



QUALYS®

Cloud Agent for Mac

Installation Guide

Agent Version 1.5 - 1.6

June 1, 2017

CONTINUOUS SECURITY

Copyright 2016-2017 by Qualys, Inc. All Rights Reserved.

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

Qualys, Inc.
1600 Bridge Parkway
Redwood Shores, CA 94065
1 (650) 801 6100

CONTENTS

Preface

Chapter 1 Get Started

Qualys Cloud Agent Introduction	5
Cloud Agent Platform Availability for Apple Mac	6
A few things to consider.....	7
Cloud Agent requirements	7
What are the installation steps?.....	7
Run as user and user's default group.....	7
Need help with troubleshooting?	7
Credentials - what are my options?	8

Chapter 2 Installation

Tips and best practices.....	10
How to download Agent image.....	11
Installation steps	12
What you'll need	12
Steps to install Agents.....	12
What happens next?.....	12
Proxy configuration.....	13
Anti-Virus and HIPS Exclusion / Whitelisting.....	14

Chapter 3 Configuration Tool

Command line options	16
Use cases	17
Example 1 - Provision Agent	17
Example 2 - Use non-root account	17
Example 3 - Raise logging level.....	17

Chapter 4 Best Practices

How to Uninstall Cloud Agent from the command line	19
Agentless Tracking and Cloud Agents.....	19

Preface

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

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,200 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.



CHAPTER 1

Get Started

Thank you for your interest in Qualys Cloud Agent!

This document tells you all about installing Qualys Cloud Agent for Apple Mac. 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 anywhere - such as laptop, desktop or virtual machine.

Watch the overview for an introduction.

Videos from the Qualys Community

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

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

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

Learn more from the Qualys Community

[CA Platform Announcement](#)

[Getting Started Guide](#)



Cloud Agent Platform Availability for Apple Mac

Current GA Release: 1.6.0

Vendor	Supported Platforms			Supported Qualys Modules/Agent Versions				
	Operating System	Arch	Installer	Inventory Scan	VM	PC	FIM Beta	IOC Beta
Apple	OS X Yosemite (10.10)	x86_64	(.rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	Not available	Not available
Apple	OS X El Capitan (10.11)	x86_64	(.rpm)	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	1.5.0.61-1.6.0.61	Not available	Not available
Apple	macOS Sierra (10.12)*	x86_64	(.rpm)	1.6.0.61	1.6.0.61	1.6.0.61	Not available	Not available

* Upgrading from El Capitan (10.11) to Sierra (10.12) will delete needed directories used by the agent, causing the agent to not start. Use the following commands to fix the directory.

- 1) `mkdir /var/log/qualys`
- 2) `chmod 640 /var/log/qualys`
- 3) if non-root: `chown non-root.non-root-group /var/log/qualys`
- 4) `/Applications/QualysCloudAgent.app/Contents/MacOS/qagent_restart.sh`

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 Mac, 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](#)

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 RPM database). 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`

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

Qualys Help

[Troubleshooting](#)

[Error messages](#)

Credentials - what are my options?

Use an account with root privileges

This is recommended as it gives the Cloud Agent for Mac enough privileges to gather necessary information for the host system's evaluation.

Use a non-root account with Sudo root delegation

Either the non-root user needs to have sudo privileges directly or through a group membership. Be sure NOPASSWD option is configured.

Here is an example of agentuser entry in sudoers file (where "agentuser" is the user name for the account you'll use to install the Mac Agent):

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

Use non-root account with sufficient privileges (VM only)

The specific privileges needed are:

- 1) execute "rpm" for automatic update
- 2) commands required for data collection (see Sudo command list at the Community)

From the Qualys Community

[Sudo command list](#)

Installation

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

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

[Tips and best practices](#)

[How to download Agent image](#)

[Installation steps](#)

[Proxy configuration](#)

[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.

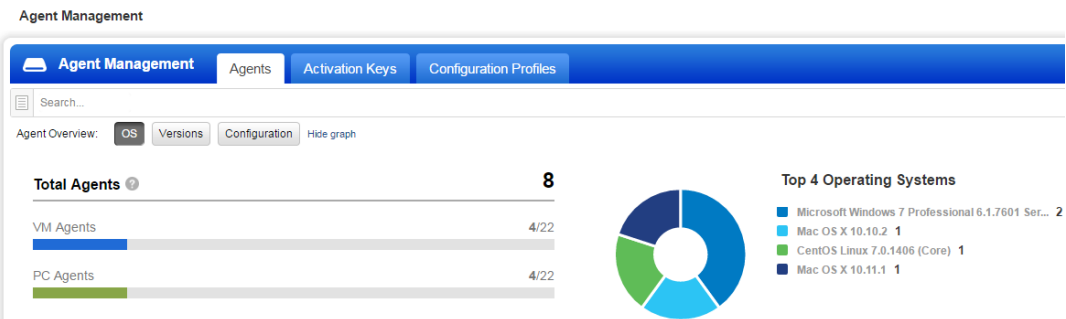
Be sure to activate agents to provision agents for modules - Vulnerability Management (VM), Policy Compliance (PC), or both. Activating an agent for a module consumes an agent license. You can set up auto activation by defining modules for activation keys, or do it manually in the Cloud Agent UI.

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:

Total Agents - All installed agents that have successfully connected to the Qualys Cloud Platform (includes unlicensed agents)

VM Agents/PC Agents - Count of licensed agents per module (i.e. activated/purchased licenses)



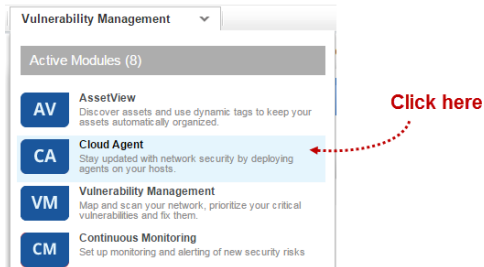
Check to be sure agents are connected Once installed agents immediately connect to the Qualys Cloud Platform and register themselves. You can see agent status on the Agents tab - this is updated continuously. If your agent doesn't have a status, it has not successfully connected to the cloud platform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

How to download Agent image

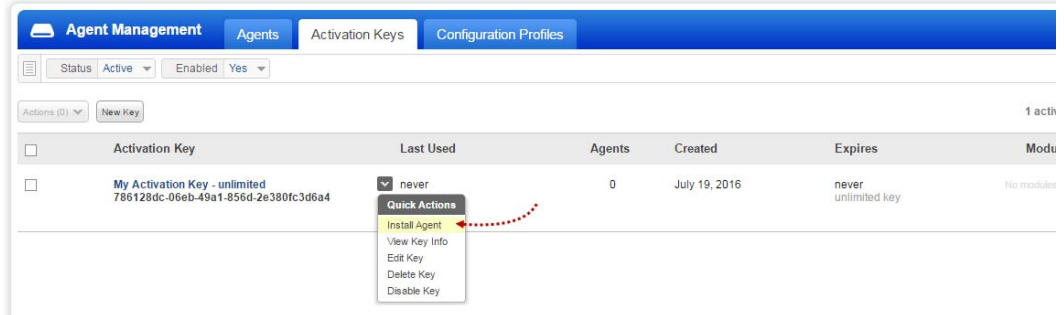
Download an image of Qualys Cloud Agent for Mac

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

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



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



Click **Install instructions** for Mac (.pkg).



Click **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 image and get the associated ActivationID and CustomerID. Just log into the Qualys Cloud Platform, go to the Cloud Agent (CA) module, and follow the installation steps for Mac (.pkg) to get everything you need.

[Cloud Agent requirements](#)

Steps to install Agents

1. Copy the Qualys Cloud Agent image onto the target host.
2. Install the Qualys Cloud Agent using the following commands:

Mac Agent 1.5 and later

```
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-xxxxxxxxxxxx  
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Mac Agent 1.4

```
sudo installer -pkg ./qualys-cloud-agent.x86_64.pkg -target /  
sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh  
ActivationId=6xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx  
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

What happens next?

We'll start syncing asset data to the cloud!

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

You might also be interested in...

[Proxy configuration](#)

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

Proxy configuration

How to enable a proxy

Good to Know The MacOS agent will consult the system settings for HTTPS proxy specification. If HTTPS proxy is not specified the agent will operate without a proxy. The proxy is set for system-wide proxy through System_Preference/Network. Only proxies set for the following options are honored: Web Proxy (HTTP), Secure Web Proxy (HTTPS).

Tell me the steps

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

- 1) if `/etc/qualys/cloud-agent/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 /etc/qualys/cloud-agent/proxy  
chmod 644 /etc/qualys/cloud-agent/proxy
```

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 Mac Agent 1.5 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/Library  
/Applications/QualysCloudAgent.app/Contents/Data
```

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

```
/Applications/QualysCloudAgent.app/Contents/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  
  
/Applications/QualysCloudAgent.app/Contents/Data/manifests/*.db  
- this contains manifests used during agent based scans
```

Configuration Tool

Our easy to use tool gives you many options for configuring Cloud Agent for Mac. 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

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.

Mac Agent 1.5 and later

Configuration tool location:

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

Mac Agent 1.4

Configuration tool location:

`/usr/local/qualys/cloud-agent/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 to report only errors (0).
LogFilePath	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 Mac 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

Use cases

The following sample commands assume you're using Mac Agent 1.5 and later. (Have Mac Agent 1.4? [Click here](#) for details).

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's best practices for managing your cloud agents.

How to Uninstall Cloud Agent from the command line

When you uninstall a cloud agent the agent is removed from the Qualys subscription account. We'll also purge the associated agent host (i.e. remove all host data from the account, including inventory data and scan data).

```
sudo /usr/local/qualys/cloud-agent/bin/qagent_uninstall.sh
```

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 hosts. This is recommended best practice if you are interested in using Mac 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 Mac 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/hosted`

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

2) Uninstall duplicate agents not communicating

Click [here](#) for instructions.