QUALYS®

Qualys Cloud Suite 2.17

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

AV AssetView

TP ThreatPROTECT

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

CA 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

CM Continuous Monitoring

Get Alerts for Active Ports

MD Malware Detection Service

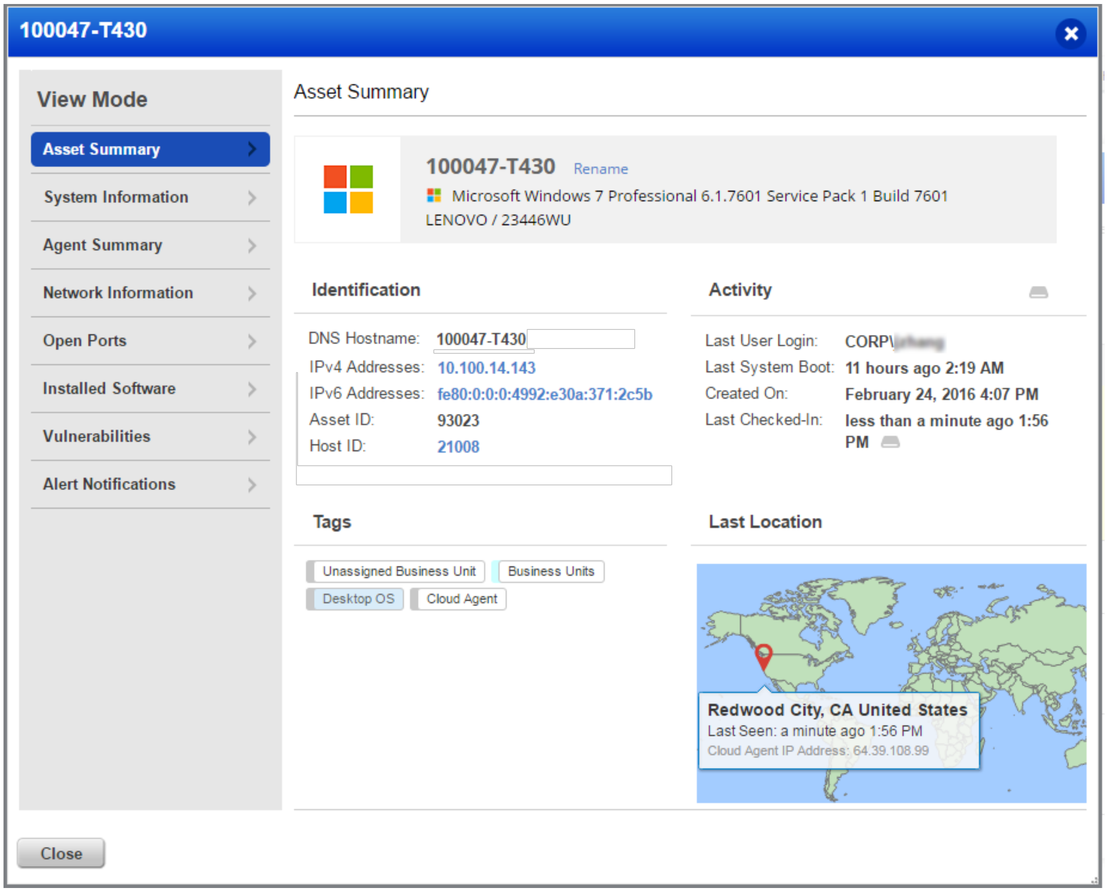
Improved Time Zone List for Malware Monitoring

AV AssetView

TP ThreatPROTECT

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

100047-T430 Rename
Microsoft Windows 7 Professional 6.1.7601 Service Pack 1 Build 7601
LENOVO / 23446WU

Identification

DNS Hostname: 100047-T430
IPv4 Addresses: 10.100.14.143
IPv6 Addresses: fe80:0:0:0:4992:e30a:371:2c5b
Asset ID: 93023
Host ID: 21008

Activity

Last User Login: CORP\[redacted]
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

IP address: 10.11.64.101
Location unknown.

Learn more

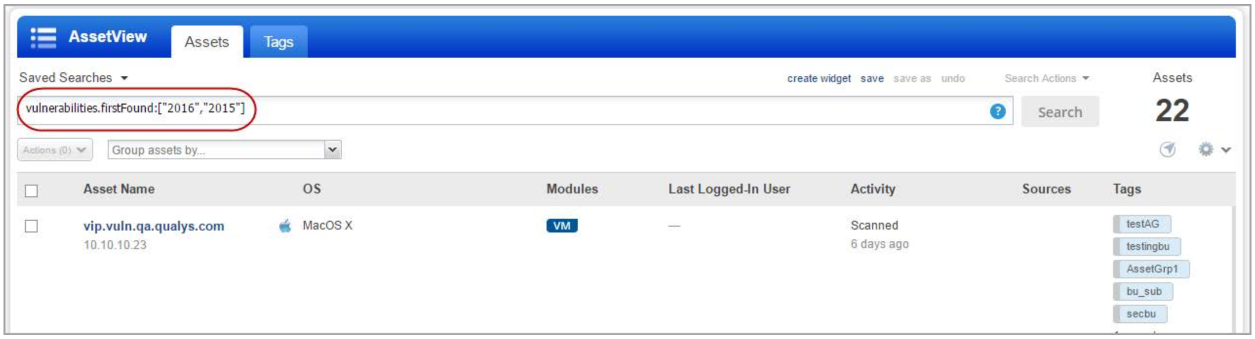
Want to enable (or disable) Asset Geolocation? Sure no problem. Just contact Qualys Support or your Qualys Account Manager and we’ll help you out.

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"]



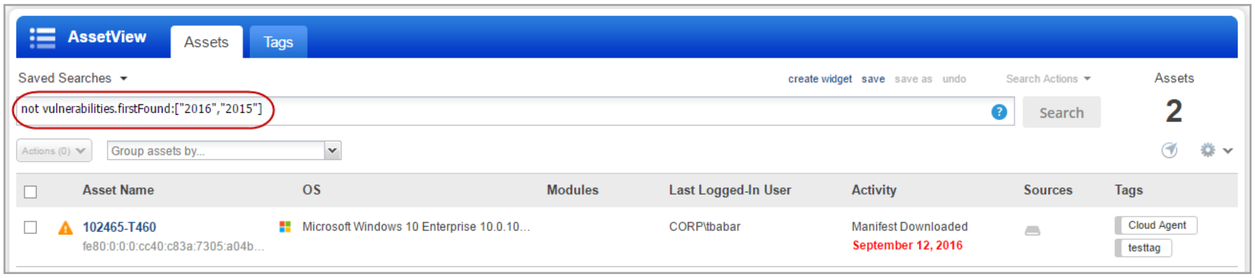
vulnerabilities.firstFound:["2016","2015"]

Assets 22

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
vip.vuln.qa.qualys.com 10.10.10.23	MacOS X	VM	—	Scanned 6 days ago		testAG testingbu AssetGrp1 bu_sub secbu

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

Query syntax:
not vulnerabilities.firstFound:["2016","2015"]



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

Assets 2

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
102465-T460 fe80:0:0:0:cc40:c83a:7305:a04b...	Microsoft Windows 10 Enterprise 10.0.10...		CORP\tbabar	Manifest Downloaded September 12, 2016		Cloud Agent testtag

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

CA Cloud Agent

Find where your agent assets are located!

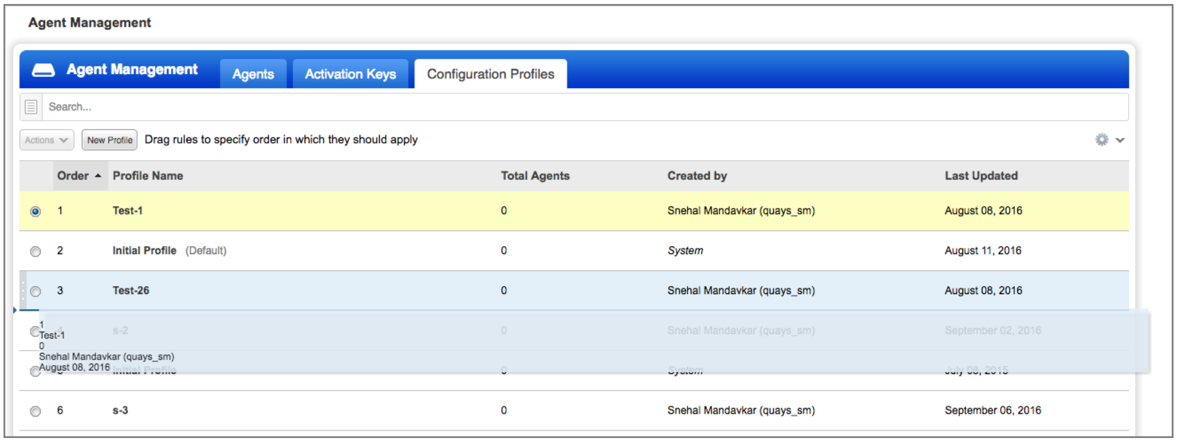
We’re now tracking geolocation of your agent assets. Learn more

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.



Drag rules to specify order in which they should apply

	Order	Profile Name	Total Agents	Created by	Last Updated
●	1	Test-1	0	Snehal Mandavkar (quays_sm)	August 08, 2016
○	2	Initial Profile (Default)	0	System	August 11, 2016
○	3	Test-26	0	Snehal Mandavkar (quays_sm)	August 08, 2016
○	4	s-2	0	Snehal Mandavkar (quays_sm)	September 02, 2016
○	5	Initial Profile	0	System	July 08, 2015
○	6	s-3	0	Snehal Mandavkar (quays_sm)	September 06, 2016

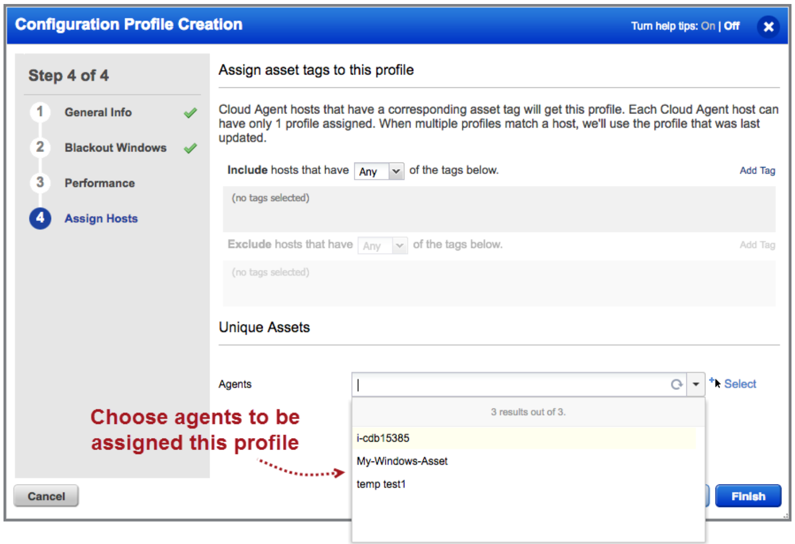
1
Test-1
0
Snehal Mandavkar (quays_sm)
August 08, 2016

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.



Assign asset tags to this profile

Cloud Agent hosts that have a corresponding asset tag will get this profile. Each Cloud Agent host can have only 1 profile assigned. When multiple profiles match a host, we'll use the profile that was last updated.

Include hosts that have Any of the tags below. Add Tag

(no tags selected)

Exclude hosts that have Any of the tags below. Add Tag

(no tags selected)

Unique Assets

Agents

3 results out of 3.

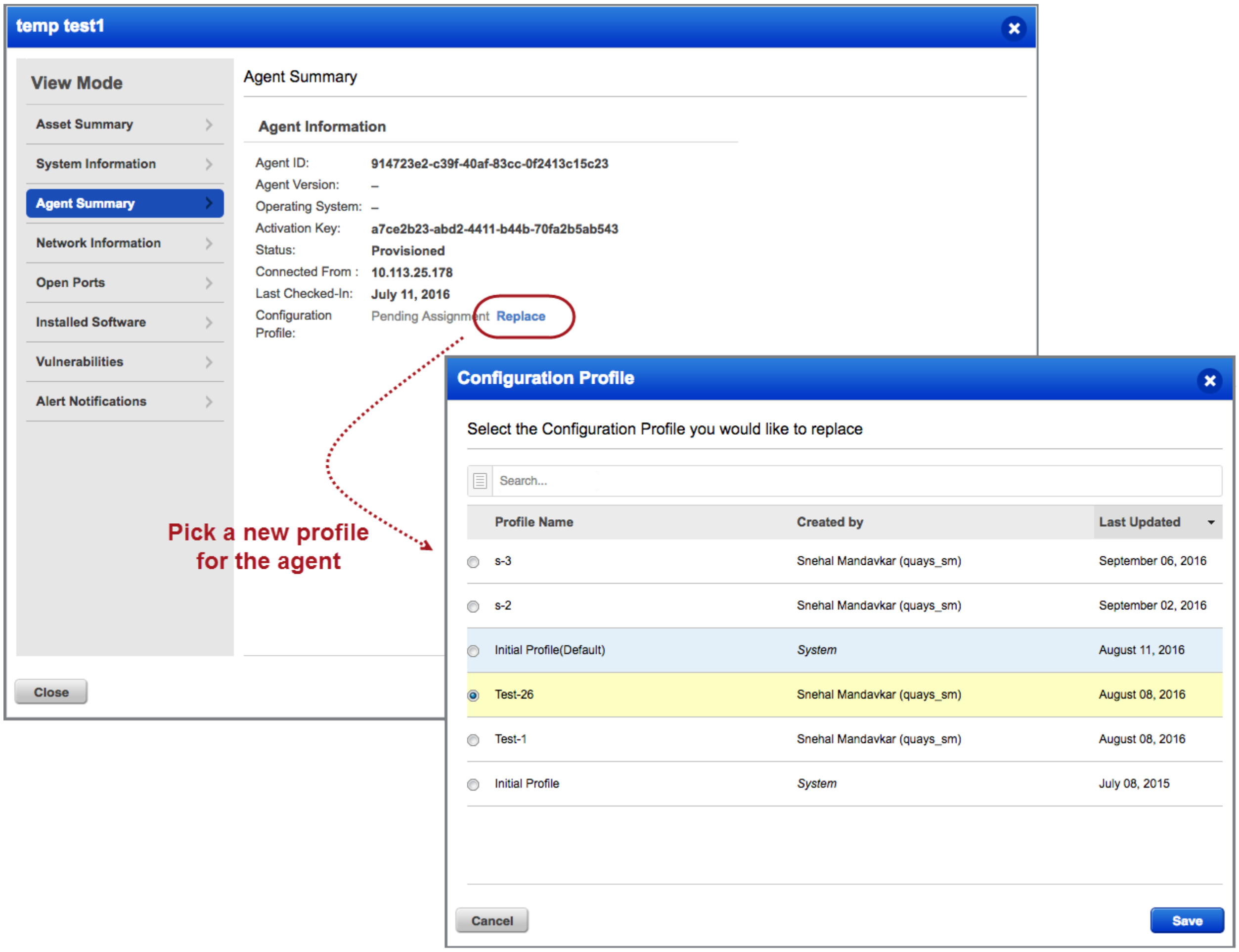
i-cdb15385

My-Windows-Asset

temp test1

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.



Agent Summary

Agent Information

Agent ID:	914723e2-c39f-40af-83cc-0f2413c15c23
Agent Version:	–
Operating System:	–
Activation Key:	a7ce2b23-abd2-4411-b44b-70fa2b5ab543
Status:	Provisioned
Connected From :	10.113.25.178
Last Checked-In:	July 11, 2016
Configuration Profile:	Pending Assignment Replace

Pick a new profile for the agent

Configuration Profile

Select the Configuration Profile you would like to replace

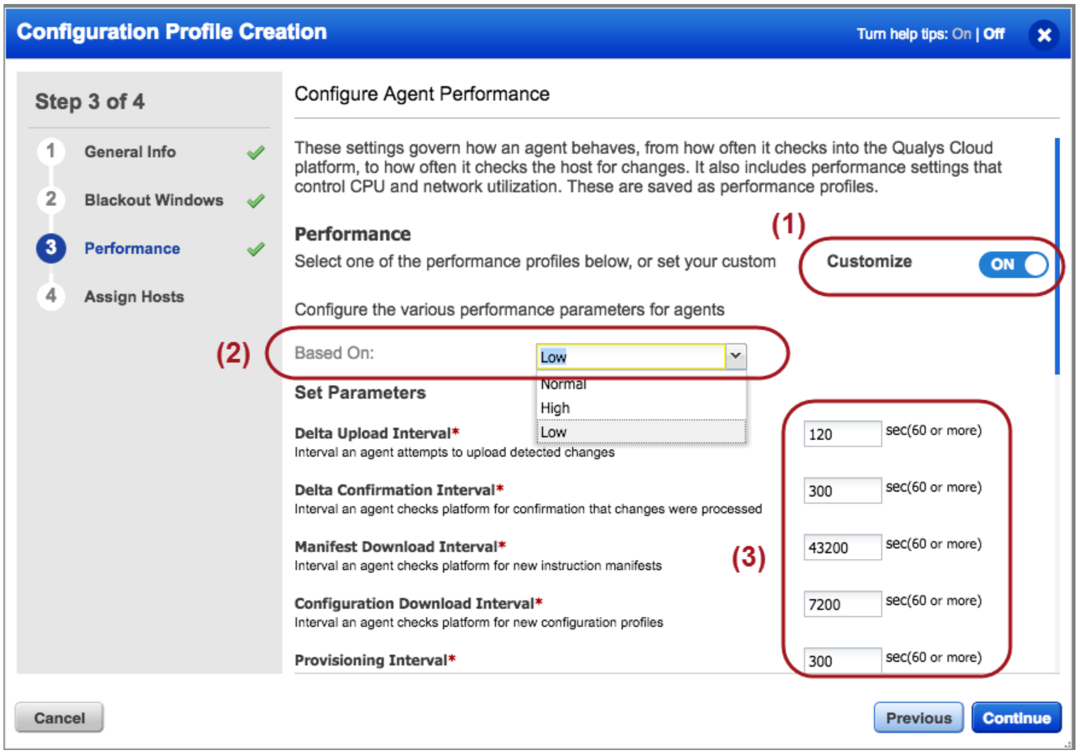
	Profile Name	Created by	Last Updated
○	s-3	Snehal Mandavkar (quays_sm)	September 06, 2016
○	s-2	Snehal Mandavkar (quays_sm)	September 02, 2016
○	Initial Profile(Default)	*System*	August 11, 2016
●	Test-26	Snehal Mandavkar (quays_sm)	August 08, 2016
○	Test-1	Snehal Mandavkar (quays_sm)	August 08, 2016
○	Initial Profile	*System*	July 08, 2015

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.



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

Configure the various performance parameters for agents

Based On: Low

Set Parameters

Delta Upload Interval* 120 sec(60 or more)
Interval an agent attempts to upload detected changes

Delta Confirmation Interval* 300 sec(60 or more)
Interval an agent checks platform for confirmation that changes were processed

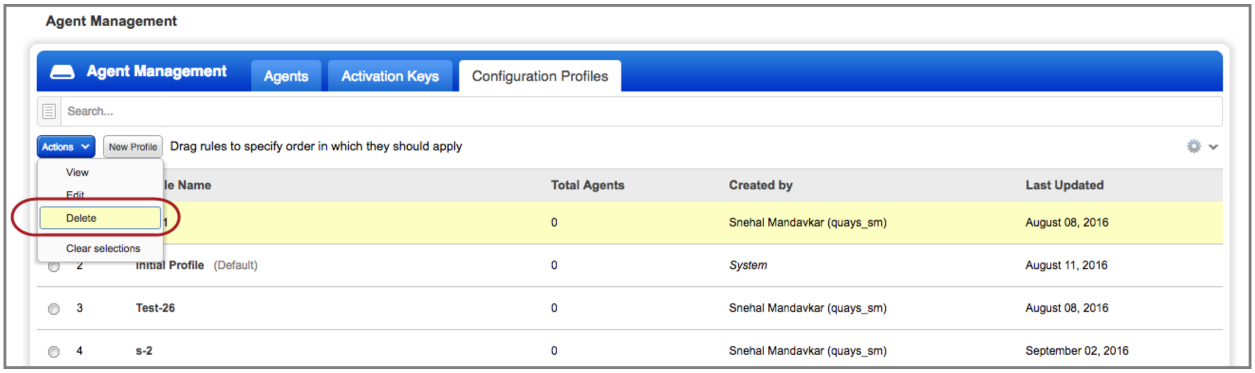
Manifest Download Interval* 43200 sec(60 or more)
Interval an agent checks platform for new instruction manifests

Configuration Download Interval* 7200 sec(60 or more)
Interval an agent checks platform for new configuration profiles

Provisioning Interval* 300 sec(60 or more)

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.



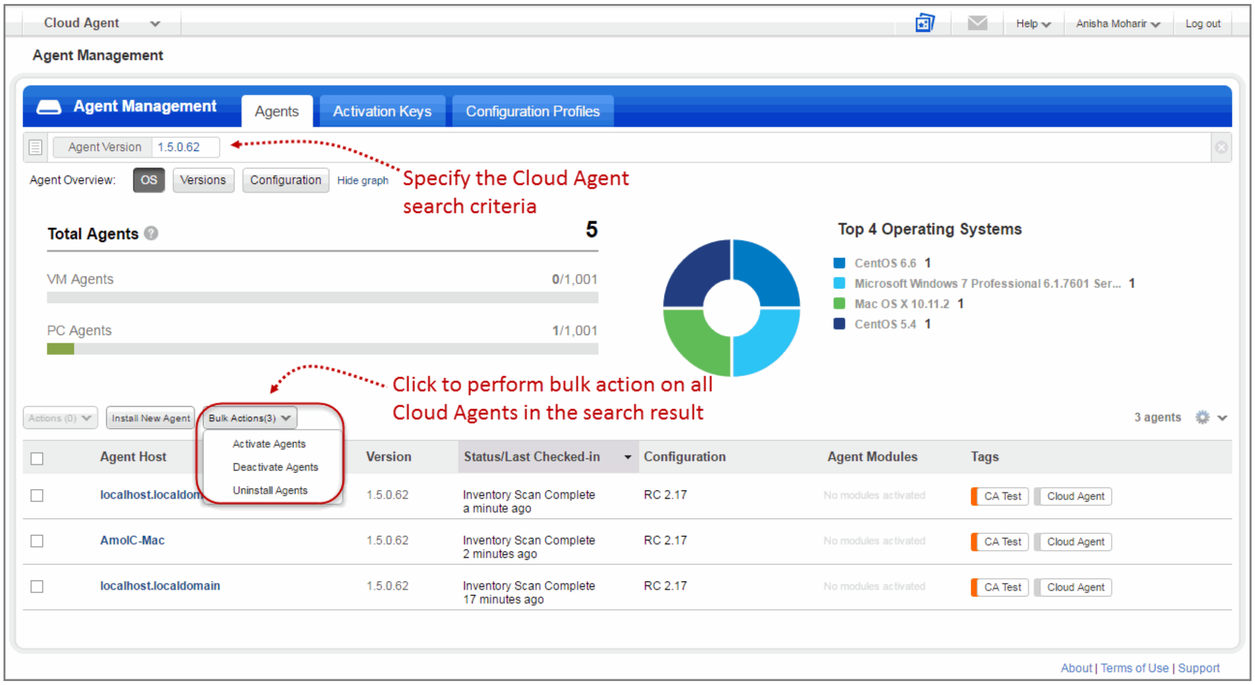
Drag rules to specify order in which they should apply

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



Specify the Cloud Agent search criteria

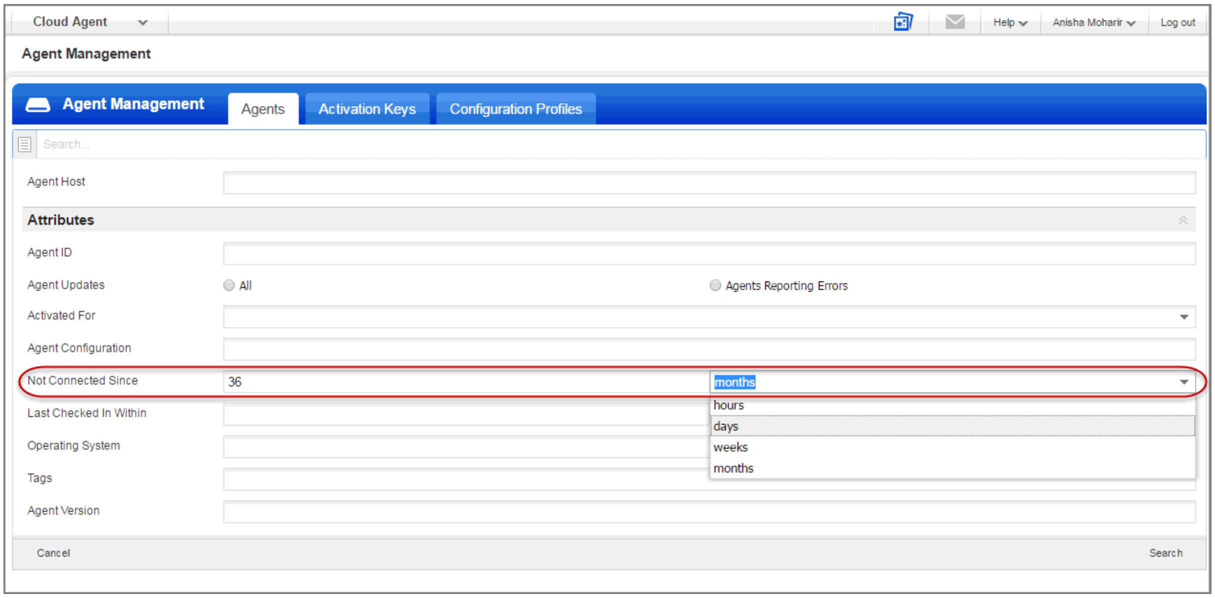
Click to perform bulk action on all Cloud Agents in the search result

□	Agent Host	Version	Status/Last Checked-in	Configuration	Agent Modules	Tags
□	localhost.localdom	1.5.0.62	Inventory Scan Complete a minute ago	RC 2.17	No modules activated	CA Test Cloud Agent
□	AmolC-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.



Agent Host

Agent ID

Agent Updates ○ All ○ Agents Reporting Errors

Activated For

Agent Configuration

Not Connected Since 36 months

Last Checked In Within

Operating System

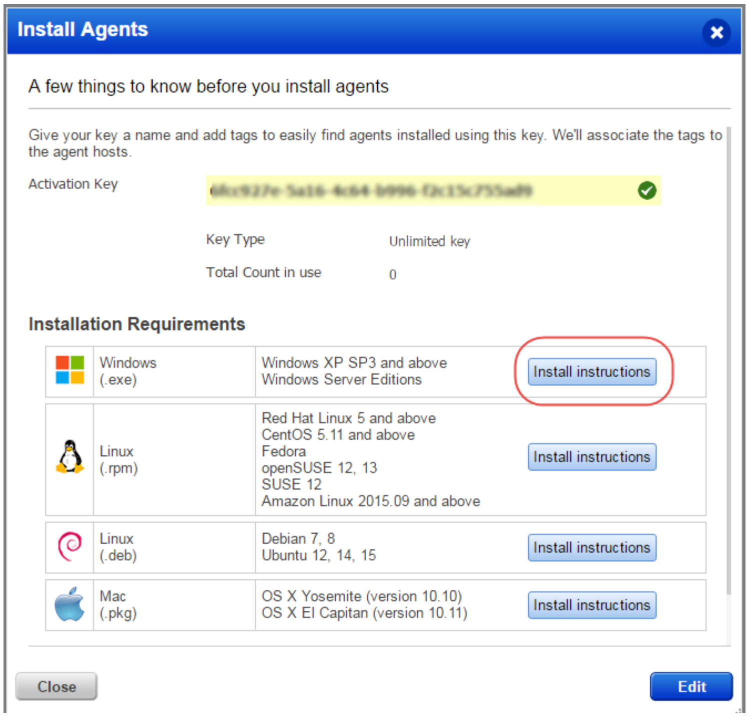
Tags

Agent Version

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.



A few things to know before you install agents

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key [redacted]

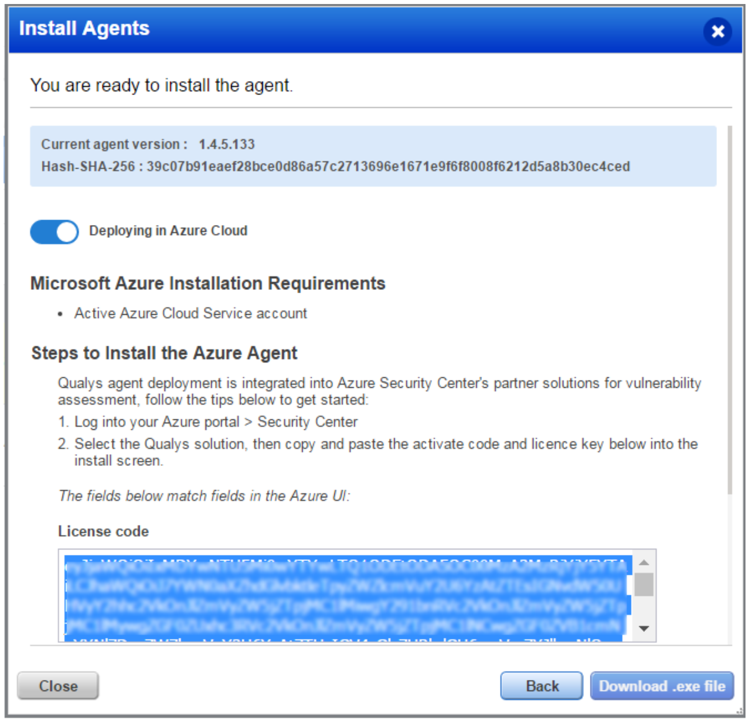
Key Type: Unlimited key

Total Count in use: 0

Installation Requirements

Windows (.exe)	Windows XP SP3 and above Windows Server Editions	Install instructions
Linux (.rpm)	Red Hat Linux 5 and above CentOS 5.11 and above Fedora openSUSE 12, 13 SUSE 12 Amazon Linux 2015.09 and above	Install instructions
Linux (.deb)	Debian 7, 8 Ubuntu 12, 14, 15	Install instructions
Mac (.pkg)	OS X Yosemite (version 10.10) OS X El Capitan (version 10.11)	Install instructions

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



You are ready to install the agent.

Current agent version : 1.4.5.133
Hash-SHA-256 : 39c07b91eaef28bce0d86a57c2713696e1671e9f6f8008f6212d5a8b30ec4ced

Deploying in Azure Cloud

Microsoft Azure Installation Requirements

- Active Azure Cloud Service account

Steps to Install the Azure Agent

Qualys agent deployment is integrated into Azure Security Center's partner solutions for vulnerability assessment, follow the tips below to get started:

1. Log into your Azure portal > Security Center
2. Select the Qualys solution, then copy and paste the activate code and licence key below into the install screen.

The fields below match fields in the Azure UI:

License code

[redacted]

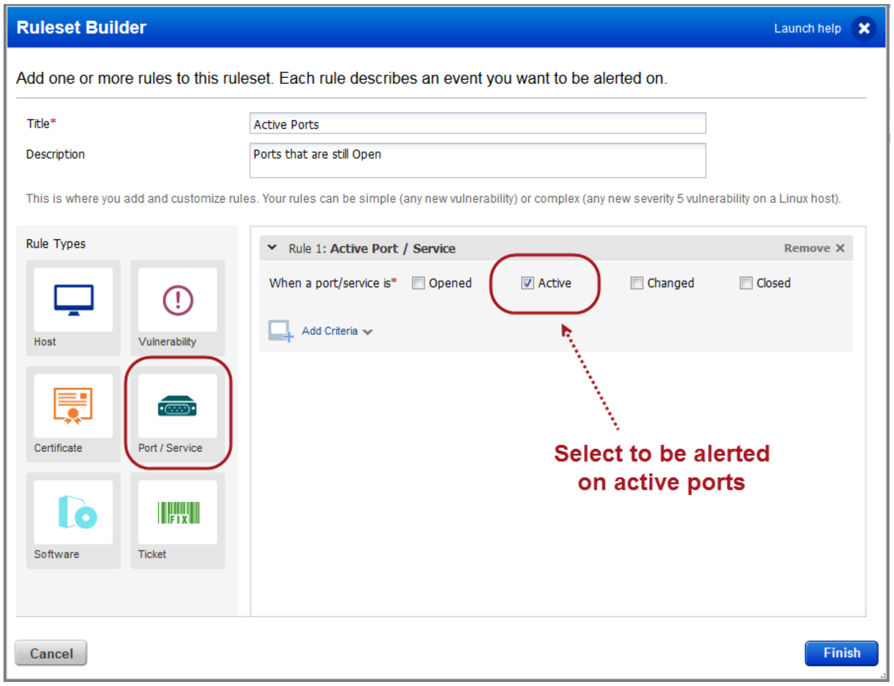
CM Continuous Monitoring

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.



Ruleset Builder

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*: Active Ports

Description: Ports that are still Open

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule 1: Active Port / Service

When a port/service is* □ Opened ☑ Active □ Changed □ Closed

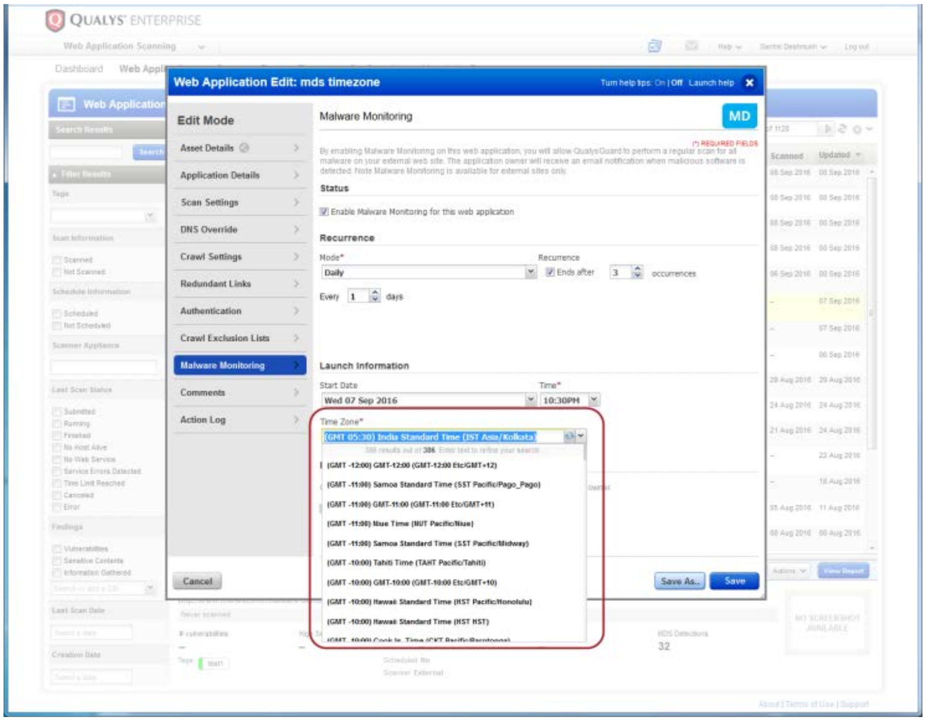
Select to be alerted on active ports

MD Malware Detection Service

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.



Web Application Edit: mds timezone

Malware Monitoring

(*) REQUIRED FIELDS

By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for all malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.

Status

☑ Enable Malware Monitoring for this web application

Recurrence

Mode*: Daily

Recurrence: ☑ Ends after 3 occurrences

Every 1 days

Launch Information

Start Date: Wed 07 Sep 2016

Time*: 10:30PM

Time Zone*: (GMT 05:30) India Standard Time (IST Asia/Kolkata)

386 results out of 386. Enter text to refine your search

(GMT -12:00) GMT-12:00 (GMT-12:00 Etc/GMT+12)

(GMT -11:00) Samoa Standard Time (SST Pacific/Pago_Pago)

(GMT -11:00) GMT-11:00 (GMT-11:00 Etc/GMT+11)

(GMT -11:00) Niue Time (NUT Pacific/Niue)

(GMT -11:00) Samoa Standard Time (SST Pacific/Midway)

(GMT -10:00) Tahiti Time (TAHT Pacific/Tahiti)

(GMT -10:00) GMT-10:00 (GMT-10:00 Etc/GMT+10)

(GMT -10:00) Hawaii Standard Time (HST Pacific/Honolulu)

(GMT -10:00) Hawaii Standard Time (HST HST)

(GMT -10:00) Cook Is. Time (CKT Pacific/Rarotonga)