Community Edition

Getting Started Guide

July 25, 2018

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

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

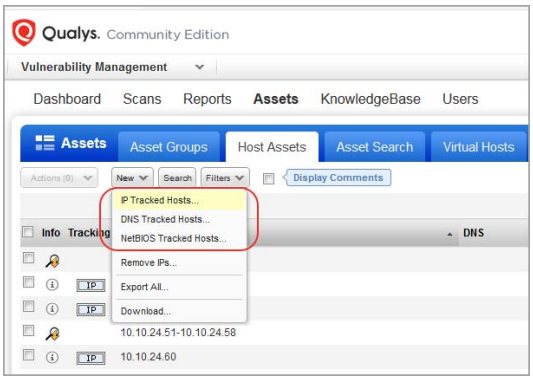
Start your first scan!

Deploy cloud agents for continuous assessments

Add and organize your assets

Add IP addresses for scanning

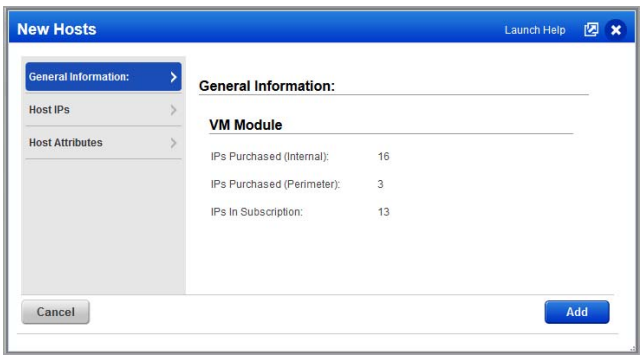
The first thing you'll want to do is tell us the IPs/ranges that you want to scan and report on. In Qualys VM, go to Assets > Host Assets. From the New menu, select IP Tracked Hosts, DNS Tracked Hosts or NetBIOS Tracked Hosts. The tracking method you choose will be assigned to all of the hosts being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



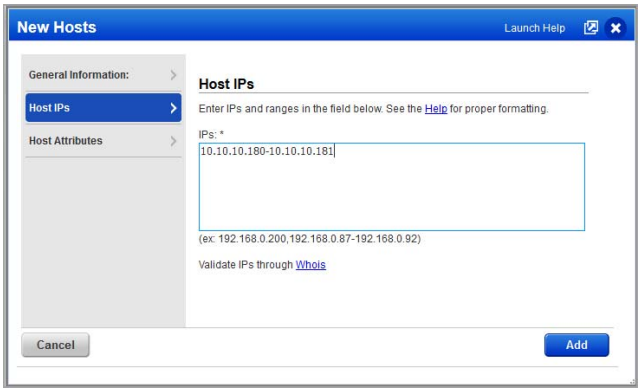
About the tracking method...

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.

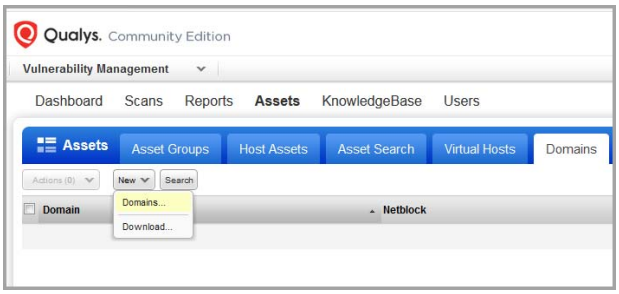


Now jump to the Host IPs tab. Enter the new IPs you're adding and click Add. That's it! The new IPs will appear on your Host Assets list, and they're ready for scanning.

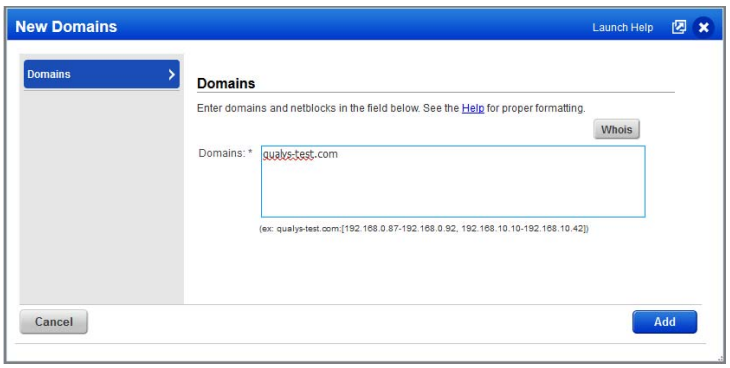


Add domains for mapping

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.

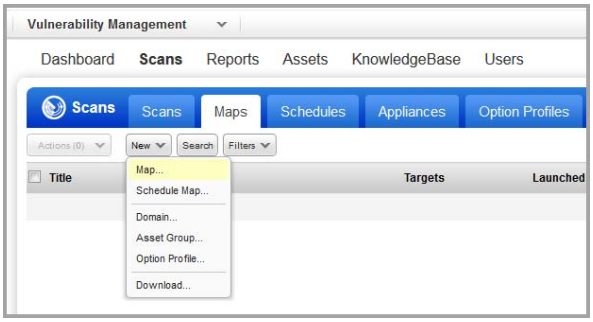


Qualys provides a demo domain called "qualys-test.com" for network mapping. This domain may already be in your account. If not you can add it yourself. Note that the devices in the demo domain reside in Qualys Security Operations Centers, so the Qualys Internet scanners can be used for mapping this domain.

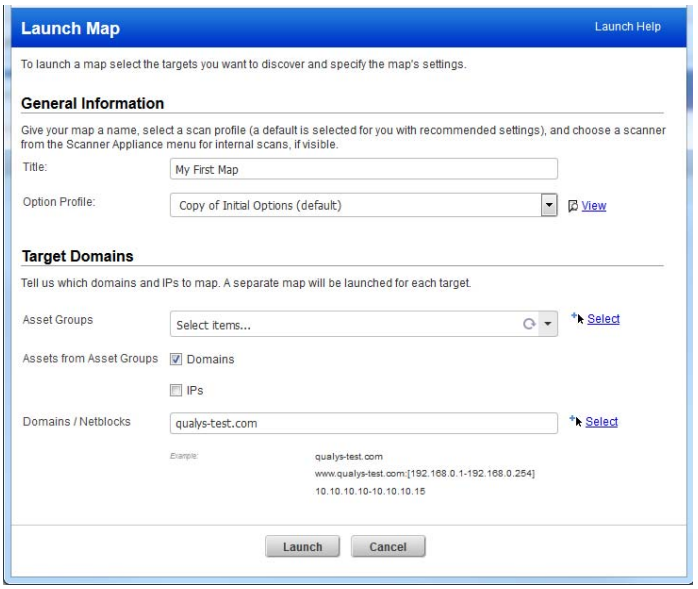
Discover your network

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.



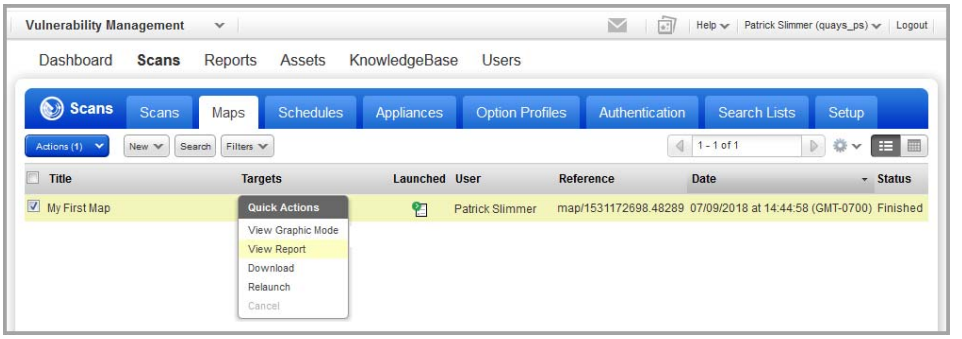
Option Profile - Choose an option profile with the map settings you want to use. Tip - For mapping IPs/ranges without a domain, be sure to enable the map option “Perform live host sweep” in the option profile applied to the task.

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.

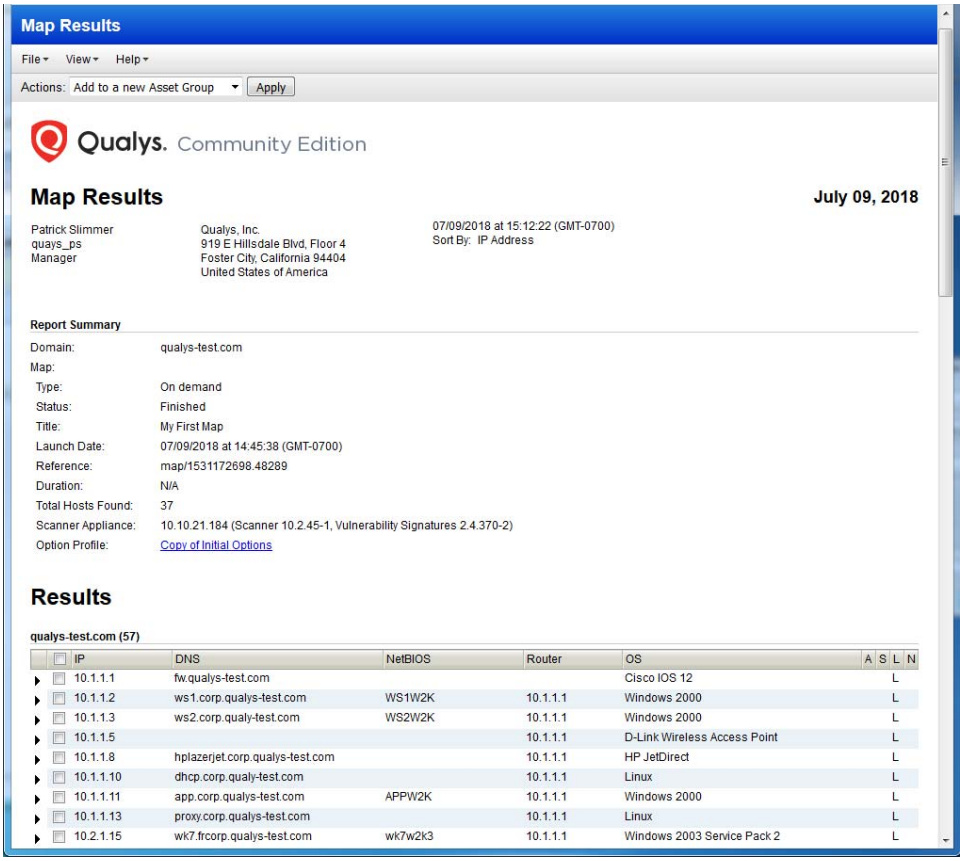
Target Domains - Specify any combination of asset groups, domains and IPs/ranges for your map target. Enter asset groups in the Asset Groups field, and enter domains and IPs in the Domains/Netblocks field.

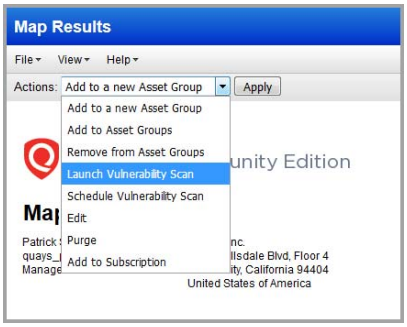
We'll create a separate map report for each target. That means we'll create a separate map for each domain plus a map for any IPs entered. These maps will run sequentially - one at a time - and each map will use a single scanner appliance.

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

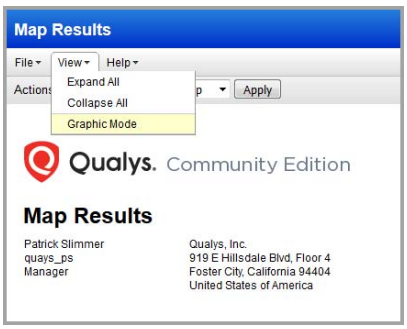


In the Results section you'll see a list of the hosts detected on the mapped domain. For each host, you'll see the IP address, DNS and NetBIOS hostnames, the router being used by the host and the operating system.



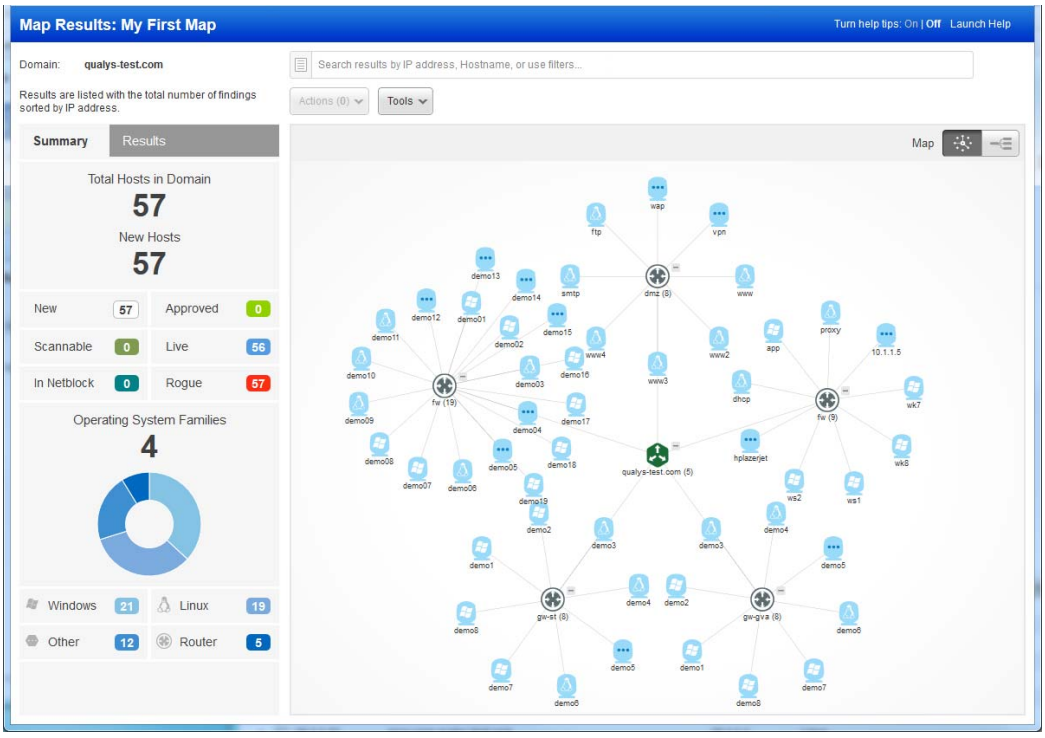


Map results are closely integrated with scan capabilities. There are several actions you can perform on the hosts listed in your map results. For example, you can scan hosts right away, you can add newly discovered hosts to your account. Select the check box next to each host to include in the action,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



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

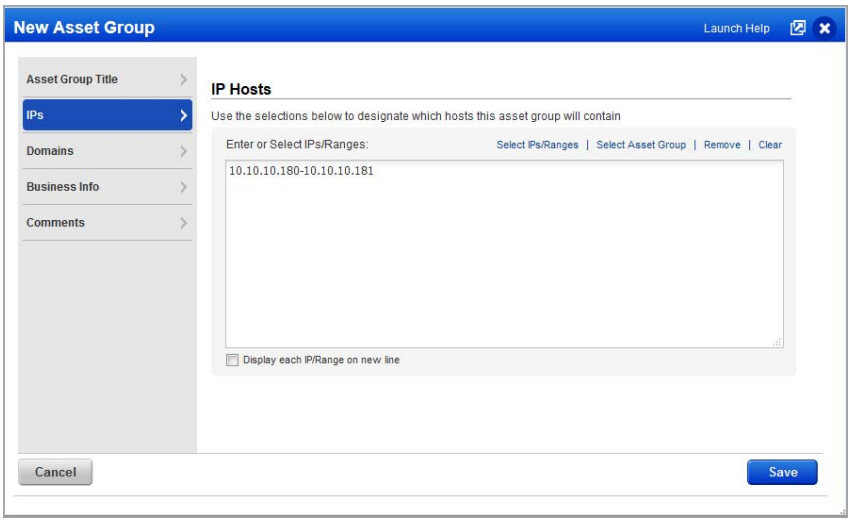
Your map results will appear in a graphical view like shown below. Use the Summary on the left to drill-down into results or enter a search query at the top of the page.



Organize assets into asset groups (optional)

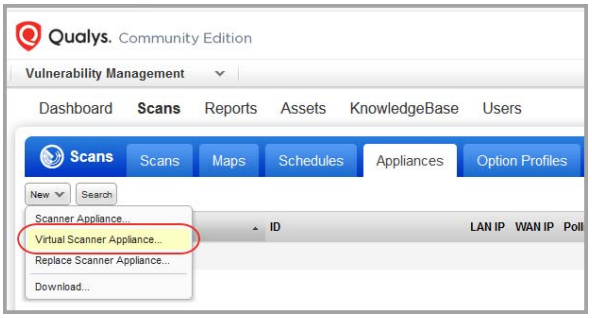
Asset groups give you a convenient way to make logical groupings of the assets you want to scan and report on. The same assets can appear in multiple groups as needed.

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.

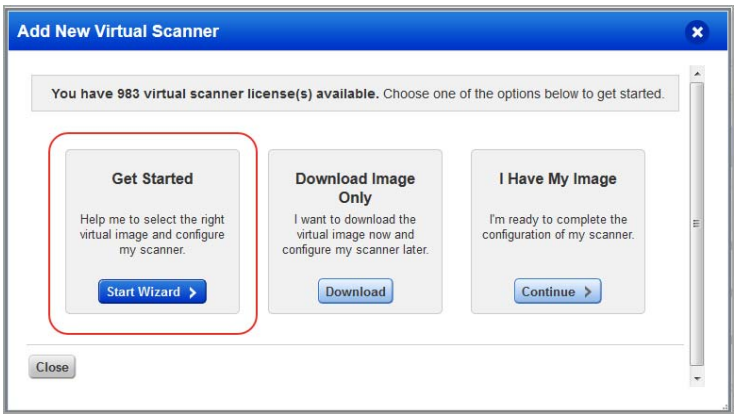


Add a Virtual Scanner Appliance

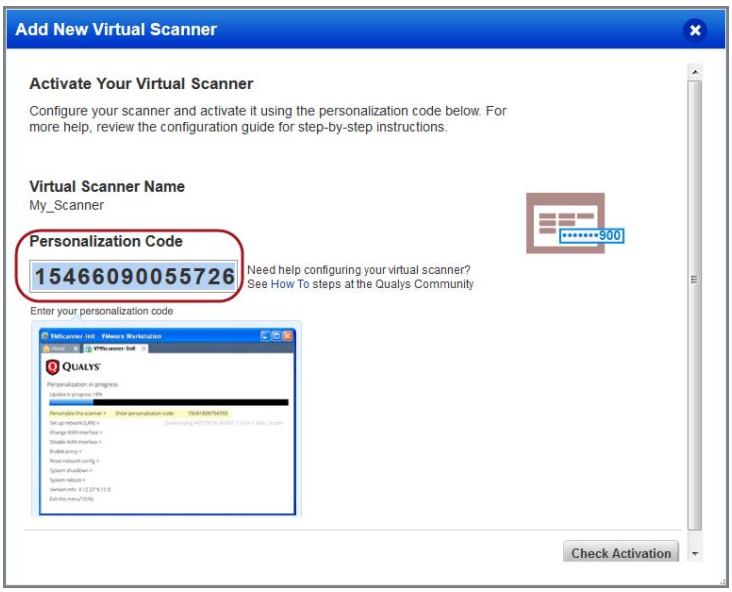
Your Community Edition subscription allows 1 virtual scanner appliance for internal scanning. Go to Scans > Appliances and select New > Virtual Scanner Appliance.



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



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



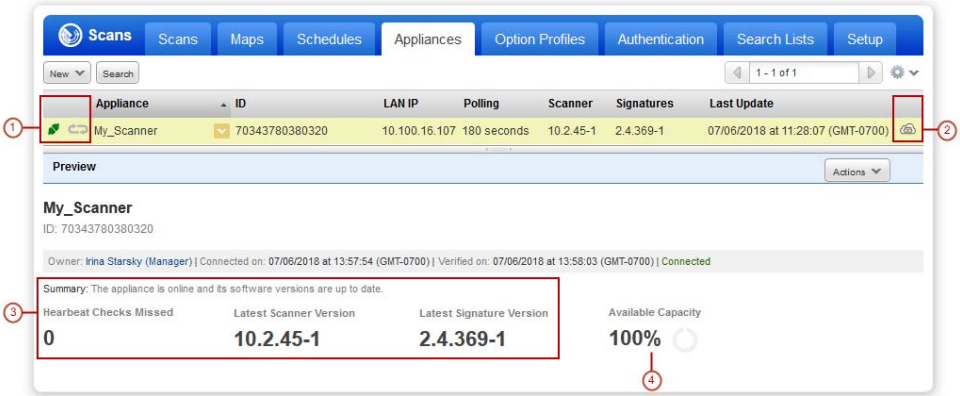
Complete the configuration using the virtual scanner console or cloud platform (this is when you'll need the personalization code).

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.



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.

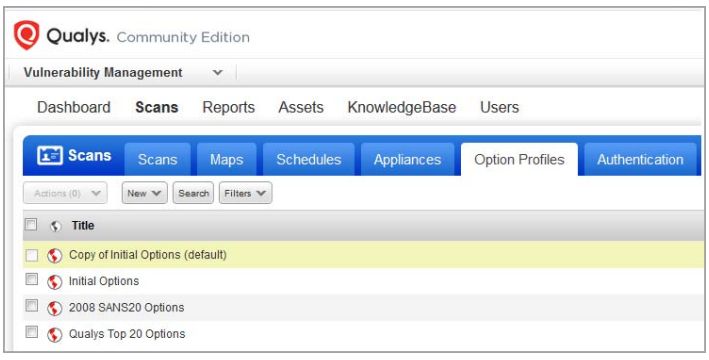
3 - Latest software versions - these are installed as part of the activation.

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.

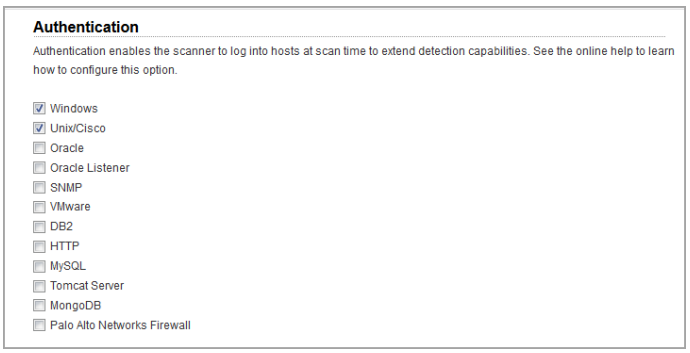


Host Authentication is recommended

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.

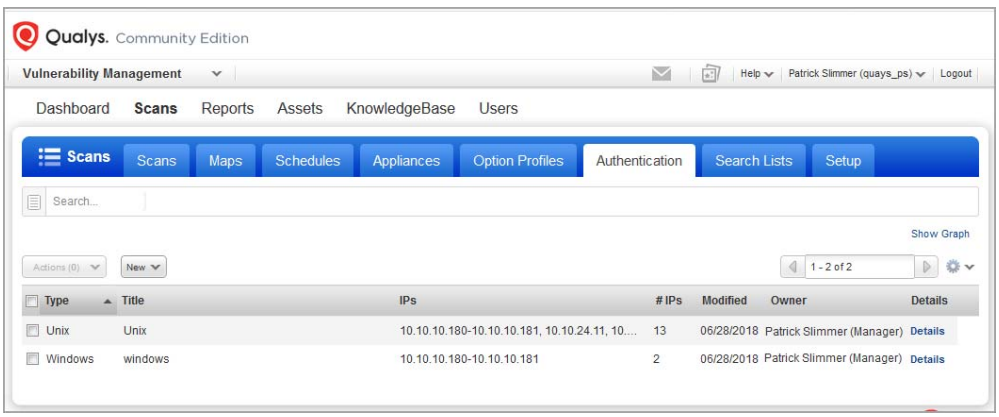
How to setup authentication:

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



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

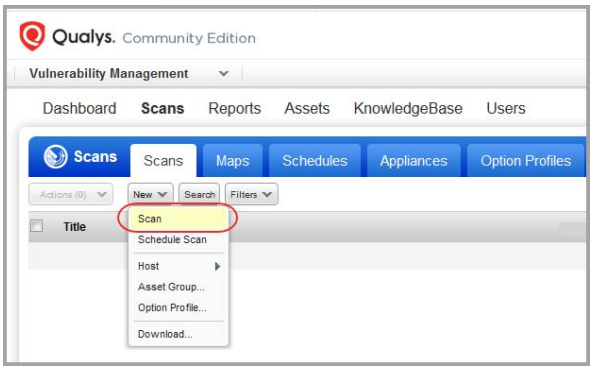
2) Add authentication records for your host technologies. Go to Scans > Authentication and create new records from the New menu. For each record you'll provide login credentials that our service will use to log in to each host at scan time.



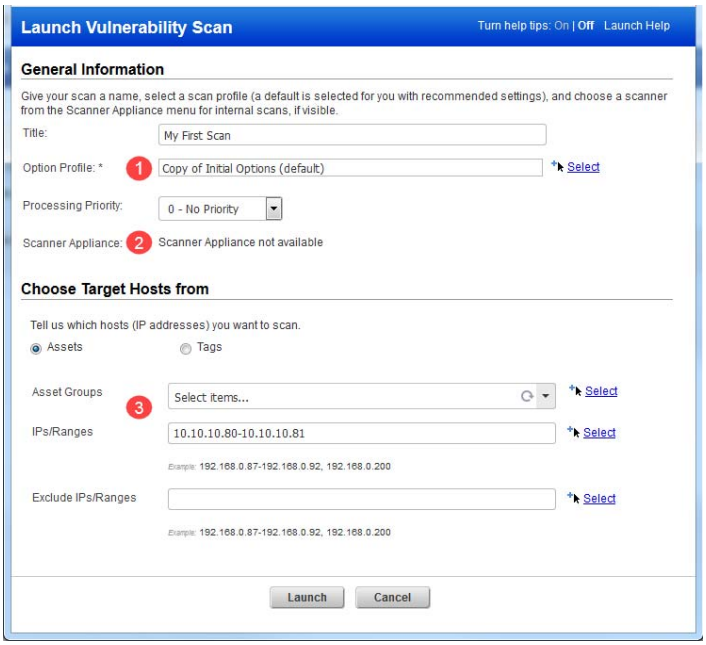
Start your first scan!

You're now ready to start a vulnerability scan.

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



Choose your scan settings.



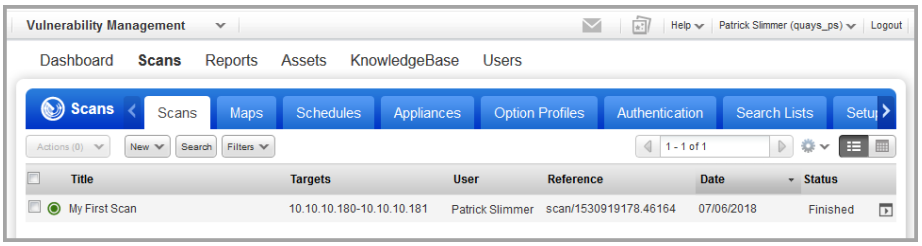
(1) Option Profile - You can choose one of the default profiles provided or the custom profile that you previously saved, if applicable.

(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.

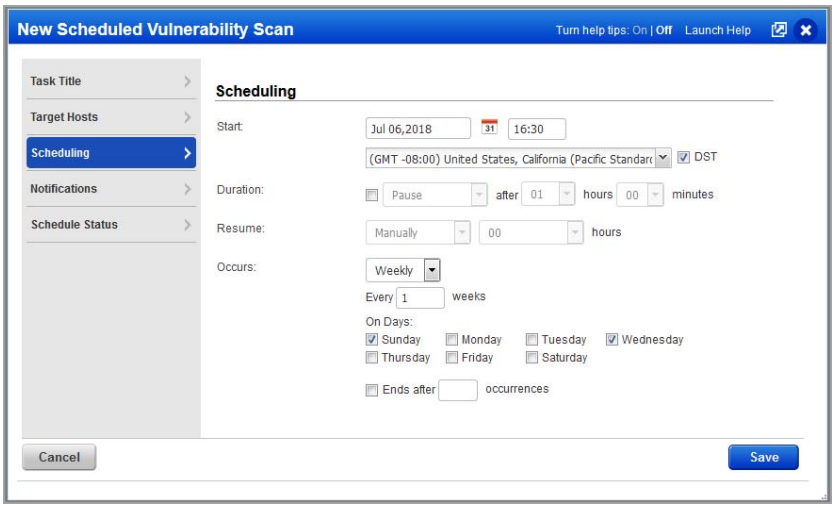


◉ means results are processed and available in your account.

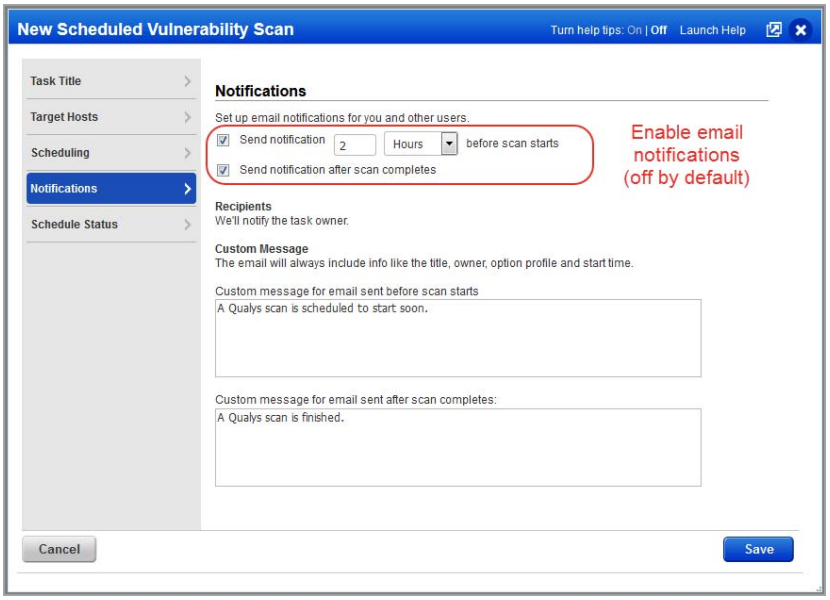
◯ means the scan is finished but the results are not processed. Go to Filters > Processing Tasks to see the status.

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.

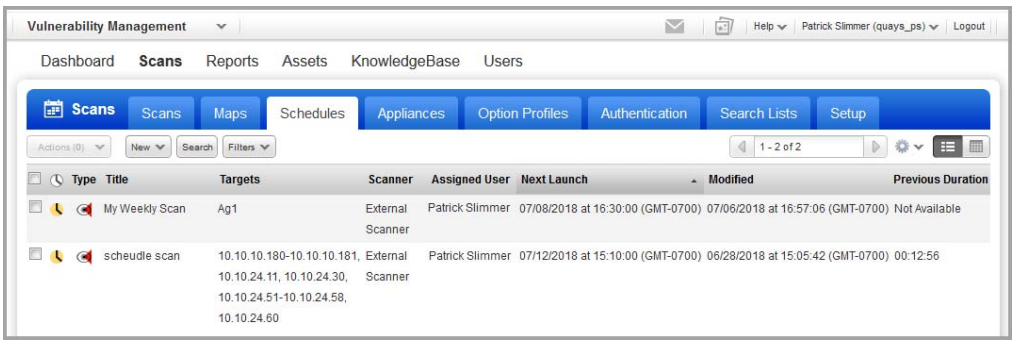


Go to the Notifications tab if you want to be notified by email before the scan starts or when it's finished. You can even customize the message included in the email body.



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 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.

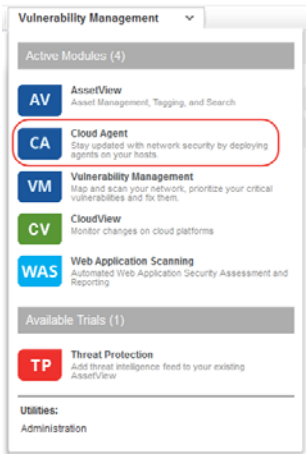
- Download the agent installer to your local machine.

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

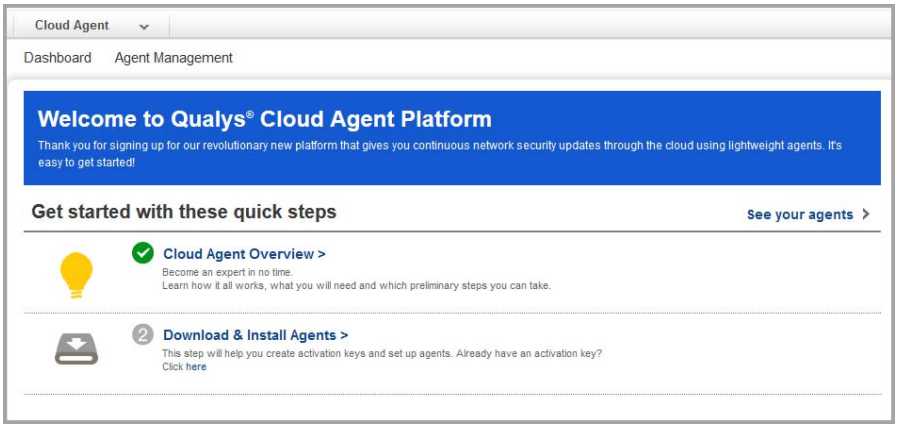
- Activate agents for modules in your subscription (i.e. VM, PC, etc). A license will be consumed for each agent activated.

Get Started

Select the Cloud Agent app from the app picker.



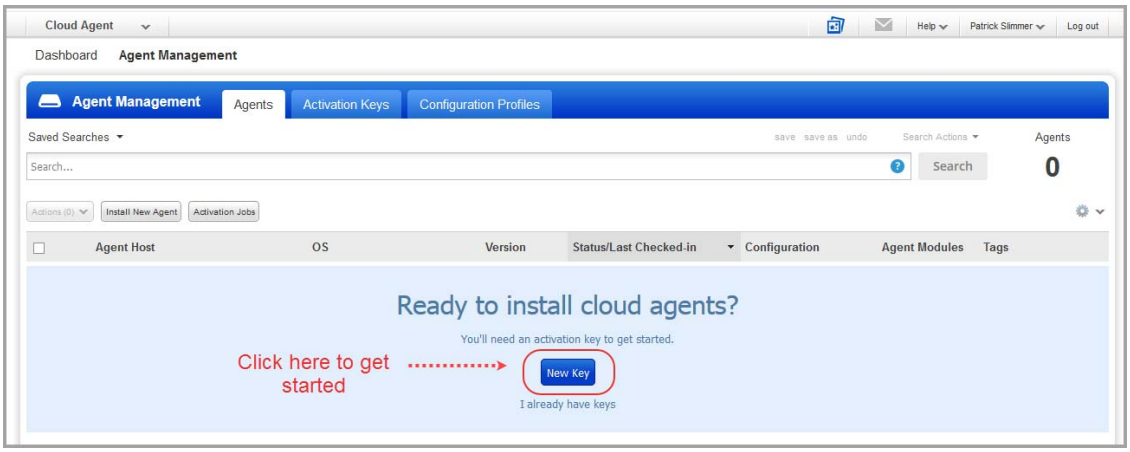
Check out the Quick Start Guide (you can go to user name menu and select this option anytime). You'll see step by step instructions with links to the right places to take actions.



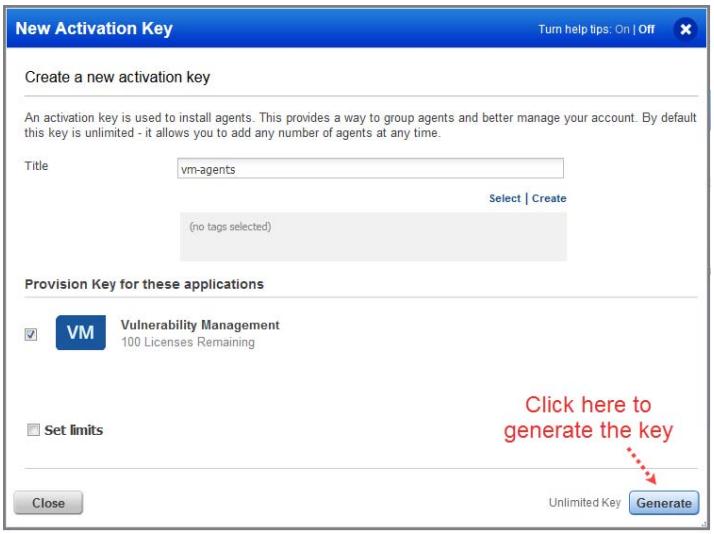
It's easy to install agents

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

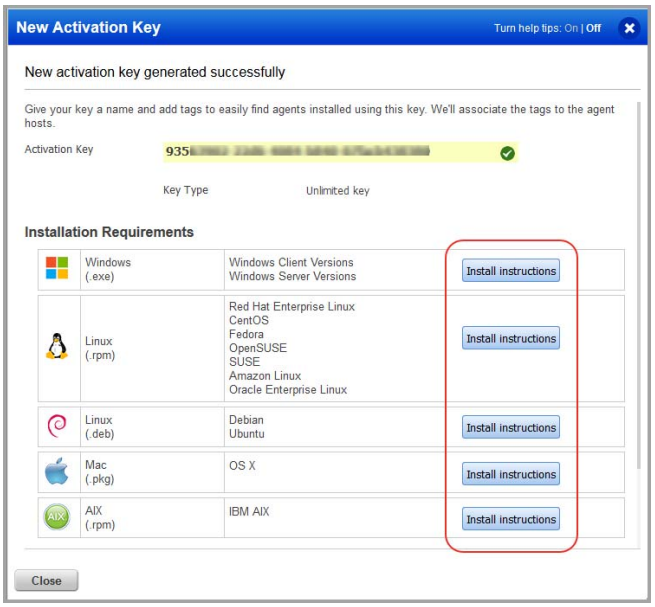
You'll need an activation key. Select New Key to create one.This key provides a way to group agents and bind them to your account. For example, you can create different keys for various business functions and users. (Already have a key? Select a key on the activation keys list and choose Install Agent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



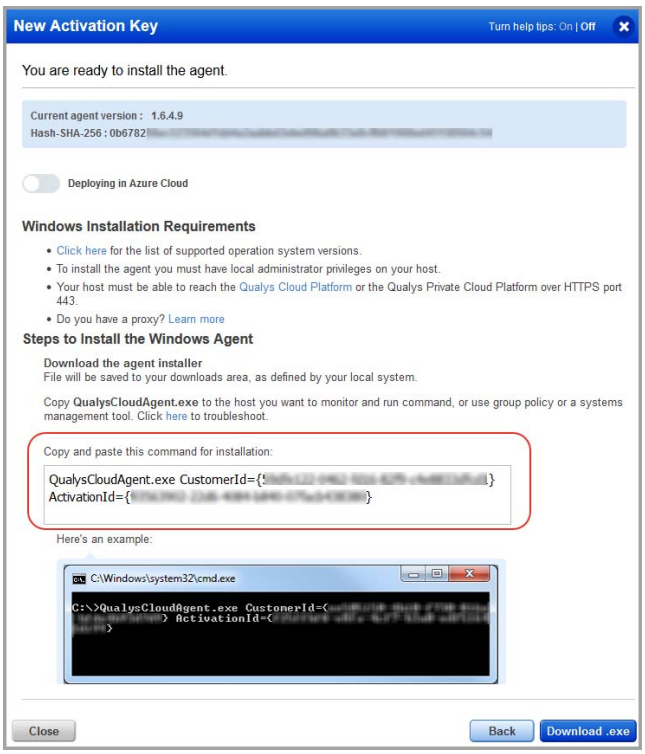
Give your key a name and provision the key for the VM application. If you have additional apps like PC, FIM and IOC then you'll see them listed as well. Click Generate.



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

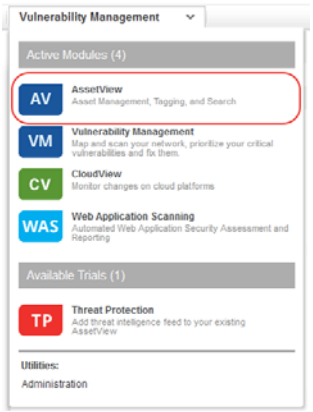
Unix Agent

Mac Agent

Analyze, Query & Report

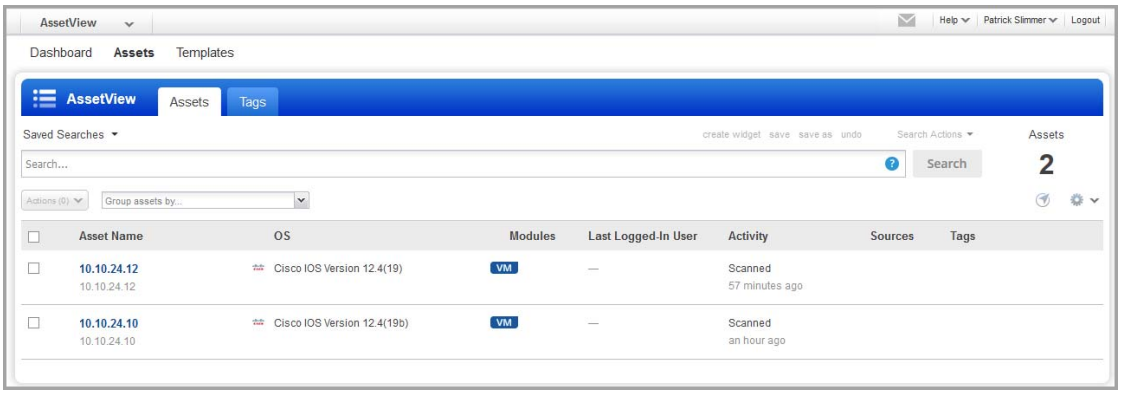
In this section we'll cover how to create reports in VM, and how to query assets, build widgets and dashboards in AssetView.

How to Query Assets

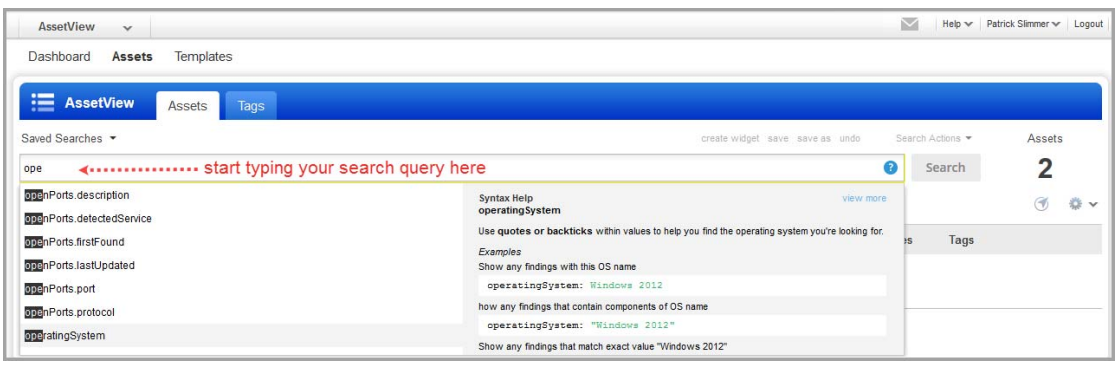


Select the AssetView app from the app picker.

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

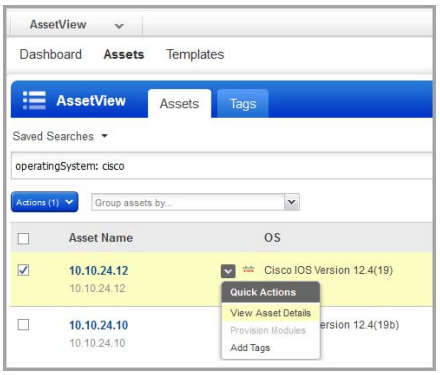


Start typing in the search field and you'll see a list of asset properties (tokens) you can use to search. Hover over the token name to see syntax help to the right.



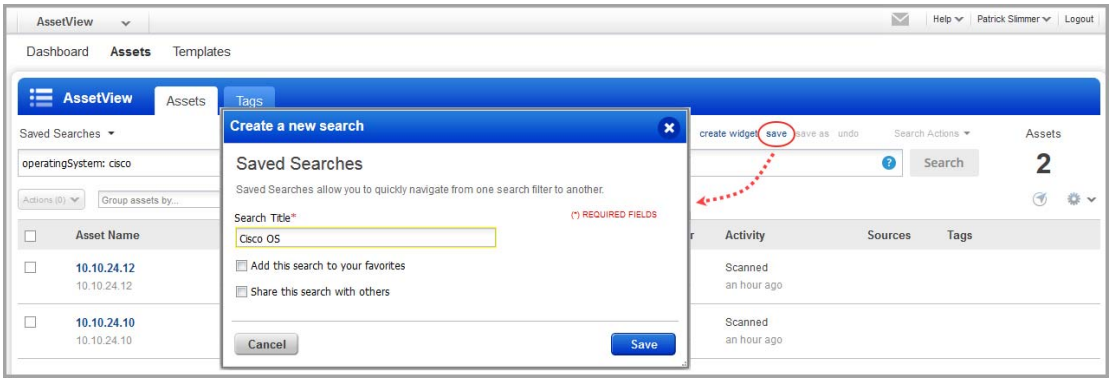
View Asset Details anytime

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.



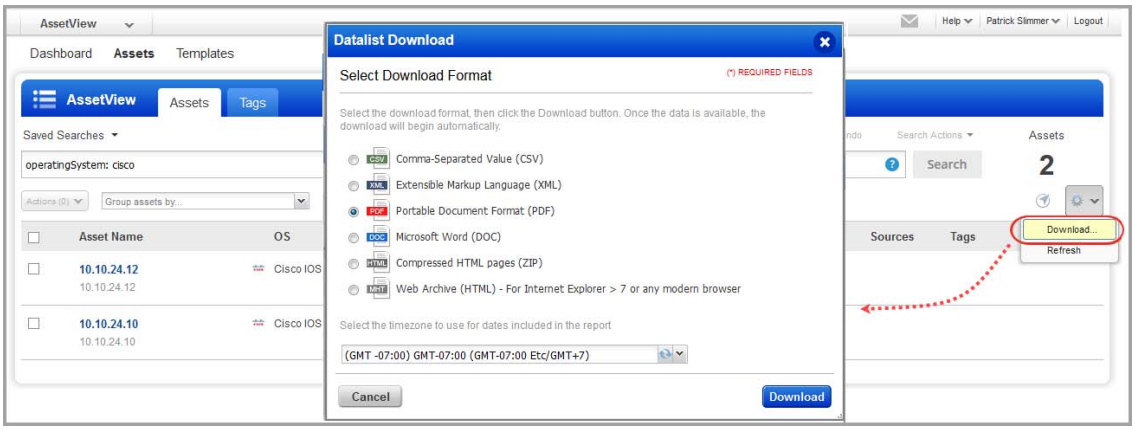
Save Query

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



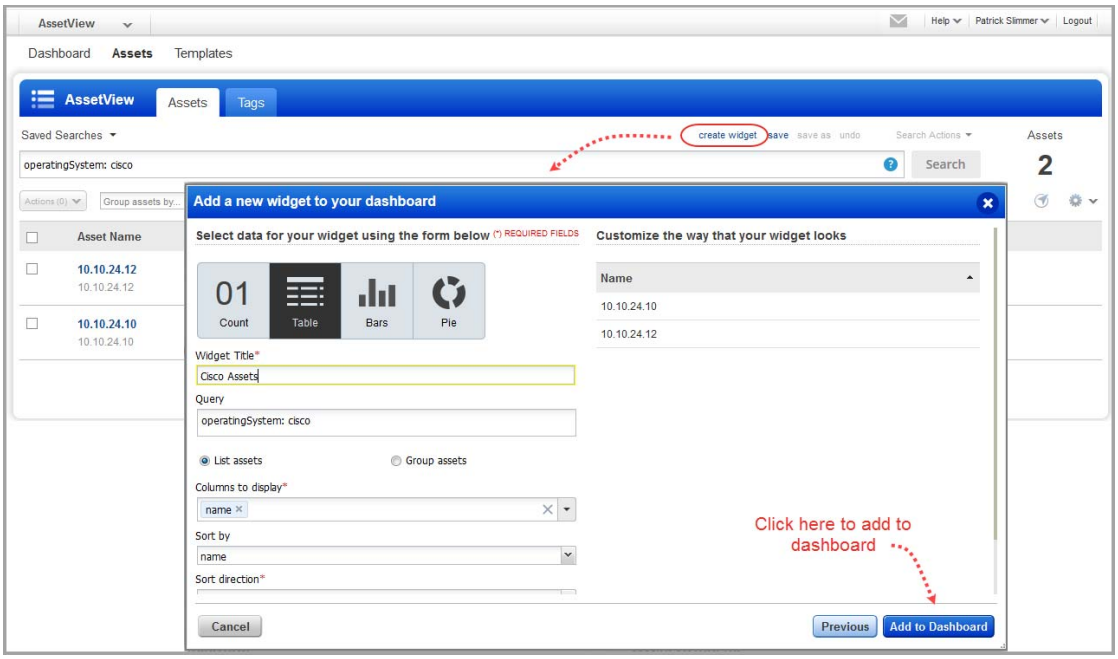
Download and export results

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



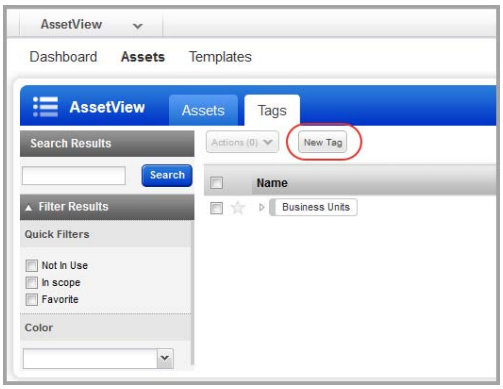
Create widget

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.

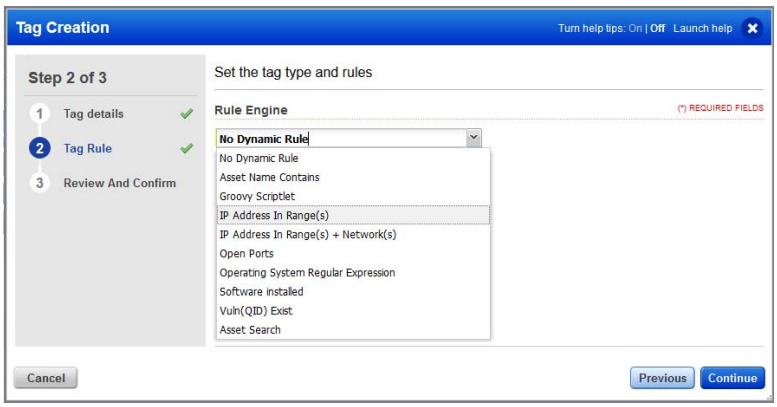


Organize assets using asset tags (optional)

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.



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.

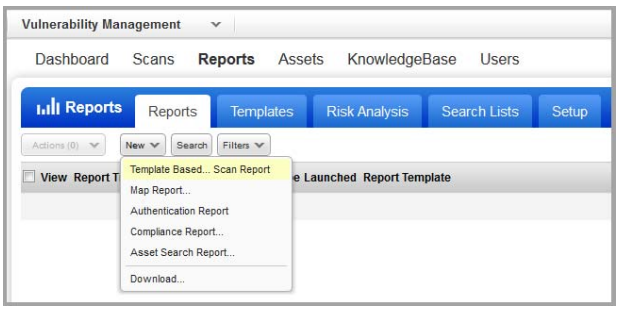


Tip - Turn help tips on (in the wizard title bar) and we'll show you help as you hover over the settings.

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

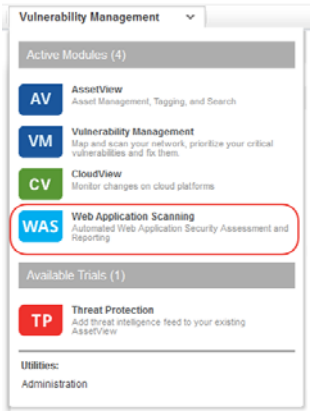
Add a web application

Launch a discovery scan

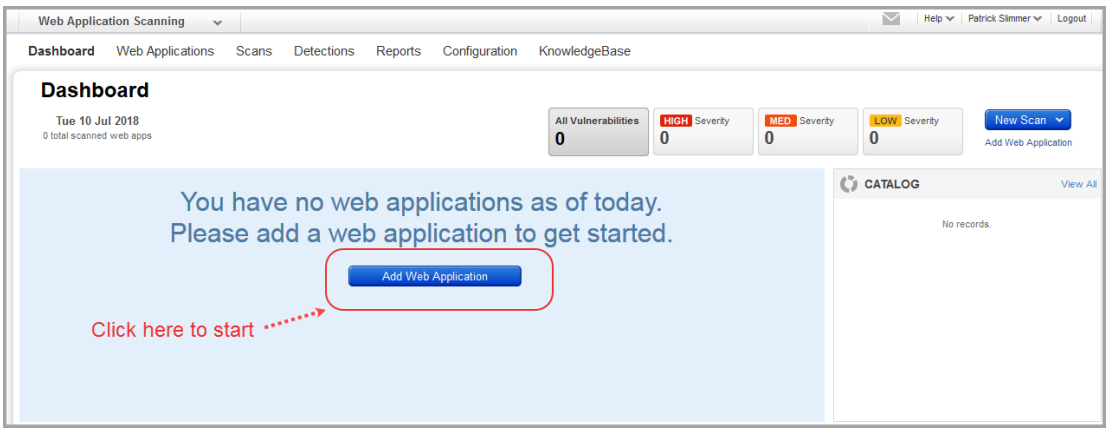
Scan for vulnerabilities

Add a web application

Select the WAS app from the app picker.

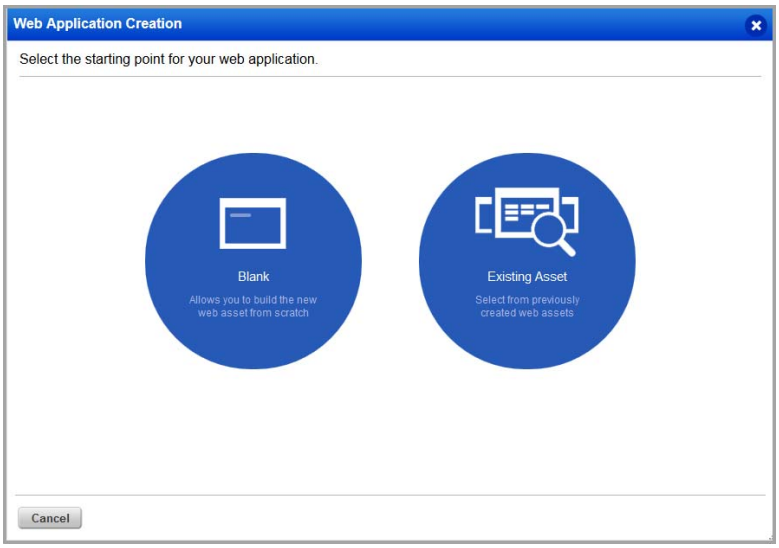


Start by telling us about the web application you want to scan. Click Add Web Application.



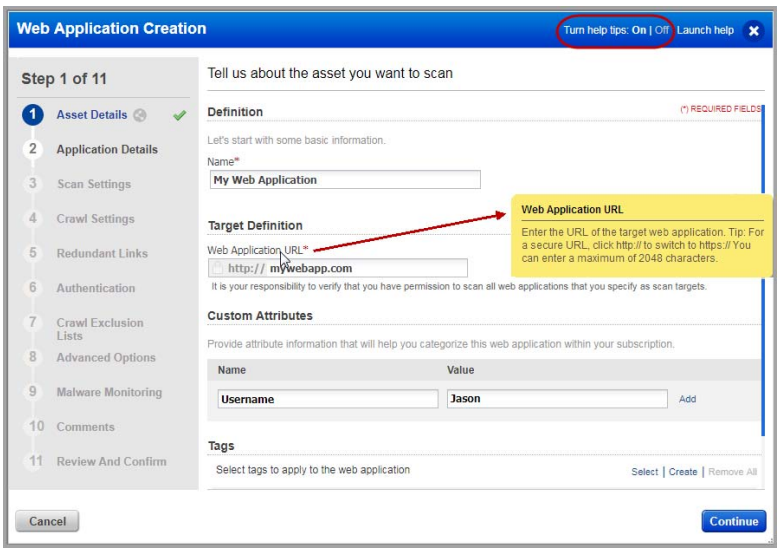
Choose the starting point

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



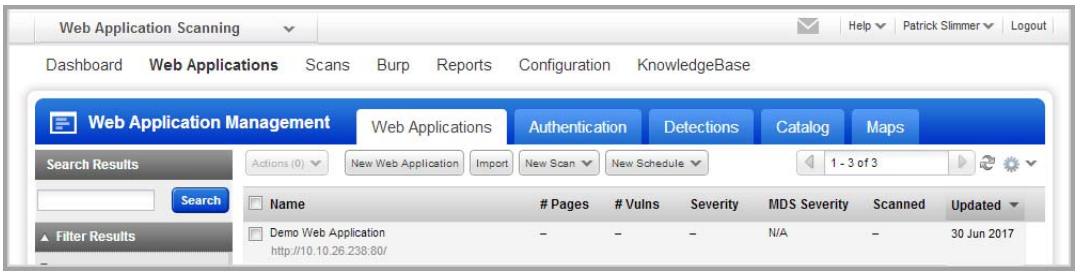
Add your web app settings

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.



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.



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.

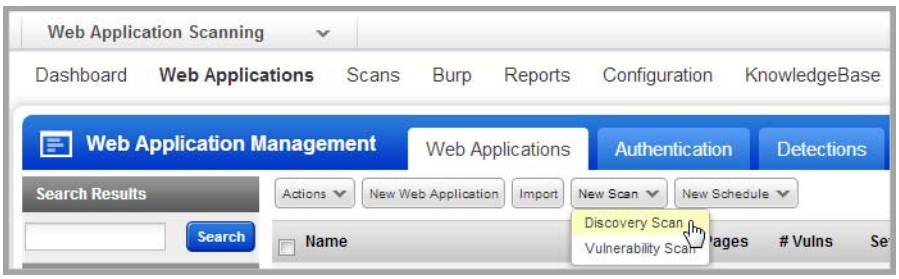
Warning about scans and their potential impact

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.

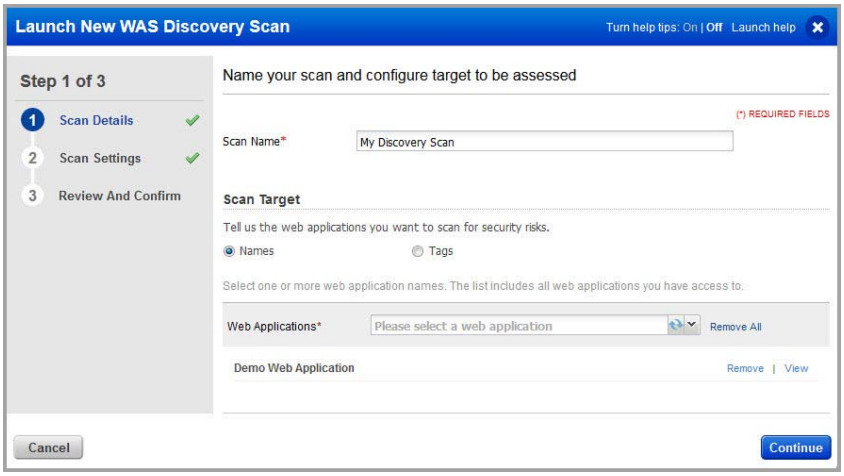
Launch a discovery scan

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.



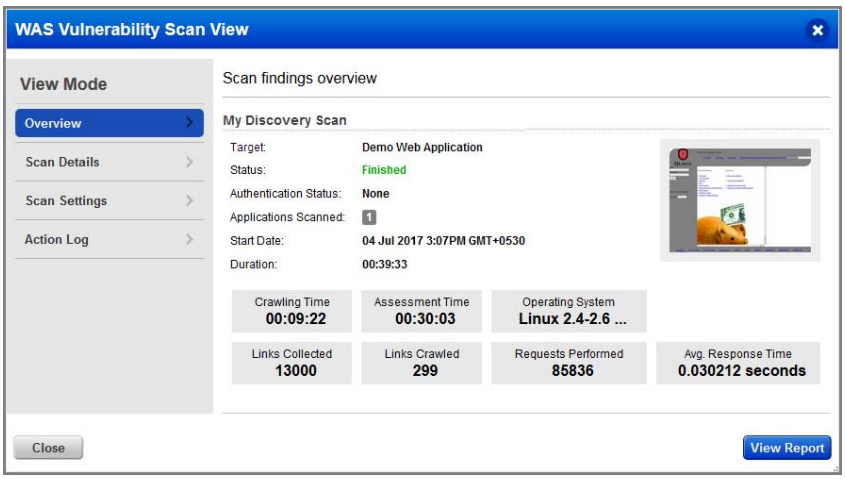
The launch scan wizard walks you through the steps. Tell us the web application you want to scan and select scan settings (* means required). Click Continue to walk through the discovery scan wizard. Then click Finish when you're done.



The scan view

Double click the finished scan to see the scan view.

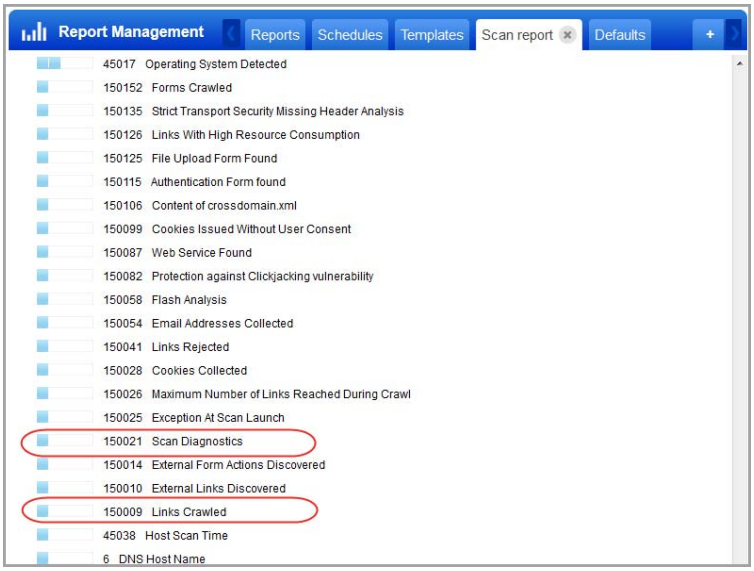
The Overview gives you an overview of the scan findings.



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

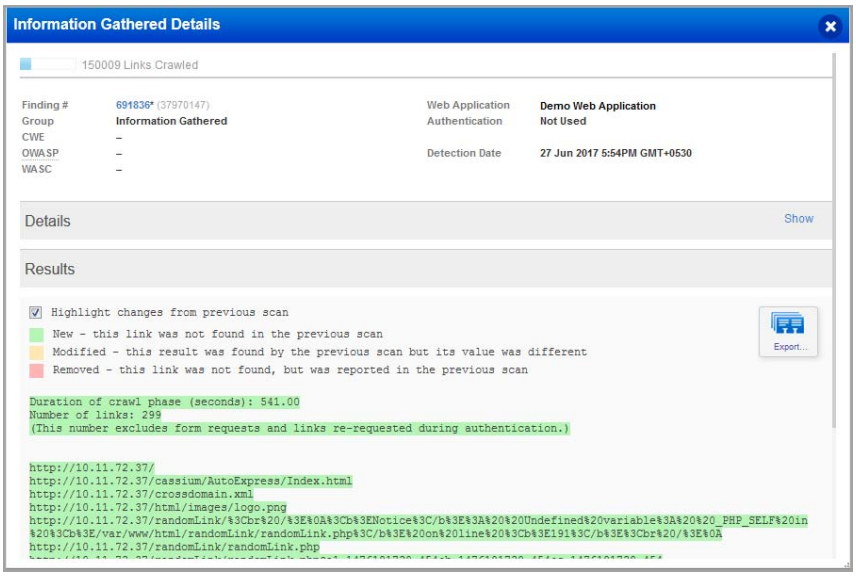
The full scan report

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



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.



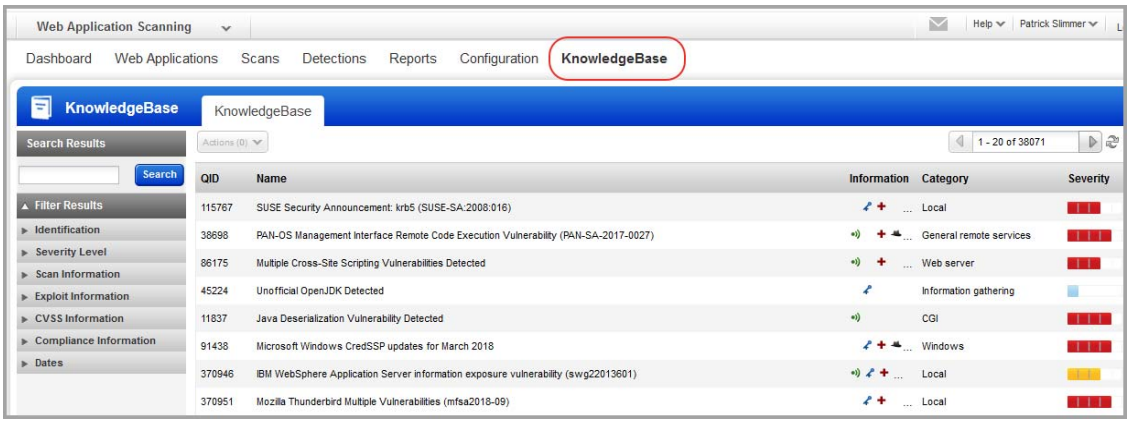
Scan for vulnerabilities

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.

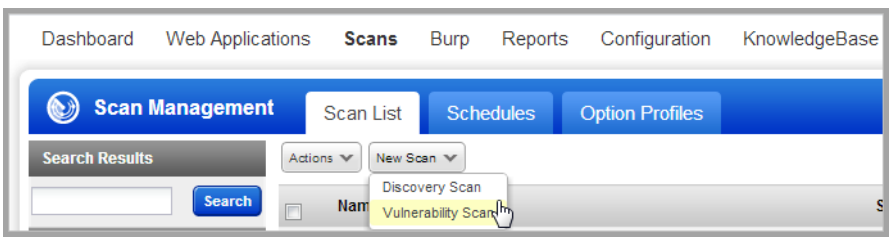
Click KnowledgeBase on the top menu.



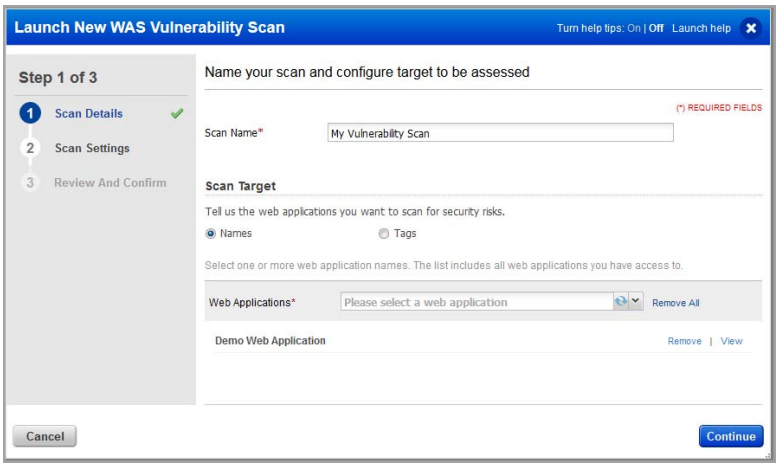
What is Severity? Each QID is assigned a severity level by our service: confirmed vulnerability (red), potential vulnerability (yellow) and information gathered (blue).

Start your scan

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

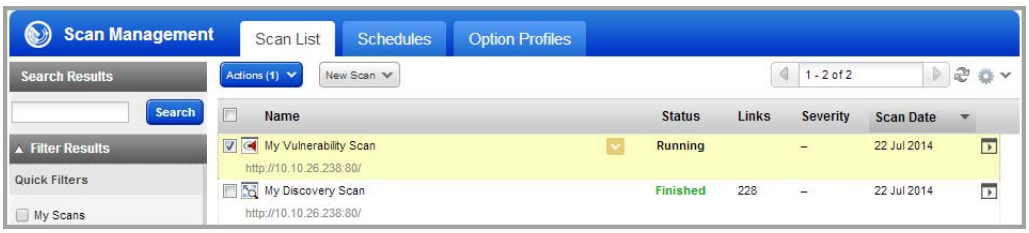


The launch scan wizard walks you through the steps. You'll tell us the web application you'd like to scan for vulnerabilities and select scan settings. Click Continue to make your settings and then click Finish.

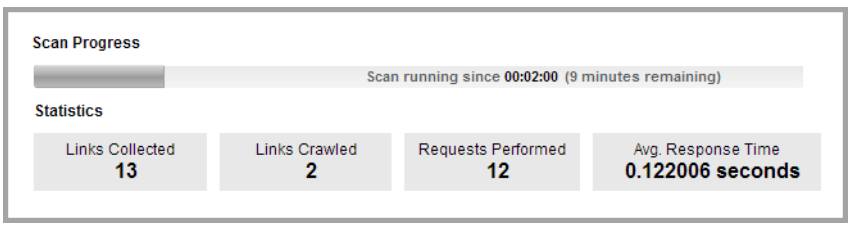


Check scan progress

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

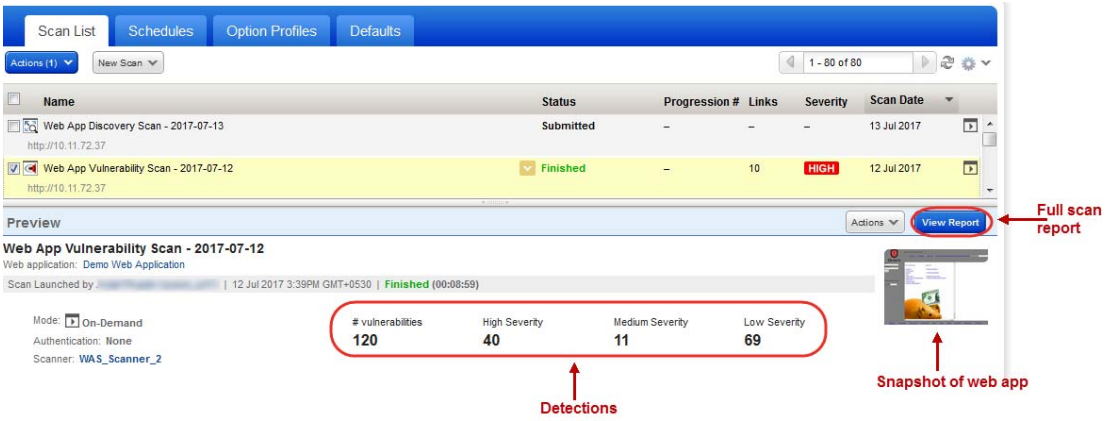


Want more info? Double click the scan row. Then you'll see the Scan Progress bar - this gives you an estimate of when the scan will finish.



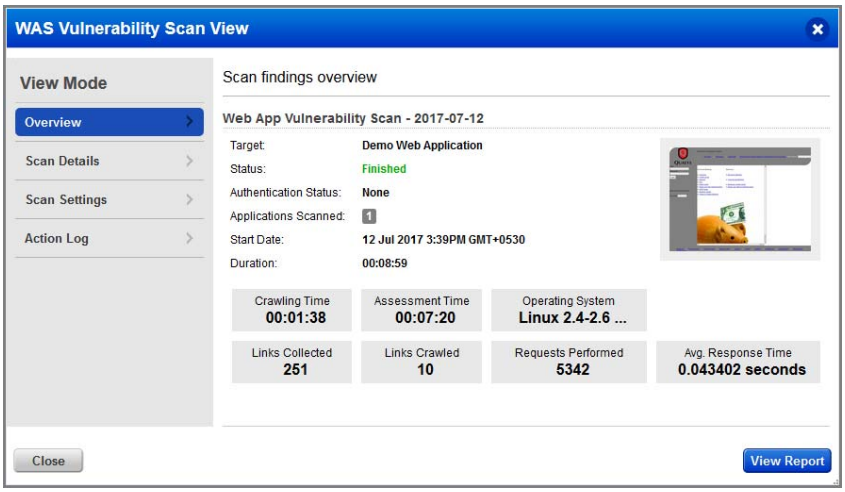
Your scan results

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



The scan view

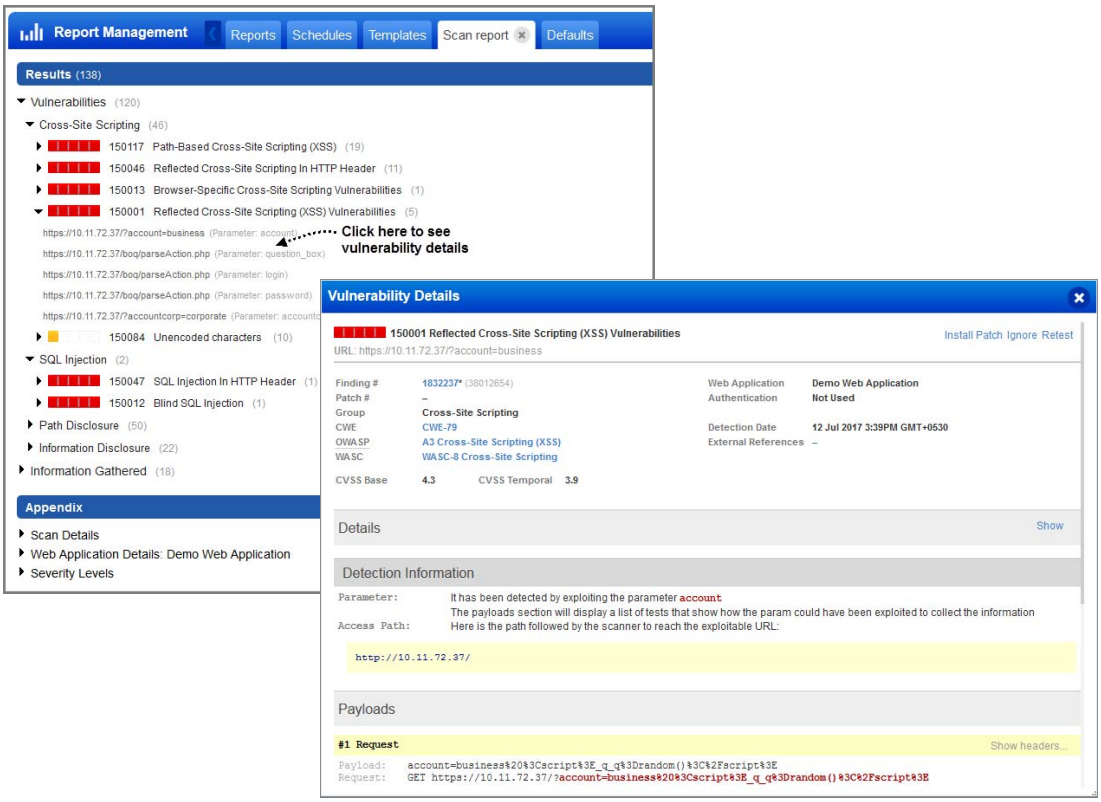
Hover over the scan and select View from the Quick Actions menu. The Overview gives you an overview of the scan findings.



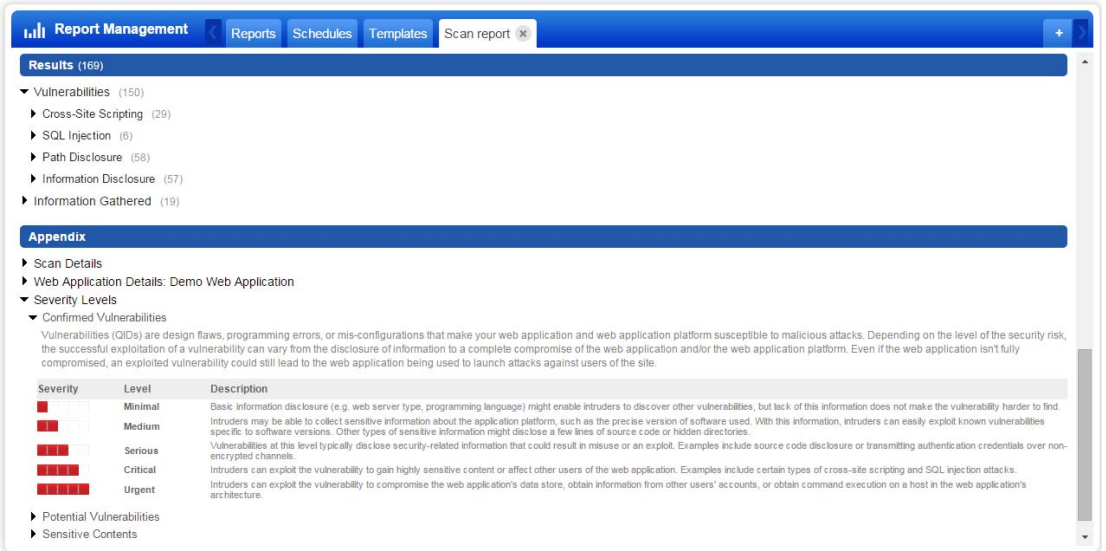
Want to see the full scan report? Just click the View Report button.

The full scan report

Vulnerabilities are sorted by group.



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



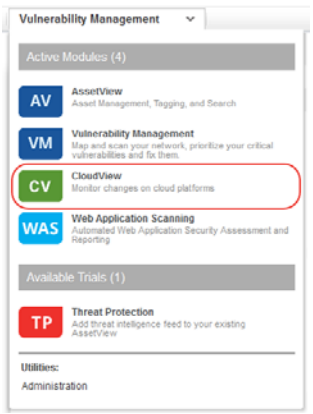
CloudView Free

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

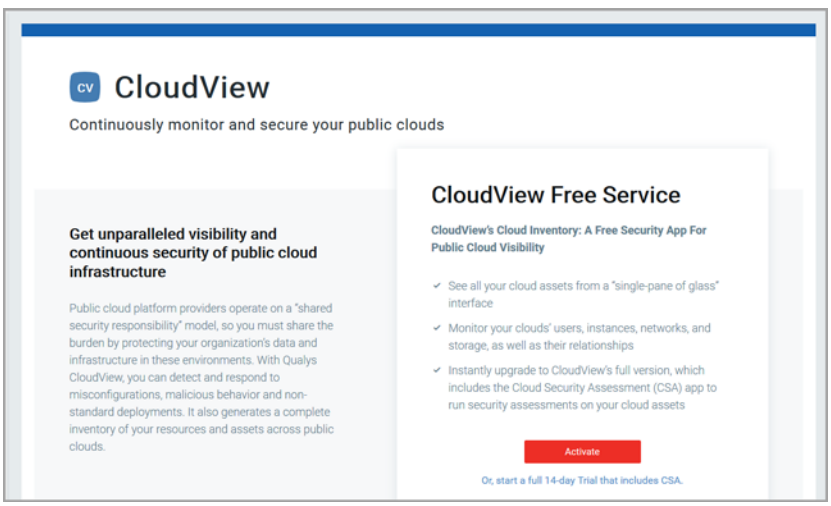
Quick Steps

Activate CloudView Free service

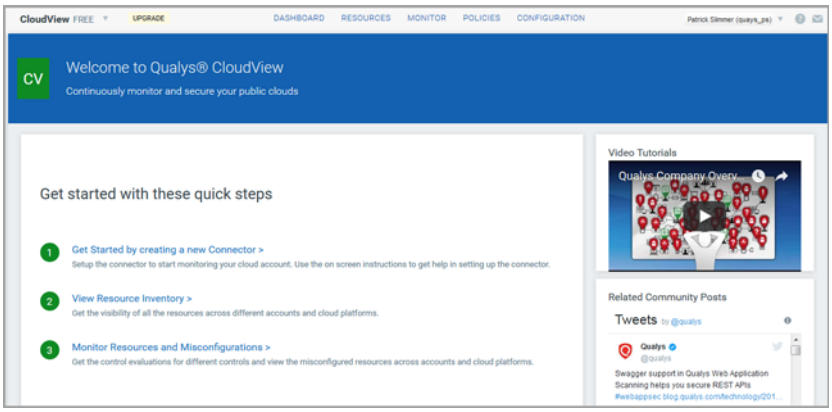
Select the CV app from the app picker.



Click Activate to get started with the CloudView Free service.



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

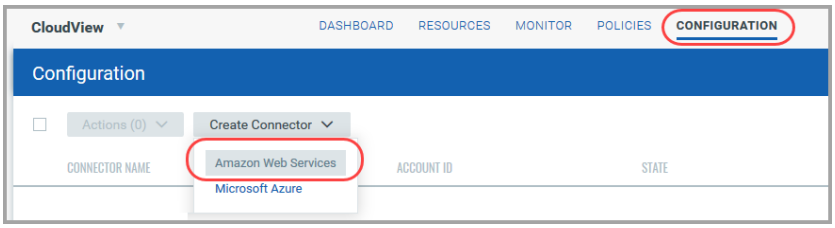


Add a connector

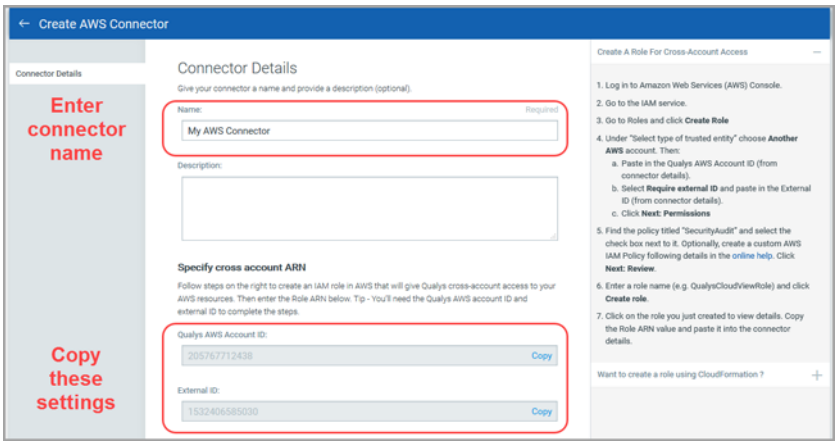
Once you have your connector, we'll start discovering resources that are present in your cloud account. You can create AWS connectors and Azure connectors.

Create AWS connector

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

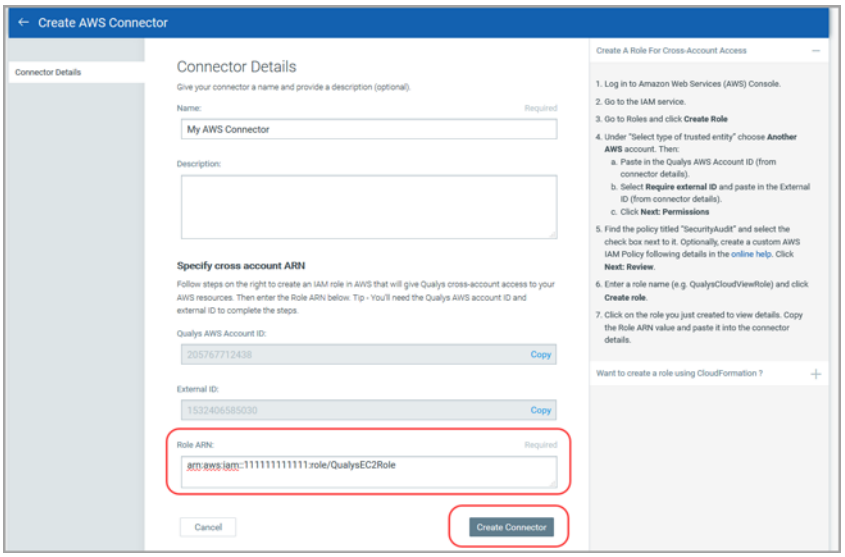


Provide a name and description (optional) for your connector. Then copy settings from the connector details: Qualys AWS Account ID and External ID. You'll need these for creating your IAM role in the AWS console..



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.



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

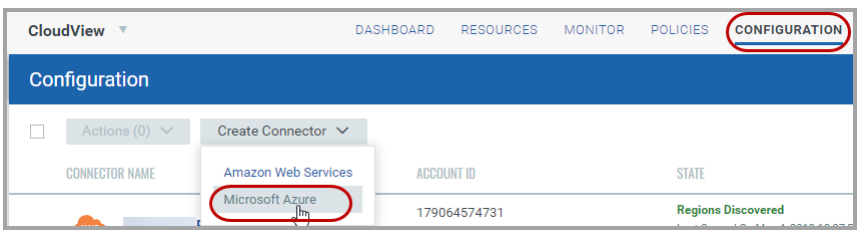
Want to create a role using CloudFormation?

Download the CloudFormation template from the Create AWS Connector window.

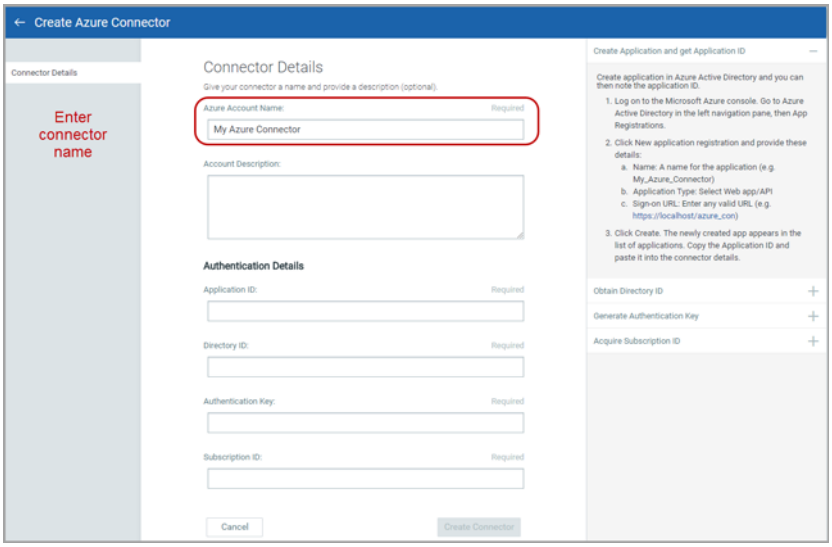
Follow the steps on the screen to create a stack and upload the template. When the stack is complete, copy the Role ARN from the output and paste it into the connector details.

Create Azure connector

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



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



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

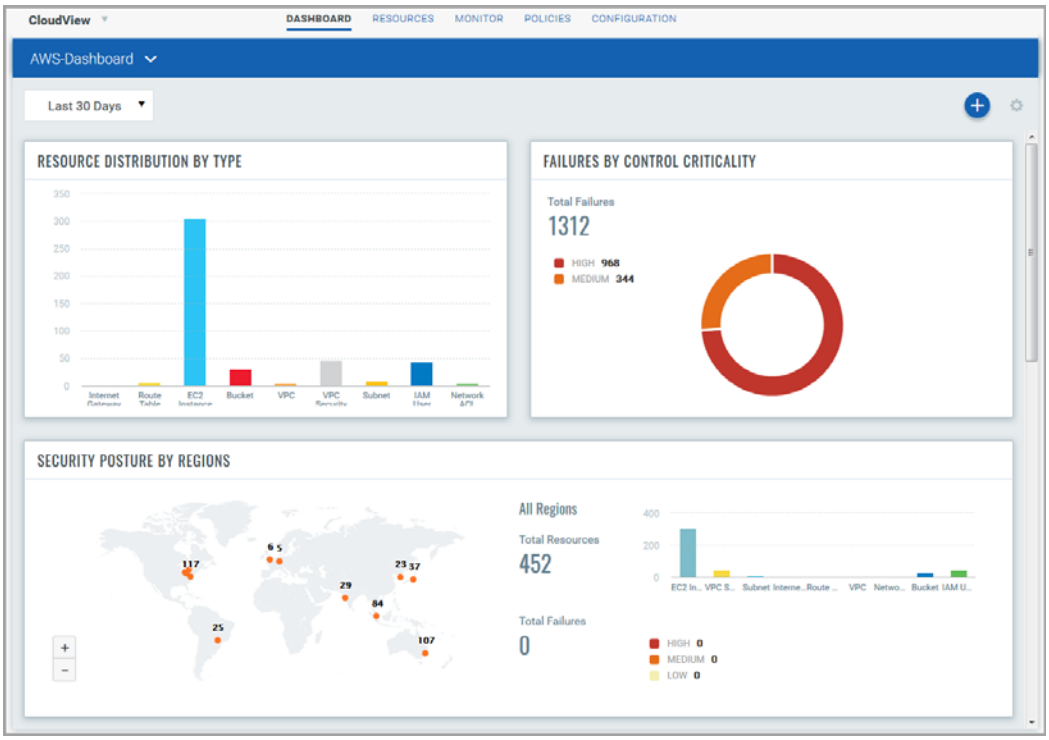
- Total evaluation failures i.e. the resources misconfigurations by control criticality

- 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

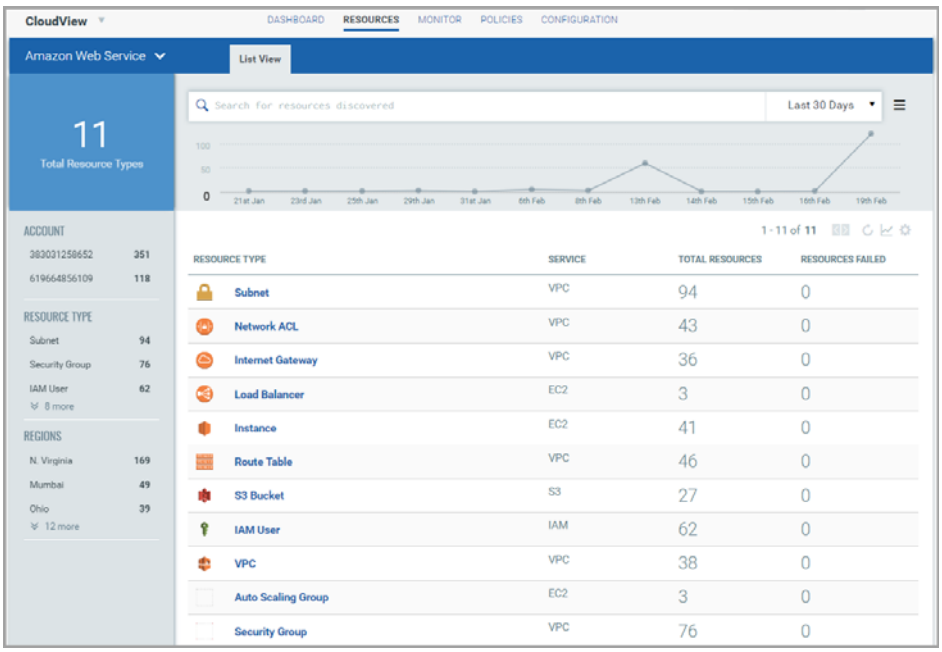


Resources Details

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