Cloud Agent for BSD

Installation Guide
Agent Version 2.4

September 9, 2019

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

Table of Contents

Preface

Welcome to Qualys Cloud Agent for BSD. 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 BSD. 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 - 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 BSD

Current Release: 2.4.1

Supported Platforms					Supported Qualys Modules/Agent Versions				
Vendor	**Operating System**	**Arch**	**Installer**	**Inventory**	**VM**	**PC**	**PC UDC**	**FIM**	**IOC**
BSD	FreeBSD 10.4, 11.2	x86_64	(.txz)	2.4.1	Same as Inventory	Same as Inventory	*not available*	*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 BSD, 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 200 MB 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. 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

Learn more

Troubleshooting

Error messages

Credentials - what are my options?

Use an account with root privileges

This is recommended as it gives the Cloud Agent for BSD 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 Agent):

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

Use non-root account with sufficient privileges

The specific privileges needed are:

1) execute “pkg upgrade” for automatic update

2) agent requires certain commands to operate. If the log states command not allowed, add permission to that command.

Installation

It's easy to install Cloud Agent for BSD. 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. Cloud Agent can be installed into gold images including VM templates.

The platform supports detection of duplicate agent IDs and automatically re-provisions the duplicate agents. The section Steps to install Agents in Gold Images describes how to install an agent into a gold image without initial provisioning. This is the recommended method to prevent duplicate asset records.

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

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 using elevated privileges.

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

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

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

Check to be sure agents are connected Once installed agents 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.

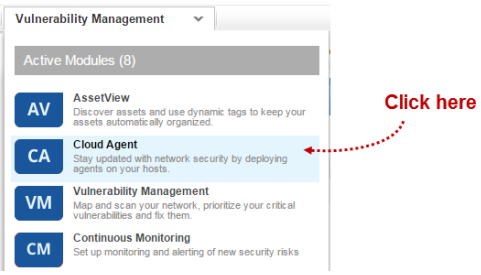
net-tools package You may need to install the net-tools package on agent endpoints, if not already present, in order to run network commands. This is required since some commands like netstat, /sbin/ifconfig, route are deprecated.

How to download Agent Installer

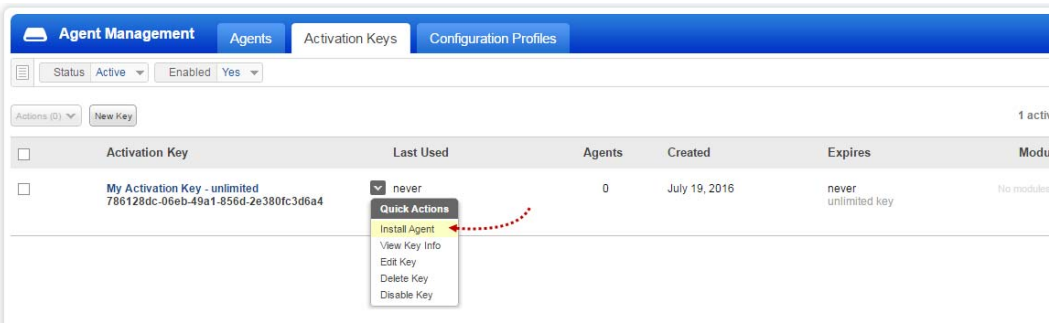
Download an installer of Qualys Cloud Agent for BSD

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

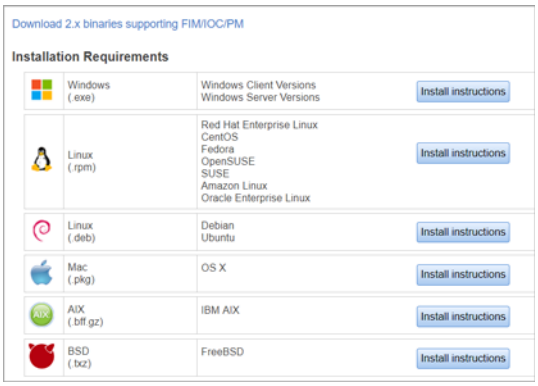
Log into the Qualys Cloud Platform and select **CA** for the Cloud Agent module.



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



Click **Install instructions** for the target host.



What happens? The Agent installer 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 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 BSD (.txz) to get everything you need.

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:

BSD (.txz)

```
> sudo pkg install -U qualys-cloud-agent.x86_64.txz
> sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
CustomerId="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
HostIdSearchDir="/mydir/"
```

Note: Dependencies for BSD agent are pkg and Bash.

Steps to install Agents in Gold Images

These steps are similar to installing on BSD (.txz) hosts, with an extra step to restart the Qualys Cloud Agent service and AMI instance.

1. Start the Gold Image instance.

2. Copy the Qualys Cloud Agent onto the instance.

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

```
> sudo pkg install -U qualys-cloud-agent.x86_64.txz
> sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
CustomerId="xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
HostIdSearchDir="/mydir/"
```

4. Stop the instance and create an image out of the instance. This completes the bake-in process.

When the instance is started it will activate the Cloud Agent which will provision itself and continue functioning as expected.

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.

Troubleshooting

You'll find helpful information in Qualys online help.

Learn more

Troubleshooting

Error messages

You might also be interested in...

Proxy configuration

Anti-Virus and HIPS Exclusion / Whitelisting

Using the hostid from previous installation

Proxy configuration

Good to Know By default the Cloud Agent for BSD 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 BSD agent to use a proxy for communication with our cloud platform:

1) if /usr/local/etc/qualys-cloud-agent 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) 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/rc.d
/etc/qualys
/etc/qualys/cloud-agent
/etc/qualys/cloud-agent/cert
/usr/local
/usr/local/qualys
/usr/local/qualys/cloud-agent
/usr/local/qualys/cloud-agent/bin
/usr/local/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

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

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

Using the hostid from previous installation

If you are reinstalling an agent on a host and you wish to use the same hostid used in the previous installation, set the hostid directory location to the same location used in the previous installation.

For example, let's say in the previous installation you use HostIdSearchDir=/root/hostdir while setting the activation key, it creates hostid under /root/hostdir/qualys/. When you uninstall the agent it doesn't remove /root/hostdir/qualys/hostid.

If you are reinstalling the agent on the same machine, and you want to reuse the earlier hostid, set HostIdSearchDir to /root/hostdir.

Configuration Tool

The Agent Configuration Tool gives you many options for configuring Cloud Agent for BSD after installation. You'll find this tool at /usr/local/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

- 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.

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 information (3).
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.

Configuration option	Description
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 BSD 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).
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.

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.

```
$ /usr/local/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.

```
$ /usr/local/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:

```
$ /usr/local/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.

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.

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.

```
sudo pkg remove 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 BSD 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 BSD 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 BSD 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/"
```

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.

To use the encryption utility:

Go to /usr/local/qualys/cloud-agent/bin, and then export the LD_LIBRARY_PATH variable to /usr/local/qualys/cloud-agent/lib.

```
export LD_LIBRARY_PATH=/usr/local/qualys/cloud-agent/lib
```

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+gaJwHOm3g==
```

Once you get the encrypted user name add/or password, unset the LD_LIBRARY_PATH variable by using the following command:

```
export LD_LIBRARY_PATH=
```

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+gaJwHOm3g==@proxy.m
yco.com:8080
```

For example (encrypting username and password):

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