



Qualys Cloud Suite 2.17

We're excited to tell you about new features and improvements coming with Qualys Cloud Suite Update 2.17.



AssetView



ThreatPROTECT

Find where your assets are located!
Form powerful queries using IN clause
Easily find agent manifest version



Cloud Agent

Find where your agent assets are located!
Improvements to Configuration Profiles
Bulk Action on Cloud Agents: Activate, Deactivate or Uninstall
Enhanced Cloud Agent Search Options
Azure Cloud Agent is now part of Install Agent for Windows UI



Continuous Monitoring

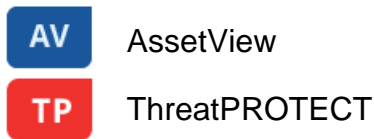
Get Alerts for Active Ports



Malware Detection Service

Improved Time Zone List for Malware Monitoring

Qualys Cloud Suite Update 2.17 brings you many more
Improvements and updates! [Learn more](#)



Find where your assets are located!

We're now tracking geolocation of your assets using public IPs. *Asset Geolocation is enabled by default for US based customers within AV, TP and CA.* For an asset that has an associated public IP, you'll see its last location on a world map in Asset Details > Asset Summary. This asset was last seen in Redwood City, CA a minute ago.

100047-T430

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Alert Notifications

Asset Summary

Identification

DNS Hostname: 100047-T430

IPv4 Addresses: 10.100.14.143

IPv6 Addresses: fe80:0:0:4992:e30a:371:2c5b

Asset ID: 93023

Host ID: 21008

Activity

Last User Login: CORP\...

Last System Boot: 11 hours ago 2:19 AM

Created On: February 24, 2016 4:07 PM

Last Checked-In: less than a minute ago 1:56 PM

Tags

Unassigned Business Unit Business Units

Desktop OS Cloud Agent

Last Location

Redwood City, CA United States

Last Seen: a minute ago 1:56 PM

Cloud Agent IP Address: 64.39.108.99

How it works

- We'll check the asset's network interfaces for a public IP
- Asset that has 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 will look for a public IP associated with the scanner used

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

Last Location



Learn more

Want to enable (or disable) Asset Geolocation? Sure no problem. Just contact Qualys Support or your Qualys Account Manager and we'll help you out.

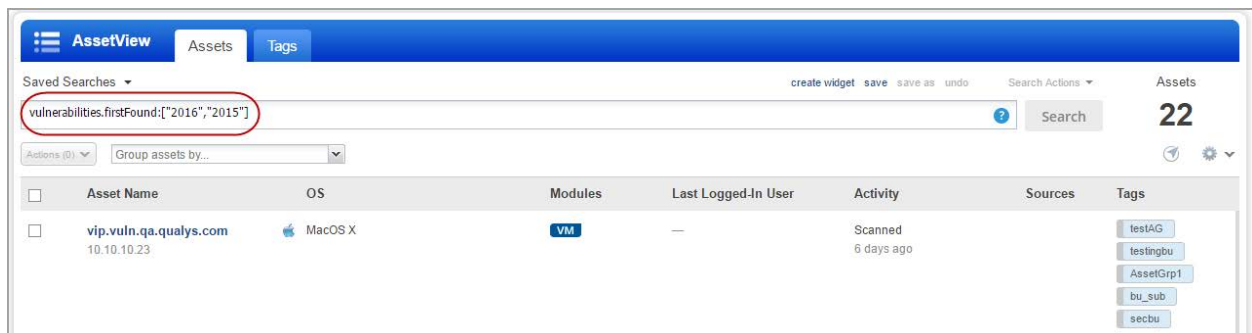
Form powerful queries using IN clause

You can now form your queries using IN and Not IN clause using AssetView and ThreatPROTECT. This search option is available for all fields with fixed values (numeric, date, fixed string).

For example you want to find assets on which the vulnerabilities were first found in the years 2016 and 2015.

Query formed:

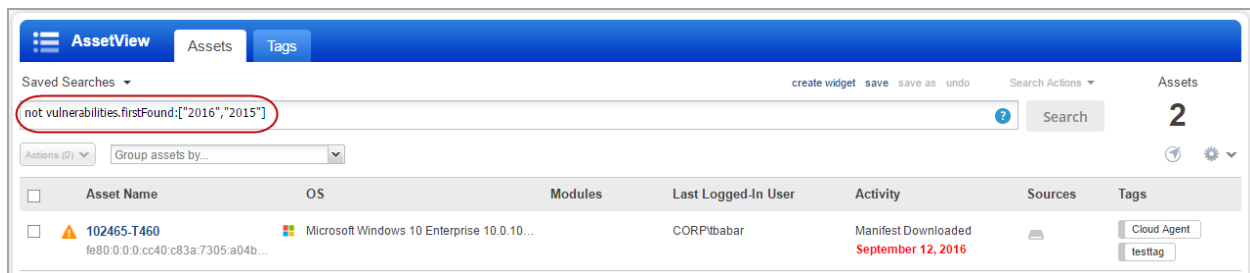
`vulnerabilities.firstFound:["2016","2015"]`



In case of Not In scenario add "not" before the query.

Query syntax:

`not vulnerabilities.firstFound:["2016","2015"]`

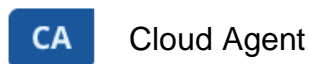


Supported date formats:

YYYY example: vulnerabilities.firstFound:["2016","2015"] //in 2016 or 2015

YYYY-MM example: vulnerabilities.firstFound:["2016-08","2015-07"] // in Aug or Sept

YYYY-MM-DD example: vulnerabilities.firstFound:["2016-08-31","2016-08-30"] // one of these dates



Cloud Agent

Find where your agent assets are located!

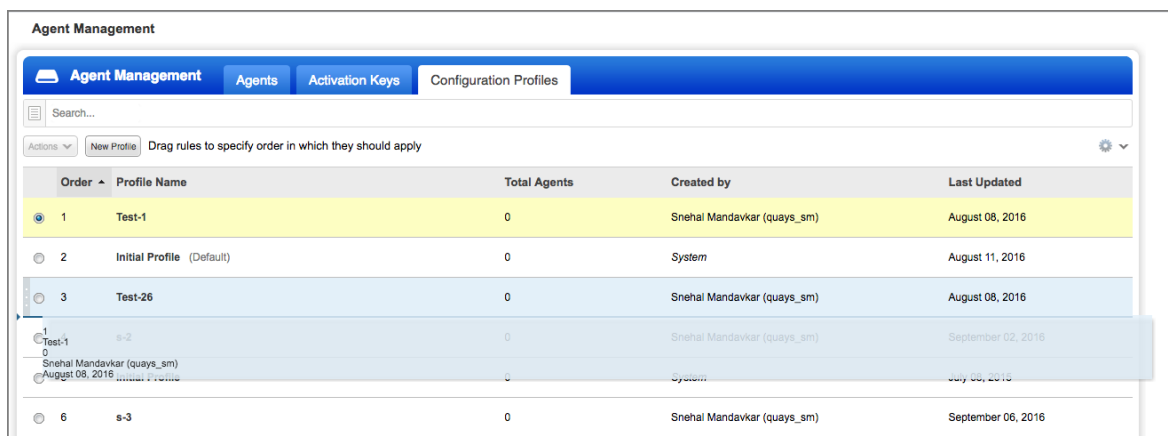
We're now tracking geolocation of your agent assets. [Learn more](#)

Improvements to Configuration Profiles

This release includes many improvements related to configuration profiles like how profiles are prioritized and assigned to agent hosts, a simplified workflow for customizing performance settings and the option to delete profiles.

Reorder profiles to set priority

You may have multiple configuration profiles that match a single agent host. When this is the case we'll apply profiles based on the order in which they are listed. The profile at the top of the list has the highest priority and is applied first. Move a rule up in the list (drag and drop the row) to increase its priority or move it down to decrease its priority.

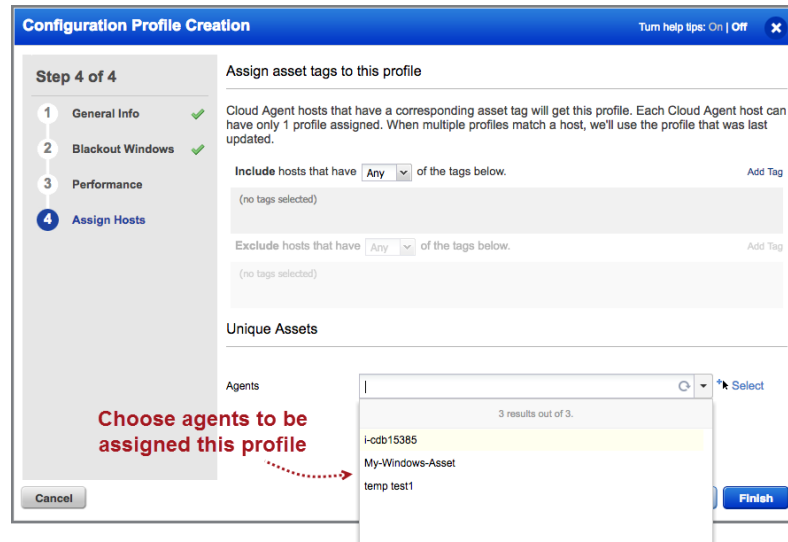


Directly assign a profile to an agent host

To ensure that an agent host always uses a certain profile you can assign it directly. This assignment will take precedence over the order in the profiles list. Each agent host can have one profile assigned. There are a few methods for doing this, as described below.

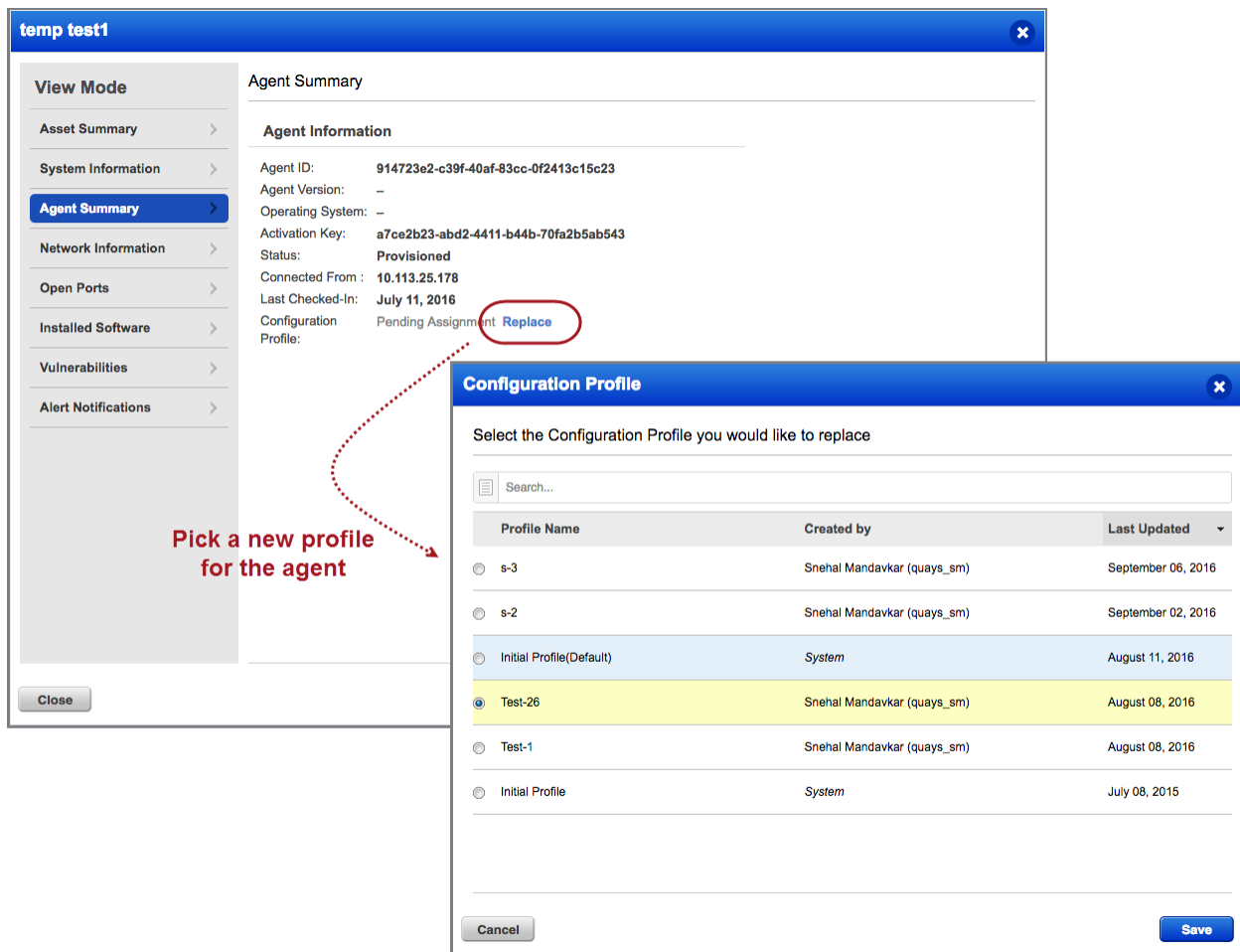
From the configuration profile

Go to the Assign Hosts section and choose one or more agent hosts. Each host you pick will be assigned the profile.



From the agent host

Go to your agents list and choose View Asset Details for any agent host. Then go to the Agent Summary section to see the profile assigned to the agent. Click Replace to change the profile. The profile will be updated at the next configuration download interval.



Why do I see “Pending Assignment”?

Any time you change the profile assignment for an agent host (from the configuration profile or agent summary) you'll see Pending Assignment until the change is downloaded to the agent. How long this takes is based on the Configuration Download Interval setting in the configuration profile (under performance settings). We recommend you set this to 1 hour (3600 seconds).

Customize performance settings in 3 easy steps

It's easier than ever to customize performance settings. In the Performance section of your configuration profile: (1) Click Customize, (2) Choose a default level (Low, Normal, High) to start with, and (3) edit the individual settings. Your custom settings will be saved with the profile.

Configuration Profile Creation Turn help tips: On | Off X

Step 3 of 4

- 1 General Info ✓
- 2 Blackout Windows ✓
- 3 Performance ✓
- 4 Assign Hosts

Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization. These are saved as performance profiles.

Performance
Select one of the performance profiles below, or set your custom

Customize ☒

Configure the various performance parameters for agents

Based On: Low

Set Parameters

- Delta Upload Interval***
Interval an agent attempts to upload detected changes
120 sec(60 or more)
- Delta Confirmation Interval***
Interval an agent checks platform for confirmation that changes were processed
300 sec(60 or more)
- Manifest Download Interval***
Interval an agent checks platform for new instruction manifests
43200 sec(60 or more)
- Configuration Download Interval***
Interval an agent checks platform for new configuration profiles
7200 sec(60 or more)
- Provisioning Interval***
300 sec(60 or more)

Cancel Previous Continue

Delete a configuration profile

You can delete any configuration profile in the list as long it's not directly assigned to an agent. Select the profile you want to delete and choose Delete from the Actions menu. If the Delete action is disabled, then you must first assign a new profile to the agent.

Agent Management

Agent Management Agents Activation Keys Configuration Profiles

Search...

Actions View Edit Delete

Drag rules to specify order in which they should apply

	Profile Name	Total Agents	Created by	Last Updated
1	Initial Profile (Default)	0	Snehal Mandavkar (quays_sm)	August 08, 2016
2	Test-26	0	System	August 11, 2016
3	s-2	0	Snehal Mandavkar (quays_sm)	August 08, 2016
4		0	Snehal Mandavkar (quays_sm)	September 02, 2016

Bulk Action on Cloud Agents: Activate, Deactivate or Uninstall

We now provide a new option to perform bulk action (activate, deactivate or uninstall) only on the cloud agents that match your search query.

For example, to activate all cloud agents that belong to a specific version, specify the version number in the search criteria. Then choose Activate Agents from the Bulk Actions menu. Want to deactivate agents or uninstall them? You can take those actions too.

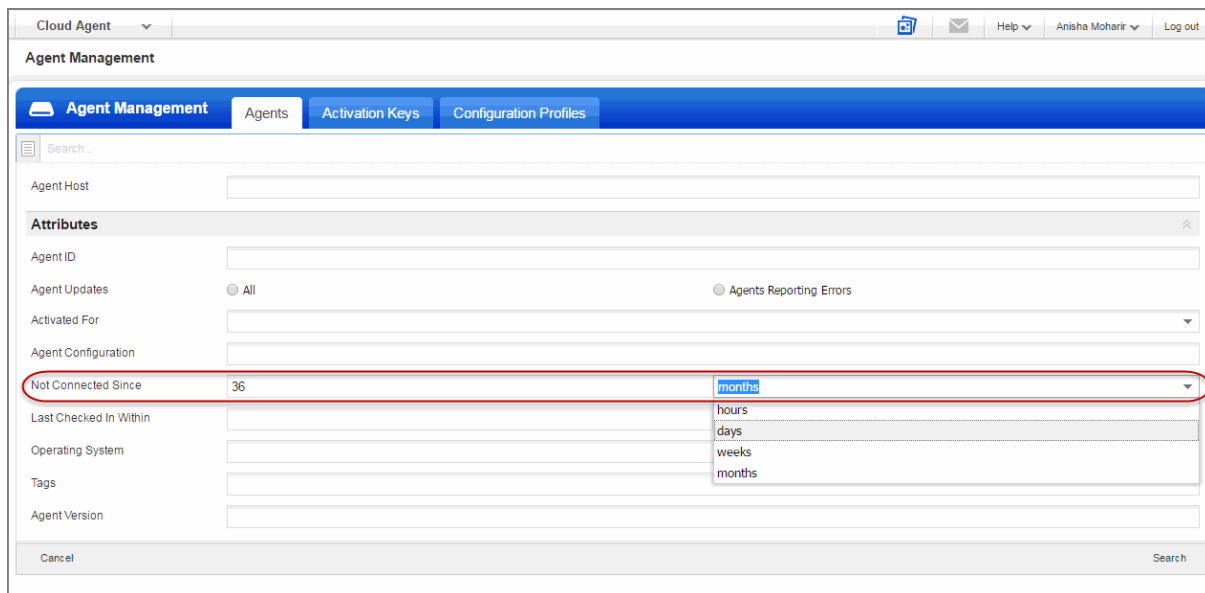
The screenshot displays the 'Agent Management' interface. At the top, there's a navigation bar with 'Agents', 'Activation Keys', and 'Configuration Profiles'. Below this, a search bar shows 'Agent Version' with the value '1.5.0.62'. A red arrow points to this search bar with the text 'Specify the Cloud Agent search criteria'. The main content area shows 'Total Agents' as 5, with a breakdown of VM Agents (0/1,001) and PC Agents (1/1,001). To the right, a donut chart titled 'Top 4 Operating Systems' shows the distribution: CentOS 6.5 (1), Microsoft Windows 7 Professional 6.1.7601 Ser... (1), Mac OS X 10.11.2 (1), and CentOS 5.4 (1). Below the chart, a table lists agents. A red box highlights the 'Bulk Actions(3)' dropdown menu, which contains 'Activate Agents', 'Deactivate Agents', and 'Uninstall Agents'. A red arrow points to this menu with the text 'Click to perform bulk action on all Cloud Agents in the search result'. The table has columns for Agent Host, Version, Status/Last Checked-in, Configuration, Agent Modules, and Tags. The first three agents listed are 'localhost.localdomain', 'AmoC-Mac', and 'localhost.localdomain', all with version '1.5.0.62'.

Agent Host	Version	Status/Last Checked-in	Configuration	Agent Modules	Tags
localhost.localdomain	1.5.0.62	Inventory Scan Complete a minute ago	RC 2.17	No modules activated	CA Test Cloud Agent
AmoC-Mac	1.5.0.62	Inventory Scan Complete 2 minutes ago	RC 2.17	No modules activated	CA Test Cloud Agent
localhost.localdomain	1.5.0.62	Inventory Scan Complete 17 minutes ago	RC 2.17	No modules activated	CA Test Cloud Agent

Enhanced Cloud Agent Search Options

We now provide a new option Not Connected Since to search for agents that have been inactive for a specific period of time. You can select the inactivity period in terms of hours, days, weeks or months.

For example, if you want to uninstall agents that are inactive since last three years, specify 36 months in the Not Connected Since field. All the cloud agents that are inactive for the last three years will be listed. You can then perform a bulk action for uninstallation of such inactive agents.

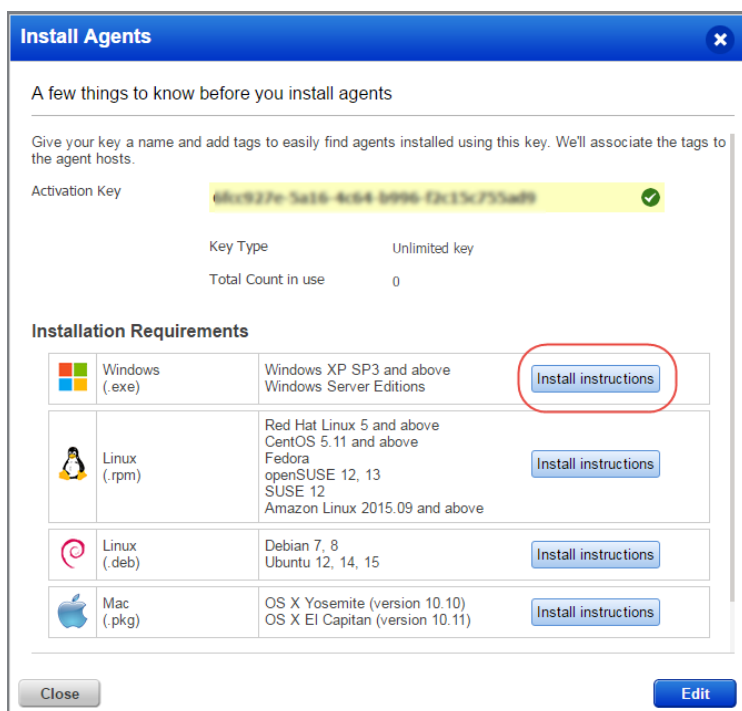


The screenshot displays the 'Agent Management' interface. At the top, there's a navigation bar with 'Agent Management', 'Agents', 'Activation Keys', and 'Configuration Profiles'. Below this is a search bar and a list of search filters. The 'Not Connected Since' filter is highlighted with a red circle, and its dropdown menu is open, showing options for 'hours', 'days', 'weeks', and 'months'. The '36' value is entered in the adjacent text field. Other filters include 'Agent Host', 'Agent ID', 'Agent Updates' (with radio buttons for 'All' and 'Agents Reporting Errors'), 'Activated For', 'Agent Configuration', 'Last Checked In Within', 'Operating System', 'Tags', and 'Agent Version'. A 'Cancel' button is on the left and a 'Search' button is on the right of the filter section.

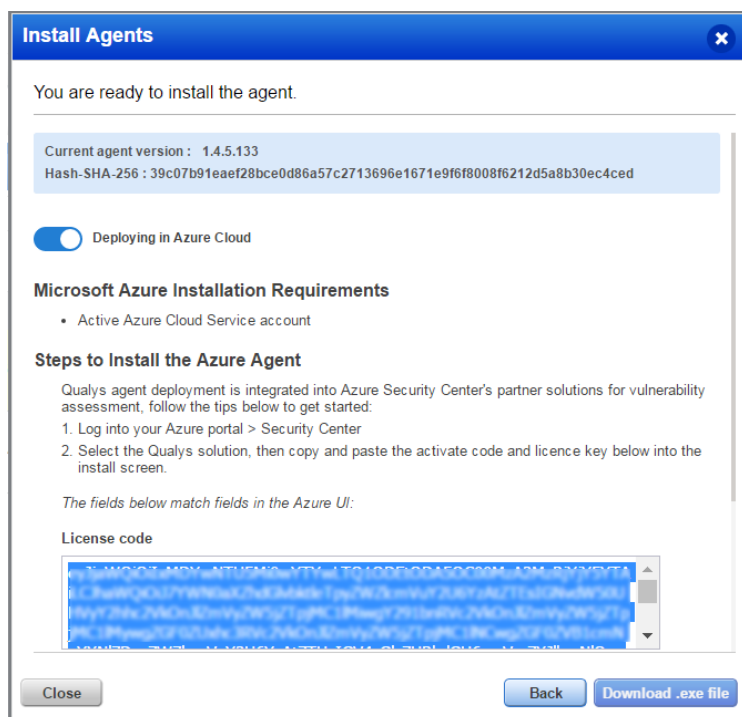
Similarly, you can now search for agents related to their checked-in status. You can specify the checked in time in terms of hours, days, weeks or months.

Azure Cloud Agent is now part of Install Agent for Windows UI

To install the Azure Cloud Agent, click “Install instructions” for Windows.



Just select new option “Deploying in Azure Cloud” and we’ll show you the steps to install the Azure Agent.

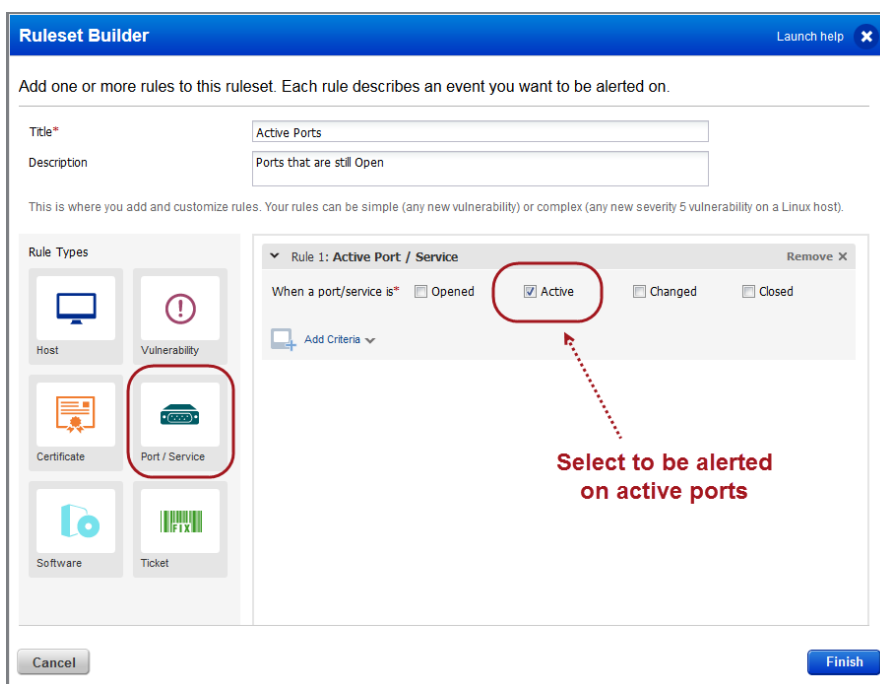


Get Alerts for Active Ports

You can now get alerts in CM for active ports discovered by your vulnerability scans. An active port is one that was previously reported as open and is still open.

Don't see the Active check box?

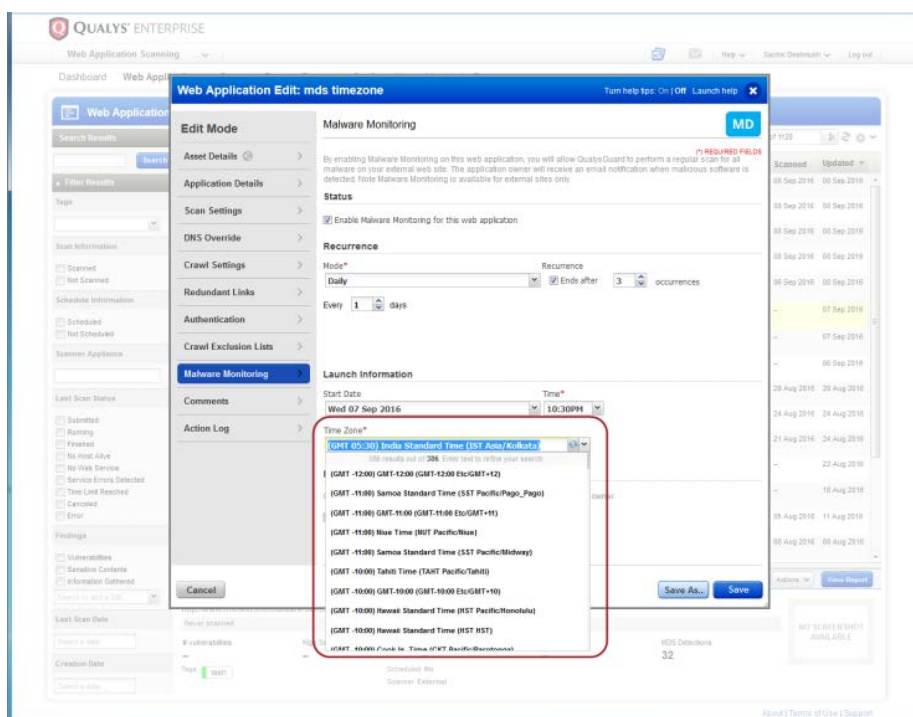
This feature must be enabled for your subscription. Contact Support or your Technical Account Manager to get it.



Improved Time Zone List for Malware Monitoring

You'll now have an easier time configuring the start time for malware scans on your web applications. We'll list all the time zones that match your search and we've removed redundant entries.

How do I set up malware monitoring? Choose the WAS application from the module picker. Edit your web application and select Enable Malware Monitoring for the web application. Configure scan settings including the start date and time.



Issues Addressed



- Fixed an issue where query "lastLoggedOnUser: <CORP>\<username>" failed to match a valid username of last logged on user.
- Fixed an issue with this query returning unexpected results: not activatedForModules: pc
The following query now returns assets not activated for PC only when the token value is PC (capital letters) like this: not activatedForModules: PC and it also pre-populates the search values.
- Fixed issue with searching for vulnerabilities with compliance type CobIT. This query returns results as expected (vulnerabilities.vulnerability.compliance.type: CobIT) and pre-populates the search values.
- Fixed issue with searching for vulnerabilities with CVSS Access Vector "LOCAL ACCESS". This query returns results as expected (vulnerabilities.vulnerability.cvssInfo.accessVector: "LOCAL ACCESS") and pre-populates the search values.
- UI update - Now we enforce that dashboard and widget template titles must be unique.
- Fixed issue with unprovision then reprovision workflow for a web application asset using the Provision Modules option. This workflow no longer reports an error.
- UI improvements to the Dashboard & Widget Template screens. "Template" text now uses the plural "Templates", and "Created Date" now appears as "Last Updated".
- Fixed issues related to queries returning no results using various tokens including agentId, agentVersion, lastCheckedIn, lastInventory.
- When selecting tags under Assets > Tags, the Actions button will now remain disabled and user can't click on it until tags are selected.
- Improvements to the Tags column auto expand on the Assets page to help users scroll through and visually look through assets.
- Fixed an issue with background color in Asset Details under Vulnerabilities Detection by Status when language is set to Japanese.
- Fixed an issue related to asset download for a service type query. Specifically the asset count downloaded did not match the asset count shown in the UI.
- Fixed an issue where the user could not view their AssetView dashboard after navigating to the Dashboard tab.
- ThreatPROTECT: When you enter a query on the Feeds page the Save button is now enabled so you can save your query.

- ThreatPROTECT: Added year to ThreatPROTECT feed articles.
- ThreatPROTECT: Fixed an issue with search for vulnerabilities at risk to exploit kit threat. Now this query returns expected results: `vulnerabilities.vulnerability.threatIntel.exploitKit: true`
- Search performance improvements and fixed issues related to query timing out.
- Asset data is indexed for vulnerabilities found only. We've removed the following field from the search list and it's no longer possible to search using it: `vulnerabilities.found`
- Corrected the quick tips for search token `interfaces.address` to show IPv6 address needs to be enclosed in single quotes like this: `interfaces.address: 'fe80:0:0:0:2501:b53c:4139:404b'`

CA

- Fixed issue with missing icon for some OSes in View Asset Details > Agent Summary tab.
- Now you can filter agents that are activated for both the VM and PC modules using the new Activated for: VM/PC option on the Agents page.
- View Key Info now shows license information for the selected activation key.
- Fixed an issue where user's account is in Japanese and an error was returned when the user downloaded an agent. Now an error message is not returned.
- Fixed an issue preventing users from saving a configuration profile with custom performance settings.
- Configuration Profile update - New filters in Assign Hosts > Agents page allow users to filter agents by agent version and agent ID.
- Fixed an issue on Agents page pie chart where the graph and legend counts did not match. Now when the user hovers over an OS in the pie chart, the count in the tooltip matches the count in the legend. A similar issue was fixed for the pie chart on the Configuration page.
- Agent last checked-in date is now updated when the portal processes scan results.
- UI update to the Replace option in View Asset Details > Agent Summary > Configuration Profile. The Replace action is now disabled until the profile status is pending assignment.
- Fixed an issue preventing users from filtering agents by hostname with capital letters on Agents page. Now users can filter hostname with mixed case letter or all upper case letters.
- Fixed an issue preventing users from downloading the cloud agent installer when the user's language is set to Japanese.
- Fixed an issue with agent activation when OS name of the machine contains non-ascii characters.

- Updated Cloud Agents documentation to describe installation path using Mac Agent 1.5 and later: /Applications/QualysCloudAgent.app. Documentation updated: Cloud Agent online help, Cloud Agent Getting Started Guide, Cloud Agent for Mac Installation Guide.
- New Revocation Interval setting added to the configuration profile - the interval an agent checks the platform to see if it should uninstall itself. The minimum interval is 3600 seconds (the default) and the user can set this to a greater value.
- Fixed some issues with internationalization in CA module, specifically for Japanese language support.

MD

- Fixed an issue where sometimes users were not able to access data for MD even though the module was enabled for their account. Now users can access this by taking these steps: select MD from the module picker, then on the Welcome page click the Get Started button.

SAQ

- Assignee can now see all Closed questionnaires in their data list.
- We've added 2 new templates for IT framework: 1) IT Service Delivery Assessment, and 2) IT Service Management Assessment.
- Due Date and Last Update dates are now shown only once in the respective columns of the My Campaign widget, either as actual date or as number of days or hours.
- We've added a new template for SANS/CIS Top 20 Critical controls and sub-controls.
- Only SAQ reports are now displayed under the Reports tab of the SAQ module.
- While creating a Single Instance Report, the search is now working properly to select accurate Questionnaires as per the provided search criteria.
- You can now import users using CSV file, even if the file contains extra spaces and/or lines.
- Reviewers can now approve a questionnaire and submit to its originator using the Submit button in the questionnaire UI.
- The Reassign menu option is no longer visible to these users: Responder, Reviewer and Approver.
- Trial page - fixed typo in the word Assessment.



- Improved functionality where scan results found for "Time Limit Reached" scan were not consolidated in Web Application report. Now these scan results are consolidated and included in Web application report. The Detections page (Web Applications > Detections) now contains the updated last scan date and web application.
- Fixed an issue where a scan did not launch and the web page became non-responsive if the user completed the new scan workflow and closed the WAS Scan Launch window.
- Fixed an issue where NTLM record details were removed when the record was added to a Web Application.
- Improved UI description to help users with defining exclusions lists, on Configuration > Global Settings page and Web Application wizard Crawl Exclusions tab.
- Improved visibility of UI elements within Advanced Search criteria for static search list. This is shown when the user navigates to Configuration > Search List > Static Search List and clicks the Advanced Search button.

Administration

- A lock icon will appear next to user roles that are Read Only. These roles cannot be modified.