



Cloud Agent for MacOS

Installation Guide

August 14, 2022

Copyright 2016-2022 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 for Apple MacOS	6
A few things to consider... ..	6
Cloud Agent requirements	6
What are the installation steps?	7
Run as user and user's default group	7
Need help with troubleshooting?	7
Privileges - what are my options?	7
Considerations to select an option best suited to your environment and needs	8
Installation	10
Tips and best practices	10
How to download Agent installer	11
Installation steps	12
What you'll need	12
Steps to install Agents	12
What happens next?	13
Proxy configuration	14
Multiple Proxy Server support in Proxy URL and PAC Files (MacOS Agent 2.5 or later)	16
Anti-Virus and HIPS Exclusion / Whitelisting	17
Qualys Agent (MacOS) Whitelisting	18
Configuration Tool	19
Command line options	19
Use cases	22
Best Practices	23
Upgrading Cloud Agent	23
Uninstalling Cloud Agent	23
Agentless Tracking and Cloud Agents	24
Known issues	25
QualysCloudAgent under MacOS Applications	25
On Demand Scan	26

Proxy Configuration Encryption Utility28

Preface

Welcome to Qualys Cloud Agent for MacOS. 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 Apple MacOS. We'll tell you about Requirements, Installation Steps, Proxy Configuration, Anti-Virus and HIPS Exclusion / Whitelisting, how to use our Agent Configuration Tool, 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 - server, virtual machine, laptop, desktop or cloud instance.

Get informed quickly on Qualys Cloud Agent (CA).

Video Tutorials

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

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

Cloud Agent Platform Availability for Apple MacOS

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](#)

A few things to consider...

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 MacOS, you must have root privileges, non-root with Sudo root delegation, or non-root with sufficient privileges (VM license only). Proxy configuration is supported. [Learn more](#)
- Minimum 512 MB RAM system memory.
- Minimum 100 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.

Run as user and user's default group

Typically, the agent installation requires root level access on the system (for example in order to access the PKG). After the Cloud Agent has been installed it can be configured to run in a specific user and group context using our configuration tool. This ability limits the level of access of the Cloud Agent. [Learn more](#)

Need help with troubleshooting?

We recommend you inspect the agent's log file located here:
`/var/log/qualys/qualys-cloud-agent.log`.

Learn more

[Troubleshooting](#)

[Error messages](#)

Privileges - what are my options?

The Qualys Cloud Agent offers multiple deployment methods to support an organization's security policy for running third-party applications and least privilege configuration. As vulnerability and configuration assessments need to be comprehensive with authenticated scans, the Cloud Agent is installed with SYSTEM level privileges eliminating the need for any authentication credentials to access local system data and artifacts.

This can be updated to any of the following options.

1. Use a non-root account with sufficient privileges:

The specific privileges required are:

- Execute "installer" for automated self-updates
- Agent requires additional commands such as "system_profiler SPInstallHistoryDataType" to operate, which vary depending upon the MAC operating system distribution and customer environment.

Non-root users with limited access may not be able to access certain areas of the system, such as applications installed with root privileges, and may have insufficient results or unable to leverage the full product capability.

2. Use a non-root account with Sudo root delegation

Either the non-root user needs to be assigned sudo privileges directly or through a group membership. Ensure that NOPASSWD option is configured.

Here is an example of an agent user entry in sudoers file (where “agentuser” is the username for the account that you use to install the Linux Agent):

```
%agentuser ALL=(ALL) NOPASSWD: ALL
```

You can also use secure Sudo. When you set UseSudo=1, the agent tries to find the custom path in the `secure_path` parameter located in the `/etc/sudoers` file. This can be used to restrict the path from where commands are picked up during data collection. If this parameter is not set, the agent refers to the `PATH` variable to locate the command by running `sudo sh`.

3. Use an account with root privileges

Typically, you may start with a comprehensive assessment for vulnerabilities and misconfigurations, including privilege access for administrators and root. This agent configuration provides the Cloud Agent for Linux with all the required privileges (for example to access the RPM database) to conduct a complete assessment on the host system and allows for high fidelity assessments with reduced management overheads.

However, after the Qualys Cloud Agent is installed, it can be configured to run as a specific user and group context using our Agent configuration tool. When you create a non-privileged user with full sudo, the user account is exclusive to the Qualys Cloud Agent and you can disable SSH/ remote login for that user, if needed.

The Qualys Cloud Agent does not require SSH (Secure Shell). You can also assign a user with specific permissions and categories of commands that the user can run. If the path is not provided in the command, the system provides the path and only a privileged user can set the `PATH` variables.

Considerations to select an option best suited to your environment and needs

The Qualys Cloud Agent uses multiple methods to collect metadata to provide asset inventory, vulnerability management, and Policy Compliance (PC) use cases. Some of these methods include running commands to collect a list of installed applications and versions, running processes, network interfaces, and so on.

Root access is required for some detections, including most detections that are part of PC (reading global config files related to system-wide security settings and gathering information from more than one user account). There is an exceptionally low number of QIDs in VM module that require root, other QIDs run fine without root. However, those that do need elevated privileges are likely to result into False negatives, if the user does not have the necessary privileges.

Qualys also provides a scan tool that identifies the commands that need root access in your environment. For this scan tool, connect with the Qualys support team. You can decide whether to elevate/grant the required permissions to run the commands or risk losing visibility to the information. You can grant permissions only for the specific commands/binaries that are failing.

Qualys sanitizes the PATH variable to remove any directory which is world writable as a security measure, which is designed to ensure that the Qualys Cloud Agent does not execute any custom-made scripts. This provides the option to harden or whitelist the path, where you can configure the set of allowed directories, on which the commands can be executed during our data collection.

Qualys uses the system-appended paths to run or assume root integrity. As per NIST SP 800-53 Revision 5, control for Vulnerability Monitoring and Scanning RA-5 indicates that in certain situations, the nature of the vulnerability scanning may be more intrusive and require privileged access authorization to selected system components to facilitate more thorough vulnerability scanning.

For **PC scans**, we require the sudo/root privilege. With non-root privilege, the PC report is unreliable and does not provide a complete covering of CIS&DISA policies. As per CIS benchmarks, root privileges are required for specific detections, including most detections that are part of PC (reading global config files related to system-wide security settings and gathering information from more than one user account). Refer to any CIS benchmark (for example, <https://workbench.cisecurity.org/benchmarks/493>) on Linux which broadly assumes that operations are being performed as the root user.

Following is the paragraph from the CIS benchmark document:

“The guidance within broadly assumes that operations are being performed as the root user. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify the root user’s path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.”

For **Patch Management, Endpoint Detection and Response (EDR), and File Integrity Monitoring (FIM)** modules, use an account with root privileges to hook into a system, perform real-time monitoring, to install patches etc., as these modules are not dependent on any signatures/command execution.

Installation

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

Qualys provides installers and packages for each supported operating system that are coded for each Qualys platform. It's not possible to connect an agent coded for one platform to another platform. Organizations can use their existing software distribution tools (SCCM, BigFix, rpm, Casper, etc.) to install the agent into target machines.

The platform supports detection of duplicate agent IDs and automatically re-provisions the duplicate agents.

Customers using software distribution tools must package the Qualys-provided installer along with the specific Activation Key and Customer ID strings to install properly. 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; doing so 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](#)

[How to download Agent installer](#)

[Installation steps](#)

[Proxy configuration](#)

[Multiple Proxy Server support in Proxy URL and PAC Files \(MacOS Agent 2.5 or later\)](#)

[Anti-Virus and HIPS Exclusion / Whitelisting](#)

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 and license count.

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 continuously. If your agent doesn't have a status, it has not successfully connected to the cloud platform and you need to troubleshoot.

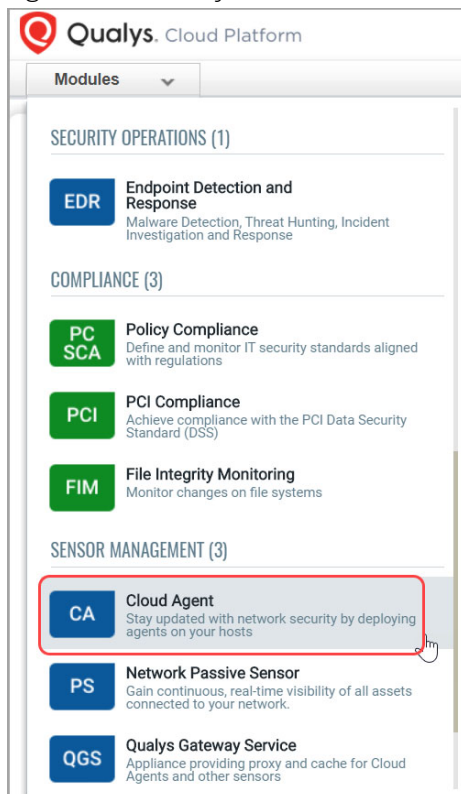
Upgrading agents manually If you upgrade the agents manually or using external deployment tools like puppet, explicit restart is required. It is recommended to restart the agent service immediately after upgrade.

How to download Agent installer

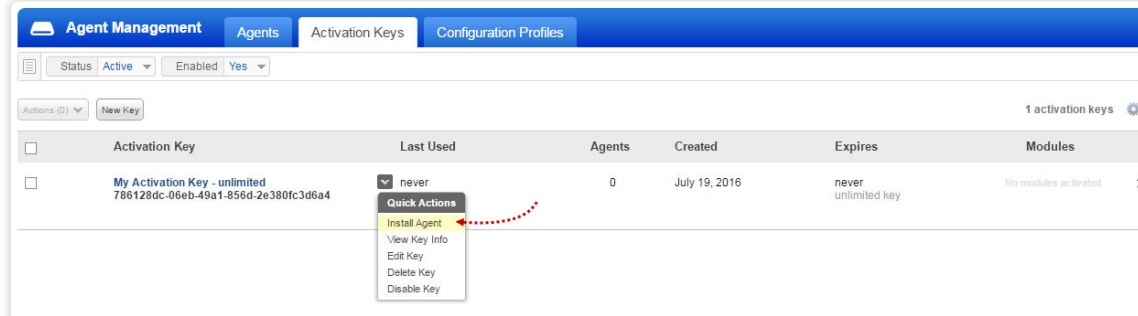
Download an installer of Qualys Cloud Agent for MacOS

Here's how to download an installer 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** for MacOS (.pkg).

Installation Requirements		
Windows (.exe)	Windows XP SP3 and above Windows Server Editions	Install instructions
Linux (.rpm)	Red Hat Linux 5 and above CentOS 5.11 and above Fedora openSUSE 11, 12 SUSE 11, 12 Amazon Linux	Install instructions
Linux (.deb)	Debian 7, 8 Ubuntu 12, 14, 15	Install instructions
Mac (.pkg)	OS X Yosemite (version 10.10) OS X El Capitan (version 10.11)	Install instructions

Click the **Download** button. This downloads the Agent .pkg file to your local system. You'll see the installation command and your Activation key ID and Subscription ID in the UI - 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 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 MacOS (.pkg) to get everything you need. See [Cloud Agent requirements](#).

Steps to install Agents

1. Copy the Qualys Cloud Agent installer onto the target host.
 2. Install the Qualys Cloud Agent using the following commands:
- If your installer package is **qualys-cloud-agent.x86_64.pkg**, use command:

```
sudo installer -pkg ./qualys-cloud-agent.x86_64.pkg -target /
sudo /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent.sh
ActivationId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
```

- If your installer package is **QualysCloudAgent.pkg**, use command:

```
sudo installer -pkg ./QualysCloudAgent.pkg -target /  
sudo /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-  
cloud-agent.sh  
ActivationId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx  
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx
```

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. 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.

Note: Qualys Cloud Agent is designed to run in the background and requires no user interaction. As such you are advised not to try launching the Qualys Cloud Agent from the Applications folder. The Qualys Cloud Agent should be already running in the background.

You might also be interested in...

[Proxy configuration](#)

[Multiple Proxy Server support in Proxy URL and PAC Files \(MacOS Agent 2.5 or later\)](#)

[Anti-Virus and HIPS Exclusion / Whitelisting](#)

Proxy configuration

This section helps you to enable the MacOS agent to use a proxy for communication with our cloud platform.

Note:

If proxy connection fails then agent will NOT attempt a direct connection outbound (Fail Closed).

Proxy configuration on MacOS 1.7 or later agents

- 1) if /Library/Application Support/QualysCloudAgent/Config/proxy file doesn't exist create it
- 2) add 1 of the following lines to the file (1 line only):

```
https_proxy=https://[<username>:<password>@]<host>[:<port>]
qualys_https_proxy=https://[<username>:<password>@]<host>[:<port>]
```

where <username> and <password> are specified if the https proxy uses authentication. If special characters are embedded in the username or password (e.g. @, :, \$) they need to be url-encoded. where <host> is the proxy server's IPv4 address or FQDN. where <port> is the proxy's port number.

If the proxy is specified with the https_proxy environment variable, it will be used for all commands performed by the Cloud Agent. If the proxy is specified with the qualys_https_proxy environment variable, it will only be used by the Cloud Agent to communicate with our cloud platform.

Note: You can use the [Proxy Configuration Encryption Utility](#) to encrypt the user name and password that you provide to the proxy environment variable.

- 3) change the permissions using these commands:

```
chown root /Library/Application Support/
QualysCloudAgent/Config/proxy

chmod 660 /Library/Application Support/
QualysCloudAgent/Config/proxy
```

Alternatively, you can set automatic proxy by going to Mac System Preferences > Network > Advanced > Proxies tab. Select Automatic Proxy Configuration and provide the pac file.

Note: Qualys proxy configured in the **.../QualysCloudAgent/Config/proxy** file will take preference over any proxies set in System Preferences (including Automatic Proxy, Web Proxy (HTTP), or Secure Web Proxy (HTTPS)).

Proxy configuration on MacOS 1.5 and 1.6 agents

1) if /Applications/QualysCloudAgent.app/Contents/Config/proxy file doesn't exist create it

2) add 1 of the following lines to the file (1 line only):

```
https_proxy=https://[<username>:<password>@]<host>[:<port>]  
qualys_https_proxy=https://[<username>:<password>@]<host>[:<port>]
```

where <username> and <password> are specified if the https proxy uses authentication. If special characters are embedded in the username or password (e.g. @, :, \$) they need to be url-encoded. where <host> is the proxy server's IPv4 address or FQDN. where <port> is the proxy's port number.

If the proxy is specified with the https_proxy environment variable, it will be used for all commands performed by the Cloud Agent. If the proxy is specified with the qualys_https_proxy environment variable, it will only be used by the Cloud Agent to communicate with our cloud platform.

3) change the permissions using these commands:

```
chown root /Applications/QualysCloudAgent.app/  
Contents/Config/proxy
```

```
chmod 660 /Applications/QualysCloudAgent.app/  
Contents/Config/proxy
```

Need to Bypass Proxy?

By default the Cloud Agent for MacOS will operate in non-proxy mode.

But in the event, if you are already using proxy mode and need to switch to non-proxy mode, you need to configure agent to use no_proxy in /Library/Application Support/QualysCloudAgent/Config/proxy. Environment variable 'no_proxy' is used to bypass proxy. Curl library honors 'no_proxy' environment variable. If 'no_proxy' is set, curl will not use proxy even if any proxy environment variable is set.

Here are the steps to enable the MacOS agent to use a no_proxy for communication with our cloud platform:

1) Edit /Library/Application Support/QualysCloudAgent/Config/proxy file.

2) Add following lines (bold faced) where qualys_https_proxy is mentioned:

```
export qualys_https_proxy=https://[<username>:<password>@]<host>[:<port>]  
export no_proxy=<pod domain name>
```

Multiple Proxy Server support in Proxy URL and PAC Files (MacOS Agent 2.5 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 until all proxy servers are attempted. You can have up to five proxy servers included in the proxy URL.

Each time the Cloud Agent connects to the Qualys Platform, it always uses the first proxy server in the ordered list. You can use the [Configuration Tool](#) to set the proxy order to be sequential or random. 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.

You can configure multiple proxies in the proxy file mentioned in the section [Proxy configuration on MacOS 1.7 or later agents](#).

Multiple proxies can be configured with `qualys_https_proxy` or `https_proxy` environment variables. It is recommended that you provide multiple proxies in the `qualys_https_proxy` environment variable.

The following example shows how to set multiple proxies:

```
qualys_https_proxy="https://[username]:<password>@<host1>:<port>;  
https://[username]:<password>@<host2>:<port>;  
https://[username]:<password>@<host3>:<port>"
```

The list of proxies must be given in double quotes (“...”) and separated by a semi-colon (;), and if “;” is embedded in username/password, you must url-encode it. You can use the [Proxy Configuration Encryption Utility](#) to encrypt the user name and/or password that you provide to the proxy environment variable.

You can combine multiple proxy certificates into a single file, and place it at same location as earlier `/Applications/QualysCloudAgent.app/Contents/Config/cert/ca-bundle.crt`. Ensure that all certificates are valid, else you might get SSL/certificate errors.

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. The following information applies to MacOS Agent 1.7 and later.

Directory list used by Cloud Agent installation

```
/etc/qualys  
/Applications/QualysCloudAgent.app  
/Applications/QualysCloudAgent.app/Contents  
/Applications/QualysCloudAgent.app/Contents/MacOS  
/Applications/QualysCloudAgent.app/Contents/Frameworks  
/Applications/QualysCloudAgent.app/Contents/Docs  
/Applications/QualysCloudAgent.app/Contents/Info.plist  
/Applications/QualysCloudAgent.app/Contents/Resources  
/Applications/QualysCloudAgent.app/Contents/_CodeSignature  
/Library/Application Support/QualysCloudAgent/Data  
/Library/Application Support/QualysCloudAgent/Config
```

Note: On MacOS 1.5 and 1.6 agents, the Data and Config directories are located at:

```
/Applications/QualysCloudAgent.app/Contents/Data  
/Applications/QualysCloudAgent.app/Contents/Config
```

Agent daemon process “qualys-cloud-agent”

The agent runs as daemon process “qualys-cloud-agent”.

The agent runs various read-only commands during the scanning process. These are the same commands run by a scan using a scanner appliance. [Learn more](#)

Some transient files are created during agent execution

```
/Library/Application Support/QualysCloudAgent/Data/*.db
```

- these are various sqlite DB files necessary for Qualys Cloud Agent functionality.

```
/Applications/QualysCloudAgent.app/Contents/MacOS/*.sh
```

- these are various utility scripts used by Qualys Cloud Agent

```
/Library/Application Support/QualysCloudAgent/Data/manifests/*.db
```

- this contains manifests used during agent based scans

Note: On MacOS 1.5 and 1.6 agents, the Data directory is located at:

```
/Applications/QualysCloudAgent.app/Contents/Data
```

Qualys Agent (MacOS) Whitelisting

MacOS 10.15 and onwards, applications need to be granted appropriate permissions for privacy features and services.

QualysCloudAgent.app does not install kernel extensions (KEXT) or System Extensions.

QualysCloudAgent.app needs to be explicitly whitelisted for below privacy feature:

Enable Full Disk Access (FDA)

This privacy permission can be manually managed by users in **System Preferences > Security & Privacy > Privacy > Full Disk Access**.

To grant authorization for FDA for QualysCloudAgent.app with help of MDM like Jamf/Meraki, use below Bundle Identifier and Team Identifier:

Bundle Identifier=com.qualys.cloud-agent

TeamIdentifier=CLRUMG7LZ6

Configuration Tool

The Agent Configuration Tool gives you many options for configuring Cloud Agent for MacOS. Our configuration tool allows you to:

- Provision agents
- Configure logging - set a custom log level and log file path
- Enable Sudo to run all data collection commands
- Configure the daemon to run as a specific user and/or group
- Change the ActivationID, CustomerID and/or platform configuration

The Agent will automatically pick up changes made through the configuration tool so there is no need to restart the agent or reboot the agent host.

Configuration tool location:

/Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent.sh

Command line options

qualys-cloud-agent.sh supports these command line options.

Configuration option	Description
ActivationId	A valid activation key ID (UUID). This value is obtained from the Cloud Agent UI (go to Activation Keys, select a key then View Key Info). This parameter is required to provision an agent.
CustomerId	A valid customer ID (UUID). This value is obtained from the Cloud Agent UI (go to Activation Keys, select a key then Install Agent). This parameter is required to provision an agent.
LogLevel	A log level (0-5). A higher value corresponds to more verbosity. Default is mapped to information (3). 0 - mapped to fatal 1 - mapped to error 2 - mapped to warning 3 - mapped to information 4 - mapped to debug 5 - mapped to trace Note: In a debug/trace mode, the log file may contain sensitive command-line parameters or passwords for configuration files, if the passwords are in clear-text format. Qualys recommends you use a password vault or token-based authentication instead of storing passwords in the configuration file. Storing passwords in configuration files can result in non-compliance with ISO, SOC, PCI-DSS, HIPAA, and FedRAMP guidelines.

Configuration option	Description
LogFileDir	A full path to the log file. By default the path is /var/log/qualys/
UseSudo	Set to 1 to run all data collection commands using the sudo escalation method. By default sudo is not used (0).
SudoCommand	A command for privilege escalation such as SudoCommand pbrun. If the command has spaces it must be double quoted.
User	A valid username if you want the daemon to run as a certain user. The daemon will start as root but will drop to the specified user, and continue running as the specified user.
Group	A valid group name if you want the daemon to run as a certain group. The daemon will switch to the specified group (if any).
HostIdSearchDir	The directory where the host ID file is located. This file contains a host ID tag assigned to the system by Qualys. By default the directory is /etc/ and the location of the host ID file is /etc/qualys/hostid
LogDestType	The destination of log lines generated by MacOS Agent. Set to file or syslog . If set to file specify the location of the log file. By default the destination is a log file: /var/log/qualys/qualys-cloud-agent.log
ServerUri	Use this option to migrate the agent from one Qualys subscription to another (on same POD or PCP). ServerUri takes the URL of the Qualys shared Pod or PCP you want to migrate the Agent to, in the following format: ServerUri=<http_url>/CloudAgent where <http_url> is the URL of the Qualys shared Pod or PCP. If the subscription is on the same POD, the ServerUri is the same. Use this option along with ActivationId and CustomerId in order to move the agent to another Qualys shared Pod or PCP. Note: The agent requires the appropriate Activation ID and Customer ID that are on the new subscription/platform. The original IDs cannot be used as they are unique per subscription.
CmdMaxTimeOut	Execution of a command is dropped if the time taken to execute is more than the specified value. Default timeout is 1800 seconds (30 minutes).

Configuration option	Description
ProcessPriority	Specify the Linux niceness scale between -20 to 19 to set a priority for the Qualys cloud agent process. The lower the number the more priority the agent process gets. Default value is zero.
QualysProxyOrder	If you are using multiple proxies, set the proxy order to be sequential or random. Sequential: <code>QualysProxyOrder=sequential</code> OR <code>QualysProxyOrder=seq</code> Random: <code>QualysProxyOrder=random</code>

Use cases

Example 1 - Provision Agent

The following example shows how to provision Qualys Cloud Agent. Please note that this method of activation will assume that root user should be used by the agent.

```
$ /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent.sh  
ActivationId="022224c8-31c7-11e5-b4f7-0021ccba987e"  
CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e"
```

Example 2 - Use non-root account

The following example shows how to configure Qualys Cloud Agent to use a non-root account for running data collection commands.

```
$ /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent.sh  
ActivationId="022224c8-31c7-11e5-b4f7-0021ccba987e"  
CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e" UseSudo=1  
User=scanuser  
Group=wheel
```

Keep in mind - A new group needs to exist when the configuration command runs. The expectation is that the non-root user will be added to the specified group to allow it to access binary and temporary files that comprise Qualys Cloud Agent. In order to perform unattended data collection the non-root user needs to have sudo privilege without a password.

Example 3 - Raise logging level

It is also possible to instruct Qualys Cloud Agent to log events at a higher than normal logging level using the following command:

```
$ /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent.sh LogLevel=4
```

Note: We've omitted the ActivationID and CustomerID parameters to illustrate the configuration tool can be used to adjust the log level after provisioning.

Best Practices

Here are some best practices for managing your cloud agents. Refer to the Cloud Agent Technical Whitepaper for additional documentation and best practices.

Upgrading Cloud Agent

The Qualys Cloud 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 to upgrade already installed agents. In those cases the agents are not configured to auto-upgrade versions.

Use following commands to upgrade your Cloud Agent:

```
sudo /Applications/QualysCloudAgent.app/Contents/MacOS/qagent_upgrade.sh  
package_file
```

Where *package_file* is the installer of the agent version you want to upgrade to.

Note: If needed, restart agent using following command

```
/Applications/QualysCloudAgent.app/Contents/MacOS/qagent_restart.sh
```

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 from the host itself (using the uninstall utility), the agent record, 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.

Sample uninstall of agent using uninstall utility:

```
sudo /Applications/QualysCloudAgent.app/  
Contents/MacOS/qagent_uninstall.sh
```

Note: On macOS High Sierra (10.13), launchd takes some time to remove the **com.qualys.cloud-agent** process, although the agent is already uninstalled.

Agentless Tracking and Cloud Agents

Say you're already using Agentless Tracking on hosts and now you're ready to install Cloud Agent on the same hosts. You'll want to use the same host ID tag installed on the host. This will help you to avoid duplicate assets for the same host in your account.

You can configure the location of the host ID file installed on your MacOS hosts with the recommended default of /etc (the agent will create/use a 'qualys' directory under /etc). This is recommended best practice if you are interested in using MacOS Agent and Agentless Tracking to evaluate the same host.

Once configured, the same file with the same host ID tag is accessed by our service when the host is evaluated using 1) Agentless Tracking AND 2) Cloud Agent.

What are the steps?

1) Check your Unix authentication record

This is the record you're using to access the system using Agentless Tracking. You'll see the location of the host ID file configured for the authentication record.

Want help with Agentless Tracking? Log into the Qualys Cloud Platform, go to Help > Contact Support and search for **Agentless Tracking**.

2) Install the Agent

Use the agent configuration tool (qualys-cloud-agent.sh) and the HostIdSearchDir option to install the MacOS Agent and configure the location of the host ID file. Be sure this location matches the location defined in your authentication record. By default HostIdSearchDir is set to /etc/. To stay consistent with the Agentless Tracking location Qualys appends "/qualys/hostid" to the path provided.

Example - Install as root user and set host ID file to /mydir/qualys/hosted

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh  
ActivationId="022224c8-31c7-11e5-b4f7-0021ccba987e"  
CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e"  
HostIdSearchDir="/mydir/"
```

How you can resolve this

1) Configure HostIdSearchDir for your agent

Configure the location of the host ID file using the agent configuration tool (qualys-cloud-agent.sh) and the HostIdSearchDir option.

Example - Install as root user and set host ID file to /mydir/qualys/hostid

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh HostIdSearchDir="/mydir/"
```

2) Uninstall duplicate agents not communicating

Click [here](#) for instructions.

Known issues

Here are some known issues/limitations in the cloud agents.

QualysCloudAgent under MacOS Applications

MacOS 10.10.x may show the old Qualys logo for QualysCloudAgent under MacOS Applications folder. Quick Look for QualysCloudAgent also displays the old Qualys logo.

Note: Qualys Cloud Agent is designed to run in the background and requires no user interaction. As such you are advised not to try launching the Qualys Cloud Agent from the Applications folder. The Qualys Cloud Agent should be already running in the background.

On Demand Scan

You can run an On Demand Scan to instruct the agent to immediately scan as long as the agent is not already scanning. The On Demand Scan runs independently of the interval scan that you configure in the Configuration Profile and will reset the scan interval on the local agent after a successful scan.

Prerequisite: The agent must be activated for that specific Qualys application for which you are running the On Demand Scan. When activated, the Agent downloads manifests for that application from the Qualys platform; if the manifest is not present for that type, On Demand Scan will not execute.

Use the `cloudagentctl.sh` script to run the OnDemand Scan. You'll find this script at `/Applications/QualysCloudAgent.app/Contents/MacOS/`.

```
># ./cloudagentctl.sh action={demand} type={vm|pc|inv|udc|sca|vmpc}
cputhrottle={0-1000}
```

Where `action` and `type` are mandatory parameters.

action is "demand", meaning an On Demand Scan.

type is the application for which you want to run the scan (the agent must be activated for the respective application first).

Note: "vmpc" is a legacy application manifest and most likely may not be present.

cputhrottle is 1-1000. Default is 0, which is no throttling.

For example, to initiate an On Demand Scan for the Vulnerability Management application (VM) with no throttling:

```
># ./cloudagentctl.sh action=demand type=vm
```

The script calls the agent to run asynchronously in the background and returns to the shell prompt. The script prints a `ControlId` that you can track in the log file. The `ControlId` is the timestamp of the script initiation, e.g. On-Demand-Request `ControlId`:
20200427151136.0

The On Demand Scan logs to the same log file as the agent at `/var/log/qualys/qualys-cloud-agent.log`. You can find the logging for the scan initiation and completion in the log file.

```
2020-04-27 15:11:36.474 [qualys-cloud-agent][9710]:[Information]:[140048573286144]:OnDemandRequest Params:
ControlID=20200427151136.0, Action=OnDemand, Type=VM, CPUThrottle=0"
```

If the agent is currently performing an interval scan for the same type, the On Demand Scan will delay waiting for the currently running scan to finish. The script will print a log line with this status.

```
2020-04-27 15:11:36.474 [qualys-cloud-agent][9710]:[Information]:[140048573286144]:Interval Event of same type
is in progress with state INTERVAL_EVENT_SCAN
```

```
2020-04-27 15:11:36.474 [qualys-cloud-agent][9710]:[Information]:[140048573286144]:OnDemand request for Control ID : 20200427151136.0 will be delayed.
```

If the script errors due to the manifest file not being present, check whether the Cloud Agent is activated for that particular application. If agent is activated but you still get manifest related errors while running the On Demand Scan command, the agent may not have downloaded the manifest for that application. You can manually force a manifest download by deactivating then reactivating the agent for that application from the Cloud Agent user interface module. If that doesn't correct the issue, contact Qualys Support.

Once an On Demand Scan is complete the results are logged in the log file located at `/var/log/qualys/qualys-cloud-agent.log`.

Proxy Configuration Encryption Utility

You can use the Proxy Configuration Encryption utility to encrypt the user name and/or password (as needed) that you provide to the proxy environment variable `qualys_https_proxy` or `https_proxy`.

The **string-util** utility is included in the Cloud Agent installation package. Install or extract the Cloud Agent installation package to get the utility.

The `string-util` utility is to be used once on any system where it's installed to encrypt the values that will be used on all systems running Cloud Agent that have the same credentials. It is not required to run the utility on each system running Cloud Agent.

Use the following command to run the utility to encrypt the user name and/or password. If you want to encrypt both, run the utility twice to separately encrypt the user name and password.

Note: You need root privileges to run `string-util`. If the user name or password contain special characters (e.g., @, :, \$) they need to be url-encoded prior to using the utility.

To encrypt the user name (use double quotes):

```
./string-util "<user name_to_be_encrypted>"
```

For example,

```
./string-util "sys_account"
```

To encrypt the password (use double quotes):

```
./string-util "<password_to_be_encrypted>"
```

The utility returns the user name or password in encoded format.

For example,

```
sRpSHQP582a1+gaJwH0m3g==
```

Provide the encrypted user name and password to your proxy environment variable.

```
qualys_https_proxy=https://[<#encrypted_username>:<#encrypted_password>@<host>[:<port>]
```

The # delimiter indicates to the Cloud Agent that the user name and password are encrypted. Not including the # indicates that the user name and password are in plain text format.

For example (only encrypting password):

```
qualys_https_proxy=https://sys_account:#sRpSHQP582a1+gaJwH0m3g==@proxy.myc.com:8080
```

For example (encrypting username and password):

```
qualys_https_proxy=https://#uWpsHMSY932b2+fdcH723d==:#sRpSHQP582a1+gaJwH  
Om3g==@proxy.myco.com:8080
```