Qualys AssetView

User Guide

March 31, 2022

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

Table of Contents

About this Guide

Welcome to Qualys AssetView! AssetView is our free asset discovery and inventory service. We'll help you get instant visibility on all your assets in one place!

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Get Started

Qualys AssetView gives you a comprehensive view of your network that is continuously updated.

What assets are included?

You'll see all assets (IP addresses, web sites) that have been scanned using Qualys external scanners, scanner appliances and/or cloud agents. Not seeing assets? Do one of these things: launch scans and/or install agents.

Launch scans

Set up scans using these applications: VM/VMDR, PC, WAS. Your assets inventory will be updated once scan results are processed. Using WAF? Set up a firewall on a web site using WAF.

Tip - The New Data Security Model must be configured for your account. Be sure you've opted in. A Manager can do this by going to VM/VMDR > Users > Set Up > Security.

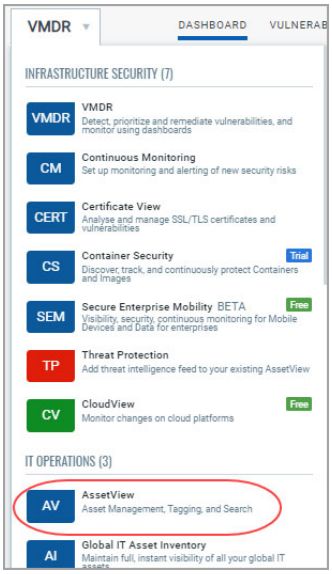
Install agents

Choose Cloud Agent (CA) from the application picker and we'll help you with the steps. It only takes a few minutes. Agents can be installed on your on-premise systems, dynamic cloud environments and mobile endpoints. Agents are self-managed, and self-updating.

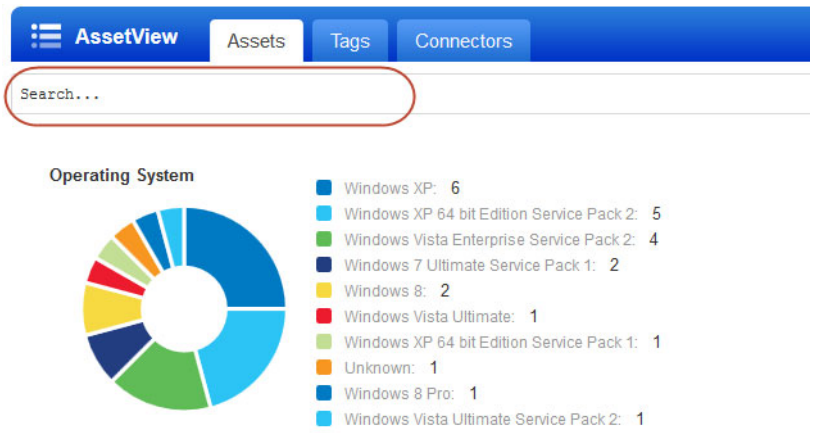
Search Your Assets

The search field in the assets section gives you the power and flexibility to search all your asset data returned from scans and cloud agents in a matter of seconds.

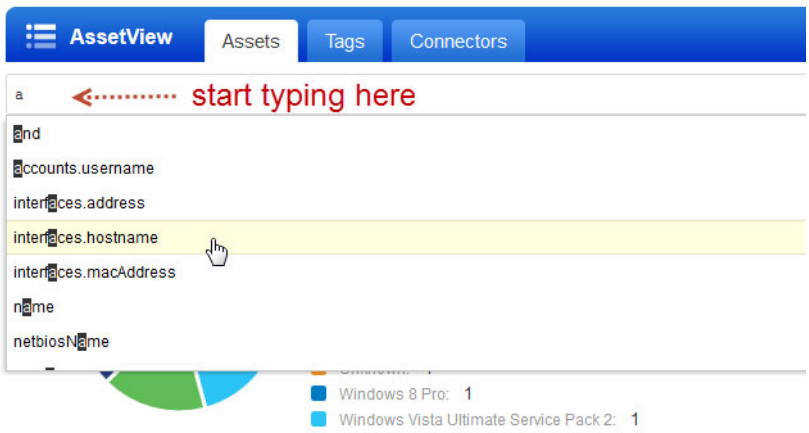
Start by choosing AssetView from the application picker.



You'll notice the Search field above the Assets dashboard (on the Assets tab). This is where you'll enter your search query.



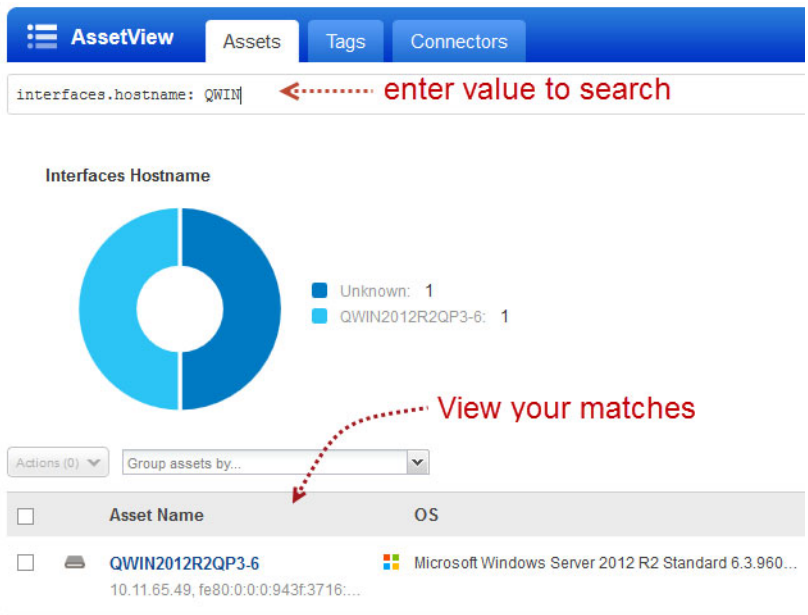
Start typing and we'll show you the asset properties you can search like username, hostname, etc. Select the one you're interested in.



Tip for Threat Protection users:

Type threat and we'll show Real-Time Threat Indicators RTI).

Now enter the value you want to match, and click Search. Your matches appear in your assets list.



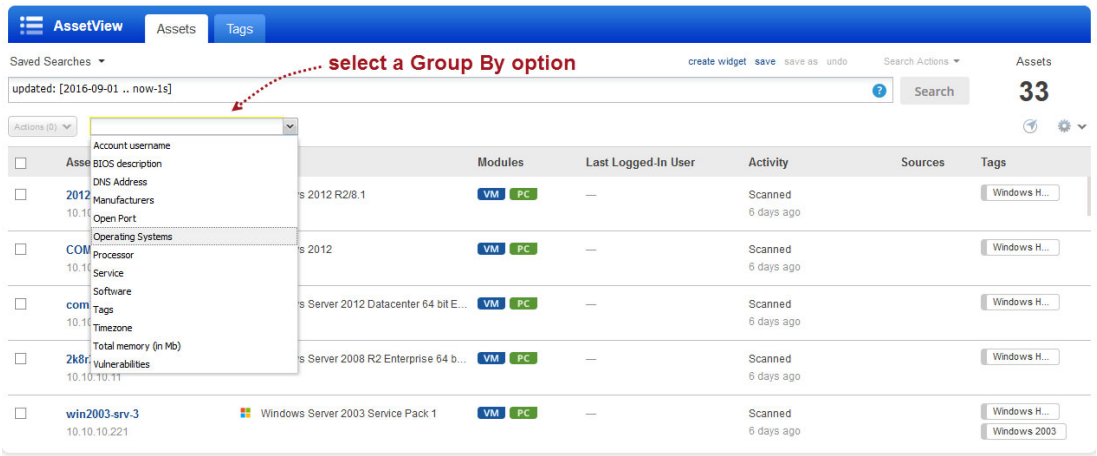
Tip:

Use your queries to create dashboard widgets on the Dashboards tab.

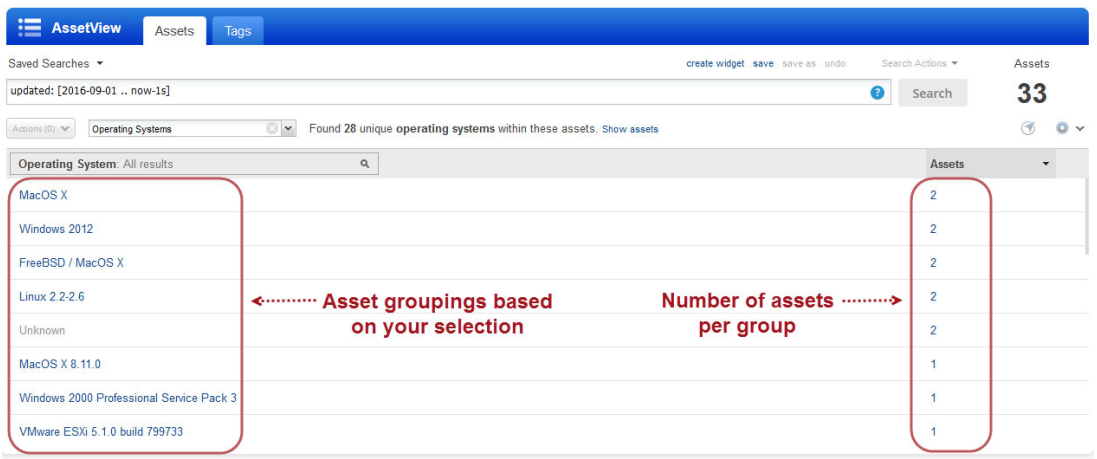
Group By Option

Once you have your asset search results you may want to organize them further into logical groupings. We offer several group by options like operating system, open port, DNS address, tags, vulnerabilities and more.

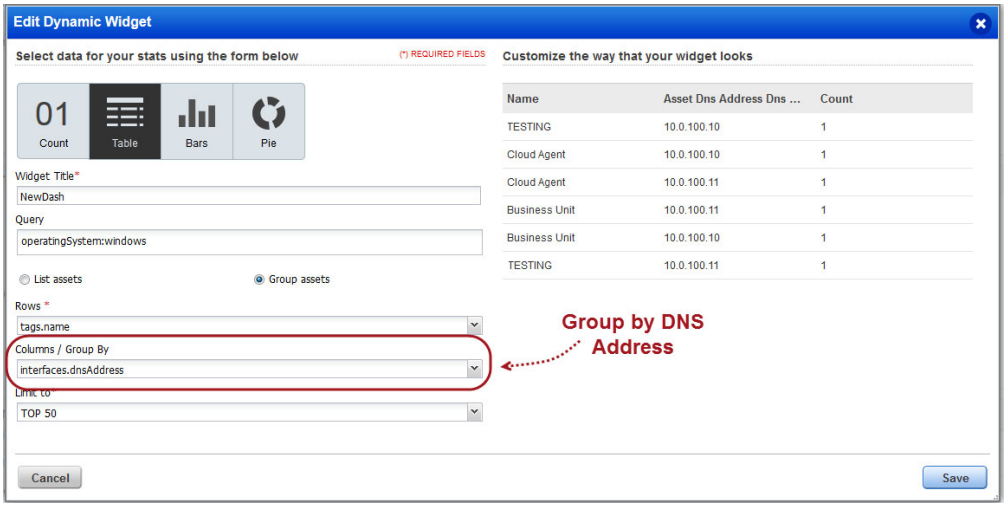
Enter an asset search query and get your asset search results. Then choose a group by option from the “Group assets by...” drop-down.



You’ll see the number of unique groupings based on your selection (e.g. 28 unique operating systems) and the number of assets per group. Click on any grouping to update the search query and view the matching assets.

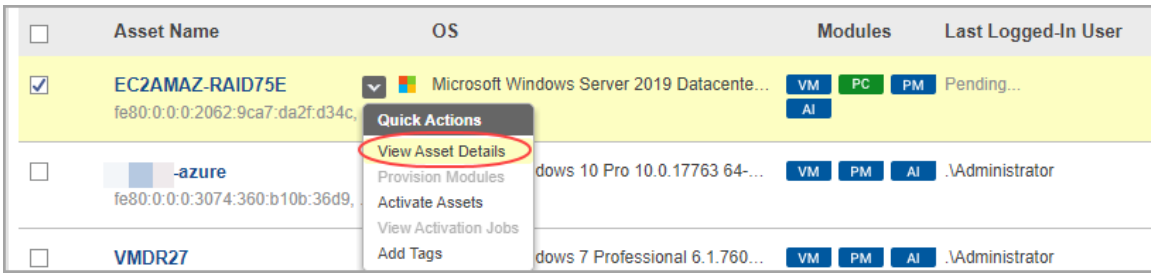


You can also use group by options in dashboard widgets. For example, this widget is grouped by DNS address.

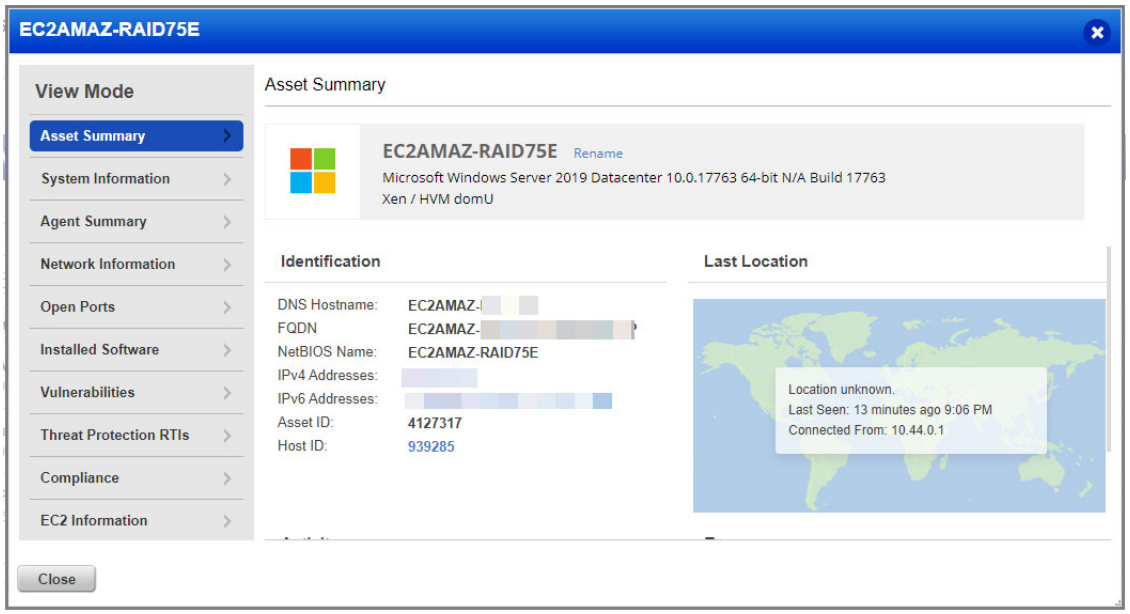


View Asset Details anytime

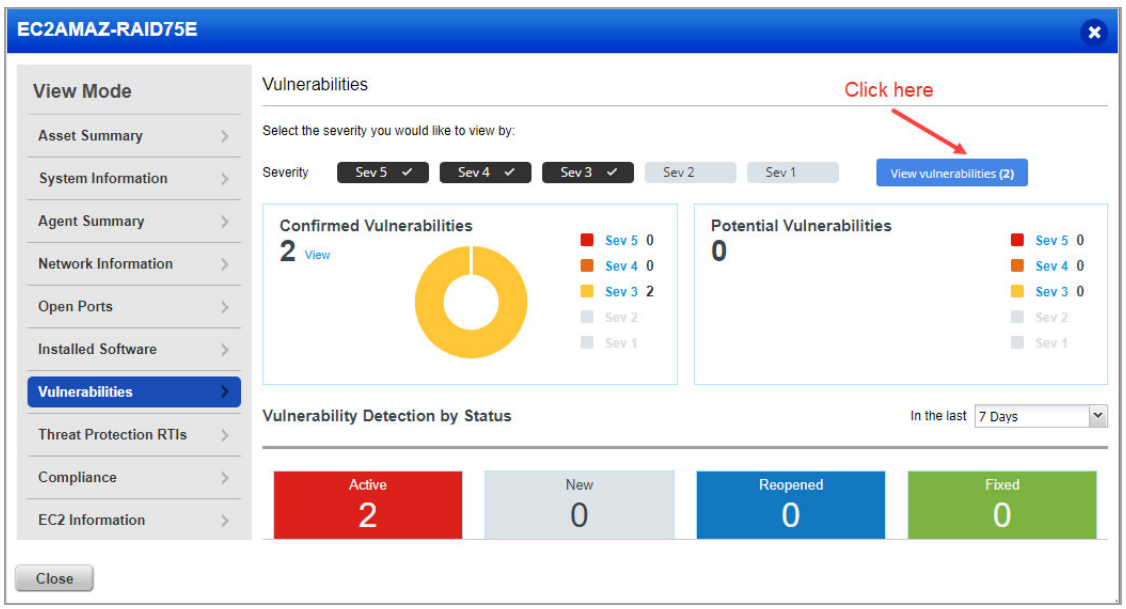
View details to get the security and compliance posture of a particular host asset. Select the asset of interest and choose View Asset Details from the menu.



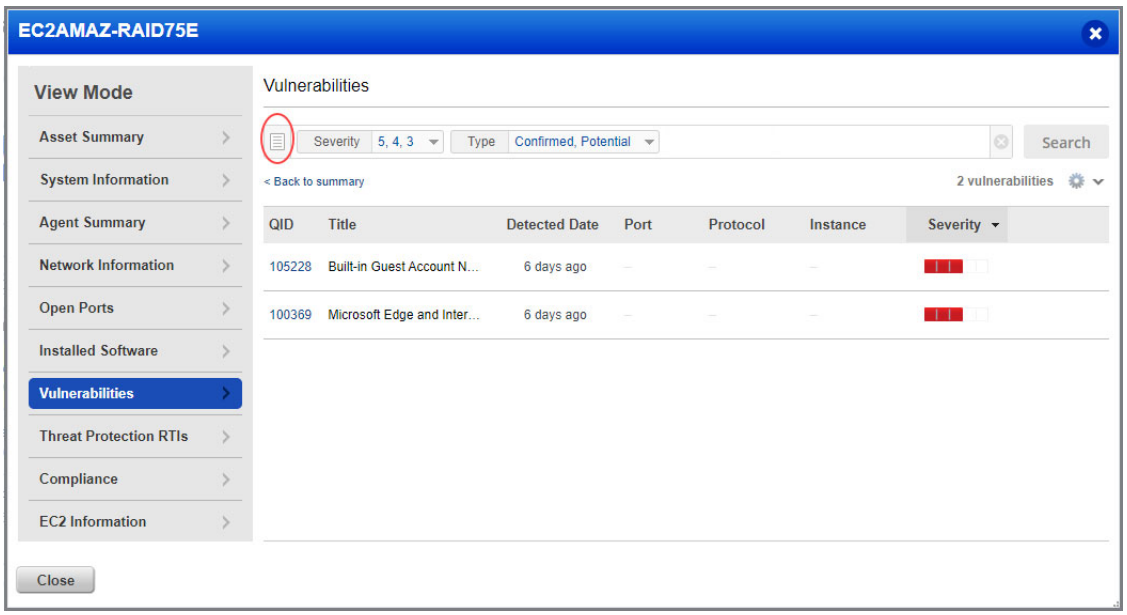
Select the sections on the left to see details on the asset.



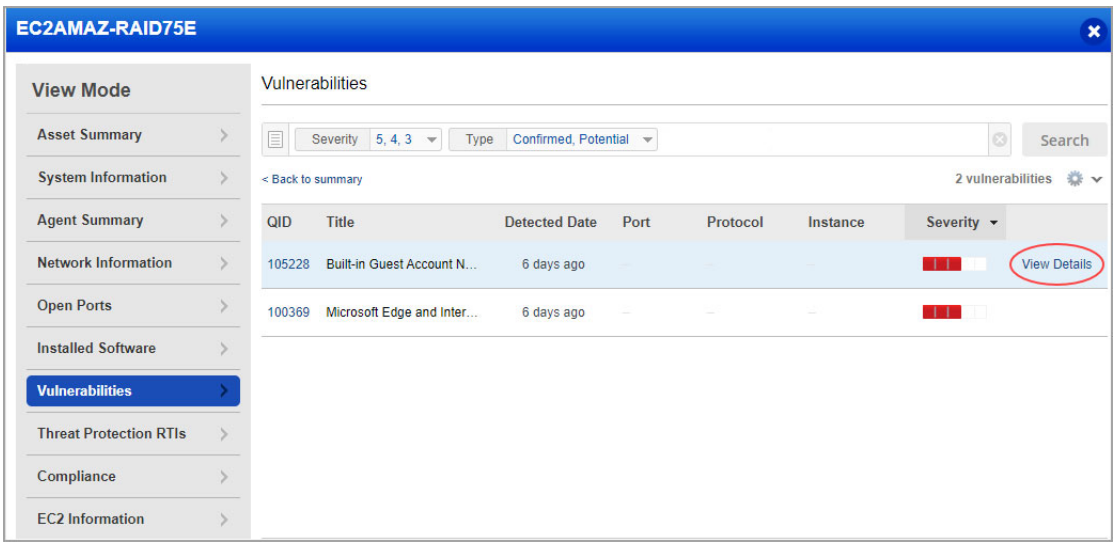
In Vulnerabilities, click View vulnerabilities to see vulnerabilities on the asset.



From here you can search vulnerabilities. Click the option to help you apply custom filters (QID, title, detected date, and more). By default all ignored vulnerabilities are listed here. Use the Ignored option to show or hide the ignored vulnerabilities.



Click View Details to see the latest detection results for any QID in the list.



View all your Policy Compliance Summary for an asset in the new Compliance tab. Here you can see the compliance policies this asset is associated with and how the policies are doing in terms of secure configuration controls on this asset. (This tab is visible only if you have the PC app enabled for the asset.)

Explore even more! You might see additional tabs depending on your subscription settings.

For example:

Threat Protection RTI - View Real-time Threat indicators (RTI) and associated vulnerabilities for the asset. (This tab appears only when the TP app is enabled for the asset.)

Alert Notifications - View alert notifications on vulnerabilities of interest for the asset based on alerting rulesets you've configured using Continuous Monitoring). (This tab appears only when the CM app is enabled for the asset.)

Find where your assets are located!

We're tracking geolocation of your assets using public IPs. Asset Geolocation is enabled by default for US based customers. For an asset that has an associated public IP, you'll see its last location on a world map in Asset Details > Asset Summary.

Want to enable (or disable) Asset Geolocation? Just contact Qualys Support or your Qualys Account Manager and we'll help you out.

How it works

- We'll check the asset's network interfaces for a public IP

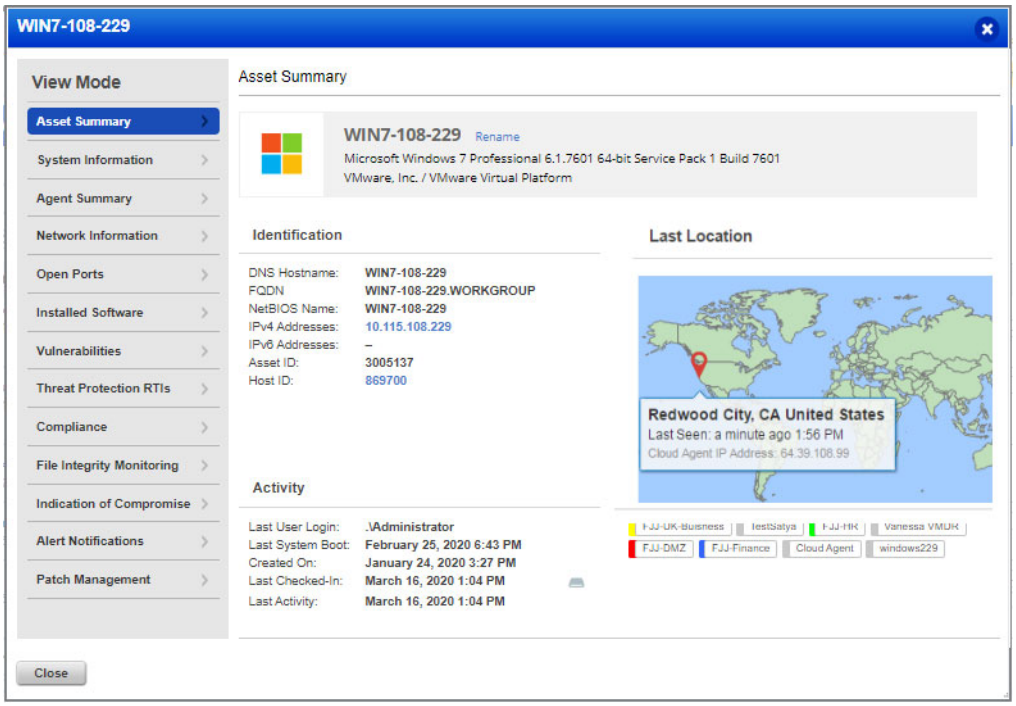
- Asset with an agent installed - we'll check the IP reported by the agent

- AWS/EC2 asset - we'll use the EC2 instance public IP

- Asset associated with a network - we'll look for the public IP associated with the scanner used

- If no public IP is found, we'll show the location as unknown.

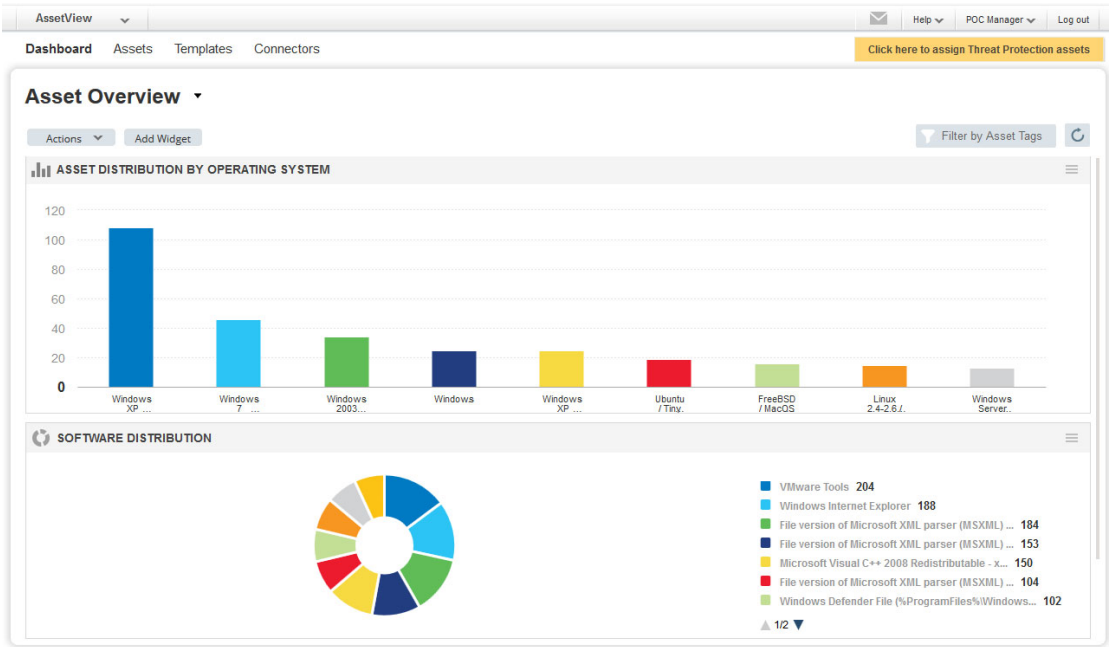
In the following example, the asset was last seen in Redwood City, CA a minute ago.



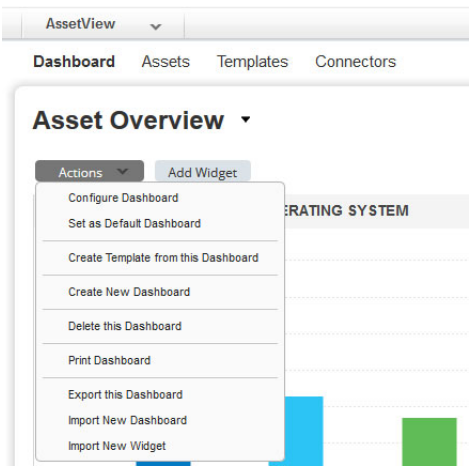
Dynamic Dashboards

Dashboards help you visualize your assets and prioritize vulnerabilities for remediation. Add widgets with search queries to see exactly what you're interested in. You can also export and import Dashboard and Widget configurations, from the Actions menu, to a file in a json format allowing you to share them between accounts or within the Qualys community.

Create multiple dashboards and switch between them for different views of your data.



Use the Actions menu to manage your dashboards.



Adding widgets

1) Start by clicking the Add Widget button on your dashboard.

2) Pick one of our widget templates - there are many to choose from - or create your own.

3) Each widget is unique. For some you'll select asset data, a query and layout - count, table, bar graph, pie chart.

4) From the Actions menu you can also import and export widget configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.

Tips:

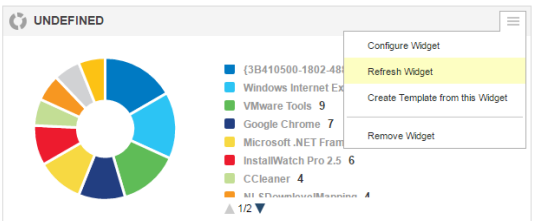
- Wondering how we created the widgets on the default dashboard? Choose Action > Configure Widget to see the settings.

- You can resize any widget vertically or horizontally, and drag & drop widgets on the page to change the layout.

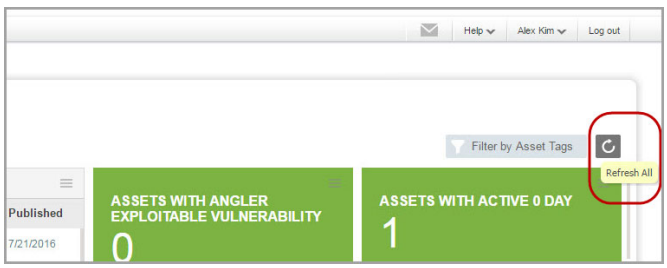
- Click on any section of a chart to see matching assets in your assets inventory.

Refresh your view

You might want to see the latest asset data for a widget. Just select the label to the right of the widget title and select Refresh Widget from the widget menu.

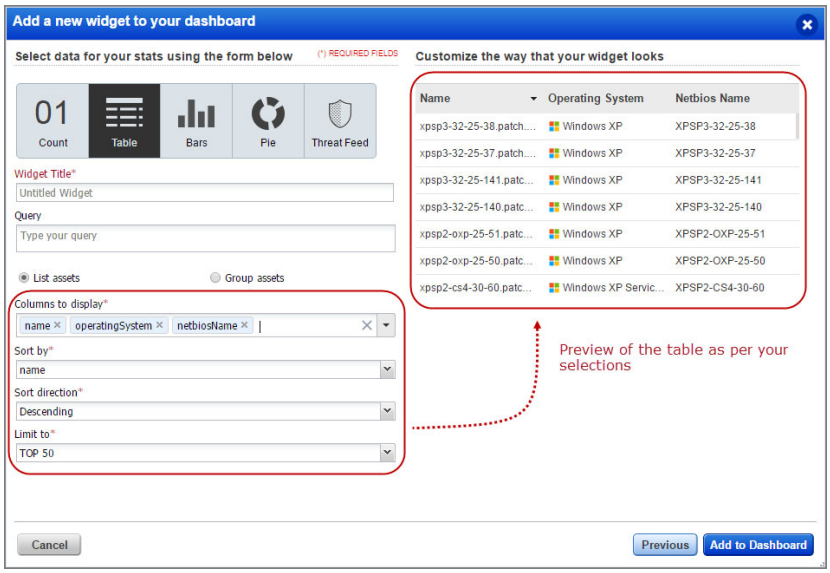


To refresh all widgets in one go, simple click Refresh All on the dashboard and all your widgets will be refreshed.



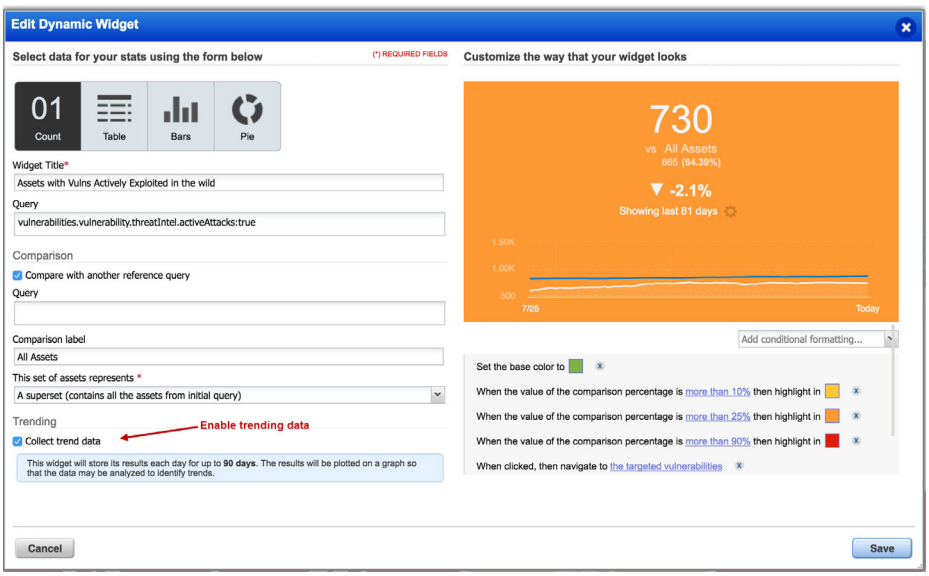
Add tables in widgets

You have multiple ways to configure a table in a widget to help you visualize your assets and their security. Create tables with multiple columns, sort by any column you like or set the sort order (ascending or descending).



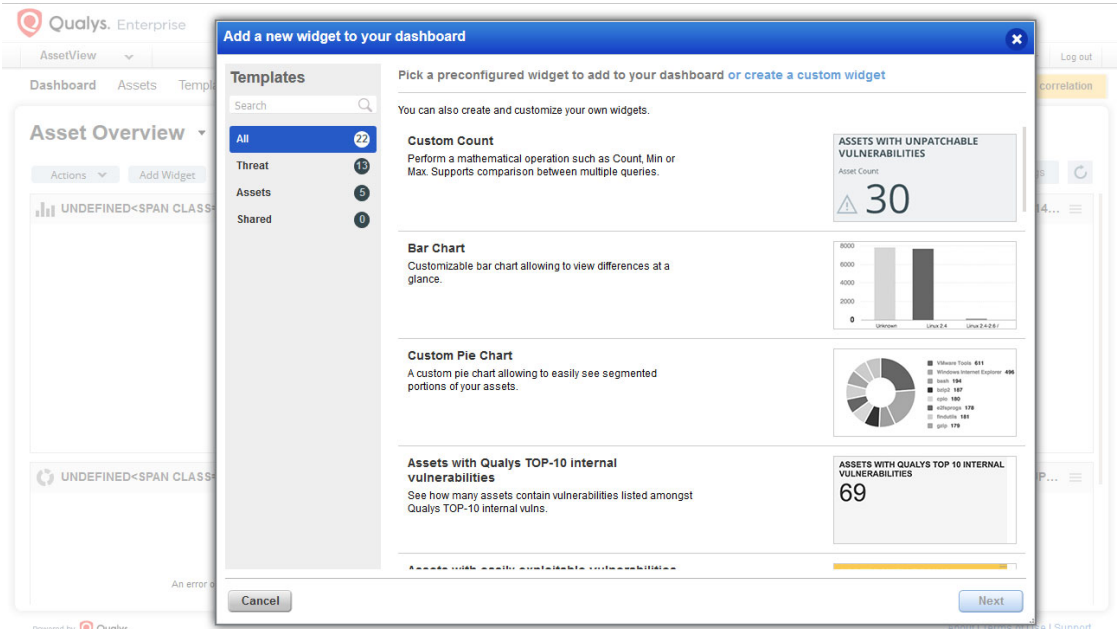
Display trend data

Configure dashboard count widgets to display trend data. Enable the Collect trend data option in the dynamic widget wizard. Once enabled, the widget trend data is collected daily and stored for up to 90 days. This is used to plot a line graph in the count widget.



About templates

When you create a new dashboard or widget the first step is to choose a template from our Library. The Library shows system-provided templates and user-created templates.



The Templates section is where you'll go to change how your templates appear in the Library. You can:

- rename templates

- update template descriptions

- remove templates from the list

Which templates can I change or remove?

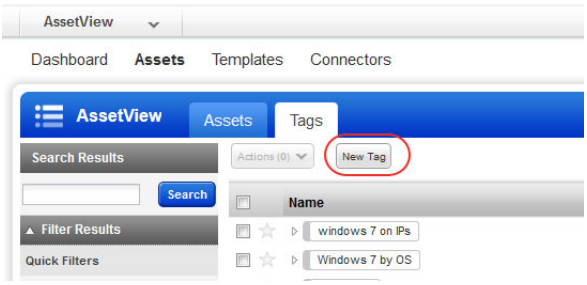
You can take actions on the templates that you created. You cannot edit or delete System templates.

Apply Tags to Your Assets

Configure tags so you can apply them to assets in your subscription. This helps you to organize your assets and to manage user access to them. You can apply tags to IP addresses and web applications.

Configure tags

1) Go to Tags and select New tag.



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

3) Set up a dynamic tag rule (optional). If there is no dynamic rule then your tag will be saved as a static tag.

When you save a tag with a dynamic tag rule, we apply it to all scanned hosts that match the rule you defined. You can filter the assets list to show only those that match your rule.

Tags we've defined for you

We create certain tags for you automatically.

Business Units

We create the Business Units tag with sub tags for the business units in your account. Assets in a business unit are automatically assigned the tag for that BU.

A sub tag can be:

- Unassigned Business Unit

- A custom business unit name, when a custom BU is defined in your account

Asset Groups

We create the tag Asset Groups with sub tags for the asset groups in your account. Assets in an asset group are automatically assigned the tag for that asset group. For example, if you have an asset group called West Coast in your account, then you'll have a tag called West Coast.

Cloud Agent

We create the Cloud Agent tag with sub tags for the cloud agents in your account. All the cloud agents are automatically assigned Cloud Agent tag by default.

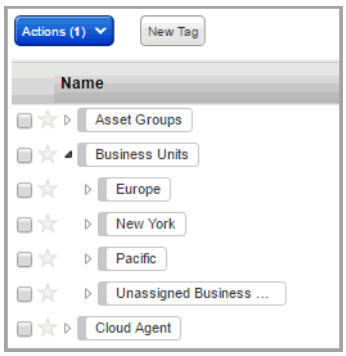
A sub tag can be:

- Location specific agents

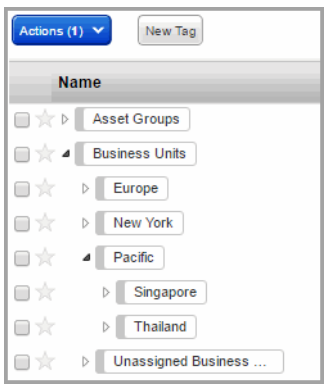
- Machine specific agents

Tell me about the tag tree

You'll see the tag tree here in AssetView (AV) and in apps in your subscription. We present your asset tags in a tree with the high level tags like the Business Units tag, Cloud Agent tag and the Asset Groups tag at the top-most level and sub-tags like those for individual business units, cloud agents and asset groups as branches.



As tags are added and assigned, this tree structure helps you manage your assets by mimicking organizational relationships within your enterprise.



A benefit of the tag tree is that you can assign any tag in the tree to a scan or report. For example, if you select Pacific as a scan target, we automatically scan the assets in your scope that are tagged Pacific and all assets in your scope that are tagged with it's sub-tags like Thailand and Singapore.

How do I find out what assets have a tag?

You'll use our advanced asset search. For example, if you want to find assets with the tag "Windows All" go to the Assets tab and enter a search query for tags.name: Windows All. Then click Search to see the results.

Tags for cloud instances

It's easy to group your cloud assets according to the cloud provider they belong to. Tags are applied to assets found by cloud agents (AWS, AZURE, GCP) and connectors.

Create dynamic tag rules to tag cloud instances based on metadata collected by your cloud connector. For each tag rule you'll provide a search query with instance information.

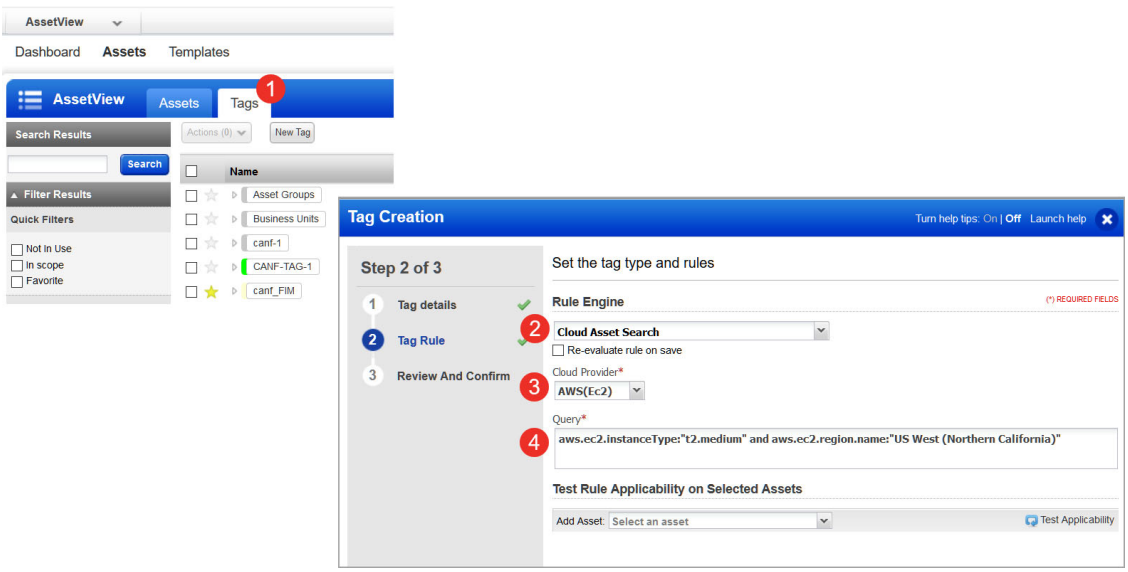
The steps:

1) Go to Assets > Tags and click New Tag.

2) Choose the Cloud Asset Search tag rule.

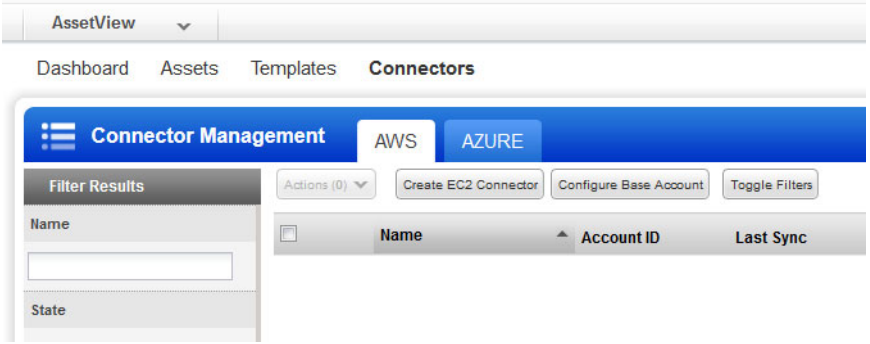
3) Choose a Cloud Provider: AWS (EC2), GCP or AZURE

4) Enter a search query in the Query field (this example is for AWS/EC2). See the online help for common search queries you can use.



Configure Connectors

Set up connectors and we'll start discovering resources that are present in your cloud account.



AWS

Configure EC2 connectors for scanning EC2 instances for security issues using the Qualys Cloud Platform. Go to the Connectors tab, select Create EC2 Connector and our wizard will walk you through the steps - set up ARN authentication, select EC2 regions and activate your EC2 assets for scanning.

Tip - We recommend you create at least one generic asset tag (for example EC2) and have the connector automatically apply that tag to all imported assets. You can add more tags to your EC2 assets based upon discovered EC2 metadata.

Watch Video Series | Download User Guide

Azure

Configure Azure connectors for scanning Microsoft Azure resources for security issues using the Qualys Cloud Platform. Go to the Connectors > Azure tab, select Create Azure Connector and our wizard will walk you through the steps.

Tip - We recommend you create at least one generic asset tag (for example Azure) and have the connector automatically apply that tag to all imported assets. You can add more tags to your Azure assets based upon discovered Azure metadata.