Cloud Agent for Windows

Installation Guide

Agent Version 1.4 - 1.6, 2.0.2

December 22, 2017

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

CONTENTS

Preface

Welcome to Qualys Cloud Agent for Windows. This user guide describes how to install cloud agents on hosts in your network.

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 a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact 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/.

CHAPTER 1

Get Started

Thank you for your interest in Qualys Cloud Agent!

This document tells you all about installing Qualys Cloud Agent for Windows. We'll tell you about Requirements, Installation Steps, Proxy Support, Certificate Supports, Anti-Virus and HIPS Exclusion / Whitelisting, Best Practices and more.

Qualys Cloud Agent Introduction

Qualys Cloud Platform gives you everything you need to continuously secure all of your global IT assets. Now with Qualys Cloud Agent, there's a revolutionary new way to help secure your network by installing lightweight cloud agents in minutes, on any host anywhere - such as laptop, desktop or virtual machine.

Watch the overview for an introduction.

Videos from the Qualys Community

Cloud Agent Platform Introduction (2m 10s)

Getting Started Tutorial (4m 58s)

Get informed quickly about Qualys Cloud Agent (CA)..

Learn more from the Qualys Community

CA Platform Announcement

Getting Started Guide

Cloud Agent Platform Availability for 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

Supported Platforms				Supported Qualys Modules/Agent Versions				
Vendor	**Operating System**	**Arch**	**Installer**	**Inventory**	**VM**	**PC**	**FIM**	**IOC**
Microsoft	Windows XP SP 3+	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Vista	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 7	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 8/8.1	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows 10 (1511, 1607, 1703, 1709)	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2003 SP2+	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2008/R2*	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2012/R2*	x86_64 for 1.6 x86_32 for previous	(.exe)	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	1.4.5.232-1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192
Microsoft	Windows Server 2016*	x86_64 for 1.6 x86_32 for previous	(.exe)	1.5.6.46 1.6.2.19, 2.0.2.192	1.5.6.46 1.6.2.19, 2.0.2.192	1.5.6.46 1.6.2.19, 2.0.2.192	2.0.2.192	2.0.2.192

*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

A few things to know...

Cloud Agent requirements

- Your hosts must be able to reach your Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Log into the Qualys Cloud Platform and go to Help > About to see the URL your hosts need to access.

- To install Cloud Agent for Windows, you must have Local administrator privileges on your hosts. Proxy configuration is supported. Learn more

What are the installation steps?

Our Cloud Agent UI walks you through the steps to install agents on your hosts. Once the agent is installed you will need to provision it using our agent configuration tool.

Get help with troubleshooting

We recommend you inspect the agent's log file 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

You'll also find helpful information in Qualys online help.

Qualys Help

Troubleshooting

Error messages

CHAPTER 2

Installation

It's easy to install Cloud Agent for Windows. We'll walk you through the steps quickly.

Keep in mind - Depending on your environment, you might need to take steps to support communications between agent hosts on your network and the Qualys Cloud Platform.

Tips and best practices

What is an activation key? You'll need an agent activation key to install agents. This provides a way to group agents and bind them to your subscription with Qualys Cloud Platform. You can create different keys for various business functions and users.

Benefits of adding asset tags to an activation key Tags assigned to your activation key will be automatically assigned to agent hosts. This helps you manage your agents and report on agent hosts.

Running the agent installer You'll need to run the installer from an elevated command prompt, or use a systems management tool.

Be sure to activate agents to provision agents for modules - Vulnerability Management (VM), Policy Compliance (PC), or both. Activating an agent for a module consumes an agent license. You can set up auto activation by defining modules for activation keys, or do it manually in the Cloud Agent UI.

What happens if I skip activation? Agents will sync inventory information only to the cloud platform (IP address, OS, DNS and NetBIOS names, MAC address), host assessments will not be performed.

How many agents can I install? You can install any number of agents but can activate an agent only if you have a license. The Agents tab in the Cloud Agent UI tells you about your installed agents.

Check to be sure agents are connected Once installed agents immediately connect to the Qualys Cloud Platform and register themselves. You can see agent status on the Agents tab - this is updated continuously. If your agent doesn't have a status, it has not successfully connected to the cloud platform and you need to troubleshoot.

Cloud Agent Platform Windows hotfixes needed

The following hotfixes are required to install Windows Agent

Windows XP SP3 x86 SHA2 Cert Hotfix
KB Article Number: 968730
Language: English
Platform: i386
Location:
http://hotfixv4.microsoft.com/Windows%20XP/sp4/Fix251294/2600/free/375554_ENU_i386_zip.exe

Windows XP SP3 x86 SHA2 Cert Hotfix
KB Article Number: 968730
Language: English
Platform: i386
Location:
http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375510_ENU_i386_zip.exe

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

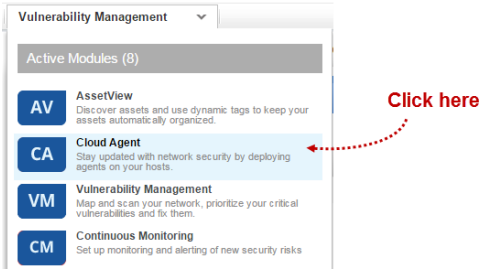
KB Article Number: 968730
Language: English
Platform: i386
Location:
http://hotfixv4.microsoft.com/Windows%20Server%202003/sp3/Fix262679/3790/free/375510_ENU_i386_zip.exe
Microsoft KB Article to request additional hotpatches for this fix:
http://support2.microsoft.com/hotfix/KBHotfix.aspx?kbnum=968730&kbln=en-US

How to download Agent image

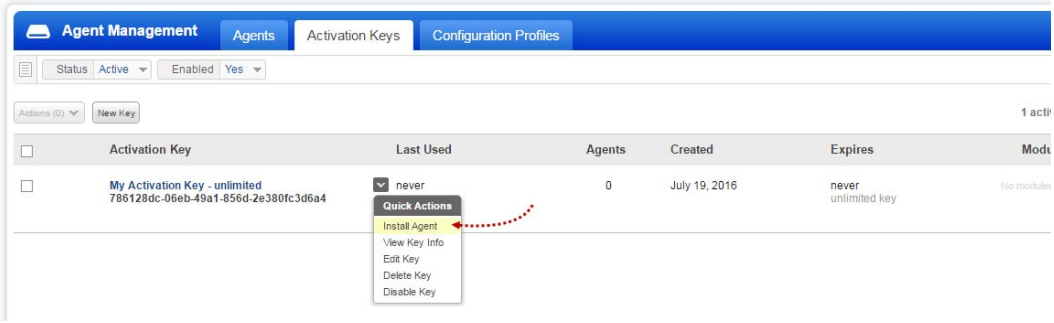
Download an image of Qualys Cloud Agent for Linux

Here's how to download an image from the Qualys Cloud Platform and get the associated Activation ID and Subscription ID.

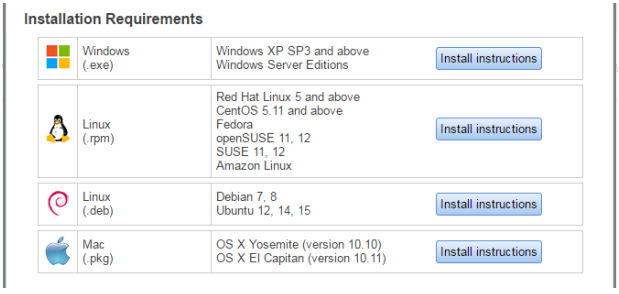
Log into the Qualys Cloud Platform and select **CA** for the Cloud Agent module.



Choose an activation key (create one if needed) and select **Install Agent** from the Quick Actions menu.



Click **Install instructions** next to Windows (.exe).



What happens? The Agent image is downloaded to your local system, and in the UI you'll see the associated Activation key ID and Subscription ID - copy and paste this to a safe place, you'll need it to complete the installation.

Installation steps

What you'll need

To install cloud agents, you'll need to download the Cloud Agent image and get the associated ActivationID and CustomerID. Just log into the Qualys Cloud Platform, go to the Cloud Agent (CA) module, and follow the installation steps for Windows (.exe) to get everything you need.

Cloud Agent requirements

Steps to install Agents

Copy the Qualys Cloud Agent image onto the host you want to monitor, and run the command or use group policy or a systems management tool.

```
> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
```

What happens next?

We'll start syncing asset data to the cloud!

Once installed an agent immediately connects to the Qualys Cloud Platform and registers itself. We would expect you to see your first asset discovery results within a few minutes. The first assessment scan in the cloud takes some time, after that scans complete as soon as new host metadata is uploaded to the cloud platform.

You might also be interested in...

Proxy Configuration

Certificate Support

Anti-Virus and HIPS Exclusion / Whitelisting

Certificate Support

Qualys Cloud Platform certification uses SHA2-512. Windows XP and Windows Server 2003 do not include SHA2 support by default so you must install a SHA2 hotfix on these systems, otherwise certification will fail.

Download the SHA2 hotfix you need

Windows XP SP3 x86 SHA2 Cert Hotfix

Windows Server 2003 SHA2 Cert Hotfix

Windows XP x64 & Windows Server 2003 x64 SP2 SHA2 Cert Hotfix

Get more information

Microsoft KB Article on SHA-256 support

Microsoft Developer Troubleshooting help

Anti-Virus and HIPS Exclusion / Whitelisting

Have Anti-Virus or HIPS software installed? It's required that the following files, directories, and processes are excluded or whitelisted in all security software installed on the system in order to prevent conflicts with the Cloud Agent.

Agent processes

QualysAgent.exe - this is the Qualys endpoint service

setup.exe - non-MSI installer needs access to disk and registry locations (see below)

uninstall.exe - this is the Qualys endpoint service uninstaller - needs r/w/d access to following disk and registry locations

File whitelisting

%PROGRAMDATA%\Qualys\QualysAgent - we read/write/create/delete files in this directory and sub-directories

%ProgramFiles(x86)%\Qualys\QualysAgent - this is where the service and uninstall live. The service will create processes so HIPS needs to make sure to unblock this action

For version 2.0.2, on x64 systems, the agent is located at:

%ProgramFiles%\Qualys\QualysAgent

Registry whitelisting

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\QualysAgent - this is where the agent setup installs the service into the system.

HKEY_LOCAL_MACHINE\SOFTWARE\Qualys - this is where breadcrumb information lives to merge agent and appliance scanner results. The agent needs c/r/w/d access here; setup needs to create the key; uninstall needs ability to delete the key.

QualysAgent.exe

Calls CreateProcess to launch external proceses on occasion

Calls CoCreateInstance to instantiate COM objects

Creates/Reads/Writes/Deletes files out of its programdata directory

Creates/Reads/Writes/Deletes from the hklm\software\qualys registry key

Enumerates and reads from all file and registry locations

Uninstalling Cloud Agent

Uninstalling the agent from the Cloud Agent module UI or API

When you uninstall a cloud agent using the Cloud Agent module user interface or Cloud Agent API, the agent and license is removed from the Qualys subscription. We'll also purge the associated agent host record and scan results for any licensed modules, i.e. Vulnerability Management, Policy Compliance.

Uninstalling the agent from the host itself

When you uninstall a cloud agent the agent from the host itself using the Uninstall utility, the agent, its license usage, and scan results are still present in the Qualys subscription. In order to remove the agent's host record, license, and scan results use the Cloud Agent module user interface or Cloud Agent API to uninstall the agent.

The setting Force=True is optional. This removes the registry keys and agent UUID from the host. If an agent is later re-installed on that host a new agent UUID is created (the old one is not used).

Sample Uninstall agent commands

For 32 bit machine:

"%programfiles%\qualys\qualysagent\uninstall.exe" Uninstall=True Force=True

For 64 bit machine:

"%programfiles(x86)%\qualys\qualysagent\uninstall.exe" Uninstall=True Force=True

CHAPTER 3

Proxy Configuration

Our lightweight QualysProxy tool lets you configure proxy settings for Windows Agent (available with Windows Agent 1.2 and later). This tool stores proxy information in a Qualys owned registry path that is ACL'd to SYSTEM and Administrators. Authentication credentials are encrypted and used by the agent.

QualysProxy lets you:

- Configure proxy username and password credentials

- Configure PAC file URLs for cases when WPAD is not available

- Configure a private proxy URL that the Agent communicates through

Proxy configurations prior to Windows Agent 1.2

The QualysProxy tool replaces "netsh winhttp" usage. Setting the agent proxy using "netsh winhttp" will no longer work. Installations that previously used "netsh winhttp" (1.1 and older) will need to have proxy configuration set again by using the QualysProxy tool. This is to ensure that the agent does not inadvertently inherit proxy settings previously intended for other purposes.

What do I need to know?

Tell me about installation The QualysProxy tool, and proxy tool updates, are downloaded to the cloud agent whenever the agent is self-patched. The tool is also distributed in the agent setup when manually installed. You'll find the tool here:

On all 1.x builds on x86 systems, the QualysAgent program path is located at:

```
C:\Program Files\Qualys\QualysAgent\QualysProxy.exe
```

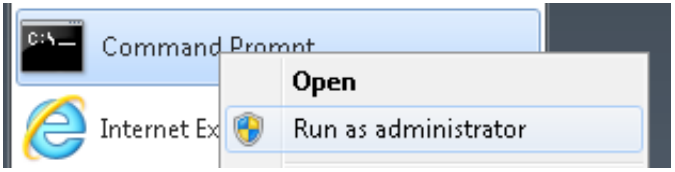
On all 1.x builds on x64 systems, the QualysAgent program path is located at:

```
C:\Program Files (x86)\Qualys\QualysAgent\QualysProxy.exe
```

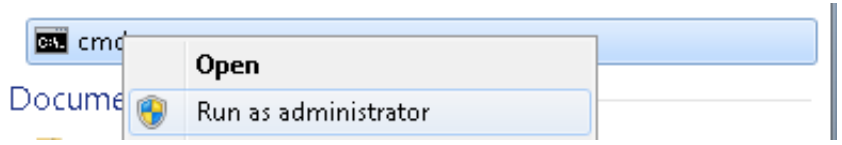
On all 2.x builds on x86 and x64 systems, the QualysAgent program path is located at:

```
C:\Program Files\Qualys\QualysAgent\QualysProxy.exe
```

Run from elevated prompt The proxy tool must be run from an elevated command prompt by right clicking the command prompt start menu item:



… or by typing cmd into the Search/Run start menu edit control and right clicking on the cmd.exe menu item:



Support for systems management software The command line interface (CLI) tool is designed to be used in shell scripts executed by systems management software. When execution of the tool completes, the ERROR_LEVEL will be set to 0 (zero) on success, and non-zero on error. No window'd UI is displayed to the user.

Changes made through the proxy tool happen automatically and there's no need to restart the agent service. Changes can be verified by inspecting the Agent's log.txt file:

```
C:\ProgramData\Qualys\QualysAgent
```

On XP and Windows Server 2003, the Agent's log.txt file is located here:

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

All connection errors will be logged and proxy configuration archived each time the Agent attempts to communicate with the cloud.

QualysProxy syntax

QualysProxy [/u <proxy url> [/n <proxy username>] [/p <proxy password] [/a <PAC file url>]] | [/d]

Option	Description
/u	Proxy URL. If set, do not set /x option.
/n	Username used to access proxy. If set, /u option must be set.
/p	Password used to access proxy. If set, /u option must be set.
/a	URL path to PAC file for proxy auto-configuration. If set, do not set /u option.
/d	Deletes all Qualys cloud agent proxy settings.

Notes

If any argument contains spaces, please surround that argument with quotes.

If any argument contains a " character, precede that character with a backslash '\'.

Use cases

Example 1 – Set proxy and port number

The following example shows how to set a proxy and port number:

```
QualysProxy /u http://my-proxy:12345
```

Example 2 – Set proxy and credentials

The following examples shows hot to set a proxy (default port: xxx) along with proxy credentials:

```
QualysProxy /u http://my-proxy /n ProxyUsername /p ProxyPassword
```

Example 3 – Tell agent to use PAC file

The following example shows how to tell the cloud agent to use a PAC file directly in lieu of allowing it to be found through WPAD:

```
QualysProxy /a http://my-pac-file-server/QualysAgent.pac
```

Example 4 – Specify credentials for use with PAC file

The following example shows how to specify credentials for use with a PAC file. The credentials will get passed to the resulting proxy URL:

```
QualysProxy /n ProxyUsername /a ProxyPassword /a http://my-pac-
file-server/QualysAgent.pac
```