



# Cloud Agent

## Getting Started Guide

June 11, 2020

Copyright 2015-2020 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



# Table of Contents

<b>About this Guide .....</b>	<b>4</b>
About Qualys .....	4
Qualys Support .....	4
<b>Get Started .....</b>	<b>5</b>
Overview .....	5
What do I need to know? .....	5
Cloud Agent Platform Availability Matrix .....	8
Cloud Agent Platform Windows Hotfixes Needed .....	13
It's easy to install agents .....	14
Installing agents in AWS .....	17
We're syncing asset data to the cloud! .....	17
Continuous scanning in the cloud.....	18
Cloud Agent Cloud Provider Metadata.....	19
<b>Manage Your Agents.....</b>	<b>21</b>
A quick look at your agents.....	21
Tell me about agent status.....	22
Easily view current Asset Details.....	24
Take bulk actions on agents.....	25
Change configuration.....	25
Tagging agent hosts .....	26
Looking for agent files? .....	27
<b>Using Qualys Platform Apps .....</b>	<b>28</b>
Vulnerability Management.....	28
Policy Compliance .....	31
Continuous Monitoring.....	32

## About this Guide

Thank you for your interest in our revolutionary new Qualys Cloud Agent Platform. This new platform extends the Qualys Cloud Platform to continuously assess global IT infrastructure and applications using lightweight agents. All you have to do is install agents on your IT assets. We'll help you get started quickly!

## 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 a founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit [www.qualys.com](http://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 support information at [www.qualys.com/support/](http://www.qualys.com/support/)

# Get Started

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!

## Overview

**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?

Here's a few things to know before you install agents on hosts within your network.

Get informed quickly about Qualys Cloud Agent (CA).

### Video Tutorials

[Cloud Agent Platform Introduction \(2m 10 s\)](#)

[Getting Started Tutorial \(4m 58s\)](#)

## **Cloud Agent requirements**

- We support these systems: Windows, Linux/Unix (.rpm), Linux (.deb), BSD(.txz), Apple Mac OSX (.pkg)

### [Cloud Agent Platform Availability Matrix](#)

- 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, BSD 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 provides a way to 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 (VM, PC, FIM, IOC, PM, etc). A license will be consumed for each agent activated.

## **Our Quick Start Guide helps you get started**

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

Tip - You can click **Cloud Agent Overview** to get helpful information on requirements, proxy support and more.

The screenshot shows the 'Agent Management' page of the Qualys Cloud Agent Platform. At the top, there's a navigation bar with 'Cloud Agent' selected, and links for 'Help', 'Steve King', and 'Log out'. Below the navigation bar, the main content area is titled 'Welcome to Qualys® Cloud Agent Platform' and includes a thank-you message. A section titled 'Get started with these quick steps' lists three steps: 1. 'Cloud Agent Overview' (with a lightbulb icon), 2. 'Download & Install Agents >' (with a download icon), and 3. 'We're Ready to Start Syncing to the Cloud! >' (with a lightning bolt icon). A fourth step, 'Change Configuration (optional) >' (with a gear icon), is also visible. To the right, there's a 'Video Tutorials' section with two videos: 'CA Platform Introduction' (2m 10s) and 'Getting Started Tutorial' (4m 58s). Below that, a 'Qualys Top Community Posts' section lists 'CA Platform Announcement', 'Webcast - An Introduction to CA' (58m), and 'Getting Started Guide'.

Looking for training? You might want to check out these options.

### Free Training

[Take a free CA self paced class](#)

[CA video library](#)

# Cloud Agent Platform Availability Matrix

[Windows](#) | [Linux](#) | [BSD](#) | [IBM AIX](#) | [Apple Mac](#)

## Windows

Current Release: 3.1.5

End-of-Support versions: 1.3.0.18, 1.4.0.x, 1.5x

Vendor	Supported Platforms		Installer	Supported Qualys Modules/Agent Versions					
	Operating System	Arch		Inventory	VM	PC	PC UDC	IOC	FIM
Microsoft	Windows XP SP 3+ Vista	x86_64 x86_32	(.exe)	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	Same as Inventory	Same as Inventory	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101
Microsoft	Windows Embedded 7	x86_64 x86_32	(.exe)	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	Same as Inventory	Same as Inventory	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	not available
Microsoft	Windows 7 Windows 8/8.1 Windows 10 (1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909) 2004 certified on 3.1.5 or later	x86_64 x86_32	(.exe)	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	Same as Inventory	Same as Inventory	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101
Microsoft	Server 2003 SP2+ Server 2008/R2* Server 2012/R2* Server 2016* Server 2019*	x86_64 x86_32	(.exe)	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	Same as Inventory	Same as Inventory	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101	3.1.5, 3.1.3.34, 3.1.2.12, 3.1.0.140, 3.0.0.101

\*all editions plus Server Core

**Important Note** Windows XP and Server 2003 do not have Cryptography Next Generation (CNG) Suite B algorithms (including SHA2) included in the operating systems. The Qualys certification uses SHA2-512 so any validation against that certification will fail because the platform doesn't have the algorithm to validate the certification installed or to install the certification. Hotfixes must be installed to add the necessary SHA2-256/318/512 support to the system.

[Click here for the hotfixes needed](#)



## Linux

Current Release: 2.6.0

End-of-Support versions: 1.3.3.23, 1.3.1.16

Supported Platforms					Supported Qualys Modules/Agent Versions				
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
Red Hat	Red Hat Enterprise Linux 5.4+	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available
Red Hat	Red Hat Enterprise Linux 6	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4, 2.2	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91 (RHEL 6.5+)
Red Hat	Red Hat Enterprise Linux 7 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4, 2.2	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Red Hat	Red Hat Enterprise Linux 8, 8.1	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4	Same as Inventory	Same as Inventory	Same as Inventory	not available	2.6.0
Red Hat	CentOS 5.4+	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available
Red Hat	CentOS 6	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4, 2.2	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91 (centOS 6.5+)
Red Hat	CentOS 7 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Red Hat	CentOS 8, 8.1	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71,	Same as Inventory	Same as Inventory	Same as Inventory	not available	Same as Inventory
Red Hat	Fedora 22, 23, 24, 25, 26, 27, 28, 29, 30, 31	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	2.6.0, 2.4.0.71	2.6.0	not available	not available
SUSE	SUSE Linux Enterprise Server (SLES) 15	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4	Same as Inventory	Same as Inventory (PC only, no SCA/CIS)	not available	not available	not available

Supported Platforms				Supported Qualys Modules/Agent Versions					
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
SUSE	SUSE Linux Enterprise Server (SLES) 12 SUSE Linux Enterprise Server (SLES) 11	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	Same as Inventory
SUSE	openSUSE Leap 15.2 (2.6.0 or later) openSUSE Leap 15.1 openSUSE Leap 15.0 OpenSUSE 13 OpenSUSE 12	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	not available	not available	not available	not available
SUSE	Leap 42.1	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	not available	not available	not available	not available
Amazon	Amazon Linux 2016.09 Amazon Linux 2015.09	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available
Amazon	Amazon Linux 2, Amazon Linux 2018.03, Amazon Linux 2017.09, Amazon Linux 2017.03	x86_64 arm_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Oracle	Oracle EnterpriseLinux 5.11	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available
Oracle	Oracle EnterpriseLinux (OEL) 7 7.1, 7.2, 7.3, 7.4, 7.5 Oracle EnterpriseLinux (OEL) 6	x86_64	(.rpm)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Debian	Debian 10.x	x86_64 arm_64	(.deb)	2.6.0, 2.4.0.71	Same as Inventory	not available	Same as Inventory	not available	not available
Debian	Debian 9.x Debian 8.x Debian 7.x (Vendor EOL May 2018)	x86_64 arm_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available

Supported Platforms				Supported Qualys Modules/Agent Versions					
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
Ubuntu	12.04 LTS	x86_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	not available	not available	not available
Ubuntu	14.04 LTS	x86_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	Same as Inventory	2.6.0, 2.4.0.71, 2.3.4	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Ubuntu	15.x	x86_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	not available	not available	not available	not available
Ubuntu	16.04 LTS	x86_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	2.6.0, 2.4.0.71	2.6.0, 2.4.0.71, 2.3.4	not available	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91
Ubuntu	18.04 LTS	x86_64 arm_64	(.deb)	2.6.0, 2.4.0.71, 2.3.4, 2.1.0.91	Same as Inventory	2.6.0, 2.4.0.71	2.6.0, 2.4.0.71, 2.3.4	not available	2.6.0, 2.4.0.71
Ubuntu	19.10	x86_64 arm_64	(.deb)	2.6.0, 2.4.0.71	Same as Inventory	Same as Inventory	Same as Inventory	not available	2.6.0, 2.4.0.71
Ubuntu	20.04 LTS	x86_64	(.deb)	2.6.0 2.4.0.71	Same as Inventory	Same as Inventory	Same as Inventory	not available	2.6.0

## BSD

Current Release: 2.4.1

Supported Platforms				Supported Qualys Modules/Agent Versions					
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
FreeBSD	FreeBSD 12.0, 11.x	x86_64	(.txz)	2.4.1	Same as Inventory	not available	not available	not available	not available

## IBM AIX

Current Release: 2.5.2

Supported Platforms				Supported Qualys Modules/Agent Versions					
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
IBM	AIX 7.1 TL1, TL2, TL3, TL4, TL5 AIX 7.2 TL1, TL2, TL3, TL4 (Standard and Enterprise Editions)	POWER 64-bit	.bff (.rpm)	2.5.2, 2.3.1.20, 2.3, 1.7.3	2.5.2, 2.3, 1.7.3	2.5.2, 2.3, 1.7.3	2.5.2, 2.3, 2.2	<i>not available</i>	<i>not available</i>
IBM	AIX 6.1 TL0-9 (Standard and Enterprise Editions)	POWER 64-bit	.bff (.rpm)	2.5.2, 2.3.1.20, 2.3, 1.7.3	2.5.2, 2.3, 1.7.3	2.5.2, 2.3, 1.7.3	2.5.2, 2.3, 2.2	<i>not available</i>	<i>not available</i>

## Apple Mac OS X

Current Release: 2.5.1

End-of-Support versions: 1.5, 1.4, 1.3, and prior

Supported Platforms				Supported Qualys Modules/Agent Versions					
Vendor	Operating System	Arch	Installer	Inventory	VM	PC	PC UDC	IOC	FIM
Apple	macOS High Sierra (10.13) macOS Sierra (10.12) OS X El Capitan (10.11) OS X Yosemite (10.10)	x86_64	(.pkg)	2.5.1, 2.3.2, 1.7.2, 1.6.0.61	Same as Inventory	Same as Inventory	<i>not available</i>	<i>not available</i>	<i>not available</i>
Apple	macOS Mojave (10.14)	x86_64	(.pkg)	2.5.1, 2.3.2, 1.7.2	Same as Inventory	2.5.1, 2.3.2	2.5.1, 2.3.2	<i>not available</i>	<i>not available</i>
Apple	macOS Catalina (10.15) including Supplement Update 1,2,3,4	x86_64	(.pkg)	2.5.1, 2.3.2	Same as Inventory	2.5.1, 2.3.2	2.5.1, 2.3.2	<i>not available</i>	<i>not available</i>

# Cloud Agent Platform Windows Hotfixes Needed

The following hotfixes are required to successfully install the Windows Agent.

Hotfix	KB Article	Archive	Language	Platform
Windows XP SP3+ x86 SHA2 Cert Hotfix	968730	375554_ENU_i386_zip.exe	English	i386
Windows Server 2003 SP2+ x86 SHA2 Cert Hotfix	968730	375510_ENU_i386_zip.exe	English	i386
Windows XP SP3+ x64 & Windows Server 2003 SP2+ x64 SHA2 Cert Hotfix	968730	375531_ENU_x64_zip.exe	English	x64

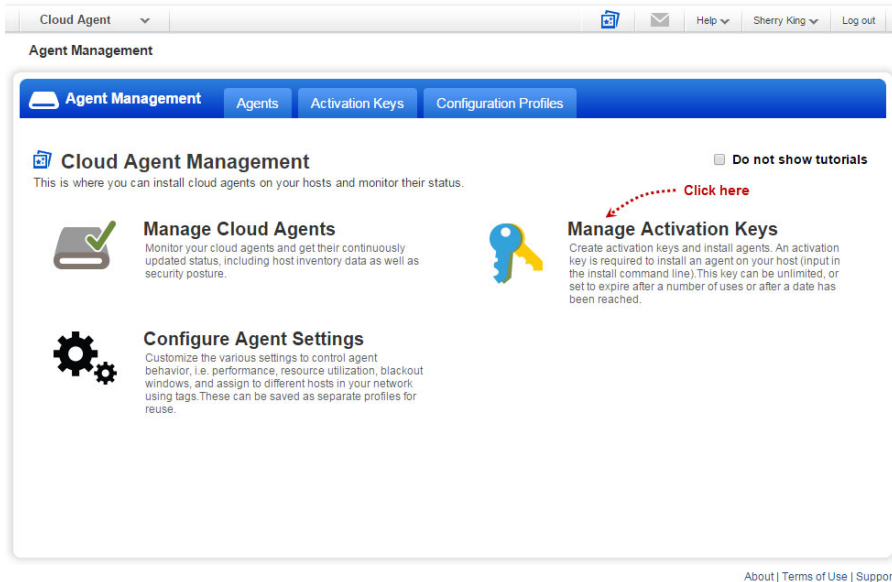
Note: Archive names may change in the future.

## It's easy to install agents

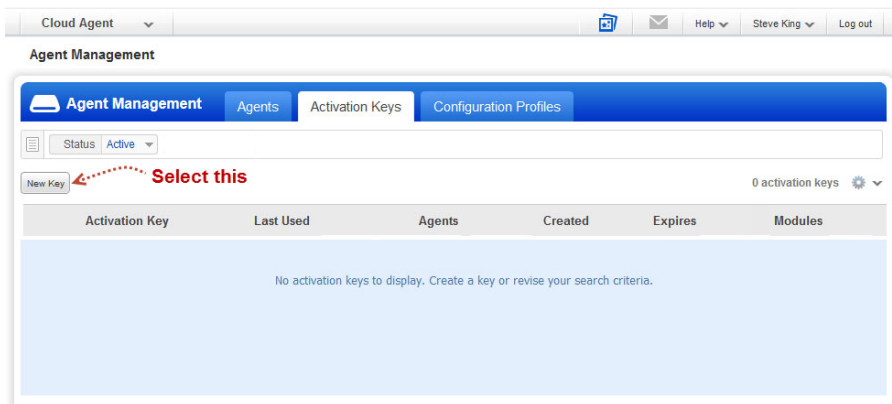
It just takes a couple minutes to install an agent. Our wizard will help you do it quickly!

### Help me with the steps

**Start the wizard** Choose Agent Management and select Manage Activation Keys (or go to the Activation Keys tab).



Select New Key to create a new activation key. An activation key is used to install agents.



The activate 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

Already have a key? Just select a key from the list, and select Install Agent from the Quick Actions menu.

**Generate a new activation key** Click the Generate button.

New Activation Key

Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title

example: My New Title

Select | Create

(no tags selected)

Provision Key for these applications

☐

PM

Patch Management

100001 Activations Remaining

☐

VM

Vulnerability Management

100000 Activations Remaining

☐

PC

Policy Compliance

100000 Activations Remain

☐

FIM

File Integrity Monitoring

100000 Activations Remaining

☐

IOC

Indication of Compromis

10000 Activations Remain

☐

SCA

Secure Config Assessment

10000 Activations Remaining

Select the Network

Global Default Network

☐ Set limits

Give your key a meaningful name to easily identify it later.









Why add tags? This helps you manage agents - we'll associate tags to agent hosts.

Your key is unlimited by default - install any number of agents at any time.

Set limits if you want the key to expire after a number of agents, or on a certain date, or both.

Auto activate agents for apps in your account. Skip this step to activate agents at a later time.

**Review requirements** and click Install Instructions for the target agent host.

Installation Requirements				
	Windows (.exe)	x86-32/64	Microsoft Windows Client Microsoft Windows Server	<a href="#">Install instructions</a>
	Linux (.rpm)	x64	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Enterprise Linux Amazon Linux Oracle Enterprise Linux	<a href="#">Install instructions</a>
	Linux (.rpm)	ARM64	Red Hat Enterprise Linux CentOS Amazon Linux	<a href="#">Install instructions</a>
	Linux (.deb)	x64	Debian Ubuntu	<a href="#">Install instructions</a>
	Linux (.deb)	ARM64	Debian Ubuntu	<a href="#">Install instructions</a>
	Mac (.pkg)	x64	Apple macOS Apple OS X	<a href="#">Install instructions</a>
	AIX (.bff.gz)	Power5	IBM AIX	<a href="#">Install instructions</a>
	BSD (.tbz)	x64	FreeBSD	<a href="#">Install instructions</a>

Don't see all of the options?  
Just go to [Help > Contact Support](#) and we'll help you with this quickly

**Install your agents** You'll download the agent installer and run on your hosts. To run the installer you just copy and paste the command shown - it's that simple.

Depending on the OS type, you'll download respective agent installer and install the agent from Install Instructions.

Few examples:

For Linux (.rpm) ARM64, you'll click Download .rpm button to download the agent installer.

For Linux (.deb) ARM64, you'll click Download .deb button to download the agent installer.

For Mac (.pkg) x64, you'll click Download .pkg button to download the agent installer.

**Setup proxy support** Our installation guides help you with this and more options.

Installation Guides: [Windows Agent](#) | [Linux Agent](#) | [BSD Agent](#) | [Unix Agent](#) | [Mac Agent](#)



## Installing agents in AWS

Please follow the installation steps provided at the link below.

**Learn more**

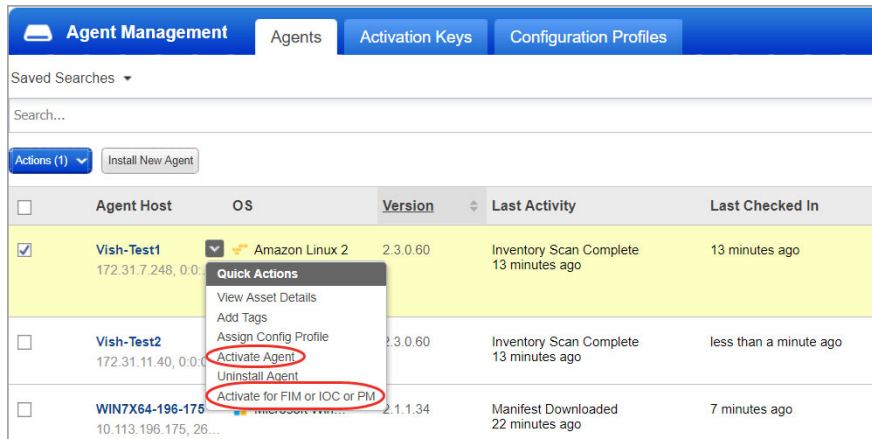
[Installing Cloud Agent in AWS](#)

## We're syncing asset data to the cloud!

The agent immediately connects to the cloud agent platform and registers itself. We would expect you to see your first asset discovery results within a few minutes. This is a light scan that collects asset inventory data: IP address, OS, DNS/NetBIOS names, MAC address.

Status messages are continuously updated. [Learn more](#)

**Be sure to Activate Agents** for modules (VM/PC) or (FIM/IOC/PM). Activate Agent from the Quick Actions menu (or do it for many agents in bulk using the Actions menu). If you skip this step your agents will sync inventory information only (IP address, OS, DNS and NetBIOS names, MAC address) and the cloud agent platform will not perform host assessments and report security threats.



Agent Management					
Agents					
Activation Keys					
Configuration Profiles					
Saved Searches ▾					
Search...					
Actions (1) ▾ Install New Agent					
<input type="checkbox"/>	Agent Host	OS	Version	Last Activity	Last Checked In
<input checked="" type="checkbox"/>	Vish-Test1 172.31.7.248, 0.0.0.0	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 13 minutes ago	13 minutes ago
<input type="checkbox"/>	Vish-Test2 172.31.11.40, 0.0.0.0	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 13 minutes ago	less than a minute ago
<input type="checkbox"/>	WIN7X64-196-175 10.113.196.175, 26...	Microsoft Windows	2.1.1.34	Manifest Downloaded 22 minutes ago	7 minutes ago

**No agent status?** You should see the status of your agent (on the Agents tab) a few minutes after installation. If there's no status this means your agent has not been installed - it did not successfully connect to the cloud platform and register itself.

There are 2 common reasons for this:

- 1) The agent host cannot reach the Qualys Cloud Platform (or the Qualys Private Cloud Platform if this applies to you) over HTTPS port 443. Check network access and be sure to whitelist the platform URL listed in your account. Just go to Help > About for details.
- 2) You have a custom proxy. Our Quick Start Guide > Cloud Agent Overview will help you with this quickly.

**Still need help?** Keep in mind your agents must connect to the cloud platform to start syncing asset data to the cloud. Click [here](#) to troubleshoot.

## Continuous scanning in the cloud

The first assessment scan in the cloud takes some time, after that scans complete as soon as new host metadata is uploaded to the platform.

Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules
WIN7X64-196-175 10.113.196.175, 26...	Microsoft Win...	2.1.1.34	Inventory Scan Complete 4 minutes ago	4 minutes ago	LCI	FIM IOC

**How it works** The agent sends up an upload of the baseline snapshot to the cloud agent platform for assessment. For the initial upload the agent collects comprehensive metadata about the target host (a few megabytes) and sends a baseline snapshot to the cloud for assessment. The status Scan Complete is reported upon success. This first scan typically takes 30 minutes to 2 hours using the default configuration - after that scans run instantly on the delta uploads (a few kilobytes each).

**The asset data the agent collects** includes many things for the baseline snapshot like network posture, OS, open ports, installed software, registry info, what patches are installed, environment variables, and metadata associated with files. The agent stores a snapshot on the agent host to quickly determine deltas to host metadata it collects.

**What signatures are tested?** Agent-based scanning uses the same signatures (vulnerabilities, compliance datapoints) as traditional scanning with Qualys scanners. If you've activated your agents for VM, we'll test for vulnerability signatures. If you've activated your agents for PC we'll check for compliance datapoints.

## Cloud Agent Cloud Provider Metadata

Available starting with Cloud Agent Linux 1.7.0 and Cloud Agent Windows 1.6.0 releases, the Qualys Cloud Agent collects instance metadata from supported public cloud providers, including Amazon Web Services, Microsoft Azure, and Google Compute Platform.

The agent collects the instance metadata from the cloud provider's instance metadata web services locally available from each running instance via HTTP as part of the agent's default inventory collection. The collected instance metadata is available in the Qualys AssetView module (Asset Details and new search tokens) and Asset Management API.

### Cloud Provider Instance Metadata

The following table lists the instance metadata currently collected by the Cloud Agent for each cloud provider. Refer to the Cloud Agent Release Notes for additional instance metadata collected from public cloud providers in future versions of the Cloud Agent.

Amazon Web Services	Cloud Agent Linux	Cloud Agent Windows
accountId ami-id availability-zone instance-id instance-type kernel-id local-hostname local-ipv4 network/interfaces/macs/mac/mac network/interfaces/macs/mac/subnet-id public-hostname public-ipv4 region reservation-id security-groups security-groups-ids vpc-id	Supported	Supported
Microsoft Azure	Cloud Agent Linux	Cloud Agent Windows
compute.location compute.name compute.offer compute.osType compute.publisher compute.resourceGroupName compute.subscriptionId compute.tags compute.version compute.vmId compute.vmSize network.interface.ipv4.ipaddress.privateIpAddress network.interface.ipv4.ipaddress.publicIpAddress network.interface.ipv4.subnet.address network.interface.ipv6.ipaddress.ipAddress network.interface.macAddres	Supported	Supported

Google Compute Platform	Cloud Agent Linux	Cloud Agent Windows
instance/hostname instance/id instance/machine-type instance/network-interfaces/ instance/network-interfaces/0/access- configs/0/external-ip instance/network-interfaces/0/ip instance/network-interfaces/0/mac instance/network-interfaces/0/network instance/zone project/numeric-project-id project/project-id	Supported	Supported

# Manage Your Agents

## A quick look at your agents

The screenshot shows the 'Agent Management' section of the Qualys Cloud Platform. It features a search bar (2), a table of agents, and various action buttons. The table has columns for Agent Host (3), OS, Version, Last Activity (1), Last Checked In, Configuration (4), Agent Modules, and Tags (5). Three agents are listed: WIN7PATCH99-95, WIN7X64-196-175, and Vish-Test2.

Agent Host	OS	Version	Last Activity	Last Checked In	Configuration	Agent Modules	Tags
WIN7PATCH99-95 10.115.76.105, fe8...	Microsoft Win...	2.1.1.34	Inventory Scan Complete 8 minutes ago	8 minutes ago	Initial Profile 1	VM, PC, FIM, IDS	Cloud Agent, tag1
WIN7X64-196-175 10.113.199.175, 26...	Microsoft Win...	2.1.1.34	Scan Complete 14 minutes ago	7 minutes ago	LCI	VM, PC, FIM, IDS	Cloud Agent
Vish-Test2 172.31.11.40, 0:0:0...	Amazon Linux 2	2.3.0.60	Scan Complete 20 minutes ago	4 minutes ago	LCI	VM, PC, FIM	Cloud Agent

- 1 You should see status messages within a few minutes after installation. [Learn more](#)
- 2 Search your agents - your agents list includes all installed agents that have connected to the Qualys Cloud Platform.
- 3 Agent hostname - NetBIOS name for a Windows host, DNS name for a Linux host. You can configure the name displayed. Just select View Asset Details from the Quick Actions menu.
- 4 A configuration profile has settings that impact agent behavior. Initial Profile is the profile provided by our service to help you get started. Want create a profile with customized settings? Just go to Configuration Profiles and select New Profile.
- 5 We assign the Cloud Agent tag to agent hosts automatically. This helps you manage and report on your agent assets.

<input type="checkbox"/>	Agent Host	OS	Version	Last Activity
<input checked="" type="checkbox"/>	Vish-Test1 172.31.7.248, 0.0.0.0	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 13 minutes ago
<input type="checkbox"/>	Vish-Test2 172.31.11.40, 0.0.0.0	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 13 minutes ago
<input type="checkbox"/>	WIN7X64-196-179 10.113.196.175, 26...	Microsoft Windows 7	2.1.1.34	Manifest Downloaded 22 minutes ago

Quick Actions menu lets you

- view asset details
- activate agent for various assessments (VM, PC, etc)
- uninstall agent

Actions (2)	Install New Agent
<input checked="" type="checkbox"/>	Add Tags
<input checked="" type="checkbox"/>	Assign Config Profile
<input type="checkbox"/>	Deactivate Agent
<input type="checkbox"/>	Assign UDC Manifest
<input type="checkbox"/>	Uninstall Agent
<input type="checkbox"/>	Activate for FIM or IOC or PM
<input type="checkbox"/>	Deactivate Agent for FIM or IOC or PM
<input type="checkbox"/>	Clear selections

Version	Last Activity
Microsoft Win...	2.1.1.34
Inventory Scan Complete	2 minutes ago
Amazon Linux 2	2.3.0.60
Inventory Scan Complete	13 minutes ago

Actions menu lets you update multiple agents at once

## Tell me about agent status

The agent status is continuously updated to keep you informed about your agent. Not seeing any status? Read our troubleshooting tips (under Help > Online Help).

### Provisioned

The agent successfully connected to the cloud platform and registered itself.

### Manifest Downloaded

The cloud platform updated the manifest assigned to this agent. This tells the agent what metadata to collect from the host. The updated manifest was successfully downloaded and it is in effect for this agent. For non-Windows agents the status column shows specific manifest download status, such as Inventory Manifest Downloaded for inventory, and the following status for scans:

VM Manifest Downloaded, PC Manifest Downloaded, FIM Manifest Downloaded, or IOC Manifest Downloaded.

### Configuration Downloaded

A user updated the configuration profile assigned to this agent. This defines agent behavior, i.e. how the agent will collect data from the host. The updated profile was successfully downloaded and it is in effect for this agent.

### Agent Downloaded

A new agent version was downloaded and the agent was upgraded as part of the auto-update process. Note the agent does not need to reboot to upgrade itself.

### **Inventory Scan Complete**

The agent completed host discovery, collected some host information and sent it to the cloud platform. During host discovery the agent attempts to collect this information: IP address, OS, NetBIOS name, DNS name, MAC address.

### **Scan Complete**

The agent uploaded new host metadata and an assessment was performed on the cloud platform. If there is new assessment data (e.g. new VM vulnerabilities, PC datapoints) the cloud platform processes this data to make it available in your account for viewing and reporting.

## Easily view current Asset Details

Actions (1) <span>Install New Agent</span>				
<input type="checkbox"/>	Agent Host	OS	Version	Last Activity
<input checked="" type="checkbox"/>	Vish-Test1 172.31.7.248, 0.0.	Amazon Linux 2	2.3.0.60	Inventory Scan Complete 10 minutes ago
<input type="checkbox"/>	WIN7X64-196-178 10.113.196.175, 2e	<b>Quick Actions</b> View Asset Details Add Tags Assign Config Profile Deactivate Agent Uninstall Agent Activate for FIM or IOC or PM Deactivate Agent for FIM or IOC or PM		
<input type="checkbox"/>	WIN7PATCH69-86 10.115.76.105, fe8			Inventory Scan Complete 29 minutes ago

Select **View Asset Details** from the menu

Asset Summary and sections that follow show you current asset data returned from the latest inventory scan and the latest full scan (assessment).

101854-T450

View Mode

Asset Summary

System Information

Agent Summary

Network Information

Open Ports

Installed Software

Vulnerabilities

Asset Summary

101854-T450

Rename

Microsoft Windows 7 Professional 6.1.7601 Service Pack 1 Build 7601  
LENOVO / 20BV000DUS

Identification

DNS Hostname:

101854-T450

FQDN:

101854-T450

NetBIOS Name:

101854-T450

IPv4 Addresses:

10.0.2.15

IPv6 Addresses:

fe80:0:0:0:203:0:567e:33c4

Asset ID:

429512

Host ID:

-

Tags

Comp\_10.10.107\_10\_WinOnly

testboooxx

Cloud Agent

Activity

Last User Login:

CORPlashah

Last System Boot:

June 15, 2017 3:55 AM


Created On:

December 9, 2016 1:20 PM

Last Checked-In:

24 minutes ago 1:51 PM

Last Location



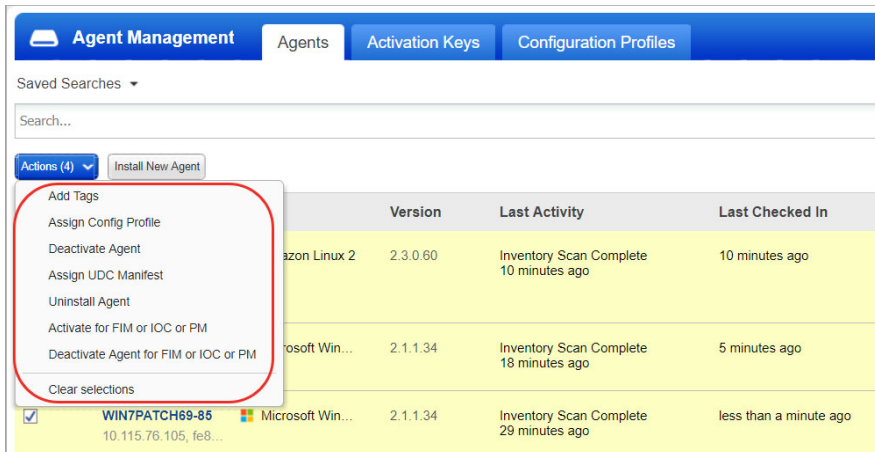
Drill down to the various sections to view comprehensive details returned from vulnerability assessments. You can view control datapoints when your account has Policy Compliance (PC) enabled, and alert notifications when Continuous Monitoring (CM) is enabled.



## Take bulk actions on agents

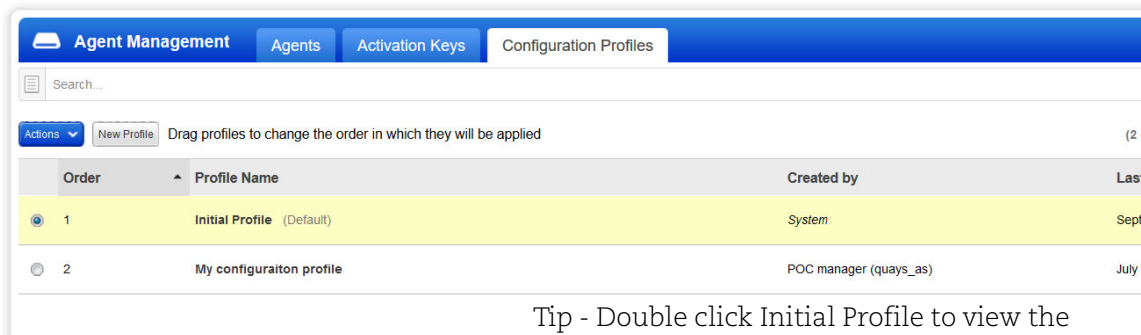
### Activate, Deactivate, Uninstall multiple agents in one go!

Select agents from your agents list, open the Actions menu and select the bulk action to apply.



## Change configuration

Agents have a default configuration and this controls how agents behave. You can change agent configuration by creating configuration profiles, and change the order they are applied.



**Initial Profile** is the default profile with configuration settings provided by Qualys. This is assigned to agents by default at installation time. You can easily view the profile settings.

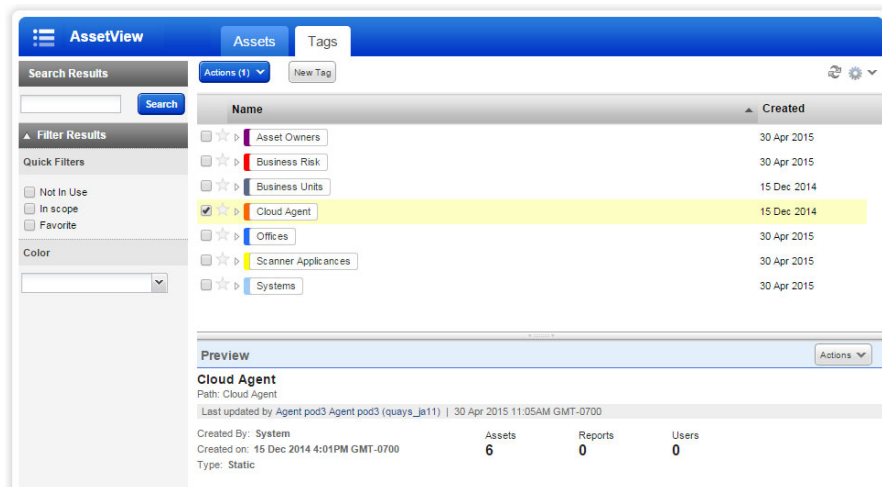
**Profile settings** impact many agent behaviors. How and when the agent collects metadata, when it should sync with the cloud platform, when to do self-updates, tuning of performance and bandwidth utilization, etc. You can create custom profiles and assign to hosts.

**Best Practices** You might want to assign different agent configurations for different parts of your network infrastructure, i.e. laptops, servers, desktops, datacenters. Just tag your hosts according to your groupings and assign these tags to different configuration profiles.

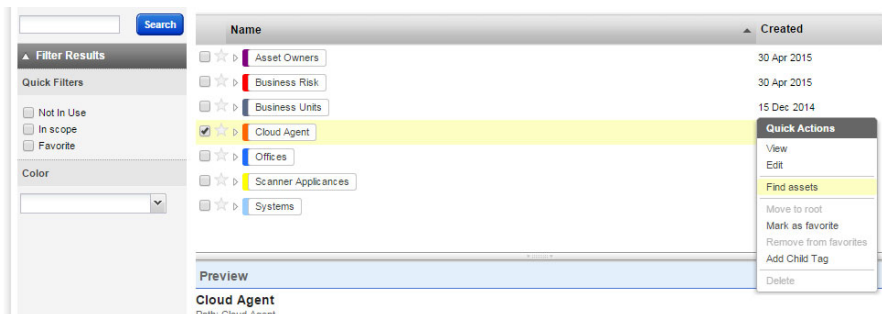
## Tagging agent hosts

The dynamic asset tagging features help you manage your agent host assets just like other assets in your subscription.

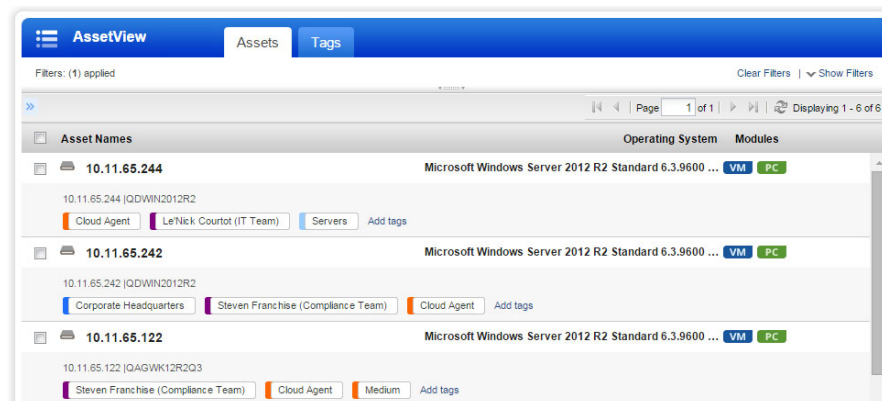
The Cloud Agent tag is assigned to every agent host. Select this tag and you'll see the number of agent hosts (assets).



The Find assets option lets you find agent assets.



You might want to tag agent hosts to help you organize them and report on them.



## Looking for agent files?

The agent is centrally managed by the cloud platform. For this reason you should not edit or execute the agent files installed on your hosts - we list these here for your information. For help with troubleshooting you might want to review the log files.

What's included? Program files, the manifest (instructions for what data the agent collects), configuration (how the agent behaves), snapshot database and log files.

### Windows Agent

C:\Program Files (x86)\QualysAgent\Qualys\QualysCloudAgent.exe  
C:\Program Files (x86)\QualysAgent\Qualys\Uninstall.exe  
C:\ProgramData\Qualys\QualysAgent\\*

Log files (Log.txt, Archive.txt) are located here:

C:\ProgramData\Qualys\QualysAgent

On XP and Server 2003, log files are located here:

C:\Documents and Settings\All Users\Application Data\Qualys\QualysAgent

Have custom variables? No worries, we'll install the agents following the environment settings defined for your hosts.

### Linux Agent, BSD Agent, Unix Agent, Mac Agent

/etc/init.d/qualys-cloud-agent

/etc/rc.d //BSD

/etc/qualys/cloud-agent/qagent-log.conf

/var/log/qualys/qualys-cloud-agent.log

/var/opt/qualys/qualys-cloud-agent.log //Unix

/usr/local/qualys/cloud-agent/\* //Linux/BSD, Unix

Still need help? Click [here](#) to troubleshoot.

# Using Qualys Platform Apps

**As soon as agents discover issues on your hosts you'll know about them right away!**

Our Qualys Cloud Platform applications - VM, PC, AV, CM and more! - automatically integrate vulnerability management data and policy compliance data collected by agents. A change reported by an agent to the cloud platform is immediately assessed, and updated asset data is available in your account right away.

Your Qualys applications bring you:

- Current security posture for your hosts
- Details on up-to-the minute assessments and security threats
- Reports on the latest asset data, and the ability to schedule them
- Alerts as soon as certain host changes occur (using Continuous Monitoring)

Jump in to your account anytime to get the latest security updates!

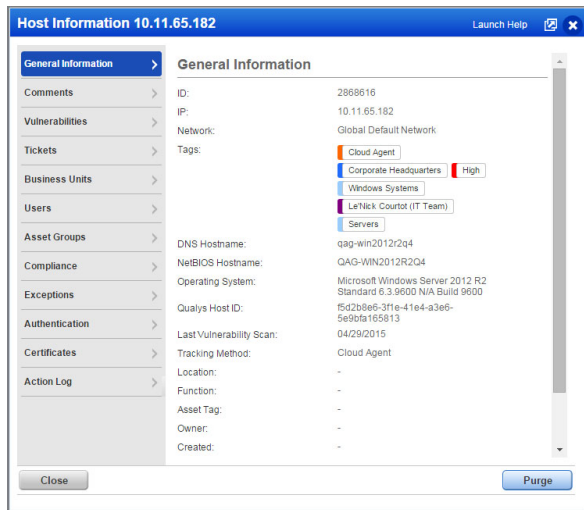
## Vulnerability Management

The latest Vulnerability Management assessment data is available in your Qualys account at all times from scans performed by the cloud agent platform.

You'll see agent hosts listed on the Host Assets tab with the tracking method Agent.

Info	Tracking	IP	DNS	NetBIOS	OS
<input type="checkbox"/>	Agent	10.90.2.33	ec2amaz-raid75e	EC2AMAZ-RAID75E	Windows Server 2019 Datacenter 64 bit Edition Version 1809 Build 17763
<input type="checkbox"/>	Agent	10.95.0.33	sanket-azure	SANKET-AZURE	Windows 10 Pro 64 bit Edition Version 1809
<input type="checkbox"/>	Agent	10.115.95.174	vmdr27	VMDR27	Windows 7 Professional 64 bit Edition Service Pack 1

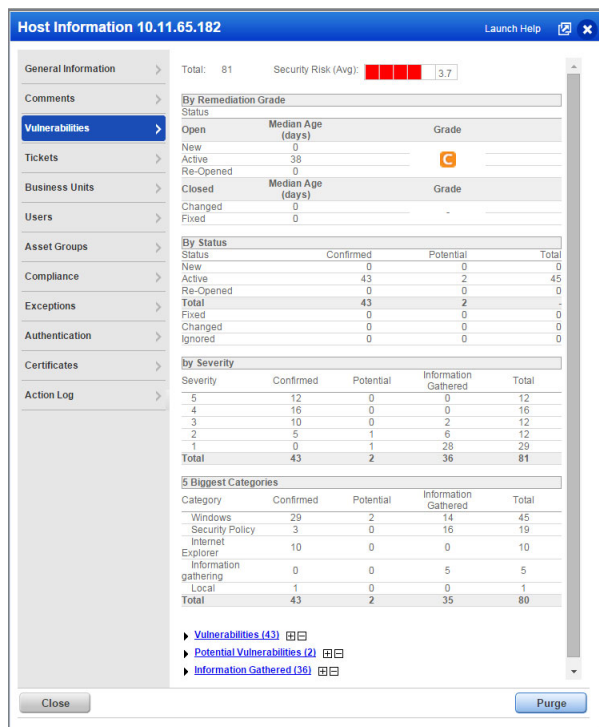
Just click ⓘ to see comprehensive host information.



Once a light scan is complete, you'll see basic information about the agent host.

For this host we already added tags using the Asset Management application.

VM assessment data appears in the Vulnerabilities section for an agent host, just like it does for traditional hosts tracked by another tracking method.



Once a full scan is complete, you'll see assessment data in the Vulnerabilities section.

You can create VM Reports on agent hosts with up to the minute asset data as needed, or schedule them to run at a convenient time.

Tip - You can select the Cloud Agent tag to report on all your agent hosts.

This sample High Severity Report shows detailed results for an agent host - the details appear just like any other host in your subscription.

**High Severity Report**

File View Help

**Detailed Results**

10.11.65.192 (qag-win2012r2q4, QAG-WIN2012R2Q4) - Global Default Microsoft Windows Server 2012 R2 Standard 6.3.9600 N/A Build 9600

**Vulnerabilities (28)**

- 5 Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS14-010) Active
- 5 Microsoft Internet Explorer Multiple Remote Code Execution Vulnerabilities (MS13-097) Active
- 5 Microsoft VBScript Remote Code Execution Vulnerability (MS14-011) Active

**First Detected:** 04/18/2015 at 04:14:52 (GMT-0700) **Last Detected:** 04/29/2015 at 06:25:36 (GMT-0700) **Times Detected:** 52

**QID:** 90942  
**Category:** Windows  
**CVE ID:** [CVE-2014-0271](#)  
**Vendor Reference:** [MS14-011](#)  
**Bugtraq ID:** -  
**Service Modified:** 02/11/2014  
**User Modified:** -  
**Edited:** No  
**PCI Vuln:** Yes  
**Ticket State:**

**THREAT:**  
 A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. Exploitation of this vulnerability will allow an attacker to execute arbitrary code. This security update is rated Critical for affected versions of the VBScript scripting engine on affected Windows clients and Moderate for affected versions of the VBScript scripting engine on affected Windows servers.  
**Affected Versions:**  
 VBScript 5.6  
 VBScript 5.7  
 VBScript 5.8 (Affecting Internet Explorer 8.9,10,11)  
 VBScript 5.7 (Affecting Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) and Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation))  
 VBScript 5.8 (Affecting Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation), Windows Server 2012 (Server Core installation) and Windows Server 2012 R2 (Server Core installation))

**IMPACT:**  
 Successful exploitation of this vulnerability will allow a remote attacker to execute arbitrary code in the context of logged in user. Failed exploits may result in denial of service.

**SOLUTION:**  
 Please refer to [MS14-011](#) for details.  
 Patch:  
 Following are links for downloading patches to fix the vulnerabilities:  
[MS14-011: Windows XP Professional x64 Edition Service Pack 2 \(VBScript 5.6\)](#)  
[MS14-011: Windows Server 2003 Service Pack 2 \(VBScript 5.6\)](#)  
[MS14-011: Windows Server 2003 x64 Edition Service Pack 2 \(VBScript 5.6\)](#)

How do I run this report? Go to VM/VMDR > Reports > Templates, select the High Severity Report and then Run from the Quick Actions menu.

The same applies to Patch Reports. You can run a Patch Report to find the patches that are needed for agent hosts, just like you do for host tracked by IP address, NetBIOS or DNS. If you select the Cloud Agent tag for the report target, your report includes all host agents in your account.

**QUALYS EXPRESS Patch Report for Agent Hosts**

**Report Summary**

Company: qualys  
Created by: Agent pod3 Agent pod3  
Created on: 05/26/2015

**Total Patches: 78** **Hosts Requiring Patches: 3** **Vulnerabilities Addressed: 108**

**HOSTS**

IP	Net...	DNS Name	NetBIOS	OS	Patches
10.11.6...	Glo...	qdwini2012r2	QDWIN2...	Microsoft Windows Server ...	26
10.11.6...	Glo...	qdwini2012r2	QDWIN2...	Microsoft Windows Server ...	26
10.11.6...	Glo...	qag-win2012r2q4	QAQ-WL...	Microsoft Windows Server ...	26

**PATCHES required on '10.11.65.242' (26)**

Vendor ID	Sev.	Title	Published	Notes
MS15-043	4	Microsoft Internet Explorer Cumulative ...	14 days ago	9
MS15-044	4	Microsoft Font Drivers Remote Code Ex...	14 days ago	2
MS15-052	3	Microsoft Windows Kernel Security Fea...	14 days ago	2
MS13-095	3	Microsoft Windows Digital Signatures D...	1 year ago	1
MS13-090	5	Microsoft Cumulative Security Update o...	1 year ago	1
MS13-098	4	Windows Digital Signatures Remote Co...	1 year ago	1
MS13-099	4	Microsoft Scripting Runtime Object Libr...	1 year ago	1
MS14-011	5	Microsoft Windows Remote Code Execution Vulnerability (MS14-011)		

How do I run this report? Go to Reports > Report Templates, select Qualys Patch Report then Run from the Quick Actions menu.

## Policy Compliance

The latest Policy Compliance data is available in your Qualys account at all times from scans performed by the cloud agent platform. You'll see agent hosts listed on the Host Assets tab with the tracking method Agent.

**Host Information 10.11.65.244**

Launch Help

The following is a list of policies with controls that have been evaluated for this host.

**View Report Title** **Controls Passed** **Controls Failed**

CIS Benchmark for Microsoft Windows Server 2012 R2, v1.1.0, [Scored, Member Server] v.1.0	66	113
---	----	-----

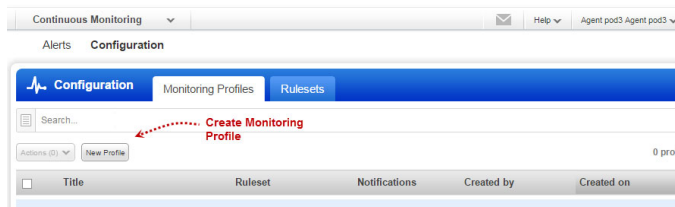
**General Information** > **Comments** > **Vulnerabilities** > **Tickets** > **Business Units** > **Users** > **Asset Groups** > **Compliance** > **Exceptions** > **Authentication** > **Certificates** > **Action Log** >

Once a full scan is complete, the Compliance section shows you a list of policies with controls that have been evaluated for this host.

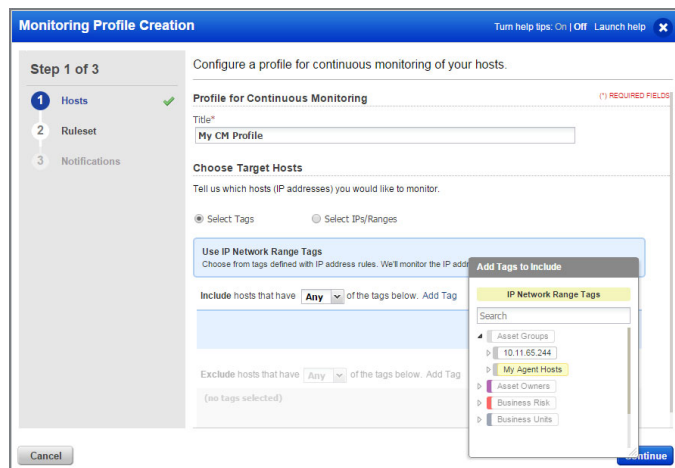
- Create PC reports on agent hosts with up to the minute asset data as needed, or schedule them to run at a convenient time.
- Download the latest Individual Host Compliance Report (pdf) from the Host Information.
- Select the Cloud Agent tag for the target to report on agent hosts in your account.

## Continuous Monitoring

Using Continuous Monitoring you'll be alerted within minutes of a change happening on an agent host, just like any other host in your subscription. Here's a quick way to get started.

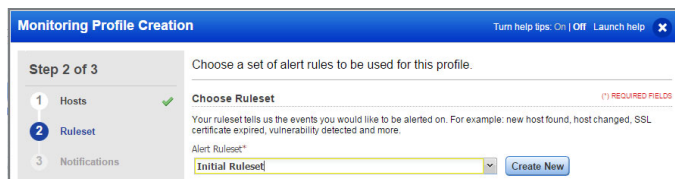


Go to Configuration > Monitoring Profiles and select New Profile

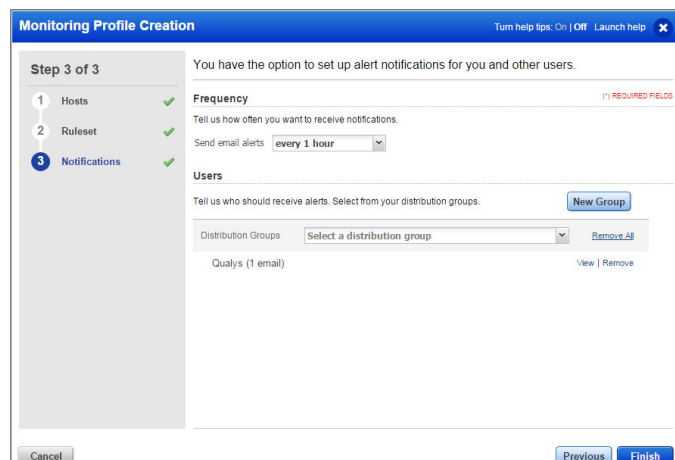


Choose agent hosts by selecting tags or IPs/Ranges.

Tip - Select from IP network range tags in your account (like a custom asset group, a business unit, or a custom tag defined using AssetView).



We recommend the Initial Ruleset to get started. (You can customize this now, or do it later)



Set up notification options - frequency and distribution group (be sure to include yourself).

That's all there is to it! You'll start getting alerts on your agent hosts. At any time you can update the ruleset or profile to change what you'll be alerted on and when.