Cloud Agent for Unix

Installation Guide

Agent Version 1.6

June 28, 2017

CONTINUOUS SECURITY

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

CONTENTS

Preface

Welcome to Qualys Cloud Agent for Unix. 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 Unix. 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 Unix

Current Release: 1.6.2

Release Status: Private Beta (on/after July 17, 2017)

For invitation only contact your Technical Account Manager to join the beta

Supported Platforms				Supported Qualys Modules/Agent Versions				
Vendor	**Operating System**	**Arch**	**Installer**	**Inventory**	**VM**	**PC**	**FIM Beta**	**IOC Beta**
IBM	AIX 7.1 TL2, TL3, TL4 AIX 7.2 TL1 (Standard and Enterprise Editions)	POWER 64-bit	(.rpm)	1.6.2	1.6.2	1.6.2	*not available*	*not available*
IBM	AIX 6.1 TL0-9 (Standard and Enterprise Editions)	POWER 64-bit	(.rpm)	1.6.2	1.6.2	1.6.2	*not available*	*not available*

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 Unix, 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. You might want to configure proxy settings for our agent to communicate with our cloud platform.

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 Unix 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 Unix 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

CHAPTER 2

Installation

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

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

Tips and best practices

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

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

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

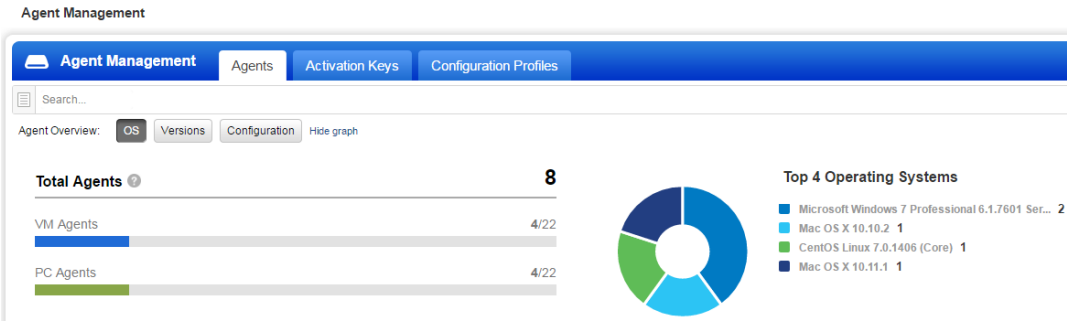
Be sure to activate agents to provision agents for modules - Vulnerability Management (VM), Policy Compliance (PC), or both. Activating an agent for a module consumes an agent license. You can set up auto activation by defining modules for activation keys, or do it manually in the Cloud Agent UI.

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

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



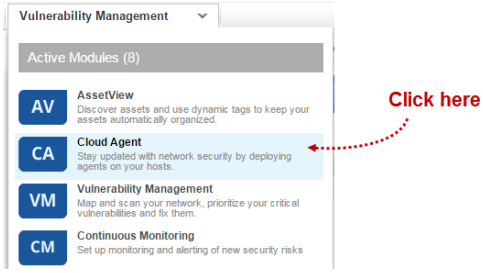
Check to be sure agents are connected Once installed agents immediately connect to the Qualys Cloud Platform and register themselves. You can see agent status on the Agents tab - this is updated continuously. If your agent doesn't have a status, it has not successfully connected to the cloud platform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

How to download Agent image

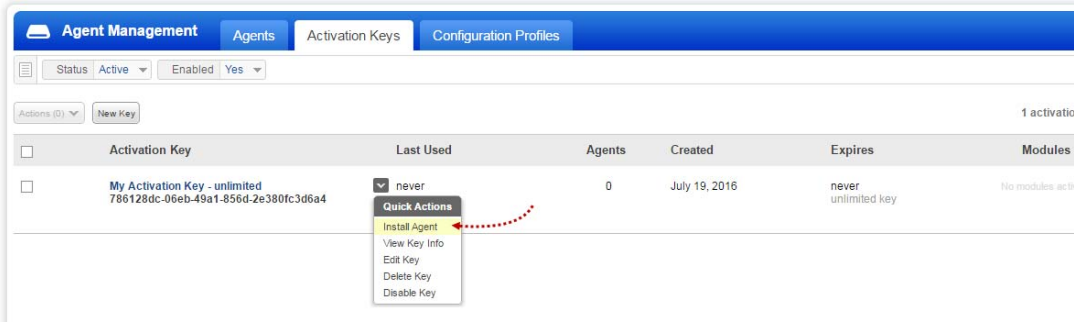
Download an image of Qualys Cloud Agent for Unix

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.

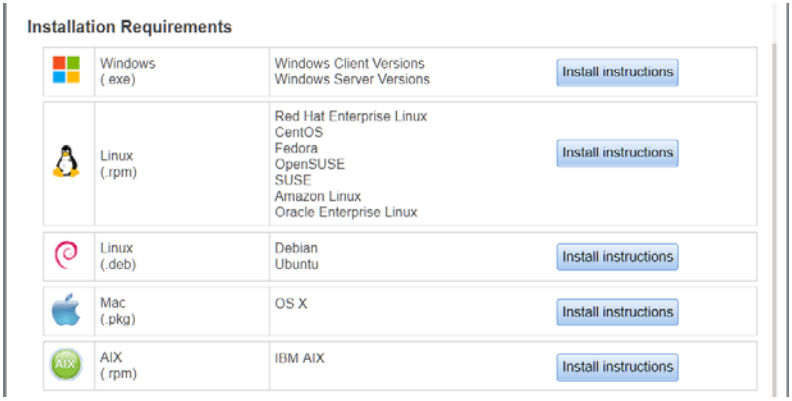


Choose an activation key (create one if needed) and select **Install Agent** from the Quick Actions menu.



Click **Install instructions** for the target host and then click **Download**.

Note that AIX should be enabled in your Qualys subscription for you to see it in this list.



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

Installation steps

What you'll need

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

Cloud Agent requirements

Steps to install Agents on AIX

1. Copy the Qualys Cloud Agent image onto the target host.

2. Install the Qualys Cloud Agent using the following commands:

```
> sudo rpm -ivh qualys-cloud-agent.aix_power_64.rpm
> sudo /opt/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId=xxxxxxxx-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.

Troubleshooting

You'll find helpful information in Qualys online help.

Qualys Help

Troubleshooting

Error messages

You might also be interested in...

Proxy configuration

Anti-Virus and HIPS Exclusion / Whitelisting

Proxy configuration

How to enable a proxy

Good to Know By default the Cloud Agent for Unix will operate in non-proxy mode. The agent can be configured to use an HTTPS proxy for internet access.

Tell me the steps

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

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

4) restart qualys-cloud-agent service using the following command:

```
service qualys-cloud-agent restart
```

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.

Directory list used by Cloud Agent installation

```
/etc
/etc/init.d
/etc/qualys
/etc/qualys/cloud-agent
/etc/qualys/cloud-agent/.centos
/etc/qualys/cloud-agent/cert
/etc/qualys/cloud-agent/.suse
/etc/qualys/cloud-agent/.systemd
/opt
/opt/qualys
/opt/qualys/cloud-agent
/opt/qualys/cloud-agent/bin
/opt/qualys/cloud-agent/lib
/usr/share/doc
/usr/share/doc/qualys-cloud-agent-<version>
```

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

https://community.qualys.com/message/16520

Some transient files are created during agent execution

`/opt/qualys/cloud-agent/Config.db`
- this is the current agent configuration

`/opt/qualys/cloud-agent/manifests/*.db`
- this contains manifests used during agent based scans

CHAPTER 3

Configuration Tool

Our easy to use tool gives you many options for configuring Cloud Agent for Unix. You'll find this tool at /opt/qualys/cloud-agent/qualys-cloud-agent.sh.

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.

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 Unix 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

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.

```
$ /opt/qualys/cloud-agent/bin/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.

```
$ /opt/qualys/cloud-agent/bin/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:

```
$ /opt/qualys/cloud-agent/bin/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.

CHAPTER 4

Best Practices

Here's best practices for managing your cloud agents.

Uninstalling Cloud Agent

Uninstalling the agent from the Cloud Agent module UI or API

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

Uninstalling the agent from the host itself

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

Sample uninstall command

```
sudo rpm -e qualys-cloud-agent
```

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 Unix hosts. This is recommended best practice if you are interested in using Unix 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 Unix 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

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