 5 Accounts with maximum control failures
- Top 5 Failed controls

Check out this sample dashboard

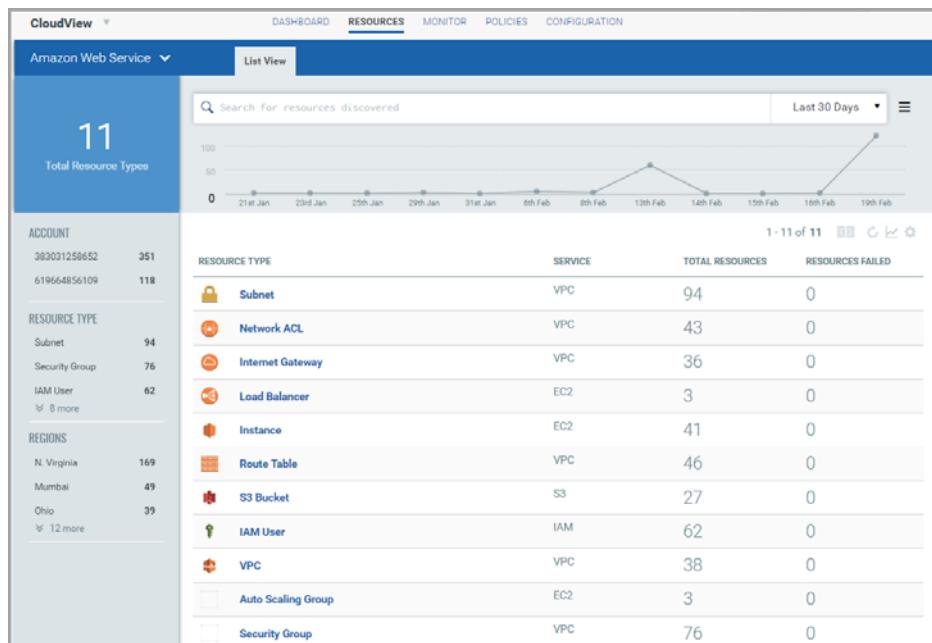


Resources Details

The Resources tab displays the information about various resources collected. It helps you to identify the number of resources for each type and the number of resources that have one or more control failures. You can click on a row to view the number of resources of a specific type. You can click on an individual resource to view the details. For each resource you will view the following information.

Resources Summary

The List View provides a summary of your resources, including the total resources and the number of failed resources for each resource type.



From here you can drill-down into any resource type to see instance details like the number of detected vulnerabilities, resource associations, location and network information.

The vulnerability related data is populated only if you are using a scanner appliance or Cloud Agent.

Community Edition vs. Express Lite

You'll get even more functionality with Qualys Express Lite. Contact your Technical Account Manager or Qualys Support to upgrade today.

Vulnerability Management (VM)

	Community Edition	Express Lite
Account		
Users	1 user	3 users
Scan data retention	3 months	Up to 13 months (user defined)
Account data retention	Account data purged after 6 months of no activity	Account data maintained indefinitely with subscription
API compatible	No	Yes
Scanning		
PCI attestation compatible	No	Yes - Fully compatible
Scan notification & distribution	Sent to account owner only	Sent to user defined distribution lists
Scheduled scans	Weekly and Monthly scans	Full scheduling functionality
Reporting		
Report templates	Scan Report, Technical Report and Executive Report	All report templates available and fully customizable
Scheduled reports	Not available	Full scheduling functionality
Report notification & distribution	Sent to account owner only	Sent to user defined distribution lists
Option Profiles		
Number of profiles	3 default profiles, 1 custom	Full library of profiles, unlimited custom profiles

Web Application Scanning (WAS)

	Community Edition	Express Lite
Scanning		
Scheduled scans	Not available	Full scheduling functionality
Reporting		
Report templates	Scan Report only	Full Report library
Scheduled reports	Not available	Full scheduling functionality
Option Profiles		
Customization	2 profiles total: Initial Options and 1 custom	Full library of profiles and full customization functionality