



Asset Management

Quick Start Guide

Dynamic Asset Tagging provides a flexible and scalable way to automatically discover and organize the assets in your environment and make them available for scanning, reporting and ticketing within Qualys. The Asset Management application allows you to easily manage your assets using dynamic asset tagging capabilities:

- Support for multiple hierarchies (by OS, region, line of business, etc.)
- Custom attributes such as location, business function, owner
- Dynamic tags automatically assigned based on any detectable attribute
- Synchronizes your scans and reports with your dynamic business environment

Requirements – The Asset Management application and Dynamic Asset Tagging **MUST** be enabled for your subscription. Please contact your Technical Account representative or Support representative for assistance. It will take 24 to 48 hours for the Qualys support team to enable this for your account.

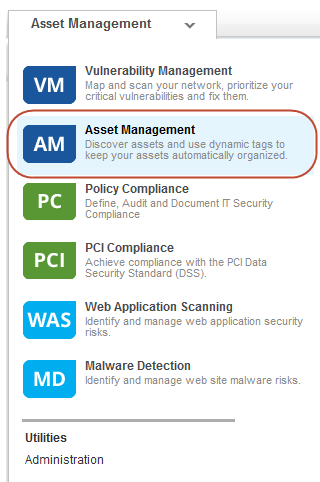
First Steps

Opt in to New Data Security Model

A user with the Manager role needs to opt in to the New Data Security Model by going to Users > Setup > Security. After opting in, users will see the Asset Management application in the application picker. (If not, Asset Management has not been added to your subscription; please contact Support or your Account Manager). Be sure to scan assets in your account so tags can be assigned to them.

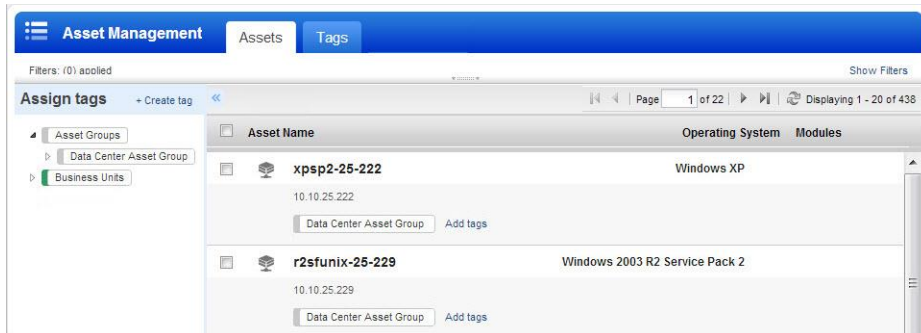
Go to Asset Management

Select the Asset Management application.



Your Assets


Click the Assets tab to view the assets in your account. Your assets list may include a combination of IP addresses, web applications and malware detection sites.



Is your assets list empty? A Manager user must opt in to the New Data Security Model. If this is not done you'll notice there aren't any IP addresses in the list. Go to VM > Users > Setup > Security to check this setting and opt in for your subscription (or ask a Manager to do it).

Are your IP addresses missing? You (or another user) needs to run scans using the VM application before your IP addresses will appear within the Asset Management application. If you have IP addresses listed under VM > Assets > Host Assets and the IPs are not listed in Asset Management, you should run vulnerability scan(s) of your hosts.

Your Tags

Click the tag tree icon  to display the "Assign tags" list, which displays all the tags currently in your subscription. To display child tags, click the triangle to the left of a parent tag.

Tags You Start With

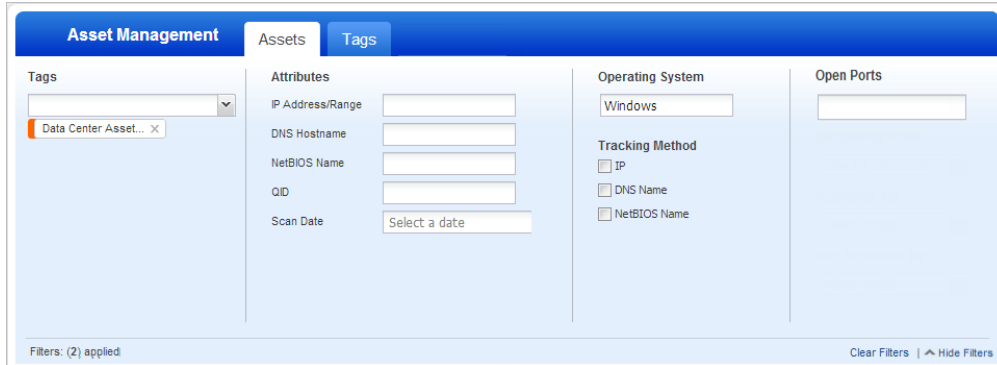
We create some initial tags based on the existing objects (configurations) in your account. The tags you start with are not assigned to assets. You can assign these tags to assets manually, and you can also edit the tags to create tagging rules for them.

Business Units. We create a Business Units tag and a sub-tag Unassigned Business Unit. For each custom business unit, we create a sub-tag with the business unit's name. For example, if your custom business units are called EU and US, you'll have a tag called Business Units, which will have sub-tags called Unassigned Business Unit, EU and US. Scanned assets in your custom business units will automatically be assigned their business unit tags.

Asset Groups. We create an Asset Groups tag and a sub-tag for each of the asset groups defined in your subscription. For example, if you have asset groups called Unix and Windows, you'll have a tag called Asset Groups, which will have sub-tags called Unix and Windows. Scanned assets in your asset groups will automatically be assigned their asset group tags.

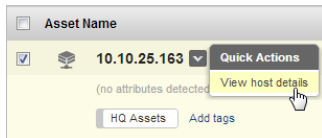
Filter Your Assets List

Click Show Filters above on the right above the assets list to display the filters. Filters represent field-level information saved in your account as part of the auto scan data (latest host scan results). Filters include tags, attributes, operating system, tracking method and open ports (multiple entries are comma separated). The assets list changes dynamically as you specify filters.

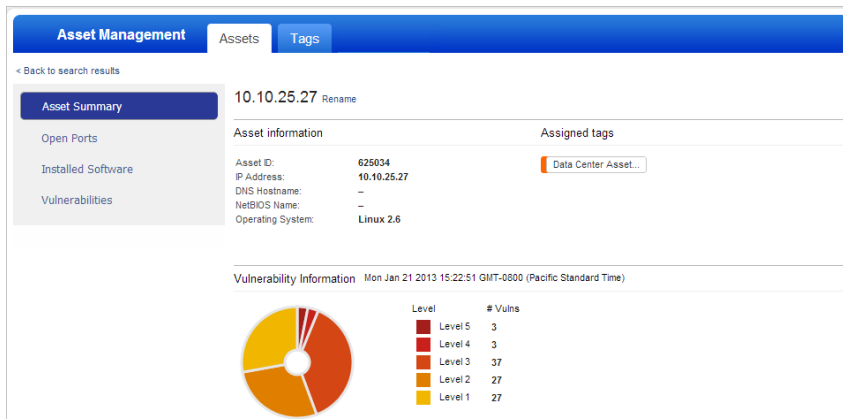


View Asset Details

Mouse over an asset row and select “View host details” from the Quick Actions menu.



Click the tabs on the left to view the host details: Asset Summary, Open Ports, Installed Software and Vulnerabilities.



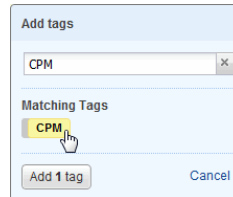
Add a Tag to an Asset

Adding tags to assets enables you to control user access to those assets. When an asset is assigned one or more tags, users with any of those tags in their assigned scopes can access that asset. You can add tags to assets manually in the assets list or automatically by defining tagging rules. Add tags manually by either of these methods:

Locate the asset you want to tag, select a tag in the tag tree and then drag and drop the tag onto the asset.

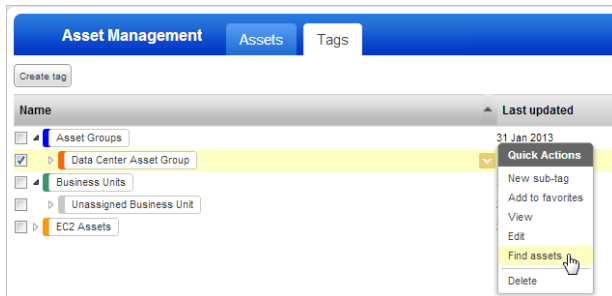


Locate the asset you want to tag and click Add tags in that asset's row. In the Add tags pop-up type a tag name in the "Search for tag" field. Matching tags appear as you type. Click the tag you want to add to the asset and then click the Add tag button.

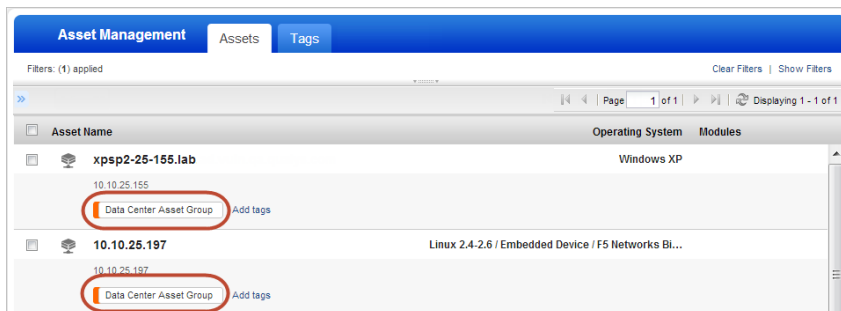


Find Assets Associated with a Tag

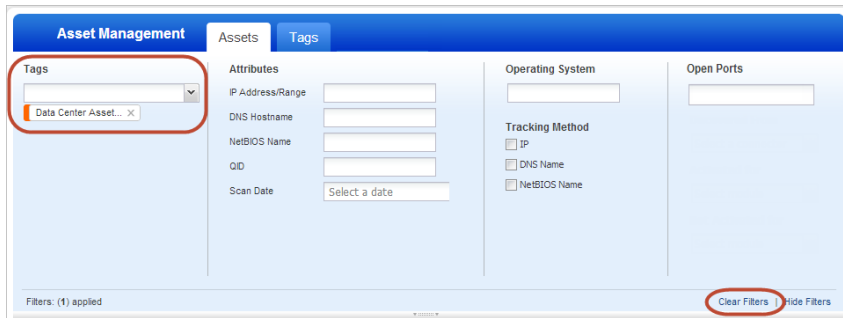
To find assets associated with a specific tag, hover over the tag on the Tags tab and select “Find assets” from the Quick Actions menu.



The assets list appears and displays only the assets with the selected tag.



If you click Show Filters above the assets list, you'll see the tags filter. Click Clear Filters to display the complete assets list.

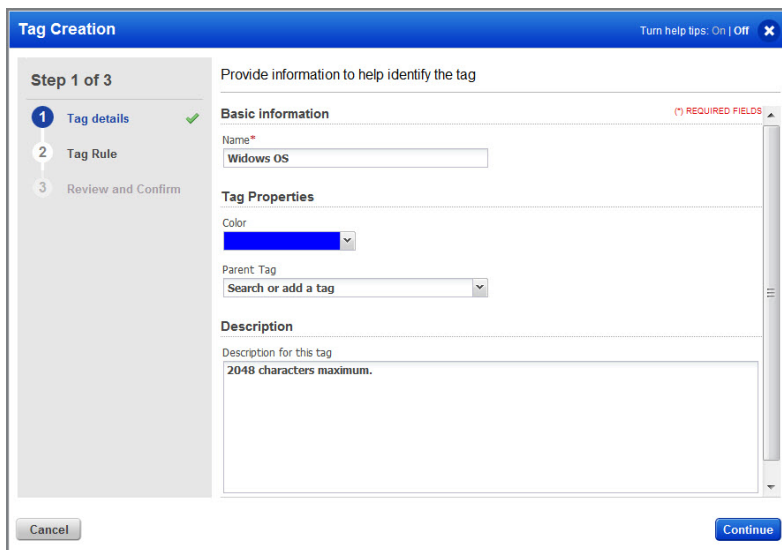


Create Tags

Click the Tags tab and then click the “Create tag” button.



The Tag Creation wizard appears. Enter a name for the tag. You have the option to select a color. Colors can be useful for grouping tags with something in common, such as an asset group or business unit. If the tag you're creating a sub-tag, select the parent tag.





Static and Dynamic Tags

Static. A static tag can be manually assigned to assets in your account. To create the tag as a static tag, just click Continue twice and then click Finish. (Static tags do not have tag rules.)

Dynamic. A dynamic tag is automatically assigned to scanned assets in your account according to its tag rule. To create the tag as a dynamic tag, click Continue and define a tag rule.

You have multiple rule engines to choose from. For example, you can define a rule for tagging hosts that have a specific operating system or a particular software application and version installed. For this example we've selected Operating System Regular Expression. In the Rule Text field, enter a regular expression (Perl format) to identify the operating system to be tagged.

Test Rule Applicability on Selected Assets. (optional) Select assets in your account to test the rule using the Add Asset drop-down menu. The result for each selected asset appears below the Add Asset drop down menu.  indicates the asset matches the rule.  indicates the asset does not match the rule.

When you click Save, we automatically add the new tag to all scanned assets in your account that match the tag rule.

Filter the Assets List. Another way to find the assets for a given tag is to use filters. On the Assets tab, click Show Filters. Under Tags, select your new tag.

The assets list is filtered to show only the assets your new tag has been added to.

More Ways to Create Tags

You can create a tag based on asset filters. Click the Assets tab and click Show Filters above the assets list to display the filtering options. Define your filters and then click Create Dynamic Tag. When prompted enter a name for the tag.

The screenshot shows a dialog box for creating a dynamic tag. It is divided into several sections: 'Tags' (with a dropdown menu showing 'No tags selected'), 'Attributes' (with input fields for IP Address/Range, DNS Hostname, NetBIOS Name, QID, and Scan Date), 'Operating System' (with a dropdown menu showing 'Windows'), and 'Open Ports' (with an empty input field). Below the 'Attributes' section, there is a 'Tracking Method' section with checkboxes for 'IP', 'DNS Name', and 'NetBIOS Name'. At the bottom of the dialog, there is a button labeled 'Create Dynamic Tag' which is circled in red. Other buttons include 'Clear Filters' and 'Hide Filters'.

Create Tags Using VM

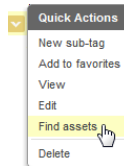
An easy way to create tags with tagging rules for automatic assignment to assets is through the Asset Search Portal in the VM application. Go to VM > Assets > Asset Search. Specify the host attributes you want to search for and then click Create Tag. When prompted enter a name for the tag and click OK.

The screenshot shows the 'Asset Search' portal in the VM application. The top navigation bar includes 'Dashboard', 'Scans', 'Reports', 'Remediation', 'Assets', 'KnowledgeBase', and 'Users'. The 'Assets' tab is selected, and the 'Asset Search' sub-tab is active. The search criteria are defined as follows: 'Asset Groups' is set to 'All', 'IPs/Ranges' is empty, and 'Include asset group titles in results' is unchecked. Under 'With the following attributes', 'DNS Hostname' and 'NetBIOS Hostname' are set to 'beginning with'. 'Tracking Method' is set to 'IP address'. 'Operating System' is set to 'matching' with 'Windows XP' selected. 'OS CPE' is set to 'beginning with'. 'Open Ports' is empty. 'Running Services' is set to 'ActiveSync'. 'QID' is set to 'with results beginning with'. 'Last Scan Date' is set to 'within' the past days. At the bottom, there are 'Search' and 'Create Tag' buttons, with the 'Create Tag' button circled in red.

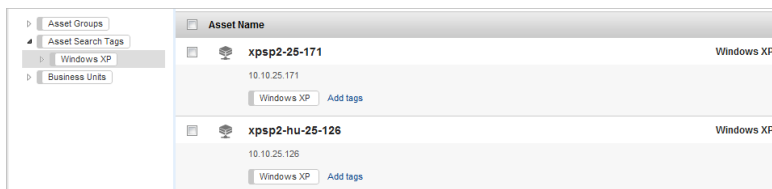
We create the tag with a tag rule based on your search criteria. Within the Asset Management application, the new tag appears in your tag tree as a sub-tag of the "Asset Search Tags" parent tag.



The new tag is automatically added to all scanned assets in your account that match your search criteria. On the Tags tab, hover over the new tag's row and select "Find assets" from the Quick Actions menu.



The assets list is filtered to display only assets that match the new tag.



Using Tags to Launch a Scan

You have the option to select tags when choosing the hosts to scans. We resolve the tags to host assets at scan time. Only hosts in your account will be scanned.

Go to VM > Scans > Scans and select New > Scan. Under "Choose Target Hosts from", select Tags and then add tags to identify hosts for the scan. Note: When "Use IP Network Range tags" is selected, only tags with IP address rule defined are shown for selection.

In the "Include hosts" section, click Add Tag to select tags. Select "All" to include hosts that match all of the tags selected. Select "Any" to include hosts that match at least one of the tags. For example, let's say you've selected tags US-West Coast, Windows XP and Port80. If you pick All, only hosts that have all three tags will be included. If you pick Any, hosts that have at least one of the tags will be included.

Add tags to the "Do not include" section. For example, you might include a tag called US-West Coast and exclude the tag California. Any host that has the California tag will be excluded from the scan even if it also has the US-West Coast tag.

Launch Vulnerability Scan Launch Help

General Information

Title:

Option Profile: * [Select](#)

Choose Target Hosts from

Assets Tags

Use IP Network Range Tags
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

Include hosts that have of the tags below. Add Tag

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

Using Tags to Schedule a Scan

Go to VM > Scans > Schedules and select New > Schedule Scan. Under Target Hosts, select Tags and then add tags to identify hosts to include in the scan and to exclude from the scan. See “Using Tags to Launch a Scan” above for information about tag selection.

New Scheduled Vulnerability Scan Launch Help

Task Title >

Target Hosts >

Scheduling >

Notifications >

Schedule Status >

Target Hosts

Assets Tags

Use IP Network Range Tags
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

Include hosts that have of the tags below. Add Tag

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

Using Tags to Run a Report

Many reports now allow asset tag selection to specify report source, including VM reports (except the Map Report) and template based PC reports. Two scorecard reports, the Most Prevalent Vulnerabilities Report and the Most Vulnerable Hosts Report, also allow asset tag selection.

Go to VM > Reports > Reports. Select New > Scan Report > Template Based. For Report Source, add tags to identify hosts to include in the report and to exclude from the report. See “Using Tags to Launch a Scan” above for information about tag selection.

The screenshot shows the 'New Scan Report' form. The 'Report Details' section includes fields for Title (My Scan Report), Report Template (High Severity Report), and Report Format (HTML pages). The 'Report Source' section has fields for Asset Groups (All) and IP/Ranges. Below these, the 'Asset Tags' section is highlighted with a red box. It shows 'Include hosts that have All of the tags below' with tags 'Asset Group 25' and 'Windows XP' selected. Below that, 'Do not include hosts that have Any of the tags below' with tags 'Southwest US' and 'Corporate Office' selected. The 'Report Options' section has a 'Scheduling' checkbox. At the bottom are 'Run' and 'Cancel' buttons.

The Summary section of the finished report displays the names of the tags used to specify the report source.

The screenshot shows the 'Report Summary' section. It lists Report Template (High Severity Report), Asset Groups (All), and IP. The 'Tags' section is highlighted with a red box, showing 'Included (all): Windows XP, Asset Group 25' and 'Excluded (any): Corporate Office, Southwest US'. Other summary items include Sort by (Host), Trend Analysis (Latest report), Date Range (N/A), Active Hosts (419), and Hosts Matching Filters (389).