



Cloud Agent for Windows

Installation Guide

April 26, 2024

Copyright 2016-2024 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

Preface	5
About Qualys	5
Contact Qualys Support	5
Get Started	6
Qualys Cloud Agent Introduction	6
Cloud Agent Platform Availability Matrix	6
A few things to know... ..	6
Cloud Agent requirements	6
What are the installation steps?	7
Get help with troubleshooting	8
Installation	9
Tips and best practices	10
Microsoft Windows hotfixes needed	10
Microsoft Windows security updates needed	11
TLS version needed	11
How to download the Agent installer	12
Installation steps for exe based package	13
What you'll need	13
Steps to install Agents	13
Steps to Install Agent with Proxy Support	14
Steps to install Agent on Golden Image	14
Installation steps for msi based package	14
What you'll need	14
What happens next?	15
You might also be interested in... ..	15
Certificate Support	16
Certificate Updates	16
Anti-Virus and HIPS Exclusions	16
Upgrading the Cloud Agent	18
Uninstalling the Cloud Agent	18
Qualys Self-Protection Feature for Cloud Agent	20
Disable Self-Protection	20
Steps to Disable Self-Protection for a Cloud Agent	21
Uninstalling Cloud Agent with Self Protection	22
Cloud Agent Health Check Tool	23
Agent Health Status Evaluation	23
Agent Health Status Report	23
Proxy Configuration	27

What do I need to know?	27
QualysProxy syntax	28
Multiple Proxy Server support in Proxy URL and PAC Files (Windows Agent 3.1 or later)	29
Use cases	30
Cloud Agent Preparation for Cloning / Gold Image	32
Scan on Demand and Scan on Startup	34
Registry Configuration	35
Deployment using Microsoft Intune.....	38
Deployment using exe Package File	38
Create .intunewin Package	38
Add App Information	40
Set Program Information	41
Set Requirements	42
Set Detection Rule	43
Scope tags	44
Assignments	45
Review + create	46
Deployment using msi Package	47
Download the Cloud Agent Package	47
Extract the msi Package File	47
Deploy the msi Package File	47

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. 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.

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/.

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 Exclusions, 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.

Get informed quickly on Qualys Cloud Agent (CA).

Video Tutorials

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

[Getting Started Tutorial \(6m 34s\)](#)

[Installing MSI Based Package](#)

Cloud Agent Platform Availability Matrix

For the most current list of supported cloud agents with versions and modules on the Qualys Cloud Platform, please refer to the following article: [Cloud Agent Platform Availability Matrix](#)

[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 or Domain administrator privileges on your hosts. Proxy configuration is supported. To learn more, refer [Proxy Configuration](#).

Hardware Requirements

For Cloud Agent Windows, the following are minimum system requirements:

- 512 MB of RAM for scan-based features such as Inventory, Vulnerability Management (VM), and Policy Compliance (PC).
- 1 GB of RAM for File Integrity Monitoring (FIM) and Patch Management (PM).
- For system requirements with Endpoint Detection and Response (EDR), refer [Qualys EDR Onboarding Guide](#).
- Minimum 200 MB of available disk space.

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

Note: Due to security permissions, it may not be possible to access the QualysAgent folder directly. Copy the QualysAgent folder to another location to inspect the log files.

Log files

For each module, the Cloud Agent creates a separate log inside the C:\ProgramData\Qualys\QualysAgent\Log directory.

If you face any issues while installing or uninstalling Cloud Agent (version 4.5 and later), refer following log files under the %ProgramData%/Qualys/QualysAgent folder:

- the CloudAgentInstaller.log file
- the MsiLog_TimeStamp.log file generated by MSI

Note: If the Cloud Agent log directory—%ProgramData%/Qualys/QualysAgent” or the log file are not accessible, the log files are created at C:\Windows\Logs\QualysAgent.

Modify the Log Level

You can enable debug-level logging for Agent by setting the registry value. In the Registry Key - HKEY_LOCAL_MACHINE\SOFTWARE\Qualys\QualysAgent\Logs, create an entry with the following values:

- Data Type - DWORD (32-bit)
- Value name - TraceLevel
- Value data - 6

Restart the Cloud Agent service to enable the Agent to start logging the debug messages in all the log files.

Note: The value set in the registry key takes precedence over the value in the config.db file.

Learn more

[Troubleshooting](#)

[Error messages](#)

Installation

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

Qualys provides installers and packages coded for each supported operating system. It's not possible to use an agent coded for one platform on another platform. You can use software distribution tools like SCCM, Intune, BigFix, rpm, Casper, etc to install the agent onto target machines. You can install Cloud Agent into gold images including VM templates and cloud provider images such as Amazon AWS, Microsoft Azure, and Google Compute Platform.

Qualys Platform supports detection of duplicate agent IDs and automatically re-provisions the duplicate agents. Refer to [Cloud Agent Preparation for Cloning / Gold Image](#) for information on how to install an agent into a gold image without initial provisioning. This is the recommended method to prevent duplicate asset records.

If you are using software distribution tools, ensure that you package the Qualys-provided installer along with the specific Activation Key and Customer ID strings. Do not package up the artifacts that are installed by the agent into your own installer as the installation environment is keyed for that specific machine when the agent is installed. Including these artifacts will create duplicates that the platform may not be able to easily de-duplicate.

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](#)

[Microsoft Windows hotfixes needed](#)

[Microsoft Windows security updates needed](#)

[TLS version needed](#)

[How to download the Agent installer](#)

[Installation steps for exe based package](#)

[Proxy Configuration](#)

[Certificate Support](#)

[Anti-Virus and HIPS Exclusions](#)

[Upgrading the Cloud Agent](#)

[Uninstalling the Cloud Agent](#)

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 for any modules licensed in your subscription - Vulnerability Management (VM), Policy Compliance (PC), File Integrity Monitoring (FIM), Endpoint Detection and Response (EDR), or Patch Management (PM). Activating an agent for a module consumes a module 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 application activation? Agents will sync inventory information only to the cloud platform (IP address, OS, DNS, NetBIOS names, MAC address, installed software).

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

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

What is default startup type of the Qualys Cloud Agent service? The Startup type is set to **Automatic (Delayed Start)** for the Qualys Cloud Agent service.

Microsoft Windows hotfixes needed

The following hotfixes are required for the Cloud Agent to run and connect to the Qualys Platform from older Windows operating systems.

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.

To acquire these hotfixes contact Microsoft Support.

Microsoft Windows security updates needed

Install Windows Security Updates [KB4474419](#) Microsoft and restart the system to load the Qualys Cloud Agent drivers successfully on Windows 7 SP1 and Windows Server 2008 R2 SP1 and SP2.

For details, see [Microsoft Support document](#).

TLS version needed

Ensure that TLSv1.2 or later is enabled on client machines to communicate with Qualys Cloud Platform.

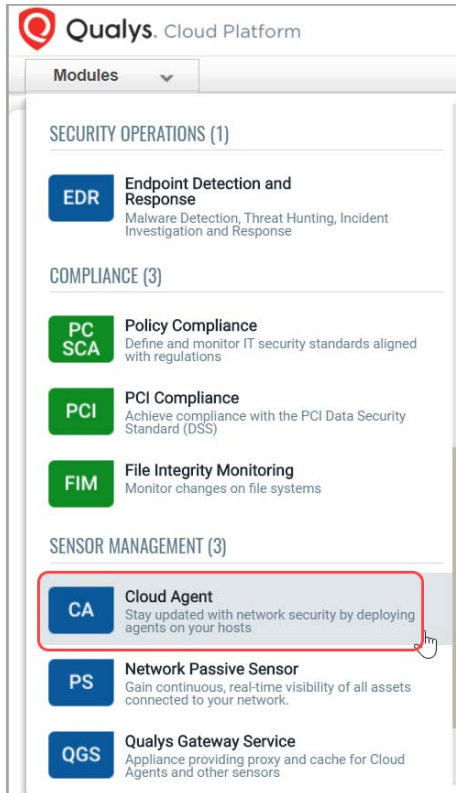
Cloud Agent for Windows uses cryptographic protocol support provided by the Windows operating system. Older Windows operating systems (including Windows XP, Embedded Standard, Server 2003/SP2, Server 2008/SP1/SP2, and potentially others if explicitly configured) do not have TLS 1.2 support on the operating system for Cloud Agent to use.

For more information, refer to [Deprecating TLSv1.0 and TLSv1.1](#).

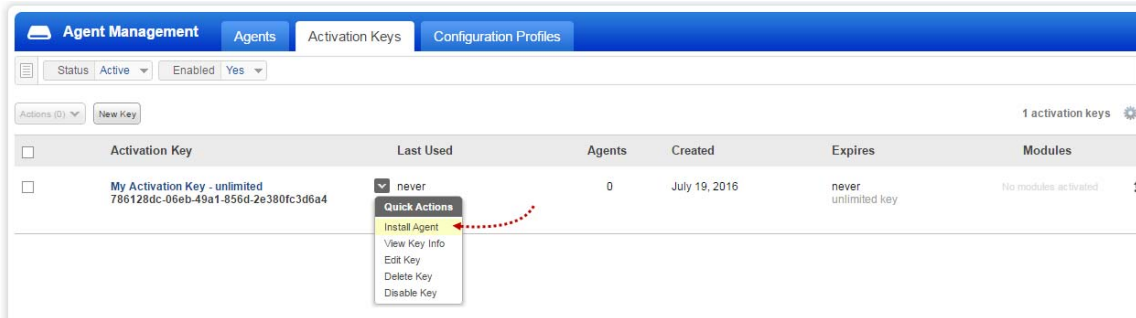
How to download the Agent installer

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

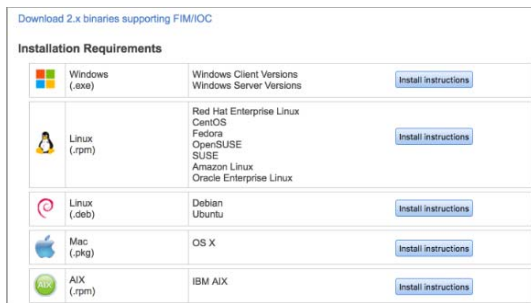
Log into the Qualys Cloud Platform and select **CA** for the Cloud Agent module.








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



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



Download 2.x binaries supporting FIM/IOC		
Installation Requirements		
 Windows (.exe)	Windows Client Versions Windows Server Versions	Install instructions
 Linux (.rpm)	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Amazon Linux Oracle Enterprise Linux	Install instructions
 Linux (.deb)	Debian Ubuntu	Install instructions
 Mac (.pkg)	OS X	Install instructions
 AIX (.rpm)	IBM AIX	Install instructions

What happens? The Agent installer is downloaded to your local system, and in the UI you'll see the associated Activation key ID and Customer ID - copy and paste this to a safe place, you'll need it to complete the installation manually or through software distribution tools.

Note: If you use GoldenImage parameter as 'True', it will install the agent in a non-running state so that it will not generate a HostID. HostID generation and provision happens on the next agent start.

Installation steps for exe based package

What you'll need

To install cloud agents, you'll need to download the Cloud Agent installer 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 installer onto the host where you want to install the agent, and run the command or use a systems management tool to install the agent as per your organization's standard process to install software.

```
> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/
```

Steps to Install Agent with Proxy Support

You can provide default proxy configuration as an argument at the time of agent installation. The proxy parameters can be passed through the Proxy argument, where, Proxy="<argument-to-pass>". The proxy argument contains proxy URL, corresponding user name and password.

```
QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <proxy url> /n <proxy username> /p <proxy password>"
```

You can also pass multiple proxies, separated by semi-colon, as an argument during agent installation.

```
QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <1st proxy url>;<2nd proxy url> /n <proxy username> /p <proxy password>"
```

Note: Multiple proxy user names and proxy passwords are not supported.

Steps to install Agent on Golden Image

If the GoldenImage=true is passed as a parameter during installation, the agent will be installed in a non-running state, hence, without the HostID in the registry. The agent is started after the machine reboots or the agent service is manually started, and then, the HostID would be generated by the agent.

Run the command or use a systems management tool to install the agent into Golden image as per your organization's standard process to install software.

```
> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ GoldenImage=true
```

For more information on deployment, see [Cloud Agent Preparation for Cloning / Gold Image](#).

Installation steps for msi based package

What you'll need

To install cloud agents, you'll need to download the Cloud Agent installer 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](#)

Extracting MSI Package

To extract MSI from the downloaded exe file, run the following command:

```
QualysCloudAgent.exe ExtractMSI=<value>
```

For ExtractMSI, use following values (*value*) as per host architecture.

For example, if you want to install cloud agent on 64-bit machine, you need to extract MSI package with value for ExtractMSI=64.

- **32**: Extracts 32-bit MSI Installer
- **64**: Extracts 64-bit MSI Installer
- **BOTH**: Extracts both (32-bit and 64-bit) the MSI Installers
- **AUTO**: Extracts the appropriate MSI based on the OS architecture. It extracts 32-bit MSI on a 32-bit machine and 64-bit MSI on a 64-bit machine

The MSI file will be extracted in the same directory where exe file is available.

Installing MSI Package

Copy the Qualys Cloud Agent installer onto the host where you want to install the agent, and run the command or use a systems management tool to install the agent as per your organization's standard process to install software. Following is the sample command for installing MSI package for 32-bit installer:

```
Msiexec.exe /i CloudAgent_x86.msi CustomerId={12345678-1234-1234-1234-123456789012} ActivationId={12345678-1234-1234-1234-123456789012} WebServiceUri=<platform_url>/CloudAgent/
```

Here CloudAgent_x86.msi is extracted MSI file for 32-bit installer.

What happens next?

We'll start syncing asset data to the cloud!

Once installed an agent connects to the Qualys Cloud Platform and provisions itself. The agent will download its associated Configuration Profile (and follow any settings defined), download manifests for any activated modules, and start collecting asset metadata for each module to send to the Qualys Cloud Platform.

You might also be interested in...

[Proxy Configuration](#)

[Certificate Support](#)

[Anti-Virus and HIPS Exclusions](#)

Certificate Support

Qualys Cloud Platform certification uses SHA-256. 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. Check [Microsoft Windows hotfixes needed](#) section.

For more information, see [Microsoft KB Article on SHA-256 support](#)

Microsoft Windows Security Updates are required to load Qualys Cloud Agent drivers on Windows 7 SP1 and Windows Server 2008 R2 SP1 and SP2. Check [Microsoft Windows security updates needed](#) section.

Certificate Updates

DigiCert has provided a new certificate for timestamping that is signed with a different certificate authority (CA) than the earlier version. The new CA name is 'DigiCert Trusted Root G4'.

If you encounter an error - 'Error: Patch: Failed to validate the signature of PE binary file...statusHandler.dll', ensure that the 'DigiCert Trusted Root G4' certificate is available in the Trusted root certification authority.

If the certificate is not available, use one of the following ways to update the certificate:

- using active directory - To update the certificate using active directory, follow the procedure detailed in [Distribute Certificates to Client Computers by Using Group Policy](#) using the [certificate link](#).

- manual update- If you are connected to internet, use the following command to update the certificate manually:

```
certutil -urlcache -f
http://cacerts.digicert.com/DigiCertTrustedRootG4.crt
DigiCertTrustedRootG4.crt
certutil -addstore -f root DigiCertTrustedRootG4.crt
```

Anti-Virus and HIPS Exclusions

Have Anti-Virus, EDR, or HIPS software installed? To avoid conflicts with Cloud Agent, ensure that you exclude the following files, directories, and processes from all security software installed on the system.

Agent processes

QualysAgent.exe - this is the Qualys endpoint service

QualysCloudAgent.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.

QualysSPConfig.exe - Qualys Cloud Agent Self Protection Configuration Utility. Used to disable the self-protection.

QualysProxy.exe - Qualys Proxy Configuration Tool. Used to configure proxy settings to Qualys Cloud Agent.

QualysAgentUI.exe – Executable used to show Patch Management Prompts/UI.

Processes under Program Files\Qualys\QualysAgent, allows Qualys FIM driver to be loaded and unloaded, if Qualys File Integrity Monitoring is activated on the agent

Executables and Processes

%ProgramData%\Qualys\QualysAgent\PatchManagement\Resources\ - Various Patch Management executables.

%ProgramFiles%\Qualys\QualysAgent\EDR\ - Driver Management Utilities.

%ProgramData%\Qualys\SandboxRO\agentid-service.exe – Agent Scan Merge executable.

%ProgramData%\Qualys\QualysAgent\LogCollector\Resources\qualys-beat_x86_64.exe - XDR executable for 64-bit.

%ProgramData%\Qualys\QualysAgent\LogCollector\Resources\qualys-beat_x86.exe - XDR executable for 32-bit.

%ProgramData%\Qualys\QualysAgent\SwCA\Resources\SwCAScanner.exe- Scanner executable for Software Composition Analysis.

%ProgramData%\Qualys\QualysAgent\QCAPS\Resources\qcaps.exe - Cloud Agent Passive Sensor.

File

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

%ProgramFiles%\Qualys\QualysAgent - this is where the service and uninstall are installed. The service will create processes so AV/EDR/HIPS needs to make sure to unblock this action. This path is same for both x86 and x64-bit systems.

Registry

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.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\qmon - this is where the agent setup installs the driver into the system if Qualys File Integrity Monitoring (FIM) is activated or Self-protection is enabled or Qualys EDR is activated on the agent.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\qnetmon - this is where the agent setup installs the driver into the system if Qualys EDR is activated on the agent.

QualysAgent.exe

Calls CreateProcess to launch external processes as needed

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

Upgrading the Cloud Agent

The Qualys Platform can be used to upgrade agents to newer available versions when agents check into the platform, depending on the settings in the Configuration Profile.

Software distribution tools can package the Cloud Agent installer of a newer version as already installed agents in those cases are not configured for auto-upgrade.

The Windows Cloud Agent installer supports a command line argument ("PatchInstall") that enables an upgrade-in-place of the installed agent so that it retains the agent UUID, Customer ID, and Activation Key configuration on the system.

***REQUIRED:** It is required for software distribution tools to use a specific command line argument to upgrade existing installed Windows agents. If the specific command line argument is not used, the installer fails to upgrade the existing installed Windows Agent.

For exe based installer:

```
QualysCloudAgent.exe PatchInstall=TRUE
```

For MSI based installer:

```
Msiexec.exe /i CloudAgent_x86.msi Patchinstall=true
```

Note: When using the "patchinstall" argument, do not append the Customer ID or Activation Key arguments.

Tell me about self-patch The Cloud Agent automatically upgrades through self-patching. For successful self-patching the Cloud Agent needs access to the following Revocation servers for the host to receive the public root certificate used to sign the agent binaries:

<http://ctldl.windowsupdate.com/>

<http://rb.symcd.com/>

<http://rb.symcb.com/>

Note: This is required only for agents upgrading from 2.0.2 - 2.0.6 to 2.1.x.

Uninstalling the 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, its asset record, any licenses for activated modules, and any associated data and assessment findings are removed from the Qualys subscription.

Agents checking into the Qualys Platform will uninstall locally from the system (service, Program Files, and Program Data), but will keep the registry entry with agent Host ID (Agent UUID), Activation Key, Customer ID, and other registry keys. This facilitates keeping the same agent personality if an agent is re-installed onto the same asset, and to support agentless tracking for authenticated scans.

Uninstalling the agent from the host itself

When you uninstall a cloud agent from the host itself using the Uninstall utility, the agent, its license usage, and scan results are still present in the Qualys Platform subscription.

Uninstalling locally from the system (service, Program Files, and Program Data) will keep the registry entry with agent Host ID (Agent UUID), Activation Key, Customer ID, and other registry keys. This facilitates keeping the same agent personality if an agent is re-installed onto the same asset, and to support agentless tracking for authenticated scans.

For exe and/or MSI based installer:

```
Uninstall.exe Uninstall=True
```

For MSI based installer:

```
Msiexec.exe /x CloudAgent_x86.msi
```

During uninstallation, do not use the Customer ID and Activation Key arguments.

To remove the agent's asset record, license, and assessment findings from the platform, use the Cloud Agent module user interface or Cloud Agent API to uninstall the agent. This can be performed after the agent has been uninstalled from the local system.

Note: The Uninstall.exe program must be called from outside the Qualys directories to delete the Qualys directories as part of the uninstallation, else the installer will stop and exit with an error.

Clean Uninstall

The default uninstall behavior retains the Agent UUID, Customer ID, and Activation Key on the system. This supports two use cases: a new agent installation will re-use the original Agent UUID so there is a consistent lifecycle of that asset in the platform; and, for cases where authenticated scanning is enabled for Agentless Tracking and needs the UUID is preserved.

The Windows Cloud Agent installer supports a clean uninstall capability, for those cases where it's needed that the Agent UUID, Customer ID, and Activation Key are removed from the system. Provide the following arguments to the installer:

```
Uninstall.exe Uninstall=True Force=True
```

Installing the agent on a system that has a clean uninstall performed will create a new Agent UUID for that system and will potentially create a duplicate host record in the platform if the original host record was not removed using the "uninstall" action in the Cloud Agent UI or API.

Note: The Uninstall.exe program must be called from outside the Qualys directories to delete the Qualys directories as part of the uninstallation, else the installer will stop and exit with an error.

Sample Clean Uninstall agent command

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

Qualys Self-Protection Feature for Cloud Agent

Qualys self-protection feature for Cloud Agent prevents non-trusted processes from making unwanted changes to a Cloud Agent.

Self-protection feature prevents the following:

- Uninstallation of Cloud Agent.
- Termination of Cloud Agent processes.
- Tampering with Cloud Agent files and directories - overwriting, deleting, renaming, modifying, and memory mapping.
- Tampering with Cloud Agent driver - unloading or detaching the driver.
- Tampering with Cloud Agent registry keys:
 - Overwriting, deleting, and modifying the registry key and value
 - Renaming the registry key
- Prevents the debugger from attaching to the Qualys agent service.
- Prevents user-defined scripts, that is the scripts uploaded by Custom Assessment and Remediation (CAR), and Patch Management, from making changes to the protected areas.

This feature is not enable by default. To enable Qualys self-protection for a Cloud Agent, contact your Qualys representative.

Note: Qualys self-protection feature is available only for Windows 7 and above operating systems.

Disable Self-Protection

You have to disable self-protection for Cloud Agent, to access the agent data artifacts required for debugging such as, log files.

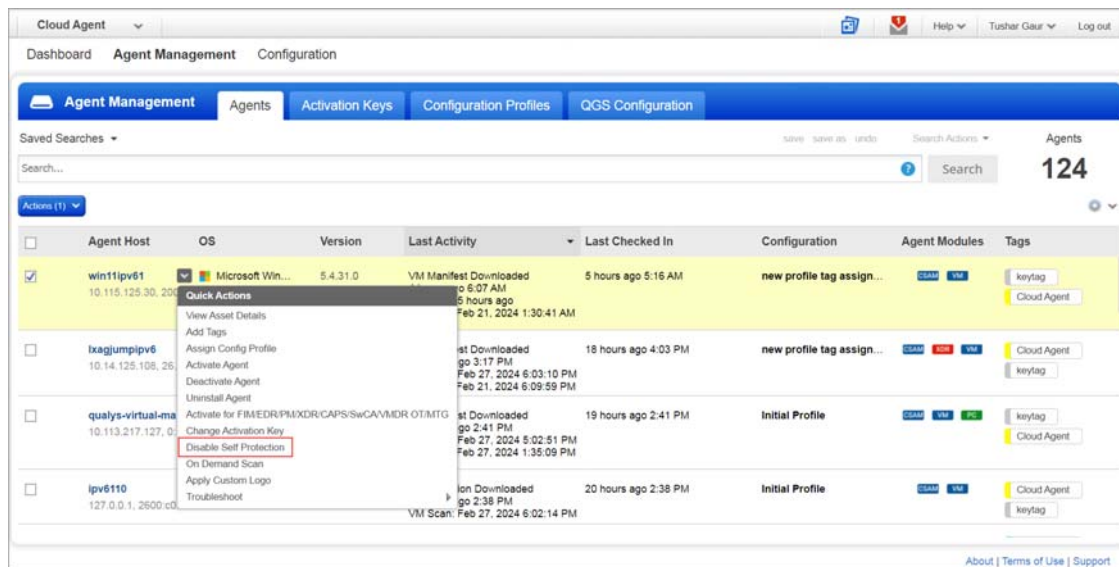
To disable self-protection for an agent, you have to generate a key. By default, the validity of a key to disable self-protection is one day (24 hours); however, you can configure it as per your requirements. You can also disable self protection for a Cloud Agent using troubleshoot option.

Note: Only users with the CA Manager role can generate the key to disable self-protection for a Cloud Agent.

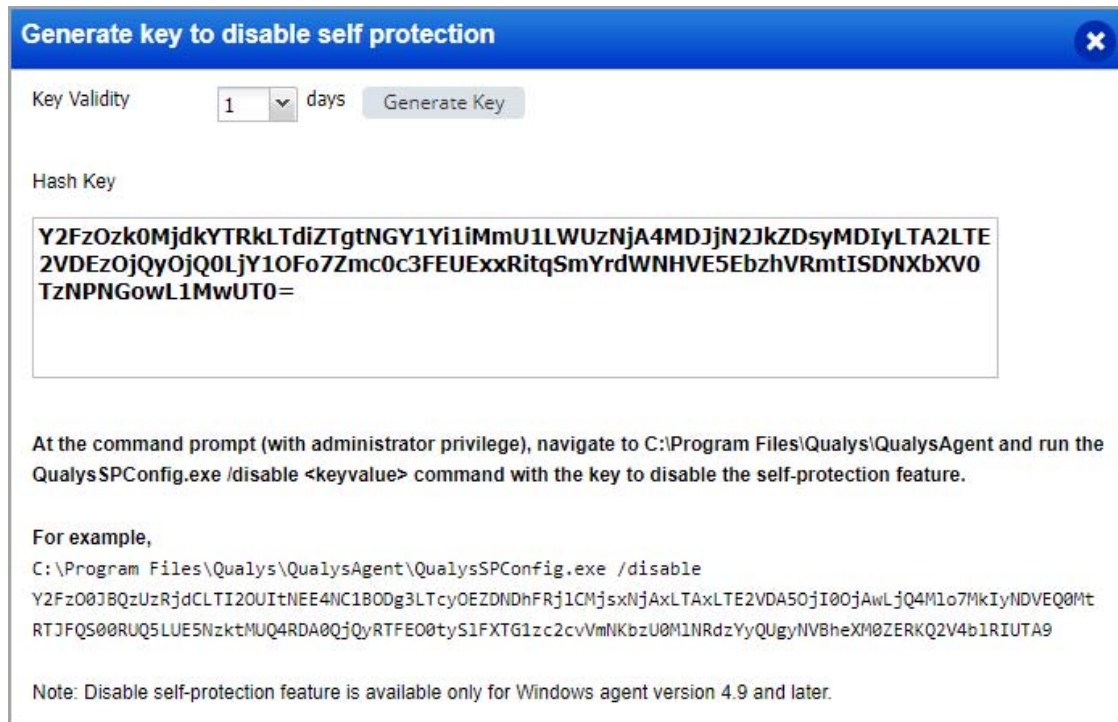
Steps to Disable Self-Protection for a Cloud Agent

To disable self-protection for a Cloud Agent:

- Open Cloud Agent application.
- Navigate to **Agent Management** > **Agents** and select a installed Cloud Agent for which you want disable self protection.
- In **Quick Actions** menu, click **Disable Self Protection**.



- In the **Generate Key to Disable Self Protection** screen, click **Generate Key** and follow the process to disable self protection for that agent.



Note: This option to disable self-protection for a Cloud Agent is available for Qualys Cloud Agent for Windows version 5 and later.

Uninstalling Cloud Agent with Self Protection

Following are the commands to uninstall a Cloud Agent with self protection enabled. Using these commands you can uninstall Cloud from agent host itself.

- For EXE and MSI based agent installer package

```
Uninstall.exe Uninstall=True SPFKEY=Hash Key
```

- For EXE and MSI based agent installer package

```
Msiexec.exe /x CloudAgent_x86.msi SPFKEY=Hash Key
```

Note: Hash key to disable self protection for a Cloud Agent must be generated using Disable Self Protection option available on Cloud Agent UI.

Cloud Agent Health Check Tool

The Cloud Agent Local Health Check tool assesses the Health of the Qualys Agent on the specific host. The tool is available with the Cloud Agent setup for the Windows platform. The tool runs independently and does not require any parameters.

The `QualysAgentHealthCheck.exe` located in the `C:\ProgramFiles\QualysAgent\Qualys` directory.

Use the following command to run the Qualys Agent Health Check tool:

```
"%programfiles%\qualys\qualysagent\QualysAgentHealthCheck.exe"
```

Note: The tool is available with the Qualys Cloud Agent for Windows 5.5.

Agent Health Status Evaluation

The tool assesses the overall health status of the Cloud Agent based on installation status, communication health, and application functionality. The applications assessed for health status are Vulnerability Management (VM), Policy Compliance (PC), Security Configuration Assessment (SCA), and Patch Management (PM).

- Agent communication health is evaluated based on proxy settings and connection to Qualys Server end points.

- Health of the scan-based applications is evaluated based on scan interval, upload interval and last scan/last upload time.

- For Patch Management health, the tool initiates the patch download from specified URLs and verifies the file hash. If a patch fails to download, patch health is flagged as bad; however, if the patch is successfully downloaded but fails verification, it does not impact Patch Management health. Instead, an entry is recorded in the error section of the JSON to indicate the failed patch verification.

Agent Health Status Report

The Agent Health Status tool provides a console output, a user-friendly text summary, and a detailed JSON report. The text report and the JSON report is generated in the `HealthCheck` directory, located in the same directory where the tool is executed.

Health Status and Descriptions

The following table presents the health status and description.

Health Status	Description
Good	Agent Health is good.
Bad	The Agent is facing some communication issues, the Agent Service is down, or none of the applications are functioning properly.
Poor	Some applications of the Qualys Agent are functioning correctly.
Not Installed	Qualys Agent is not installed on the asset.

Not Provisioned	Qualys Agent is installed but not provisioned.
Tool Error	The Agent Health Status tool encountered a critical error while determining Agent Health.

Example of health check report

The following report shows that the overall Agent health is Poor as a result of Patch Management application health as highlighted in the report.

Example of text report:

```
.....
Performing Health Checks
.....
CoreHealthCheck 1 : Verifying if the Qualys agent is installed on your system.
CoreHealthCheck 2 : Retrieving information about qualys services currently running on your system.
CoreHealthCheck 3 : Retrieving information about qualys processes currently running on your system.
CoreHealthCheck 4 : Retrieving certificate information
CoreHealthCheck 5 : Retrieving proxy details
CoreHealthCheck 6 : Assessing connectivity to the backend system.
CoreHealthCheck 7 : Retrieving information about Agent communication.
CoreHealthCheck 8 : Gathering details about Qualys modules installed on the system.
CoreHealthCheck 9 : Assessing patch connectivity.

Evaluating overall health of the system.

.....
Qualys Agent Local Health Check Tool Report :
.....

Overall Health : Poor

Services :

  Name : qualysagent
  State : Running

Certificates :

  Name : DigiCert Global Root CA
  Installed : true

Agent Communication Details :

  Last CAPI : 2024-01-24 17:16:38.489
  CAPI Interval : 900

Backend Connectivity :

  Direct Connection :
  URL : https://qagpublic.p01.eng.sjc01.qualys.com/status
  Connection Succeeded : true

Modules :

  Name : Vulnerability
  Module Type : Scan based
  State : Ready for Scan
  Enabled : true
  Last Scan Time : 2024-01-24 15:38:44.889
  Scan Interval : 14400
  Next Scan Time : 2024-01-24 19:38:44
  VM Scan Deadline : 2024-01-26 19:38:44
  Module Health : Vulnerability Health Good

  Name : PolicyCompliance
  Module Type : Scan based
  State : Ready for Scan
  Enabled : true
  Last Scan Time : 2024-01-24 15:46:04.224
  Scan Interval : 14400
  Next Scan Time : 2024-01-24 19:46:04
  PC Scan Deadline : 2024-01-26 19:46:04
  Module Health : PolicyCompliance Health Good

  Name : SCA
  Module Type : Scan based
  Enabled : false

  Name : Patch Management
  Module Type : Realtime
  Enabled : true
  Patch Connectivity :
  Direct Connection :
  URL : https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.5/npp.8.5.Installer.x64.exe
  Connection Succeeded : false
  Module Health : Patch Management Health Bad

Errors :

  Severity : CRITICAL
  Win32 Error Code : 12002
  Error Description : Patch Webrequest [Direct Connection] failed for https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.5/npp.8.5.Installer.x64.exe(winhttp code: 12002), The request has timed out

Detailed Report Location : C:\Program Files\Qualys\QualysAgent\HealthCheck\qualys_agent_health_check_124225725.json
Concise Text Report Location : C:\Program Files\Qualys\QualysAgent\HealthCheck\qualys_agent_health_check_124225725.txt
```

Example of the JSON report:

```

{
  "OverallHealth": "Poor",
  "Timestamp": "2024-01-24T17:27:25Z",
  "ToolVersion": "5.4.36.1",
  "JSONSchemaVersion": "1.0",
  "FreeDiskSpaceInMB": 1298,
  "CustomerID": "{3C59A6A1-51E6-75B4-81FD-BFFD25CDDCCFA}",
  "AgentID": "{94792BDB-A522-4E2F-8B1C-0B79DEA4E13D}",
  "ActivationID": "{F635D621-1FC4-4C70-B964-ACA13AAE642C}",
  "ConfigID": "{6E057275-2293-4634-B7AB-50A27B64FCFA}",
  "QSSEnabled": false,
  "CloudProvider": "Auto",
  "Provisioned": true,
  "QualysAgentPerformanceCounters": {
    "CPUUsageInMilliseconds": 1426859,
    "RAMUsageInMB": {
      "WorkingSet": 38,
      "PrivateUsage": 41,
      "PeakWorkingSet": 110
    },
    "ProgramDataSpaceUsageInMB": 671,
    "ProgramFilesSpaceUsageInMB": 611
  },
  "QualysDrivers": [
    {
      "Name": "qmon",
      "State": "Running",
      "Version": "5.3.0.0"
    },
    {
      "Name": "qnetmon",
      "State": "Running",
      "Version": "5.1.0.0"
    }
  ],
  "ProxyDetails": {
    "ProxyUrls": null,
    "PacFilePath": null,
    "DirectAttemptEnabled": true,
    "WinHttpEnabled": true,
    "WPADEnabled": true
  },
  "PatchManagement": {
    "Name": "Patch Management",
    "Enabled": true,
    "ModuleHealth": "Patch Management Health Bad",
    "PatchCommunicationDetails": [
      {
        "VendorUrl": "https://github.com/notepad-plus-plus/releases/download/v8.5/npp.8.5.Installer.x64.exe",
        "Proxyresolution": "NoResolution",
        "Proxyused": false,
        "Timetocompleteinseconds": 21.0931034,
        "Win32errorcode": 12002,
        "Connectionsucceeded": false
      }
    ]
  },
  "ErrorMessages": [
    {
      "ErrorCode": 87,
      "Severity": "INFO",
      "ErrorDescription": "No Proxy set hence skipping proxy test",
      "DiagnosticChecks": [
        "Tool does not contain diagnostic steps for this error"
      ]
    },
    {
      "ErrorCode": 12002,
      "Severity": "CRITICAL",
      "ErrorDescription": "Patch Webrequest [Direct Connection] failed for https://github.com/notepad-plus-plus/releases/download/v8.5/npp.8.5.Installer.x64.exe(winhttp code: 12002), The request has timed out\\",
      "DiagnosticChecks": [
        "Tool does not contain diagnostic steps for this error"
      ]
    }
  ]
}

```

Proxy Configuration

TLS 1.2 must be enabled on client machines to communicate with Qualys Cloud Platform. TLS 1.2 is a more secure protocol. In the event, if it is impossible to enable TLS 1.2, you need to run communication through a proxy server that can convert the incoming communication to TLS 1.2 protocol before sending it to Qualys Cloud Platform.

Cloud Agent Windows proxy settings are stored in the Qualys registry hive, reference a PAC file URL stored in the Qualys registry hive, or determined if the system is configured to use WPAD.

Software distribution or systems management tools can set the proxy configuration for the agent when installing the agent or after the agent has been installed.

A companion utility installed with the Cloud Agent called QualysProxy.exe can be used optionally by software distribution tools, system management, or manually to set the proxy configuration for the agent. The QualysProxy.exe utility is the only method that will encrypt any required proxy authentication credentials during the setting of the proxy configuration.

QualysProxy lets you:

- Configure proxy server(s) and port
- Configure proxy username and password credentials
- Configure PAC file URLs for cases when WPAD is not available
- Enable/disable WPAD detection

Note:

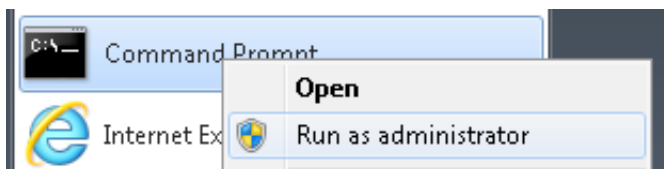
If proxy connection fails then agent will attempt a direct connection outbound (Fail Open).

What do I need to know?

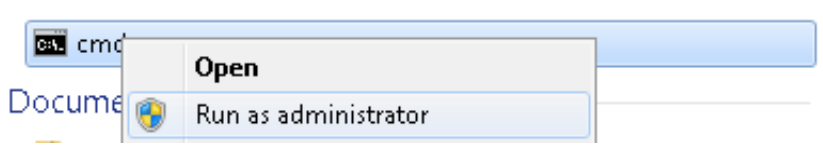
Tell me about installation The QualysProxy tool, and proxy tool updates, are installed with the Cloud Agent installation and updated, if necessary, as Cloud Agent versions are upgraded. The Qualys Proxy is located at the following location:

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:



Systems management software and remote registry management can be used to set the proxy servers. The QualysProxy.exe 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 User Interface window 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>]]
```

```
QualysProxy [/w on|off]
```

```
QualysProxy [/d]
```

```
QualysProxy [/h on|off]
```

```
QualysProxy [/c]
```

```
QualysProxy [/t on|off]
```

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.

Option	Description
/d	Deletes all Qualys cloud agent proxy settings. Note: This option does not make any changes to System's proxy settings or Web Proxy AutoDiscovery (WPAD) settings.
/w	Enables or disables agent use of the host's WPAD settings.
/h	Enables or disables agent use of the system wide winhttp(s) proxy setting.
/c	Prints current Qualys cloud agent proxy settings.
/t	Enables or disables direct connection to Qualys Cloud Platform after all proxy server failure. By default, direct connection after proxy failure is enabled.

Notes

- If any argument contains spaces, please surround that argument with quotes.
- If any argument contains a " character, precede that character with a backslash \".

Multiple Proxy Server support in Proxy URL and PAC Files (Windows Agent 3.1 or later)

The Cloud Agent has support for multiple proxy servers defined in the Proxy URL and in PAC files. Cloud Agent will use the first proxy server in the list for its connection, if it fails to connect, the agent will use the next configured proxy server in the list in sequential order until all proxy servers are attempted. When all proxy server(s) are attempted, Cloud Agent for Windows will use a Direct Connection bypassing proxy server configuration to contact the Qualys Platform directly.

Each time the Cloud Agent connects to the Qualys Platform, it always uses the first proxy server in the ordered list. The agent does not maintain a history of last proxy server used.

This proxy configuration can be used with the Qualys Gateway Service or third-party proxy servers. There is no requirement that the failover proxy servers need to be on the same subnet as the first proxy server; as long as the Cloud Agent can connect to other proxy servers even on other subnets, the agent will use those proxy server(s) if the first proxy server is not available.

Define multiple proxy servers in the Proxy URL using semi-colon separated values. For PAC files, refer to the PAC file vendor's documentation that defines how to configure multiple proxy servers.

Use cases

Note: By default, Cloud Agents connecting through Qualys Gateway Service (QGS) should use the cache port if cache or patch mode is enabled on the appliance. If the cache or patch mode is not enabled, the QGS caches cannot be used.

Example 1 - Set proxy and port number

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

- a) Any HTTP_CONNECT proxy using http connection

```
QualysProxy /u http://my-proxy:8080
```

- b) QGS cache port using http connection

```
QualysProxy /u http://my-qgs:8080
```

Example 2 - Define multiple proxy servers used for failover

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

- a) Any 2 HTTP_CONNECT proxies using http connection

```
QualysProxy /u http://my-proxy-1:8080;http://my-proxy-2:8080
```

- b) Any 2 QGS appliance cache ports using http connection

```
QualysProxy /u http://my-qgs-1:8080;http://my-qgs-2:8080
```

Example 3 - Define multiple ports on the same proxy server for failover

This can also be used to configure the Cloud Agent to use the Cache Port first and Proxy Port second (as failover) on a single Qualys Gateway Appliance.

The following example shows how to set different port numbers for the same proxy server:

- a) Any HTTP_CONNECT proxy using http connection

```
QualysProxy /u http://my-proxy:8080;http://my-proxy:1080
```

- b) QGS using cache port using http connection, then proxy port using http connection

```
QualysProxy /u http://my-qgs:8080;http://my-qgs:1080
```

Example 4 - Set proxy and credentials

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

- a) Any HTTP_CONNECT proxy using http connection

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

Example 5 - Tell agent to use PAC file

The following example shows how to tell the cloud agent to use a PAC file directly if it is not discoverable via WPAD (assumes PAC file proxy uses http connection):

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

Example 6 - 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 /p ProxyPassword /a http://my-pac-  
file-server/QualysAgent.pac
```

Cloud Agent Preparation for Cloning / Gold Image

The Qualys Cloud Agent supports configuration and deployment into cloned images in physical, virtual, and cloud environments (including Amazon AWS and Microsoft Azure). The Cloud Agent is created with a universally unique identifier (UUID) as its Agent ID as part of the provisioning process between the agent and the Qualys Platform or Private Cloud Platform. Each Cloud Agent must have a truly unique Agent ID or else there will be issues with management and reporting.

Follow these best practices deployment guidelines to ensure UUIDs generated are truly unique across agent deployments in cloned or gold images.

This method is for all supported versions of Windows.

1) Install the operating system, applications, and patches. For installing agent on Golden Image, see [QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx} WebServiceUri=<platform_url>/CloudAgent/ Proxy="/u <proxy url> /n <proxy username> /p <proxy password>](#)".

- Create a snapshot of the Gold Image before proceeding.

2) Verify that there is no network connectivity on the Gold Image instance to the Qualys Cloud Platform or deployed Private Cloud Platform(s) for the installation process of the Cloud Agent, which can include, but not limited to:

- Turn off networking to the Gold Image from the virtualization manager

- Manage the Gold Image in a network that does not have network connectivity

- Create a bogus entry in the local hosts file (located at C:\Windows\System32\drivers\etc\hosts) for the DNS name of the public POD or PCP that the agent connects to, e.g. 127.0.0.1 (make sure to remove this entry before the Gold Image is cloned)

- Create a temporary Windows firewall rule to block the Cloud Agent process from communicating over the network (make sure to remove this entry before the Gold Image is cloned)

3) Install the Qualys Cloud Agent and configure it using your assigned Activation ID and Customer ID.

- The Cloud Agent will attempt to connect to the Qualys Platform to provision. Without connectivity, the agent will remain in an unprovisioned state pending its next successful connection to the Qualys Platform.

4) If this is not the last application or service to be installed in the Gold Image, shut down the Cloud Agent service and set its auto-start to "Disabled" so that the agent doesn't start and provision itself during the remainder of the Gold Image configuration; make sure to set the Cloud Agent service to "Automatic" start before cloning the Gold Image.

5) Shut down the Gold Image and make it available for cloning.

6) Upon start-up of a cloned image, the Cloud Agent will start, connect to the Qualys Platform, get provisioned, and generate its UUID for that running cloned instance.

Alternative approach: You can install the Cloud Agent into instances in domain join script(s) as part of the final installation/provision for hosts. This approach greatly simplifies the gold image installation but requires additional processing during the domain join.

Not following these procedures (or if Software Distribution Tools are not configured correctly when deploying or upgraded agents) can create duplicate host records in the Qualys Platform. When there are two host records of the same hostname, one record has the old Agent UUID (which is no longer used) and the other has the new Agent UUID (which is used between the agent and platform). If this occurs, usually the "Last Checked In" date of the old Agent UUID record is the date when the reprovisioning occurred with the agent now using the new Agent UUID. All new vulnerability, compliance, and asset inventory information is associated with the new Agent UUID and host record.

If there are duplicate host records due to different Agent UUIDs being generated, you can remove the old host records / Agent UUIDs by uninstalling them via the Cloud Agent module user interface or the API. This does not affect the functionality of the agent communicating using the new Agent UUID.

If there are larger numbers of duplicate agents that is impractical or cumbersome to remove yourself, contact Qualys Customer Support.

Scan on Demand and Scan on Startup

Cloud Agent Windows 3.0 introduces client-side initiated "ScanOnDemand" and client-side initiated "ScanOnStartup" functions. This feature is used to trigger the agent to initiate an on-demand manifest collection or when the agent service starts for supported activated modules: Vulnerability Management, Policy Compliance and Inventory.

This capability is introduced to primarily support patch management use cases where one needs to verify that newly installed patches have remediated the associated local host vulnerabilities.

Scan on Demand is a single use execution that is initiated manually on the host itself, using locally or remotely executed scripts or GPO, or from software distribution tools at the end of a patch deployment job.

Scan on Startup is a configuration option, that once set, will initiate a manifest scan when the Qualys Agent service starts up. The primary use case is to reassess the asset when a patch deployment job requires the host to reboot to fully remediate the vulnerability or when a gold images are being built to verify that there are no vulnerabilities in the image.

In addition to initiating Scan on Demand or setting the Scan on Startup, you can set the CPU Limit to a performance value for the on demand or startup scans. This CPU Limit is only for the on demand or startup execution and is separate from the CPU Limit set in the Configuration Profile. The most common use case is setting a high CPU Limit or no throttle (100%) for this scan so that the agent portion of the processing can be run as fast as possible. This allows for fast collection as part of patch deployment jobs during change management windows while keeping a low performance profile for normal production usage.

Note: This feature only manages when the agent initiates a manifest scan to collect the requisite metadata. After collection, the agent calculates the delta changes and sends any changes to the platform for processing. Platform processing is per the normal assessment pipeline for assessments to be available in VM reports, API, VM dashboard, PC Reports, and AssetView. The Scan on Demand feature does not change or accelerate the normal assessment pipeline for assessment processing on the platform.

Registry Configuration

The configuration for this feature is set and managed in Qualys Agent hive in the registry. This allows integration into patch deployment and gold image workflows without requiring access to the Qualys platform UI or API.

The agent monitors the Qualys registry hive at HKLM/Software/Qualys/QualysAgent/ScanOnDemand key in real-time for specific values and initiates the scan for each supported manifest based on the values set.

For Cloud Agent for Windows version 4.8 or later, when a module is activated, the agent creates the registry structure and subkeys for on-demand scan automatically. For versions earlier than 4.8, only root keys are created and the subkeys, data, and values to configure and execute the scans need to be set manually, using scripts, or registry configuration tools.

```

HKEY_LOCAL_MACHINE
SOFTWARE
  Qualys
    QualysAgent
      ScanOnDemand
        Inventory
          CpuLimit
          ScanOnDemand
          ScanOnStartup
        Vulnerability
          CpuLimit
          ScanOnDemand
          ScanOnStartup
        PolicyCompliance
          CpuLimit
          ScanOnDemand
          ScanOnStartup
      UDC
        CpuLimit
        ScanOnDemand
        ScanOnStartup
      SCA
        CpuLimit
        ScanOnDemand
        ScanOnStartup

```

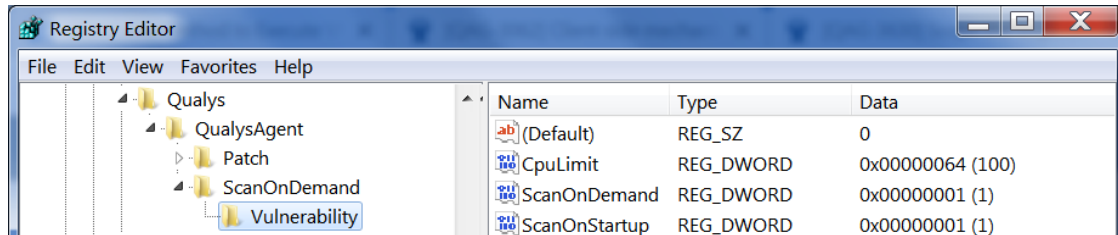
Registry Configuration Settings

The following table describes the configuration settings and functionality for the Scan on Demand and Scan on Startup feature.

Module Key	Value	Type	Data	Description
Inventory Vulnerability PolicyCompliance UDC SCA	CpuLimit	REG_DWORD (decimal)	2 - 100	Sets the CPU Limit (%) for the execution. Key is not required. Default value is 100 if no value exists or the data is not valid.
	ScanOnDemand	REG_DWORD (decimal)	0 - completed 1 - execute now 2 - in progress	Setting a data value of "1" will initiate the on demand scan. The data value will change to "2" when the scan is in progress. The data value will change to "0" when the scan is complete.
	ScanOnStartup	REG_DWORD (decimal)	1	A data value of "1" will configure the agent to execute the scan when the agent service starts up. After a completed scan, the scan interval for this manifest is reset. No execution if there is no value or the data is not valid.

Example

Configuration example for CPU Limit of 100%, Scan on Demand data of "1" to execute immediately, and Scan on Startup data of "1" to execute on agent service startup.



Functionality Notes

If the agent is already performing a manifest collection or is in the delta upload/PendingDelta state, the agent will not initiate the on-demand or on-startup scan. This ensures data integrity between the agent and the platform for the in-progress scan.

Network Blackout Windows take precedent.

- Scan on demand or scan on startup when the agent is in a network blackout window will still execute, but the delta will not upload to the Qualys platform until the agent is out of a network blackout window.
- If the agent is in a network blackout window that is preventing the previous scan's delta to be uploaded, the scan on demand or scan on startup will not execute until the previous scan's delta upload is fully completed.
- The agent will not execute an on-demand or on-startup scan for a manifest type that is not assigned (activated).

Deployment using Microsoft Intune

You can use Microsoft Intune to deploy Qualys Cloud Agent for Windows on remote assets. There are two different methods to deploy Qualys Cloud Agent remotely:

- [Deployment using exe Package File](#)
- [Deployment using msi Package](#)

Deployment using exe Package File

The following are the steps to deploy the Cloud Agent using .exe file.

Step 1: [Create .intunewin Package](#)

Step 2: [Add App Information](#)

Step 3: [Set Program Information](#)

Step 4: [Set Requirements](#)

Step 5: [Set Detection Rule](#)

Step 6: [Scope tags](#)

Step 7: [Assignments](#)

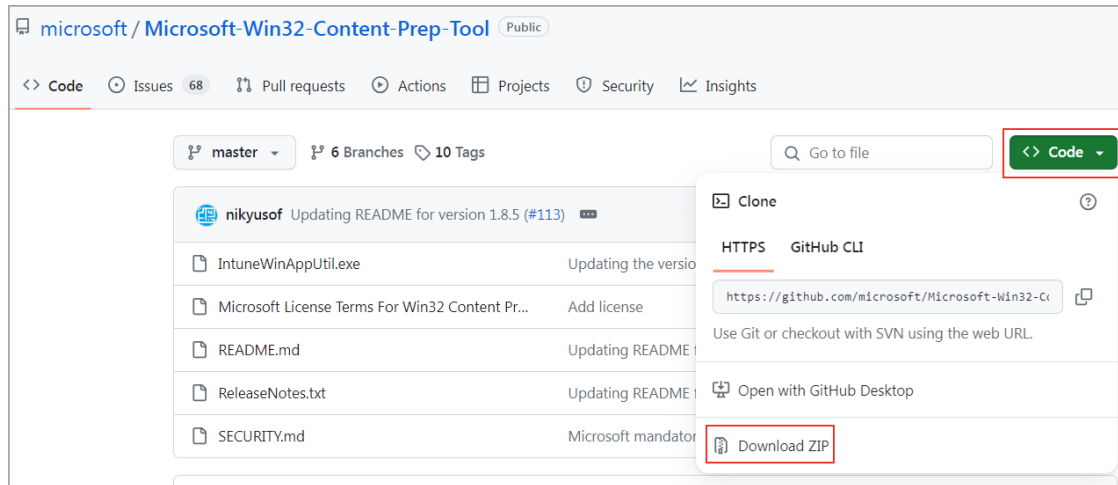
Step 8: [Review + create](#)

Create .intunewin Package

To deploy the .exe based Cloud Agent package, first you have to download the Cloud Agent installer and then convert it into .intunewin package file. Following are the steps to download Cloud Agent installer and create .intunewin package file.

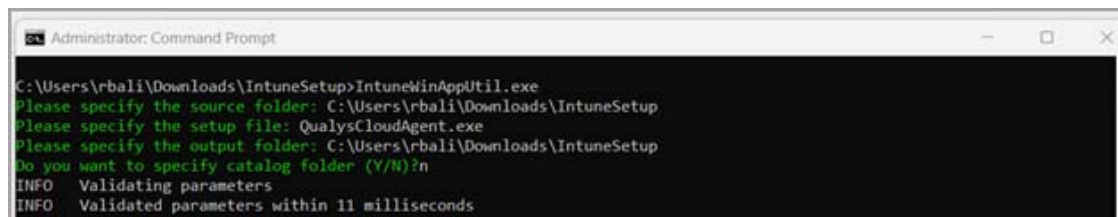
- Download the prep tool from GitHub. To download the prep tool refer to [GitHub Prep Tool](#). Ensure that you download prep tool in .zip file

- Extract the prep tool .zip file on the local folder..



- Download the Cloud Agent installer from Cloud Agent user interface. For details, refer to [How to download the Agent installer](#).

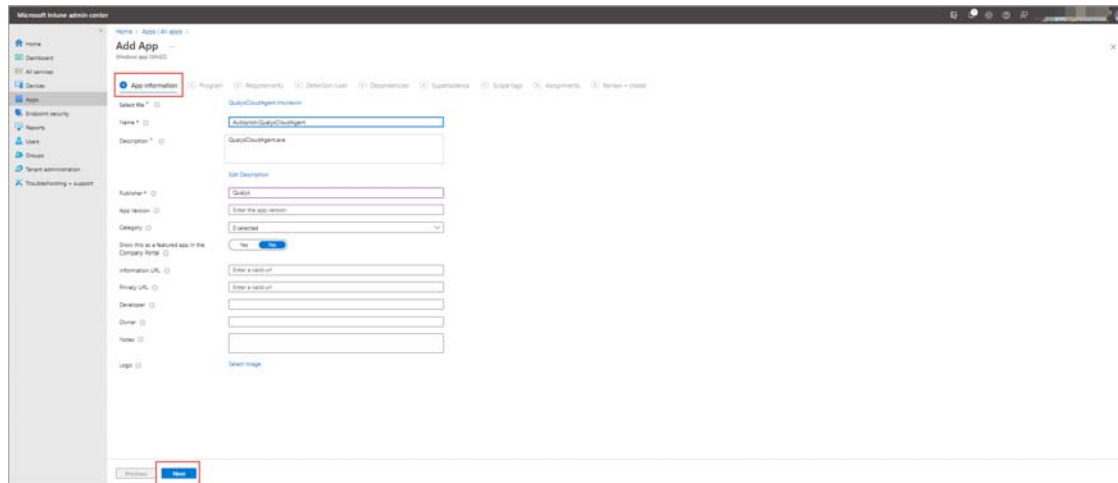
- To create the .intunewin package file:
 - Create a local folder and save the downloaded Cloud Agent file in that folder.
 - Run the IntuneWinAppUtil.exe file from the extracted prep tool files.
 - In the Command Prompt window, enter the following details:
 - Source folder containing the Cloud Installer package.
 - Cloud Agent setup file
 - Output folder for the .intunewin package file



The .intunewin file for Cloud Agent is generated and saved in the output folder.

Add App Information

- On [Microsoft Intune Admin Center](#) home page, click **Apps** > **Add App** > **Windows**.
- On the **App information** page, click **Select app package file**. The **Select app type** pane opens.
- In the **Select app type** pane, select **Windows app (Win32)** and click **Select**.
- On **App package file** pane, upload the .intunewin package file, and click **OK**.
- On **App Information** page, enter the app details and click **Next**. The **Program** page opens.



Set Program Information

- On the **Program** page, enter the **Install command** and **Uninstall command**. The **Install command** and **Uninstall command** are with the Cloud Agent installer.

- Sample installation command:

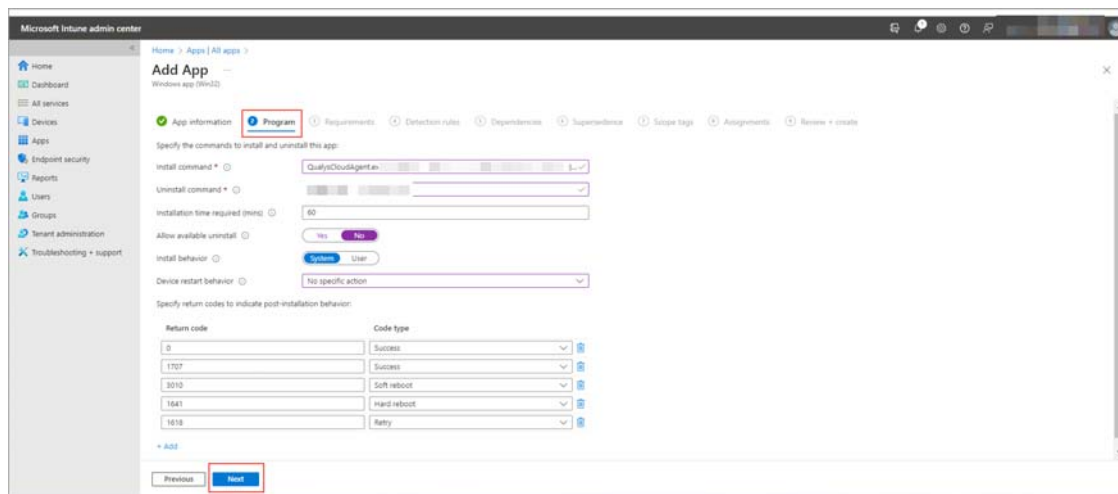
```
QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx} WebServiceUri=/CloudAgent/
```

- For uninstallation use

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

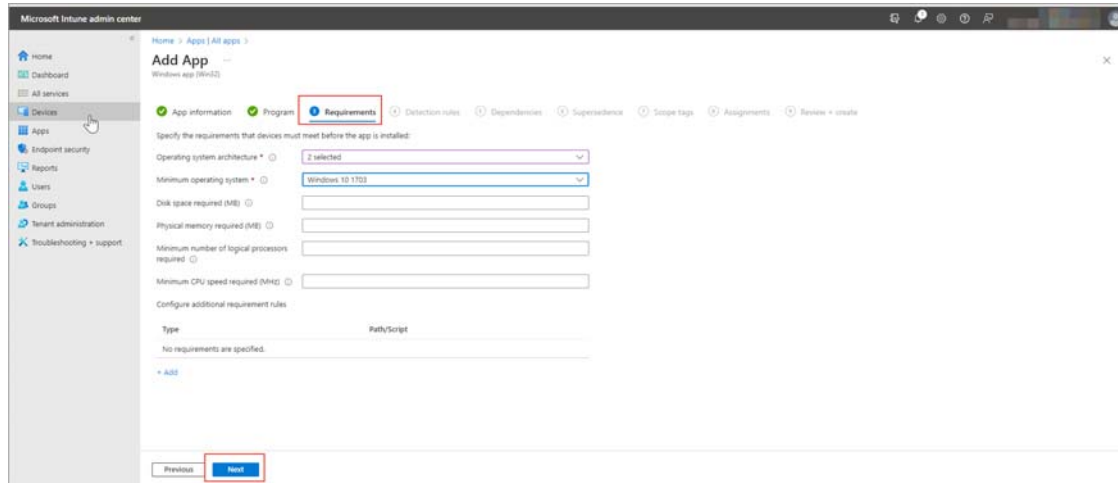
- Set the **Allow available uninstall** field to **No**.

- Click **Next**. The **Requirements** page opens.



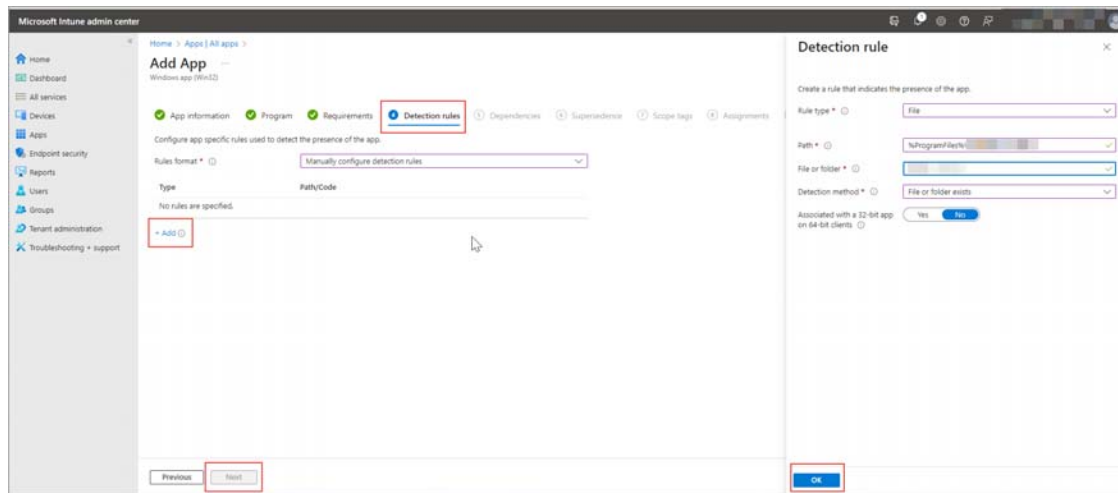
Set Requirements

- On **Requirements** page, select the values for **Operating system architecture** and **Minimum operating system** fields from the available options.
- Click **Next**. The **Detection Rule** page opens.



Set Detection Rule

- On the **Detection rules** page, in the **Rules format**, select **Manually configure detection rules**.
- In the **Detection rule** pane, in the **Rule type** select **File**.
- In the **Detection rule** pane, set the following fields:
 - **Path**: The folder path where Cloud Agent installer is downloaded.
 - **File or folder**: Cloud Agent installer file (.exe).
 - **Detection method**: File or folder exists.
- Click **Next**.

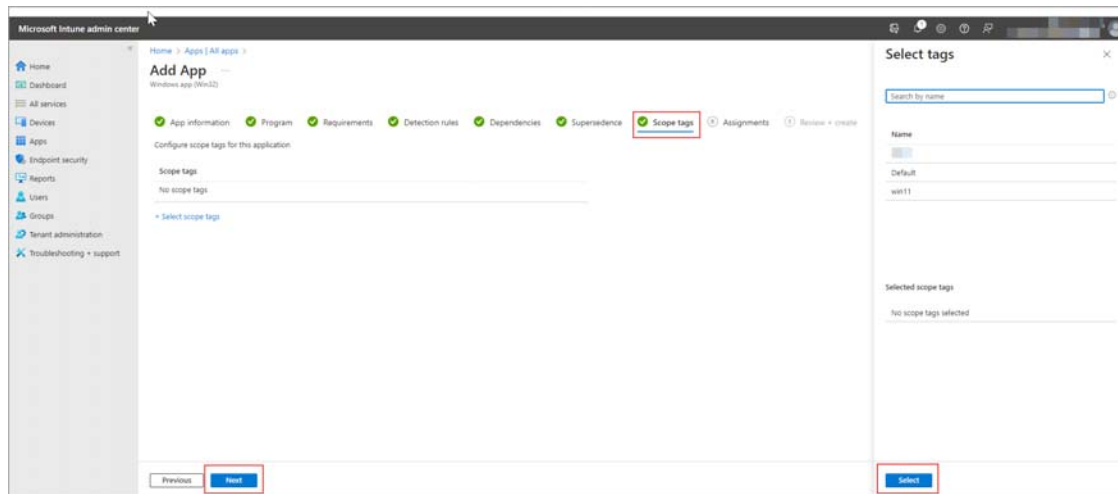


Scope tags

Complete the following steps to proceed to **Assignments** page.

- **Dependencies:** Software dependencies for the Cloud Agent are the applications that needs to installed before installing the Cloud Agent. In this step, you can enable or disable the auto installation of dependencies. Click **Next**.
- **Supersedence:** In this step, you can specify whether to update or replace a previous version of the Cloud Agent. Click **Next**.
- **Scope tags:** On this page you can specify the scope tags for your Cloud Agent.
- Click **Next**. The **Assignments** page opens.

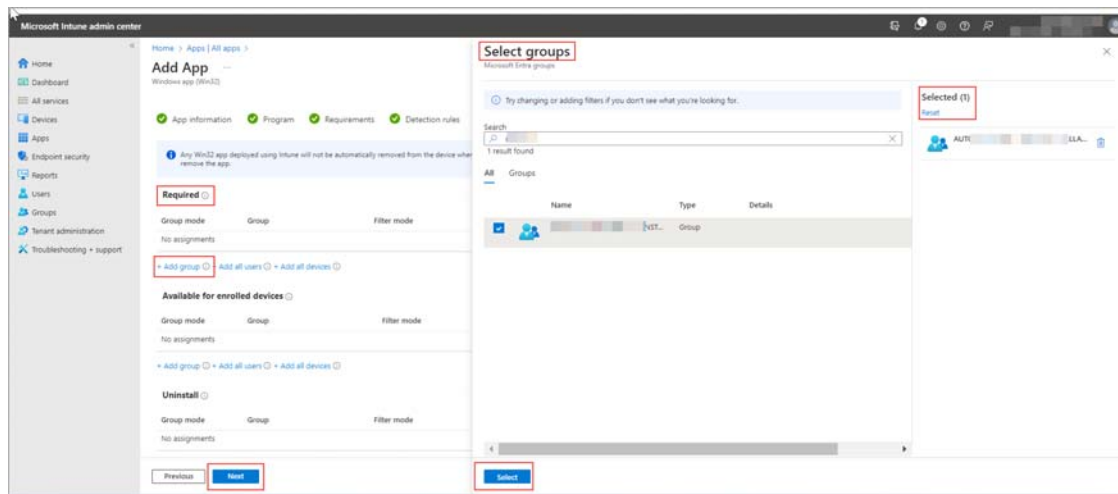
Note: The values for above steps are user defined. You can set the field values for above steps as per your requirements.



Assignments

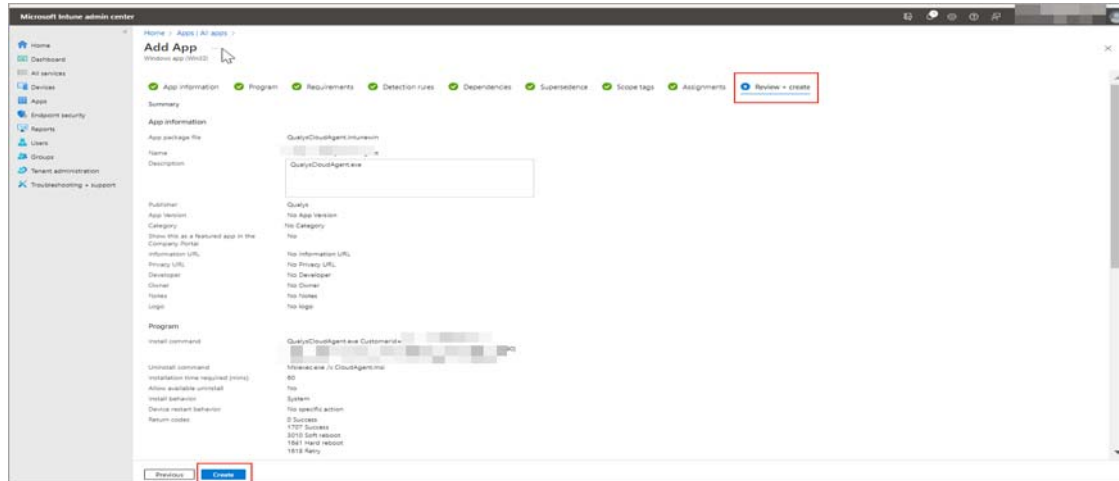
On this page, add the groups to which you want to deploy the Cloud Agent.

- On the **Assignments** page > **Required** section, click **Add groups**. The **Select groups** pane opens.
- In the **Select groups** pane, select the check box associated to the asset groups.
- Click **Select**. You can view the selected asset groups in the **Selected** pane.
- Click **Next** to proceed to the **Review + create** page.



Review + create

- Review the information you entered for the Cloud Agent deployment package.
- To navigate to earlier pages, click **Previous**.
- Click **Create** to deploy the Cloud Agent.



Deployment using msi Package

Deployment of Cloud Agent using the msi Package file involves the following steps:

Step 1: [Download the Cloud Agent Package](#)

Step 2: [Extract the msi Package File](#)

Step 3: [Deploy the msi Package File](#)

Download the Cloud Agent Package

For details on downloading Cloud Agent installer package, refer to [How to download the Agent installer](#).

Extract the msi Package File

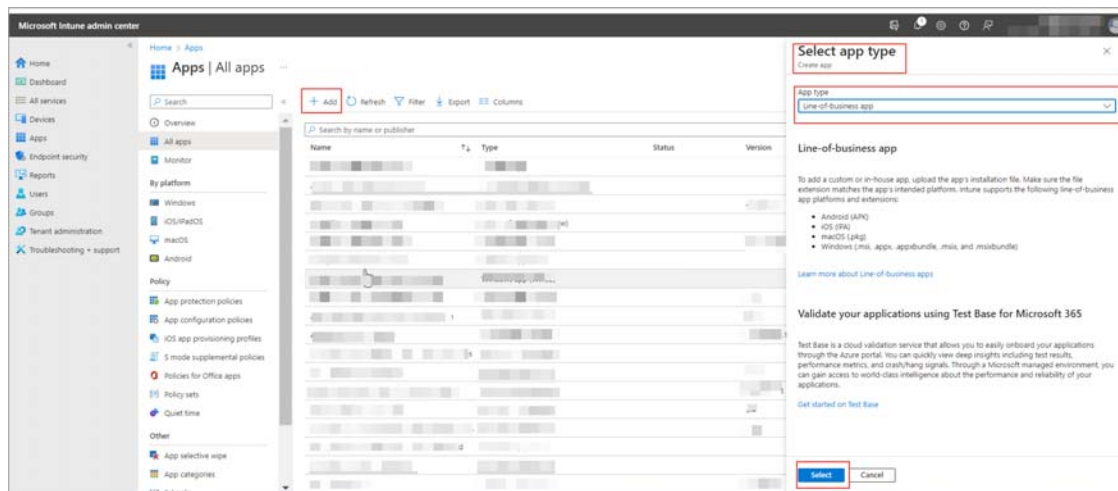
Extract the msi package file from .exe file. For more details, refer to [Extracting MSI Package](#).

Deploy the msi Package File

Following are the steps to deploy the Qualys Cloud Agent using msi package file.

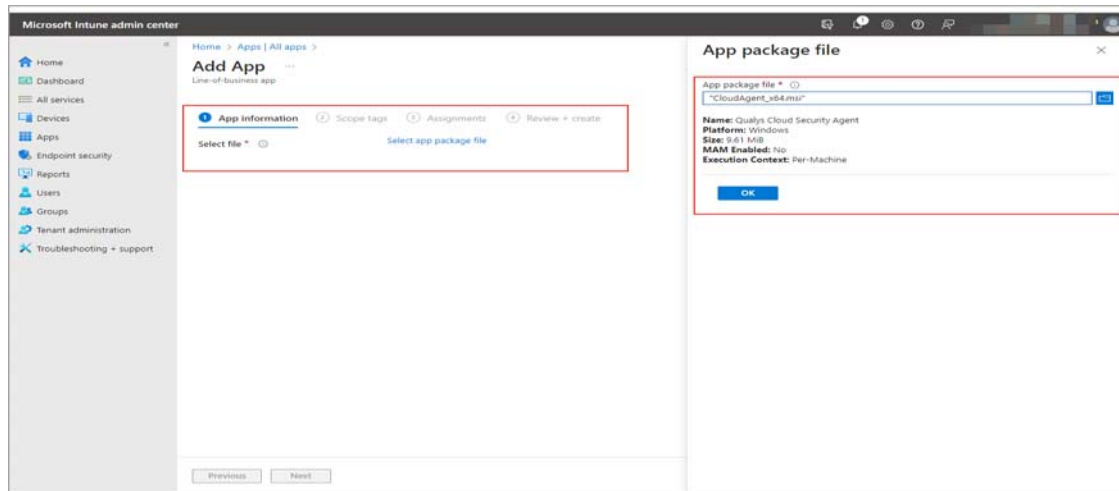
App information

- Log in to [Microsoft Intune Admin Center](#).
- On Microsoft Intune Admin Center, click **All apps** > **Add**. The **Select app type** pane opens.
- Select **Line-of-business app** and click **Select**.



- On **App information** page, click **Select app package file**. The **App package file** pane opens.

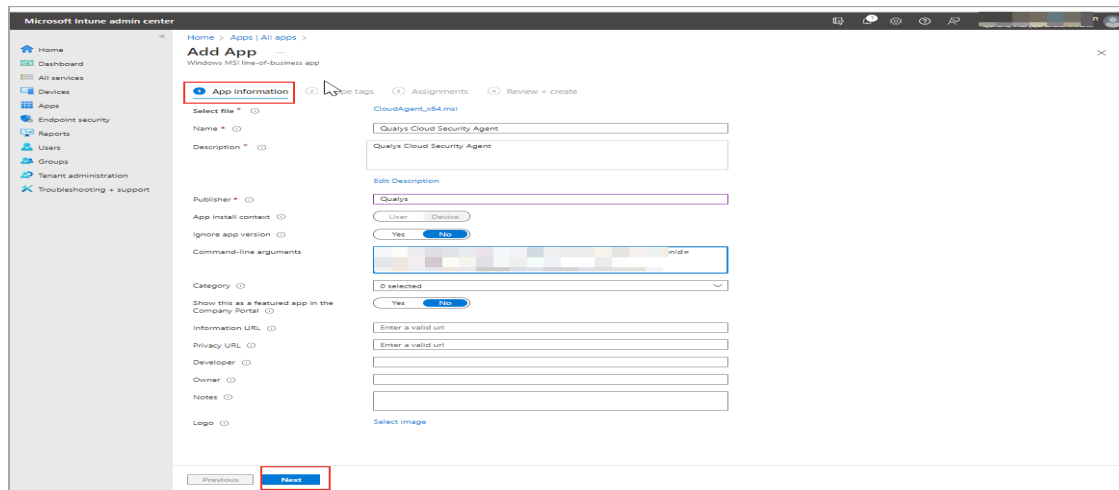
- In the **App package file** pane, upload Cloud Agent package file (.msi) and click **OK**.



- On **App information** page, enter the application information for Cloud Agent.

- In the **Command-line arguments** field, enter the following command:

```
QualysCloudAgent.msi CustomerId={12345678-1234-1234- 1234-123456789012} ActivationId={12345678-1234-1234-1234- 123456789012} WebServiceUri=/CloudAgent/
```



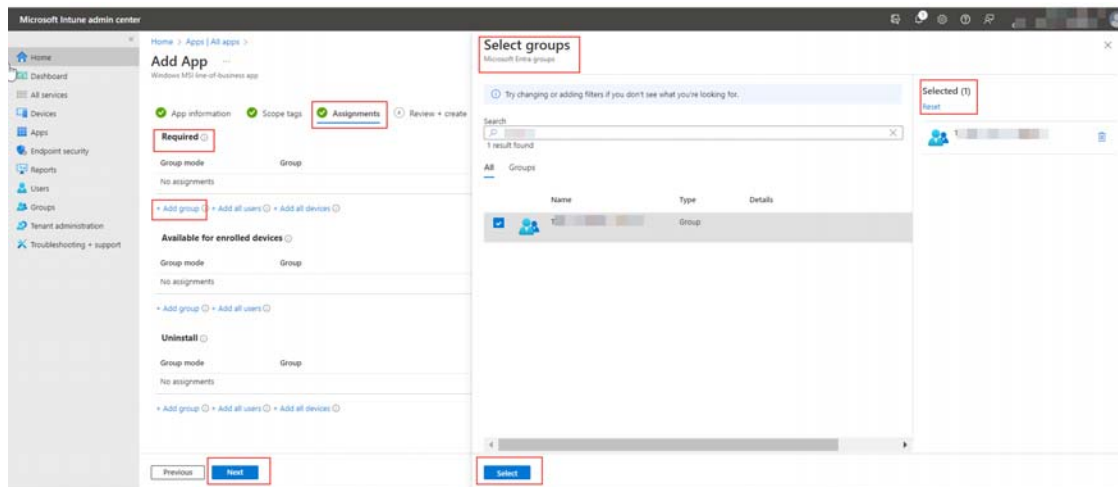
- Click **Next**.

- On the **Scope tags** page specify the scope tags for your Cloud Agent. Click **Next**.

Assignments

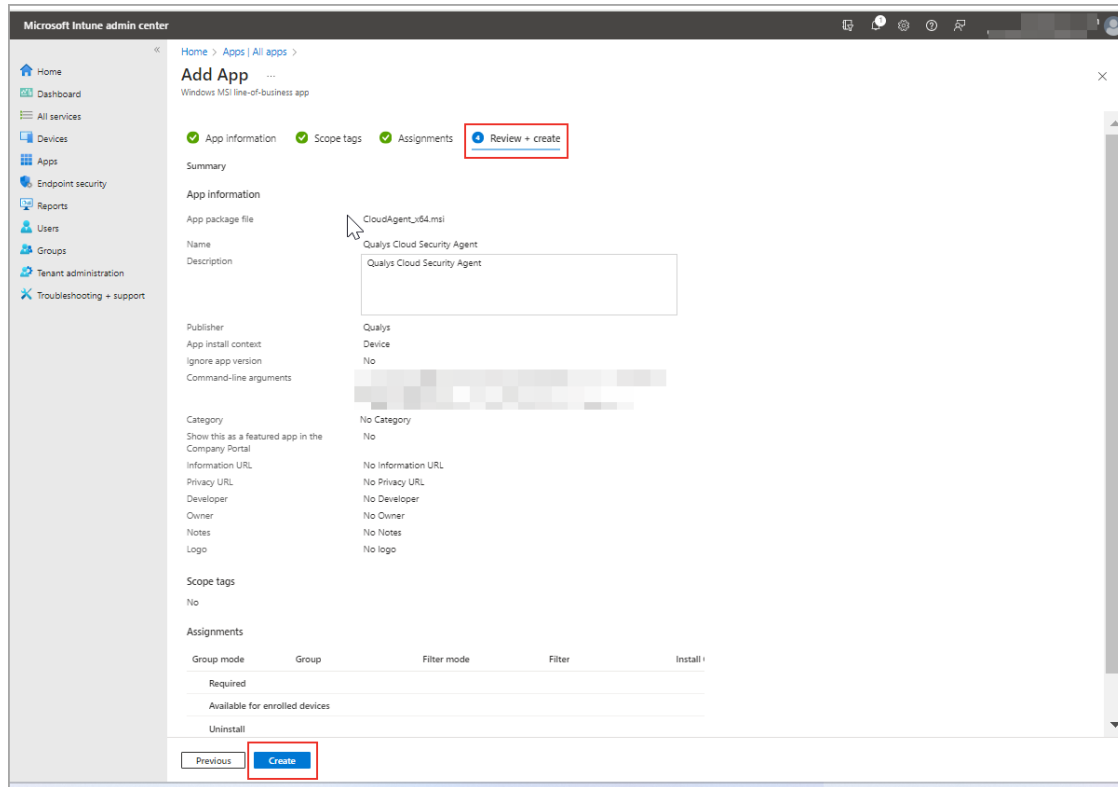
On this page, add the groups to which you want to deploy the Cloud Agent.

- On the **Assignments** page > **Required** section, click **Add groups**. The **Select groups** pane opens.
- In the **Select groups** pane, select the check box associated to the asset groups.
- Click **Select**. You can view the selected asset groups in the **Selected** pane.
- Click **Next**. The **Review + create** page opens.



Review + create

- Review information you entered for the Cloud Agent deployment package.
- Click **Create** to deploy the Cloud Agent.



Note: If required, you can edit the information by navigating to the **Previous** pages.