Cloud Agent
Getting Started Guide

December 22, 2017
## Contents

### About this Guide
- About Qualys................................................................. 4
- Qualys Support................................................................. 4

### Get Started
- Overview ................................................................................. 5
- What do I need to know?....................................................... 5
- Cloud Agent Platform Availability Matrix ............................. 7
- Cloud Agent Platform Windows Hotfixes Needed .................. 11
- It’s easy to install agents...................................................... 12
- Installing agents in AWS....................................................... 15
- We’re syncing asset data to the cloud!................................. 15
- Continuous scanning in the cloud........................................ 16

### Manage Your Agents
- A quick look at your agents............................................... 17
- Tell me about agent status................................................... 18
- View activation job progress............................................... 19
- Easily view current Asset Details........................................ 21
- Take bulk actions on agents............................................... 22
- Change configuration.......................................................... 22
- Tagging agent hosts............................................................ 23
- Looking for agent files?...................................................... 24

### Using Qualys Cloud Suite
- Vulnerability Management (VM).......................................... 25
- Policy Compliance (PC)......................................................... 28
- Continuous Monitoring (CM)............................................... 29
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 with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations 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, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit [www.qualys.com](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 Suite 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.

We recommend these resources

- Cloud Agent Platform Introduction (2m 10 s)
- Getting Started Tutorial (4m 58s)
- Qualys Cloud Platform
Get Started
What do I need to know?

Cloud Agent requirements
- We support these systems: Windows, Linux/Unix (.rpm), Linux (.deb), 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, 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 and/or PC). 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.
### Cloud Agent Platform Availability Matrix

**Windows | Linux | Unix | Apple Mac**

#### Windows

Current Release: 1.6.0.246, 2.0.2.192*

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

*Current release for customers with FIM and/or IOC enabled

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Supported Platforms</th>
<th>Operating System</th>
<th>Arch</th>
<th>Installer</th>
<th>Inventory</th>
<th>VM</th>
<th>PC</th>
<th>FIM</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Windows XP SP 3+</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Vista</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 7</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 8/8.1</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 10</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2003 SP2+</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2008/R2*</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2012/R2*</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>1.4.5.232-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows Server 2016*</td>
<td>x86_64 for 1.6</td>
<td>(exe)</td>
<td>1.5.6.46-1.6.2.19, 2.0.2.192</td>
<td>1.5.6.46-1.6.2.19, 2.0.2.192</td>
<td>1.5.6.46-1.6.2.19, 2.0.2.192</td>
<td>2.0.2.192</td>
<td>2.0.2.192</td>
<td></td>
</tr>
</tbody>
</table>

*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: 1.6.0.61, 2.0.2.79*

End-of-Support versions: 1.3.3.23, 1.3.1.16

*Current release for customers with FIM enabled

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Operating System</th>
<th>Arch</th>
<th>Installer</th>
<th>Inventory</th>
<th>VM</th>
<th>PC</th>
<th>FIM</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat</td>
<td>Red Hat Enterprise Linux 5.4x</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>2.0.2.79 not available</td>
<td></td>
</tr>
<tr>
<td>Red Hat</td>
<td>Red Hat Enterprise Linux 6, 7</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>2.0.2.79 not available</td>
<td></td>
</tr>
<tr>
<td>Red Hat</td>
<td>CentOS 5.4+</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>2.0.2.79 not available</td>
<td></td>
</tr>
<tr>
<td>Red Hat</td>
<td>CentOS 6, 7</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>2.0.2.79 not available</td>
<td></td>
</tr>
<tr>
<td>Red Hat</td>
<td>Fedora 22, 23, 24</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>SUSE</td>
<td>SUSE Linux Enterprise 11, 12</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>SUSE</td>
<td>OpenSUSE 12</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>SUSE</td>
<td>OpenSUSE 13</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>SUSE</td>
<td>OpenSUSE Leap 42.1</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>Amazon Linux 2015.09</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>Amazon Linux 2016.09</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>Amazon</td>
<td>Amazon Linux 2017.03</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>not available</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Enterprise Linux 5.11</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>2.0.2.79 not available</td>
<td></td>
</tr>
</tbody>
</table>
## IBM AIX

**Current Release:** 1.6.2

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Operating System</th>
<th>Arch</th>
<th>Installer</th>
<th>Inventory</th>
<th>VM</th>
<th>PC</th>
<th>FIM</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM AIX</td>
<td>AIX 7.1 TL2, TL3, TL4 AIX 7.2 TL1 (Standard and Enterprise Editions)</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.6.2</td>
<td>1.6.2</td>
<td>1.6.2</td>
<td>not available</td>
<td>not available</td>
</tr>
<tr>
<td>IBM AIX</td>
<td>AIX 6.1 TL0-9 (Standard and Enterprise Editions)</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.6.2</td>
<td>1.6.2</td>
<td>1.6.2</td>
<td>not available</td>
<td>not available</td>
</tr>
</tbody>
</table>

## Apple Mac

**Current GA Release:** 1.6.0.61

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Operating System</th>
<th>Arch</th>
<th>Installer</th>
<th>Inventory</th>
<th>VM</th>
<th>PC</th>
<th>FIM</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>OS X Yosemite (10.10)</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61</td>
<td>1.5.0.61-1.6.0.61</td>
<td>not available</td>
<td>not available</td>
</tr>
<tr>
<td>Apple</td>
<td>OS X El Capitan (10.11)</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.5.0.61-1.6.0.61, 2.0.2.79</td>
<td>1.5.0.61-1.6.0.61</td>
<td>1.5.0.61-1.6.0.61</td>
<td>not available</td>
<td>not available</td>
</tr>
</tbody>
</table>
Get Started
Cloud Agent Platform Availability Matrix

* Upgrading from El Capitan (10.11) to Sierra (10.12) will delete needed directories used by the agent, causing the agent to not start. Use the following commands to fix the directory.
  1) mkdir /var/log/qualys
  2) chmod 640 /var/log/qualys
  3) if non-root: chown non-root.non-root-group /var/log/qualys
  4) /Applications/QualysCloudAgent.app/Contents/MacOS/qagent_restart.sh

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Operating System</th>
<th>Arch</th>
<th>Installer</th>
<th>Inventory</th>
<th>VM</th>
<th>PC</th>
<th>FIM</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>macOS Sierra (10.12)*</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.6.0.61</td>
<td>1.6.0.61</td>
<td>1.6.0.61</td>
<td>not available</td>
<td>not available</td>
</tr>
<tr>
<td>Apple</td>
<td>macOS High Sierra (10.13)</td>
<td>x86_64</td>
<td>(.rpm)</td>
<td>1.6.0.61</td>
<td>1.6.0.61</td>
<td>1.6.0.61</td>
<td>not available</td>
<td>not available</td>
</tr>
</tbody>
</table>
Cloud Agent Platform Windows Hotfixes Needed

The following hotfixes are required to successfully install Windows Agent

Windows XP SP3 x86 SHA2 Cert Hotfix
KB Article Number: 968730
Language: English
Platform: i386
Location:

Windows XP SP3 x86 SHA2 Cert Hotfix
KB Article Number: 968730
Language: English
Platform: i386
Location:

Windows XP x64 & Windows Server 2003 x64 SP3 SHA2 Cert Hotfix
KB Article Number: 968730
Language: English
Platform: x64
Location:
http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375531_ENU_x64_zip.exe

KB Article Number: 968730
Language: English
Platform: i386
Location:

Microsoft KB Article to request additional hotpatches for this fix:
Get Started
It’s easy to install agents

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 users.

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.

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.
Get Started
It’s easy to install agents

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

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.

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

Installation Guides: Windows Agent | Linux Agent | Unix Agent | Mac Agent
Installing agents in AWS

Please follow the installation steps provided at the link below.

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). Select 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.

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.

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.
Manage Your Agents

A quick look at your agents

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 you agent assets.
**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
- 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.

View activation job progress

Once you initiate activation of agents, it may take some time for agents to get activated. You can easily check the progress of activation jobs.

Just go to your agents list and click Activation Jobs.
You’ll see a list of activation jobs that have been initiated. While a job is in progress you can choose to Stop/Cancel the activation (and activate later if you wish).
Easily view current Asset Details

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).

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.
Manage Your Agents
Take bulk actions on agents

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.

Tip - Double click Initial Profile to view the default settings provided by Qualys
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, Unix Agent, Mac Agent

/etc/init.d/qualys-cloud-agent
/etc/qualys/cloud-agent/qagent-log.conf
/var/log/qualys/qualys-cloud-agent.log
/usr/local/qualys/cloud-agent/*  //Linux, Unix
/Applications/QualysCloudAgent.app/*  //MacOS

Still need help? Click here to troubleshoot.
Using Qualys Cloud Suite

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

Our Qualys Cloud Suite applications - VM, PC, AV, CM - 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 Cloud Suite 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 (VM)

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.
Using Qualys Cloud Suite
Vulnerability Management (VM)

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.

How do I run this report?
Go to VM > Reports > Templates, select the High Severity Report and then Run from the Quick Actions menu.
Using Qualys Cloud Suite
Policy Compliance (PC)

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.

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

Policy Compliance (PC)

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.

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

You can 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.
- Create custom PC reports from the Reports tab using templates (Qualys provided and custom).
- Select the Cloud Agent tag for the target to report on agent hosts in your account.
Continuous Monitoring (CM)

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 the Asset Management application).

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.