Cloud Agent

Lab Tutorial Supplement

Table of Contents

Cloud Agent Deployment

To successfully deploy Qualys Cloud Agent (CA), the target host must have Internet access, and a clear path to the Qualys Cloud Platform. Administrative or root access to the target host is required to complete an agent installation.

Agent Activation Key

Cloud Agent
Stay updated with network security by deploying agents on your hosts.
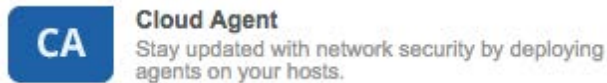
Before you can begin deploying agents, you must first generate an Activation Key in the Cloud Agent application. Activation Keys allow you to manage and control the distribution of agents throughout your organization.

Navigate to the following URL to view the "Create Activation Key" tutorial:

PLAY LAB 1 - http://ior.ad/7fyC
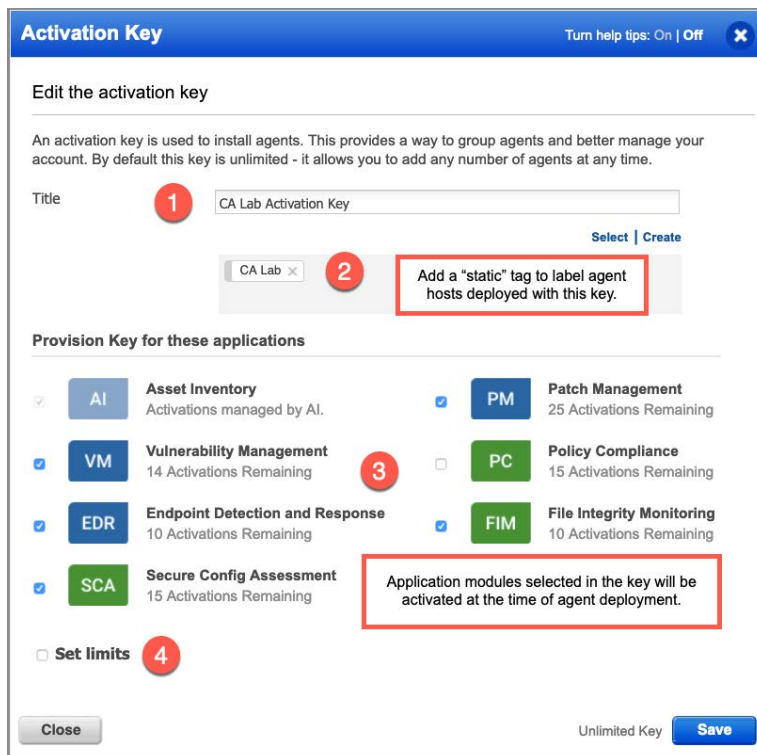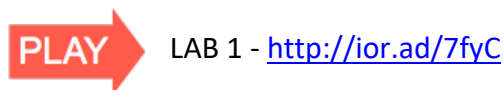
Activation Key configuration options include: 1) Title, 2) Asset Tags assigned to deployed agent hosts, 3) Qualys application modules activated for deployed agents and 4) Key limitations or restrictions.

Add a Static Tag

It's a "best practice" to configure agent Activation Keys with a static Asset Tag. The predictable nature of a static tag will make it easy to identify or track agent host assets that are deployed with any Activation Key.

Application Module Support

Select the Qualys application modules to be activated at the time of agent deployment. Any application module not selected, can be activated at a later time.

Qualys Cloud Agent collects and provides data for multiple Qualys Platform applications, including:

- Asset Inventory (AI) – enabled by default

- Vulnerability Management (VM) – includes Threat Protection (TP) & Continuous Monitoring (CM)

- Policy Compliance (PC) and/or Security Configuration Assessment (SCA)

- File Integrity Monitoring (FIM)*

- Endpoint Detection & Response (EDR)*

- Patch Management (PM)*

NOTE: Asset Inventory is enabled, by default. Threat Protection (TP) and Continuous Monitoring (CM) are supported via activation of the VM module.

FIM, EDR, and PM are agent exclusive applications (i.e., they require Cloud Agent).

You'll find complete details on agent OS and application support in the Cloud Agent Getting Started User Guide (https://www.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf)

Activation Key Limits

Create keys that are unlimited or choose the option to set limits.

☑ **Set limits**

You can set limits for more control over your activation keys - maximum number of agents or expiration date. When both are set, the key will expire when the first limit is reached.

Key limited by count
Tell us the maximum number of agents that can be installed using this key.

Maximum number: 5000

Key limited by date
Allow installation of an unlimited number of agents up until this date.

Date: 2/14/2026

If both limits are selected, the key will expire when the first limit is reached.
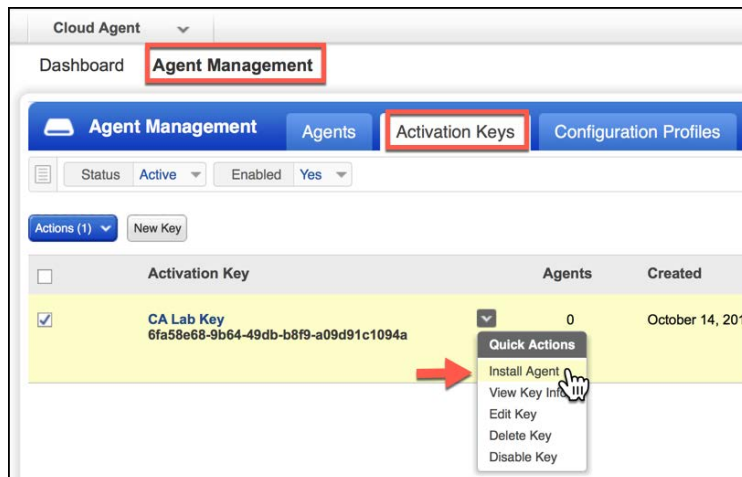
Agent Installation Components

While this lab tutorial highlights the components of a Windows agent installation, the basic principles and concepts apply equally to other agent-supported OS installations. You'll find specific instructions for Mac OS installations, RPM-based OS installations, and Debian/Ubuntu OS installations in Appendix A, B, and C, respectively.

The installation steps that follow support Windows XP SP3 or greater. Older versions of Windows that do not support TLS 1.2 (or greater) will need to connect to the Qualys Cloud Platform through a proxy or the Qualys Gateway Service (QGS).

You must have administrative access to the target Windows host, to successfully perform a Cloud Agent installation.

Navigate to the following URL to view the "Agent Installation Components" tutorial:

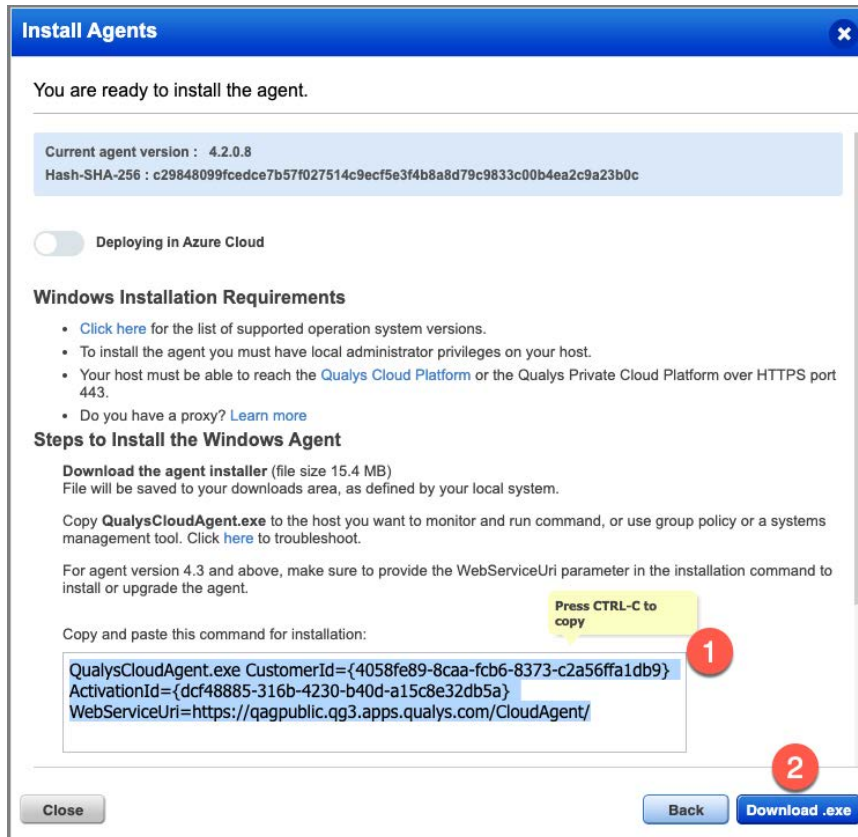**PLAY**   LAB 2 - http://ior.ad/7fzr

Use the "Quick Actions" menu of an Activation Key to select the "Install Agent" option.

To download an agent installation program and acquire its associated installation command, just click the "Install Instructions" button that matches your targeted OS.

To install Cloud Agent on a Windows host, click the "Install instructions" button for the ▦ "Windows (.exe)" option.

See Appendix A, B, and C for Mac OS, RPM, and Debian installation instructions.

Install Agents ✖

You are ready to install the agent.

Current agent version : 4.2.0.8
Hash-SHA-256 : c29848099fcedce7b57f027514c9ecf5e3f4b8a8d79c9833c00b4ea2c9a23b0c

⬤ **Deploying in Azure Cloud**

Windows Installation Requirements
- Click here for the list of supported operation system versions.
- To install the agent you must have local administrator privileges on your host.
- Your host must be able to reach the Qualys Cloud Platform or the Qualys Private Cloud Platform over HTTPS port 443.
- Do you have a proxy? Learn more

Steps to Install the Windows Agent

Download the agent installer (file size 15.4 MB)
File will be saved to your downloads area, as defined by your local system.

Copy **QualysCloudAgent.exe** to the host you want to monitor and run command, or use group policy or a systems management tool. Click here to troubleshoot.

For agent version 4.3 and above, make sure to provide the WebServiceUri parameter in the installation command to install or upgrade the agent.

Press CTRL-C to copy

Copy and paste this command for installation:

QualysCloudAgent.exe CustomerId={4058fe89-8caa-fcb6-8373-c2a56ffa1db9} ActivationId={dcf48885-316b-4230-b40d-a15c8e32db5a} WebServiceUri=https://qagpublic.qg3.apps.qualys.com/CloudAgent/ **1**

2

Close   Back   **Download .exe**

1. Copy and paste the installation command into a plain text document.

2. Click the "Download .exe file" button and save the Cloud Agent installation file (.exe).

The installation command contains your unique CustomerId and an ActivationId that identifies its associated Activation Key.

When using third-party applications to build custom deployment packages for hundreds and thousands of hosts, these two components should be included.

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployments.

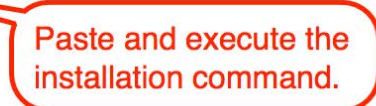Navigate to the following URL to view the "Command Line Installation" tutorial:

PLAY   LAB 3 - http://ior.ad/7qF7

Open a "Command Prompt" window on a target Windows host.

```
C:\Users\qscan\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8438-70FF

 Directory of C:\Users\qscan\Desktop

01/02/2017  02:28 PM    <DIR>          .
01/02/2017  02:28 PM    <DIR>          ..
01/02/2017  02:28 PM         1,928,224 QualysCloudAgent.exe
01/02/2017  02:27 PM               122 windows_install.txt
              2 File(s)      1,928,346 bytes
              2 Dir(s)  92,445,974,528 bytes free

C:\Users\qscan\Desktop>QualysCloudAgent.exe CustomerId={                     }
ActivationId={                      }
```

Paste and execute the installation command.

Navigate to the directory that contains the Cloud Agent installation program (QualysCloudAgent.exe).

Use the "dir" command to verify the existence of the installation program file. If you do not see file "QualysCloudAgent.exe" navigate to its correct location before executing the installation command.

Copy and paste the Cloud Agent installation command into the "Command Prompt" window and press the "Enter" key. The agent installation program will execute with your Activation Key and Customer ID.

Validate CA Installation

To verify the success of your installation, look for the Cloud Agent process within Windows Task Manager.
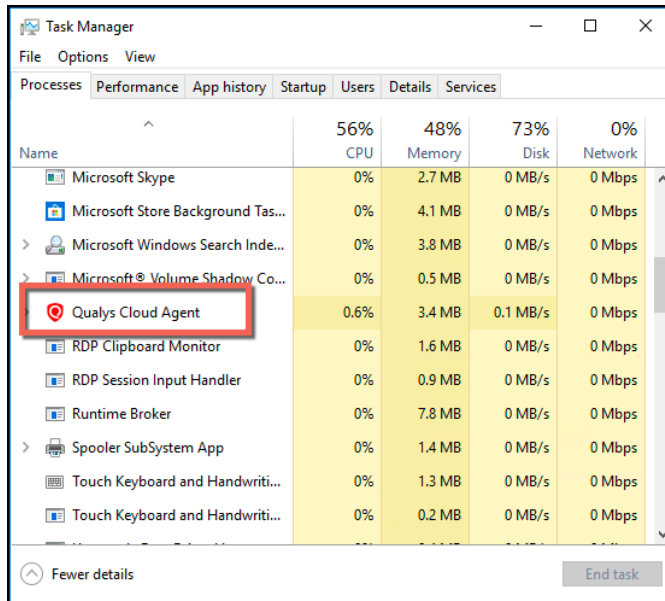
Open the Windows Task Manager and verify Qualys Cloud Agent is running (*Ensure you are viewing processes from all users).*

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Windows host, this Host ID can be found in the Windows Registry.
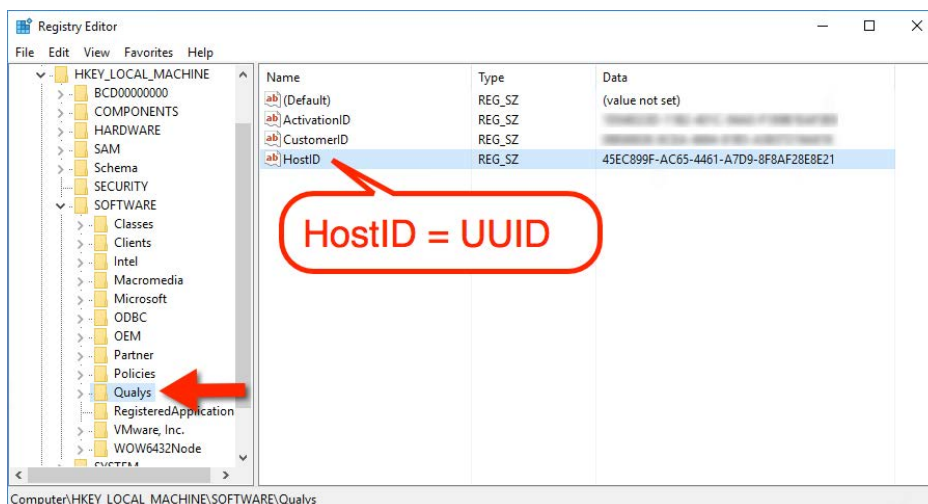
Open the Windows Registry Editor (i.e., regedit.exe) and navigate to HKLM\SOFTWARE\Qualys. The "HostID" registy value contains a universally unique ID (UUID) to track the vulnerability findings for its host.

View CA Log File (Log.txt)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Windows host in the "ProgramData" (hidden) folder.
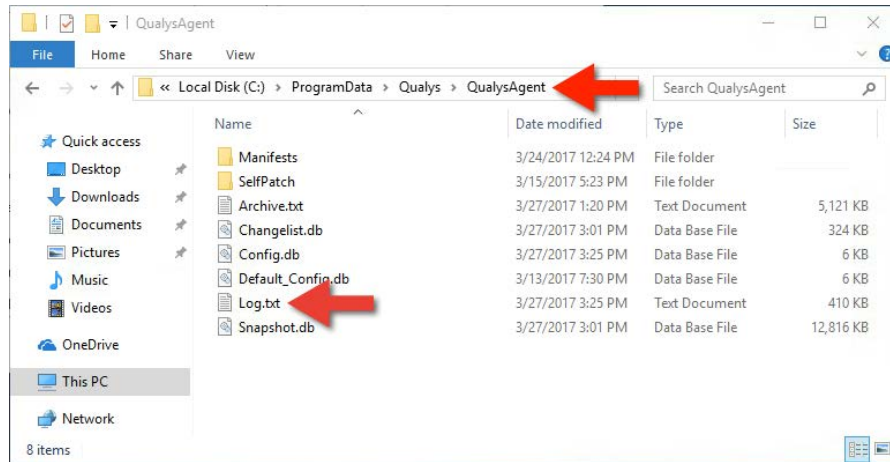
Use Windows Explorer or a Command Prompt window to navigate to the following directory path: `C:\ProgramData\Qualys\QualysAgent`

`Open file 'Log.txt' to view Cloud Agent log file entries.`

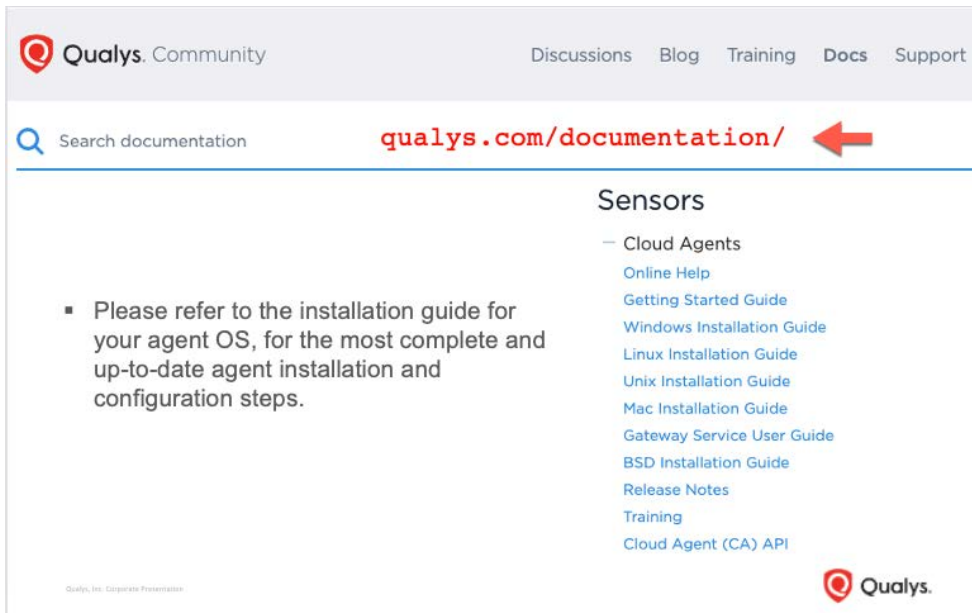*NOTE: Windows XP uses a different directory path for its agent log file:*

` C:\Documents and Settings\All Users\Application Data\Qualys\QualysAgent`

CA Log Analysis & Troubleshooting

Visit the Qualys Training Video Library for more information and details on agent log analysis and troubleshooting:

- Introduction to Troubleshooting & Log Analysis (https://vimeo.com/412764672)

- Troubleshooting & Log Analysis – Common Errors (https://vimeo.com/412762742)

- Troubleshooting & Log Analysis – Unix/Linux Distribution (https://vimeo.com/418215691)

- Common Errors and Their Solutions – Unix/Linux Distribution (https://vimeo.com/418218290)

Cloud Agent Installation Guides

Agent Proxy Configuration

By default Qualys Cloud Agent communicates directly with the Qualys Platform on TCP/443. Agents can also be configured to communicate through a proxy server, including Qualys Gateway Server (QGS). QGS also provides a patch download cache for the Qualys Patch Management (PM) application.

TLS 1.2+ Requirement

To successfully communicate with the Qualys Platform, TLS 1.2 (or greater) must be enabled on agent hosts. Agent host assets that do not meet this requirement will need to communicate to the Qualys Platform through a proxy server capable of converting host communications to the required TLS protocol. Use Qualys Gateway Server (QGS) to meet this TLS 1.2+ requirement.

Windows Agent Proxy Configuration

By default, Windows agents use the same proxy configuration as its host OS.

The QualysProxy utility for Windows (QualysProxy.exe) can be used to configure proxy server(s) and port(s), username and password, Proxy Auto-Configuration (PAC) file URL, and Web Proxy Auto-Discovery (WPAD) for agent hosts.

Windows Agent proxy settings are stored under the Qualys registry key.
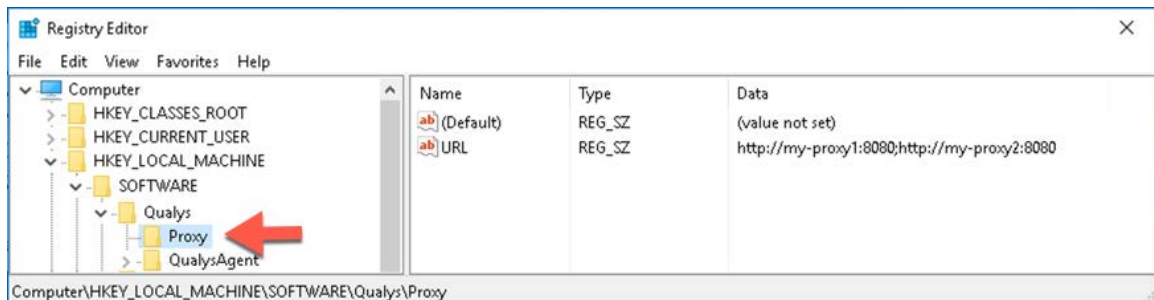
Use third-party software management and distribution tools or the Windows Remote Registry Service to set the proxy configuration for agents, during or after agent installation.

QualysProxy.exe can be used by third-party systems and software management tools.

You'll find QualysProxy.exe in the "\Program Files\Qualys\QualysAgent" folder of a Windows host. It must be executed from an elevated command prompt.

```
QualysProxy [/u <proxy url> [/n <proxy username>] [/p <proxy password>] [/a <PAC file url>]]
QualysProxy [/w on|off]
QualysProxy [/h on|off]
QualysProxy [/d]
```

Qualys Proxy Options

Option	Description
/u	Proxy URL. Do not use with /a
/n	Username used to access proxy. If set, /u option must be set.
/p	Password used to access proxy. If set, /u option must be set.
/a	URL path to PAC file for proxy auto-configuration. If set, do not set /u option.
/d	Deletes all Qualys cloud agent proxy settings.
/w	Enables or disables agent use of the host's WPAD settings.
/h	Enables or disables agent use of the system wide winhttp(s) proxy setting.

QualysProxy Examples

1. Set proxy and port number.

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

2. Define multiple proxy servers (for failover).

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

3. Define multiple ports on the same proxy server for failover

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

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

4. Set proxy and credentials

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

5. Tell agent to use PAC file

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

6. Specify credentials for use with PAC file.

   ```
   QualysProxy /n ProxyUsername /a ProxyPassword /a http://my-
   pacfile-server/QualysAgent.pac
   ```

Linux Agent Proxy Configuration

1. Create file /etc/sysconfig/qualys-cloud-agent (or /etc/default/qualys-cloud-agent) if it does not already exist.

2. Add one of the following lines to the file (one 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. Where <host> is the proxy server's IPv4 address or FQDN. Where <port> is the proxy's port number.

3. Restart qualys-cloud-agent service (e.g., service qualys-cloud-agent restart)

Temporarily Bypass Proxy

In the event agents are operating in proxy mode and need to switch to non-proxy mode, you can configure agents to use no_proxy in /etc/environment.

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 a proxy environment variable is set.

To enable Linux agents to use no_proxy for communication with our cloud platform, Edit the /etc/environment file and add the following line:

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

The `qualys_https_proxy` environment variable, is used exclusively by Cloud Agent (i.e., it will not impact other applications or services).

Note: For init.d based systems, you need to prefix 'export' to the 'qualys_https_proxy' line.

Cloud Agent Installation Guides

Asset Details & Queries

It typically takes a few minutes for a new Agent Host to appear under the "Agents" tab.
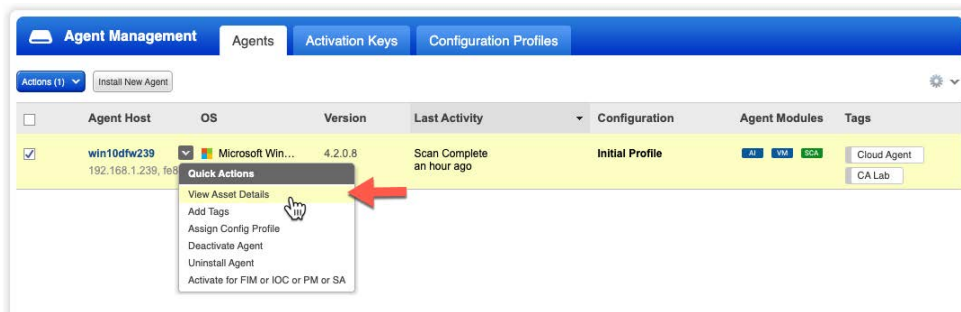
The "Quick Actions" menu of any host, will allow you to view its asset details.

Navigate to the following URL to view the "Asset Details & Queries" tutorial:

PLAY   LAB 4 - http://ior.ad/7fIF

All agent hosts are listed under the "Agents" tab. You can use the CA "Search" field to help you quickly find the agent host you are looking for.
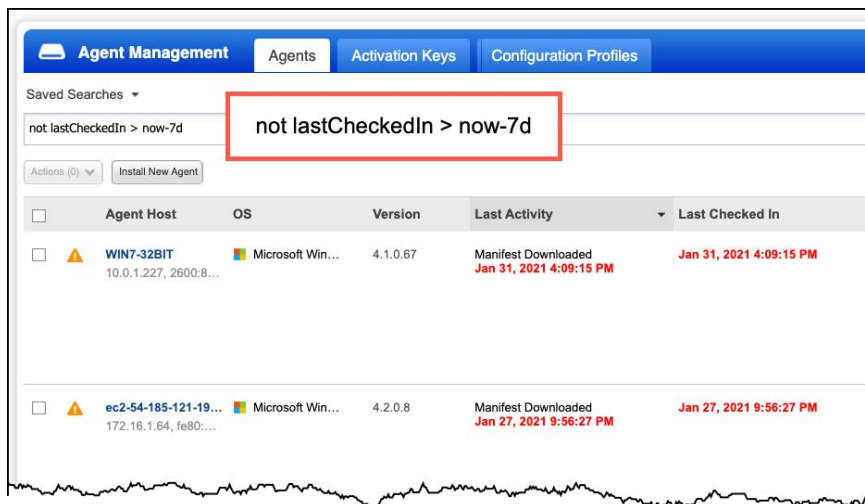
For example, you may find it useful to search your asset database for agents that have not checked-in for several days.

Queries you create can be saved for future use and query results can be downloaded and imported into spreadsheets and other types of documents.

If you start typing in the "Search" field, a list of search terms will be displayed that contain the characters you type.
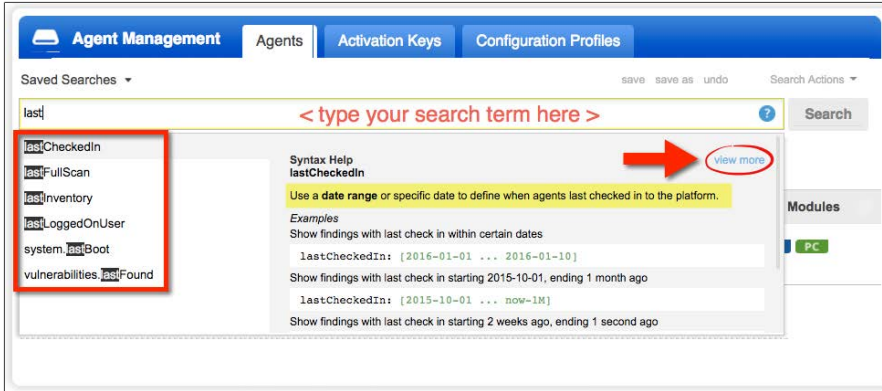
Detail is provided in the right pane, for any search term highlighted in the left pane.

Tip: Clear the "Search" field and enter any character (”a”, “e”, “i”, “o”, “u”, ect..) to identify search parameters that contain the character you typed.

Click the "?" icon in the search field, for help and instruction on creating queries.
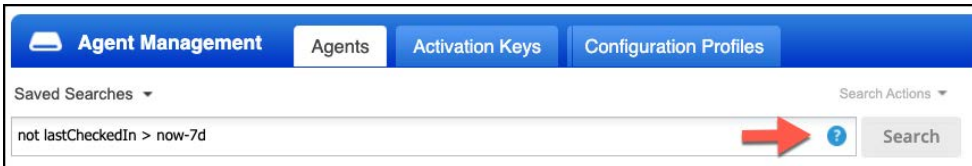
Examples are provided for common searching scenarios.

All agent hosts are labeled with the "Cloud Agent" tag, making the "tags.name" query token very useful, when attempting to "single-out" agent hosts in other Qualys applications.
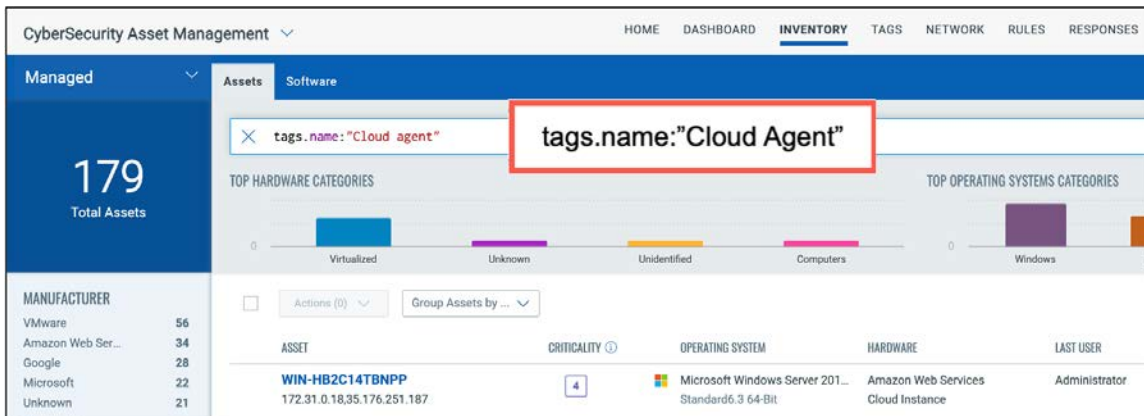
The example above was taken from the Cyber Security Asset Management application. When attempting to find agent hosts, search on the "Cloud Agent" Asset Tag (i.e., tags.name: "Cloud Agent").
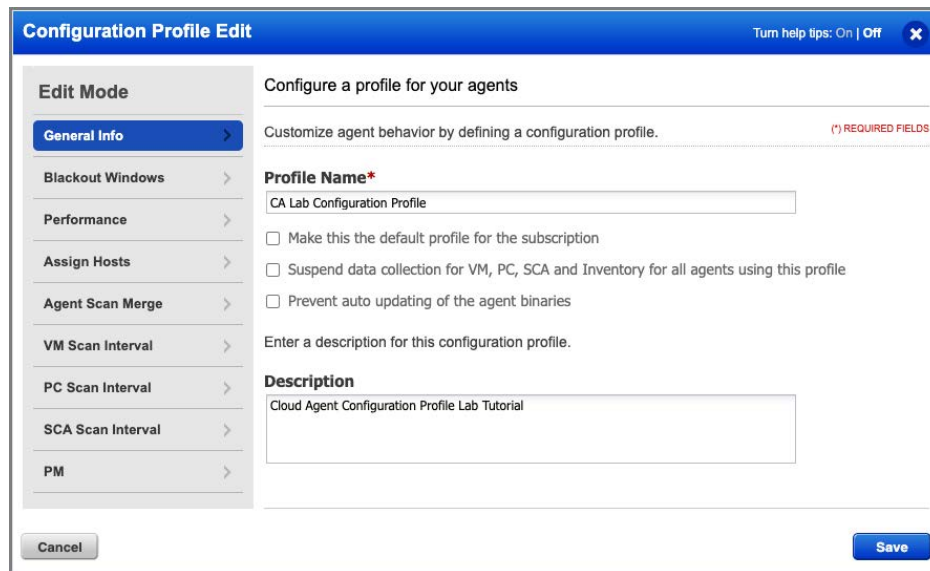
Configuration and Tuning

The Cloud Agent application is your command and control center for deploying and managing Cloud Agent.

CA **Cloud Agent**
Stay updated with network security by deploying agents on your hosts.

Cloud Agent Configuration Profile

The Cloud Agent Configuration Profile provides options to control the performance and behavior of each agent instance.

Navigate to the following URL to view the "CA Configuration Profile" tutorial:

PLAY   LAB 5 - http://ior.ad/7fAw

General Info

The General Information settings establish things like the profile name and description, along with some default data collection and update options:

- Only one profile can be designated as the default profile for your subscription. if an agent host does not meet the host assignment criteria for any other configuration profile, the default will be used.

- The option to suspend data collection from agents will effectively stop the agent from performing VM, PC, SCA and Inventory scans. Although scanning has stopped, agents will continue to receive manifest updates, configuration updates and agent version updates.

- Enable the "Prevent auto updating of the agent binaries" option, if you intend to use third-party software management and distribution tools (e.g., SCCM, RPM, BigFix, Casper, Altiris, etc…) to perform agent upgrades.

Blackout Windows

You can add blackout windows to stop communication between the agent and the Qualys Cloud platform, at specified times each day of the week.

This can be especially useful when coordinating the communication flows for different groups of agents, or simply use this option to stop agent communications during expected times of peak network traffic.

Agent Performance Settings

To control the amount of system or network resources used by each agent, you can use the preset performance settings of (LOW, NORMAL, or HIGH).
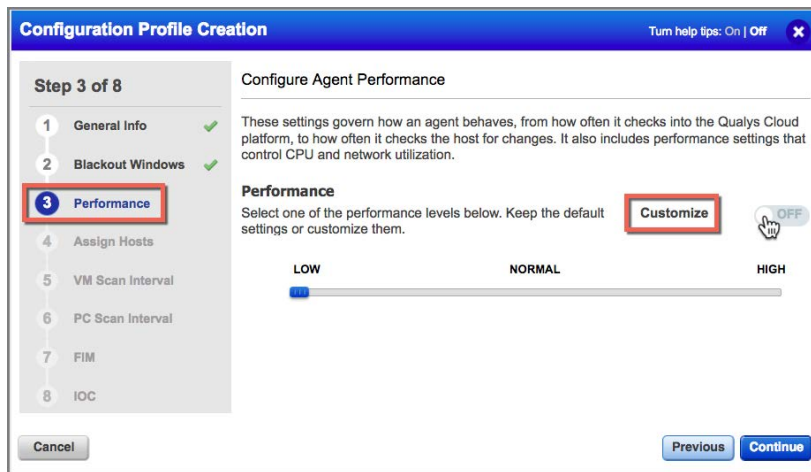
Or use the "Customize" option for more granular control.

Network Performance

Moving down through the "Performance" options, the "**Delta Upload Interval**" and "**Chunk sizes for file fragment uploads**" settings work together to control how VM and PC data is transmitted to the Qualys Cloud Platform (FIM and EDR settings are specified in a separate place).

Chunk sizes for file fragment uploads - Specifies the maximum payload size for data transmissions. If the total amount of transmission data exceeds this value, it will be broken up (or fragmented) into appropriate chunks; not to exceed this value.

Example: if "Chunk sizes for file fragment uploads" is set to 1024KB, a 4MB data transmission will be broken up into four separate chunks, each 1024KB in size.

Delta Upload Interval - Specifies the amount of time (or delay) between separate transmissions of "chunks" of data.

These two setting will have the greatest impact on network performance during times of agent scan data transmissions (specified in the Scan Interval settings).

CPU Performance

It's the CPU performance settings that determine how long it will take an agent to complete the task of collecting inventory and scan data from its agent host.

The more CPU resources you provide to an agent, the sooner it will complete its tasks. Separate CPU performance settings are provided for Windows and Linux/MacOS agents.

CPU Limit - The CPU configuration setting for a windows agent is called the "CPU Limit" and is expressed as a percentage of CPU usage.

Higher percentages will provide greater CPU resources to a Windows agent, allowing it to complete its data collection tasks in less time. Lower percentages will reduce agent performance, and more time will be required for the agent to complete its tasks.

Note: The Windows agent is single-threaded, and only executes on one core of the CPU. Because of this single-threaded behavior, a windows agent configured with a 100% value, will use the equivalent of 25% overall CPU usage on a four-core system.

CPU Throttle - The CPU configuration for a Linux or Mac host is called CPU Throttle and is expressed in milliseconds; which represents the delay between metadata collection commands executed by the agent.

Lower CPU Throttle settings improve agent performance, by minimizing the delay between agent tasks. Higher values for CPU throttle, will slow agent performance.

Assign Hosts

In the first lab tutorial, the "CA Lab" tag was added to the CA Lab Activation Key. This ensures all agents created with the CA Lab Activation Key, will receive the "CA Lab" tag. The "CA Lab" tag can now be used to assign your agent host to the correct Configuration Profile.
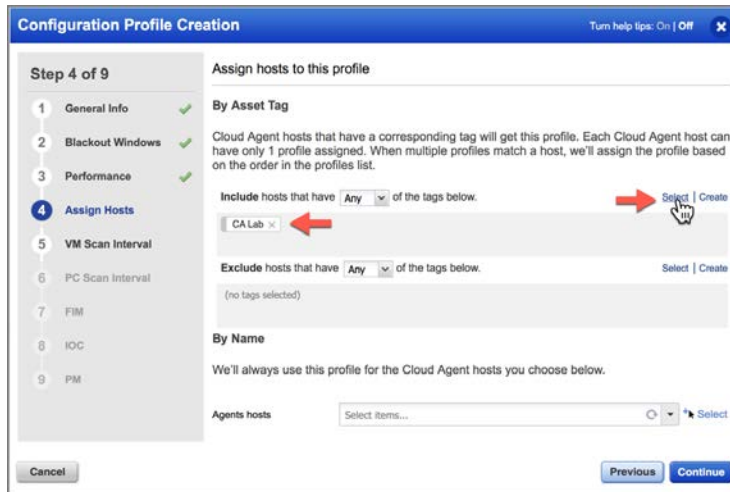
Hosts with the "CA Lab" tag will be assigned to this Configuration Profile, automatically.

Agent Scan Merge
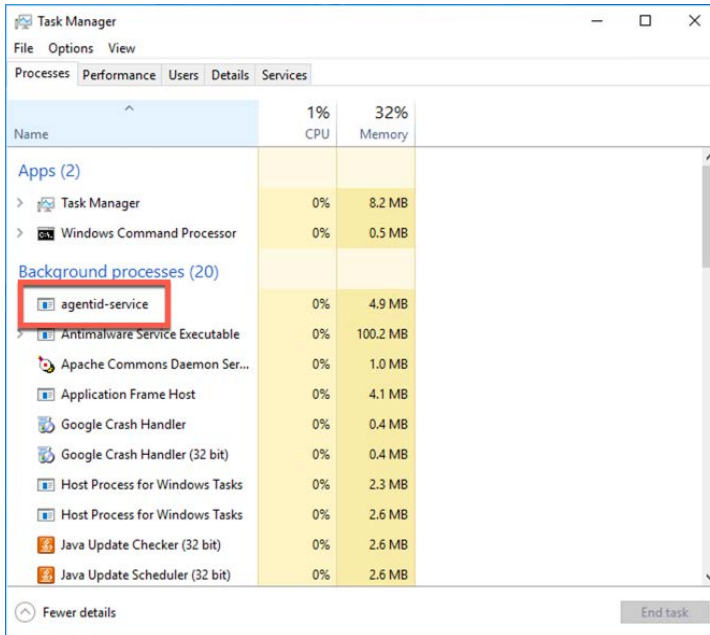
The Agent Correlation Identifier is used to link SCAN data and AGENT data together. When Agent Scan Merge is enabled in a Configuration Profile, the Agent Correlation Identifier is exposed on TCP ports 10001-10005.
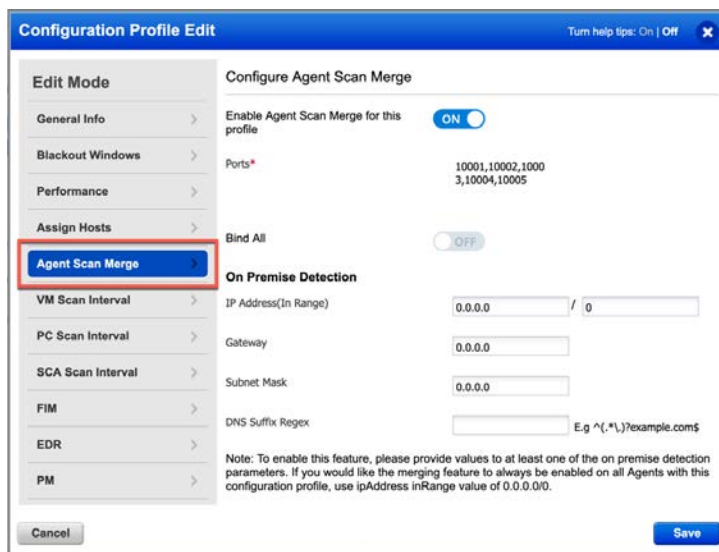
By default the lowest available port number will be used. Use the "Bind All" option to bind on all five ports simultaneously. Configure "On Premise Detection" to expose the

Agent Correlation Identifier only on a trusted network. An IP address range configured to: 0.0.0.0/0 enables this feature for all agent hosts.

The 'agentid-service' can be viewed from Windows Task Manager.

The 'agentid-service' can also be viewed within a Unix/Linux process list.
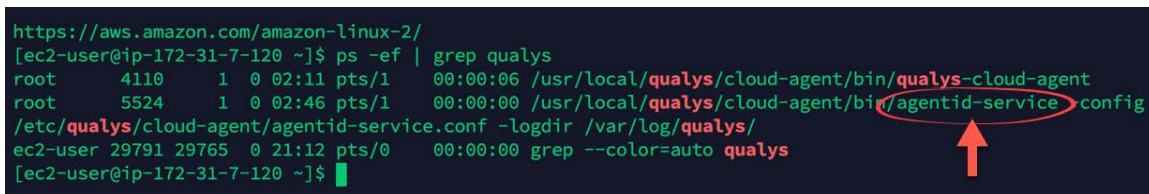
Execute the 'netstat' command (below) to view the agentid-service's assigned port number(s).
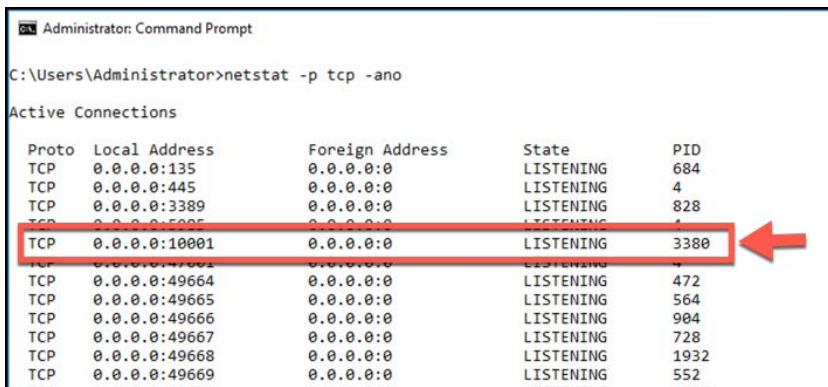
Once the Agent Correlation Identifier is accepted, within the "Asset Tracking and Data Merging Setup" options (in Qualys VM or VMDR), Qualys Scanners will attempt to read the Agent Correlation Identifier from agent hosts.
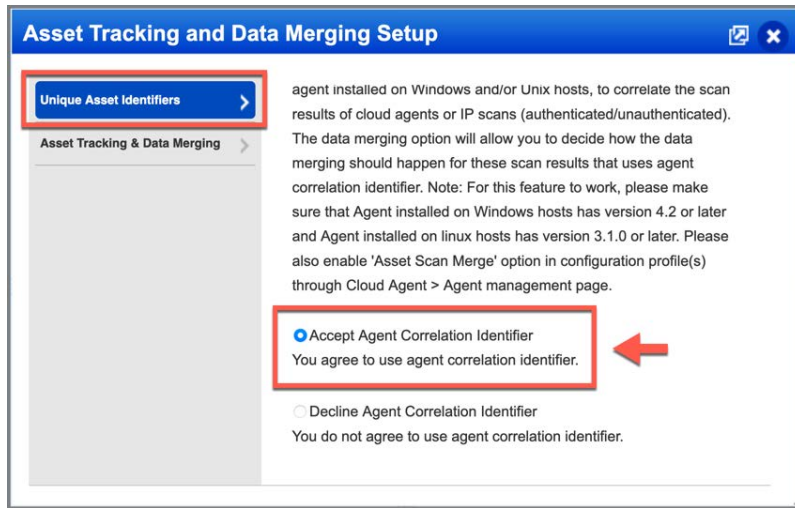
When Qualys Scanner Appliances scan agent hosts (that have the Agent Correlation Identifier enabled), they return QID 48143 – Qualys Correlation ID Detected.
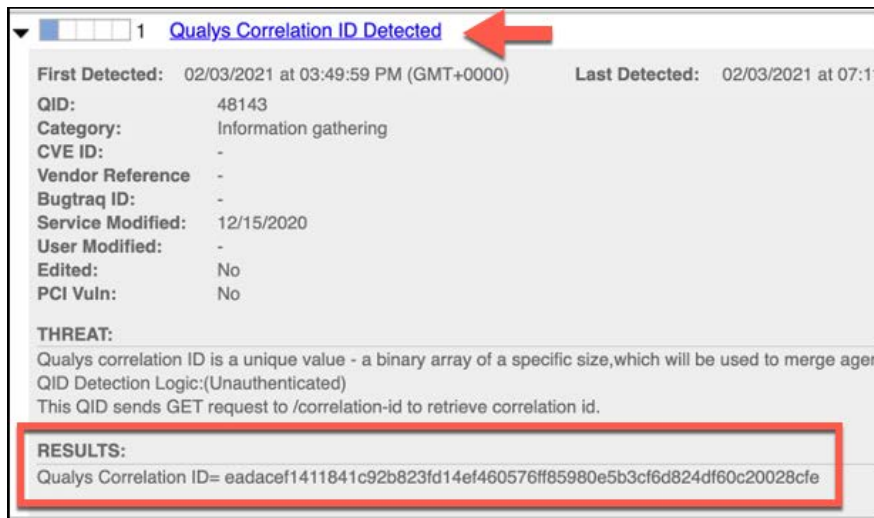
AGENT data and SCAN data can be successfully merged using the Agent Correlation Identifier attribute.

VM, PC, and SCA Scan Intervals

The VM, PC, and SCA Scan Interval setting determine how often Cloud Agent collects vulnerability and compliance assessment data. Configured at its minimal value, data collections will occur every four hours.

Scan On-Demand

Manually perform VM, PC, SCA, UDC, and inventory scans on Windows and Linux agent hosts. You can run an on-demand 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.

Windows On-Demand Scan

On-demand scans for Windows are configured in the Windows System Registry.
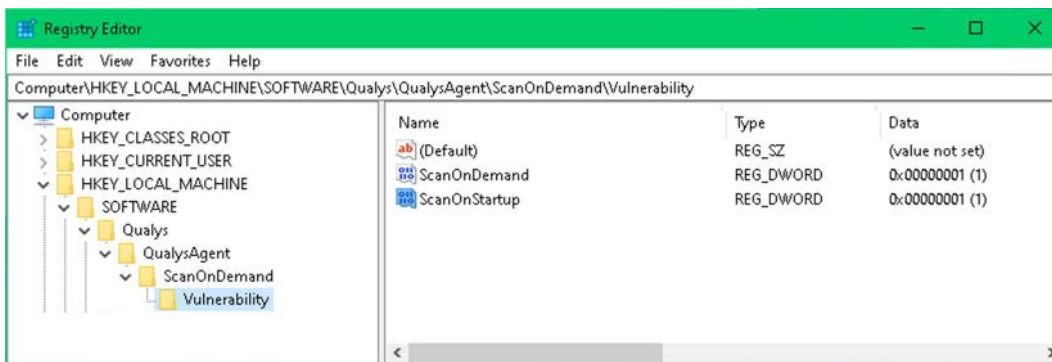
Create separate subkeys (i.e., Inventory, Vulnerability, PolicyCompliance, UDC, or SCA) for the type of on-demand scan to be performed and then set the "ScanOnDemand" registry value to '1' to activate an on-demand scan.

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

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

Alternatively, use the "ScanOnStartup" registry value to launch a scan at the very next system startup. ScanOnStartup can be very useful for validating vulnerability patches that require a reboot; just set the ScanOnStartup value to '1' and then deploy your patches. The "CpuLimit" registry value is not required and has a default value of 100.

Linux On-Demand Scan

On-demand scans for Linux are executed from the command line. Use the cloudagentctl.sh script to run the on-demand scan. You'll find this script at /usr/local/qualys/cloud-agent/bin/.

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

- The action and type parameters are mandatory.
- The value for the "action" parameter is "demand" for an "on-demand" scan.
- The value for the "type" parameter is the targeted application module.
- The default value for the "cputhrottle" parameter is 0.

Example:

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

FIM and EDR

FM and EDR use and event-driven data collection model, where events are captured and logged as they occur. Logged events are transferred to the Qualys Platform at frequent intervals (i.e., Payload Threshold Time (30 – 1800 seconds).

PM

Patch assessment scans (configured in the PM application) are performed every 4 hours to every 30 days.

Configuration Profile Precedence

You can use your mouse to grab and drag any profile to a new position in the list.
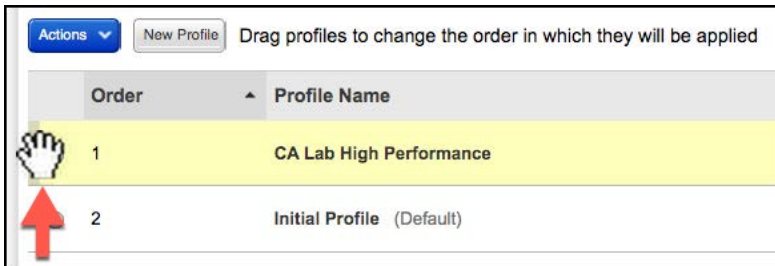
If a deployed agent host is assigned to more than one profile, the matching profile closest to the top of the list will take precedence.

Download Manifest

A "manifest" identifies the tasks to be performed and data to be collected by the agent. Qualys Application Modules have their own separate manifests.

Manifest Type	Description	Data Collection
Inventory	Collects asset inventory such as hardware, software, active services, etc...	Daily Intervals
Vulnerability	Collects data defined by QIDs in the Qualys Vulnerability KnowledgeBase.	User-Defined Intervals (240 - 43200 min.)
PolicyCompliance	Collects System Defined Control (SDC) datapoints defined in the PC Control Library.	User-Defined Intervals (240 - 43200 min.)
UDC	Collects User Defined Control (UDC) datapoints defined in the PC Control Library.	Four-hour intervals
SCA	Collects compliance datapoints defined in CIS Policy Controls.	User-Defined Intervals (240 - 43200 min.)
AutoDiscovery	Automatically discovers host middleware technologies.	Four-hour intervals
MiddlewarePC	Collects compliance datapoints for host middleware assessments.	Four-hour intervals
FIM	Collects events for targeted file and directory changes and modifications.	Event-Driven (Payload threshold time 30 - 1800 sec.)
EDR	Collects events for targeted processes, process mutex, registry keys, and suspect file locations.	Event-Driven (Payload threshold time 30 - 1800 sec.)

When a new application module is activated for an agent host, the agent receives a new manifest and *data collection begins*. Data collection also begins after an agent receives an updated manifest.

Activate, Deactivate & Uninstall Agents

Using the "Quick Actions" menu of any agent, you can activate or deactivate modules, and uninstall agents according to the licenses within your Qualys subscription.
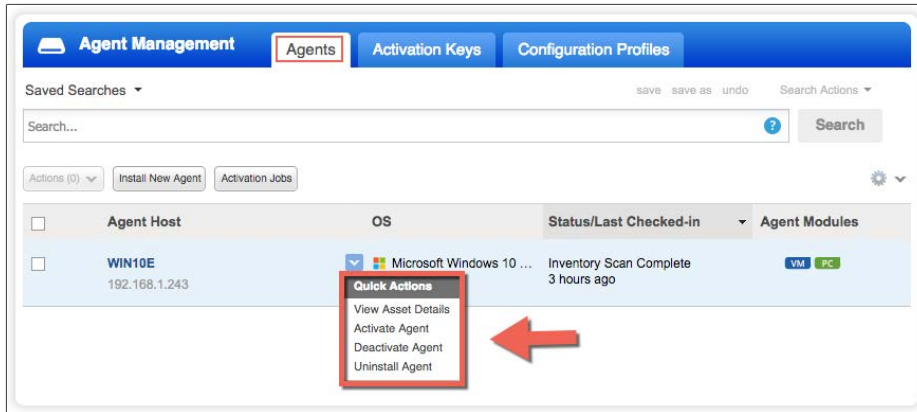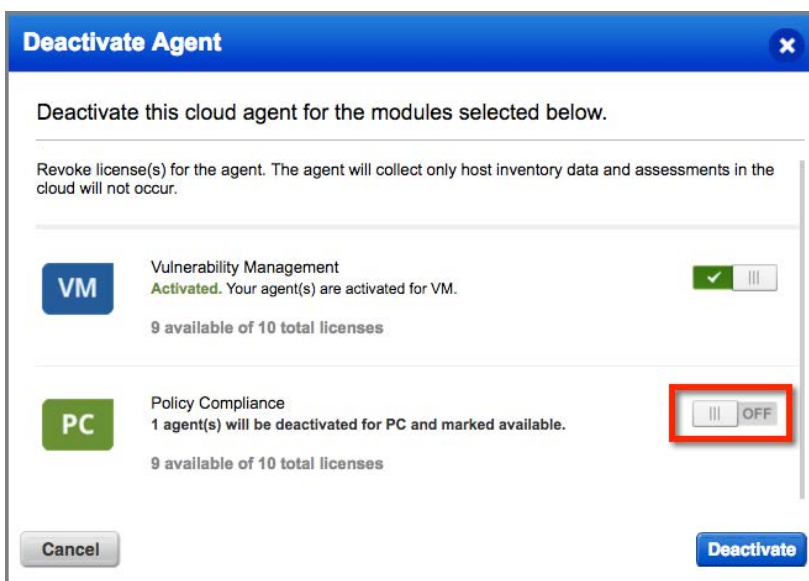

Navigate to the following URL to view the "Deactivate and Uninstall" tutorial:

LAB 6 - http://ior.ad/7fPY

Activate & Deactivate Application Modules

To deactivate an Agent Module, select "Deactivate Agent" from the "Quick Actions" menu. Then turn-off the targeted module, before clicking the "Deactivate" button.

A deactivated module can also be re-activated by using the "Activate Agent" option from the "Quick Actions" menu.

An effective technique for activating or deactivating application modules in bulk, is provided within agent Activation Keys.
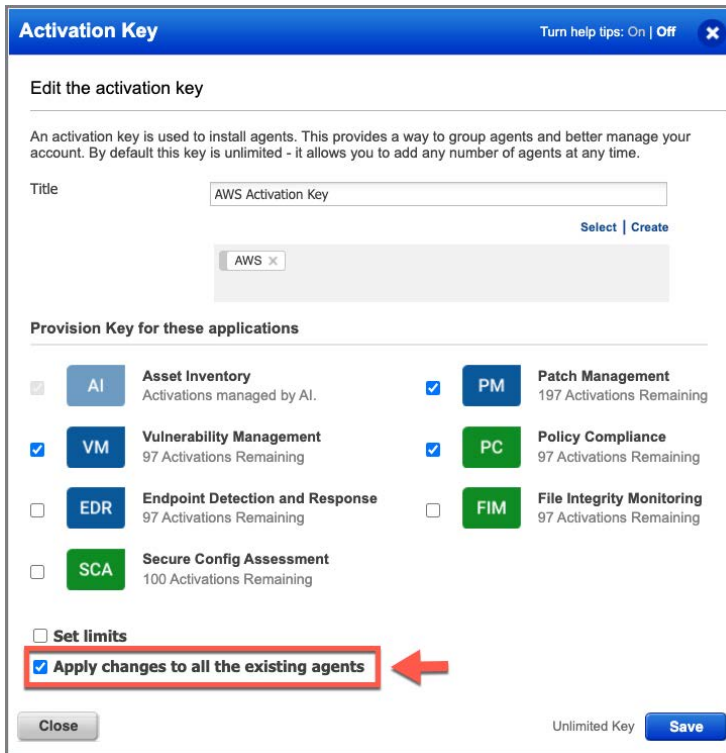

Open an Activation Key and check the modules to be activated or uncheck the modules to be deactivated. Select the "Apply changes to all the existing agents" option and save.

All existing agents (deployed with the modified key) will be updated at their very next Agent Status Interval.

Uninstall Agents

Selecting the "Uninstall Agent" option from the "Quick Actions" menu of any agent, will remove the agent from its host the very next time it checks-in.
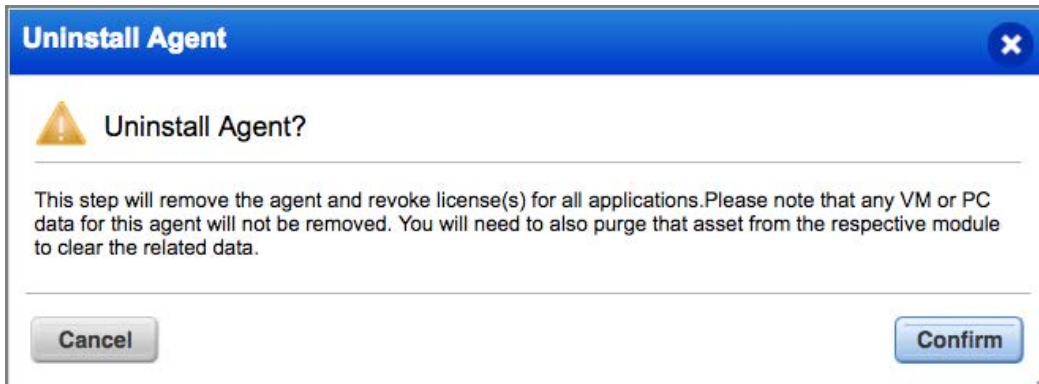
Uninstall agents in bulk using the CA Application Program Interface (API) or create Agent Purge Rules within the Qualys AssetView application.
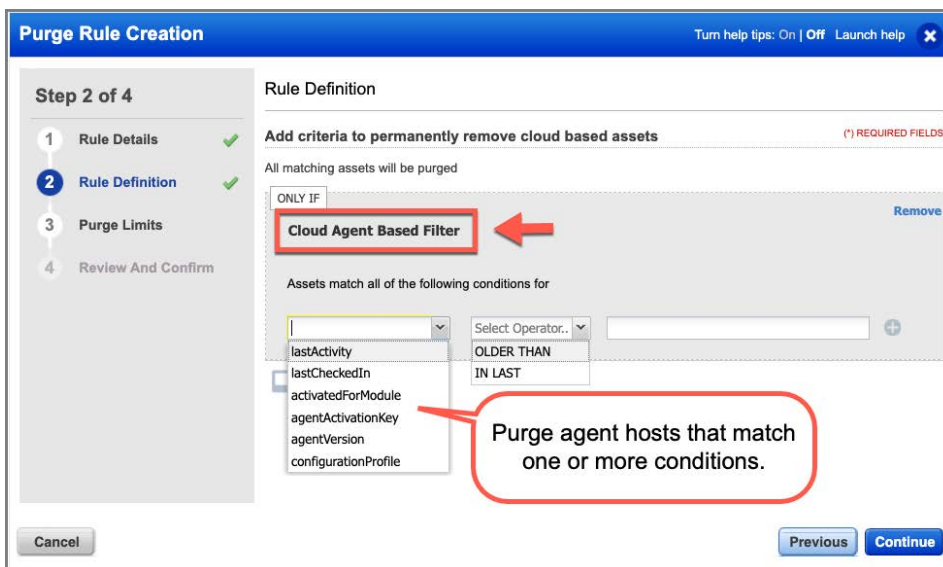
Purge Rules run daily. All assets matching your rule will be purged:

- Assets and associated asset data will be removed from your account.
- Agents will be uninstalled and licenses will be freed-up.

Cloud Agent Certification Exam

Participants in this Cloud Agent training course have the option to take the Cloud Agent Certification Exam. This exam is provided through our Learning Management System (qualys.com/learning). To take the exam, candidates will need a "learner" account.

If you would like to take the exam, but do not already have a "learner" account, click the "Request a new account" link (above), from the "Qualys Training & Certification" login page (qualys.com/learning).

Once you have created a "learner" account (and for those who already have an account), click the following link to access the "Cloud Agent- QSC 2021" course page:

https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237821

From the "Cloud Agent– QSC 2021" course page, click the "Enroll" button (lower-right corner).

After successfully completing the course enrollment, click the "Launch" button, for the Qualys Cloud Agent Exam.

Each candidate is provided five attempts to pass the exam.

With a passing score of 75% (or greater), click the "Print Certificate" button to download and print your course exam certificate.

Cloud Agent Course Survey

Please lets us know what you think about the "VMDR Overview" training course. Link to Survey - https://forms.office.com/r/rsy0Aja6Xz

Appendix A: Mac OS Agent Installation

The installation steps that follow support Mac OS 10.12 or higher.

You must have root or root-equivalent access to the target Mac host, to successfully perform the Cloud Agent installation steps that follow.

1. **From the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**

2. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**

3. **Click the "Install instructions" button next to the** "Mac (.pkg)" option.

4. *Copy and paste the installation command into a plain text document.*

5. **Click the "Download .pkg" button and save the Cloud Agent installation file (.pkg).**

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

The Mac Agent installation file (.pkg) must be installed from a "Terminal" window. Do NOT attempt to install this file using the Mac graphical user interface (GUI).

1. **Open a "Terminal" window on the target Mac host.**

2. **Navigate to the directory that contains the Cloud Agent installation file (.pkg).**

```
Air:desktop$ ls -la
total 8352
drwx------+    8       256 Aug  6 15:21 .
drwxr-xr-x+   34      1088 May 10 14:32 ..
-rw-r--r--@    1       487 Aug  6 15:11 mac_install.txt
-rw-r--r--@    1   3241714 Aug  6 15:12 qualys-cloud-agent.x86_64.pkg
```

3. **Use the "ls" command to verify the existence of the installation package.**

   If you do not see file "qualys-cloud-agent_x86_64.pkg" navigate to its correct location before executing the installation command.

4. **Copy and paste the installation command into the "Terminal" window and press the "Enter" key.**

   This first part of the command unpacks and installs the Cloud Agent package.

   This second part of the command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

5. **Use the "ps" command, to verify 'qualys-cloud-agent' is running.**

   ```
   ps -e | grep qualys
   ```

```
[macBook:desktop$ ps -e | grep qualys
 1237 ??          /Applications/QualysCloudAgent.app/Contents/MacOS/qualys-cloud-agent
 1259 ttys000   0 grep qualys
```

Locate Host ID

All agent host assets are automatically assigned a Qualys Host ID (UUID). For a Mac host, this Host ID can be found at /etc/qualys/hostid.

6. **From a Terminal window, execute the following command:**

   ```
   sudo cat /etc/qualys/hostid
   ```

If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Mac host in the /var/log/qualys directory.

7. **From a Terminal window, execute the following command:**

```
sudo cat /var/log/qualys/qualys-cloud-agent.log
```

CA Log Analysis & Troubleshooting

Visit the Qualys Training Video Library for more information and details on agent log analysis and troubleshooting:
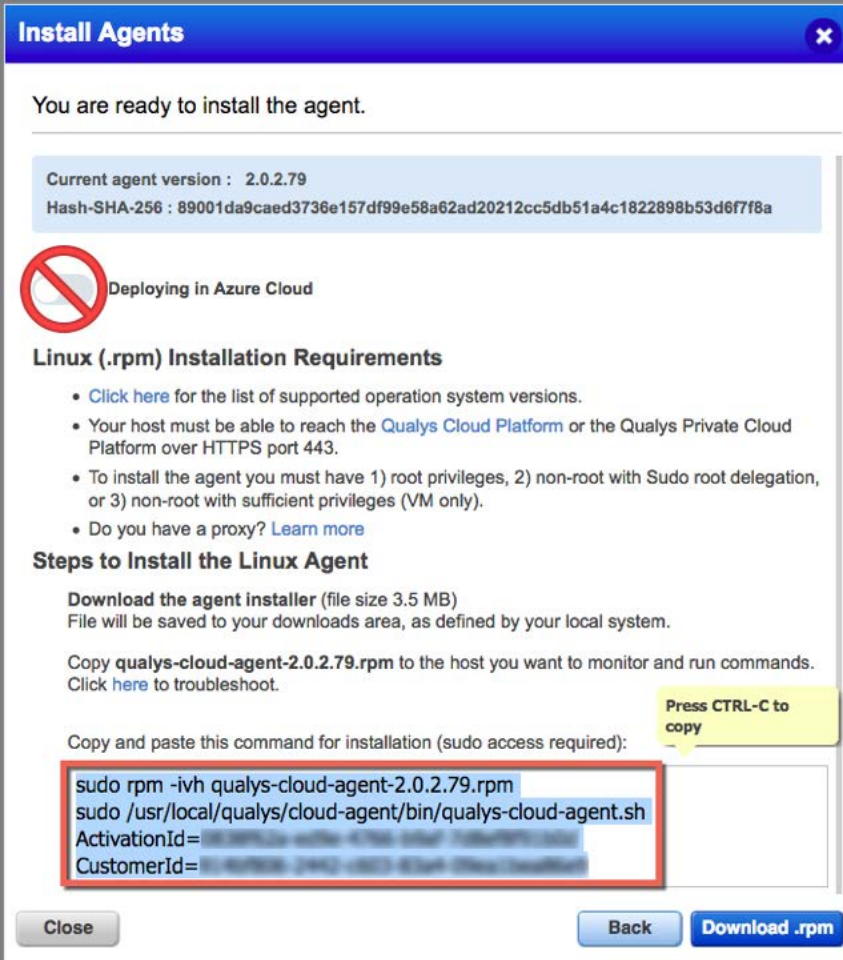
- Introduction to Troubleshooting & Log Analysis (https://vimeo.com/412764672)

- Troubleshooting & Log Analysis – Common Errors (https://vimeo.com/412762742)

- Troubleshooting & Log Analysis – Unix/Linux Distribution (https://vimeo.com/418215691)

- Common Errors and Their Solutions – Unix/Linux Distribution (https://vimeo.com/418218290)

Appendix B: RPM-Based Agent Installation

RPM-based Linux operating systems include: Red Hat Enterprise Linux, CentOS, Fedora, OpenSuSE, SuSE, Amazon Linux, and Oracle Enterprise Linux.

You must have root or root-equivalent access to the target host, to successfully perform the Cloud Agent installation steps that follow.

1. **From the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**

2. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**

3. **Click the "Install instructions" button next to the** 🐧 **"Linux (.rpm)" option.**

4. *Copy and paste the installation command into a plain text document.*

5. **Click the "Download. rpm file" button and save the Cloud Agent installation file.**

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

1. **Open a "Terminal" window on the target Unix host.**

2. **Navigate to the directory that contains the Cloud Agent installation file (.rpm).**

```
[qscan@centos7 Desktop]$ ls -la
total 3132
drwxr-xr-x.  3 qscan qscan       88 Jan  2 19:03 .
drwx------. 16 qscan qscan     4096 Jan  2 18:50 ..
drwx------.  3 qscan qscan       29 Nov  7 2015 Old Firefox Data
-rw-rw-r--.  1 qscan qscan  3195390 Jan              qualys-cloud-agent.x86_64.rpm
-rw-r--r--.  1 qscan qscan      204 Jan  2 18:40 unix_install.txt

[qscan@centos7 Desktop]$ sudo rpm -ivh qualys-cloud-agent.x86_64.rpm
```

Paste and execute the first command.

3. **Use the "ls" command to verify the existence of the installation file.**

   If you do not see file "qualys-cloud-agent_x86_64.rpm" navigate to its correct location before executing the installation command.

4. **Copy and paste the installation command into the "Terminal" window and press the "Enter" key.**

   The first part of the command unpacks and installs the Cloud Agent package.

   The second part of the command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

```
 6972 tty7      00:00:00 Xorg
 6984 ?
 6985 ?              Type "ps -e" from the command line.
 6987 ?
 6988 pts/1     00:00:00 bash
 8404 pts/2     00:00:00 qualys-cloud-ag
 8420 pts/1     00:00:00 ps
24375 ?         00:00:14 java
26814 ?         00:00:00 httpd
```

5. **Use the "ps" command, to verify 'qualys-cloud-ag' is running.**

   ```
   ps –e | grep qualys
   ```

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Unix host, this Host ID can be found at /etc/qualys/hostid.

6. **From a Terminal window, execute the following command:**

```
sudo cat /etc/qualys/hostid
```

If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Unix host in the /var/log/qualys directory.

7. **From a Terminal window, execute the following command:**

```
sudo cat /var/log/qualys/qualys-cloud-agent.log
```
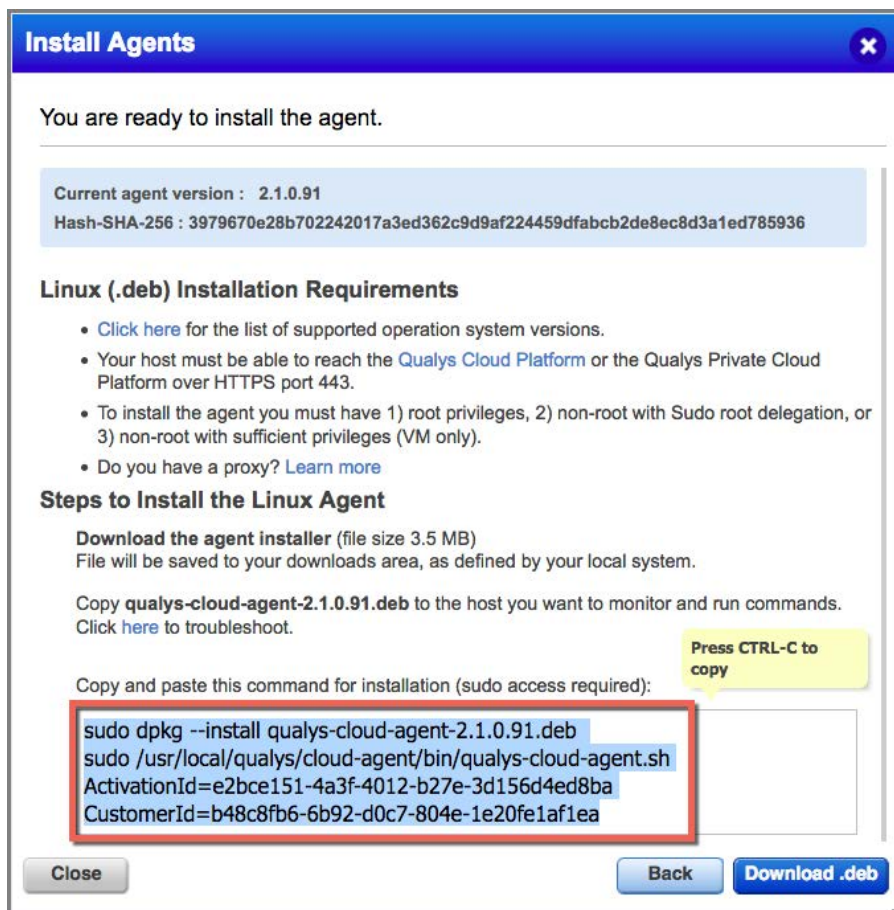
CA Log Analysis & Troubleshooting

Visit the Qualys Training Video Library for more information and details on agent log analysis and troubleshooting:

- Introduction to Troubleshooting & Log Analysis (https://vimeo.com/412764672)

- Troubleshooting & Log Analysis – Common Errors (https://vimeo.com/412762742)

- Troubleshooting & Log Analysis – Unix/Linux Distribution (https://vimeo.com/418215691)

- Common Errors and Their Solutions – Unix/Linux Distribution (https://vimeo.com/418218290)

Appendix C: Debian/Ubuntu Agent Installation

You must have root or root-equivalent access to the target host, to successfully perform the Cloud Agent installation steps that follow.

1. **From the Cloud Agent (CA) application, navigate to the "Agent Management" section, and click the "Activation Keys" tab.**

2. **Use the "Quick Actions" menu of your activation key to select the "Install Agent" option.**

3. **Click the "Install instructions" button next to the   "Linux (.deb)" option.**

4. *Copy and paste the installation command into a plain text document.*

5. **Click the "Download. deb file" button and save the Cloud Agent installation file.**

Command Line Installation

Although this lab uses a simple 'command line' technique to install Cloud Agent, other techniques and/or third-party applications can be leveraged to automate your Cloud Agent deployment.

1. **Open a "Terminal" window on the target Unix host.**

2. **Navigate to the directory that contains the Cloud Agent installation file (.deb).**

```
ubuntu@ec2-ubu1604:~$ ls -la
total 4000
drwxr-xr-x 4 ubuntu ubuntu    4096 Aug 29 15:12 .
drwxr-xr-x 5 root   root      4096 Aug  9 14:40 ..
-rw------- 1 ubuntu ubuntu    2801 Aug 29 15:17 .bash_history
-rw-r--r-- 1 ubuntu ubuntu     220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu    3771 Aug 31  2015 .bashrc
drwx------ 2 ubuntu ubuntu    4096 Aug  7 21:39 .cache
-rw-r--r-- 1 ubuntu ubuntu     655 May 16  2017 .profile
-rw-r--r-- 1 ubuntu ubuntu 4058210 Aug  7         qualys-cloud-agent-2.0.2.79.deb
drwx------ 2 ubuntu ubuntu    4096 Aug  7 21:28 .ssh
-rw-r--r-- 1 ubuntu ubuntu       0 Aug  7 21:41 .sudo_as_admin_successful
-rw------- 1 root   root      2935 Aug 29 15:12 .viminfo
ubuntu@ec2-ubu1604:~$
```

3. **Use the "ls" command to verify the existence of the installation file.**

   If you do not see file "qualys-cloud-agent_x86_64.deb" navigate to its correct location before executing the installation command.

4. **Copy and paste the installation command into the "Terminal" window and press the "Enter" key.**

   The first part of the command unpacks and installs the Cloud Agent package.

   The second part of the command runs a shell script that that restarts the Cloud Agent service and activates your license key.

Validate CA Installation

To verify the success of your "command line" installation, look for the Cloud Agent process.

```
 6972 tty7     00:00:00 Xorg
 6984 ?
 6985 ?           Type "ps -e" from the command line.
 6987 ?
 6988 pts/1    00:00:00 bash
 8404 pts/2    00:00:00 qualys-cloud-ag
 8420 pts/1    00:00:00 ps
24375 ?        00:00:14 java
26814 ?        00:00:00 httpd
```

5. **Use the "ps" command, to verify 'qualys-cloud-ag' is running.**

   ```
   ps -e | grep qualys
   ```

Locate Host ID

All agent host assets are automatically assigned a Universally Unique ID (UUID) by Qualys. For a Unix host, this Host ID can be found at /etc/qualys/hostid.

6. **From a Terminal window, execute the following command:**

```
sudo cat /etc/qualys/hostid
```

If the HostID is not displayed, your newly installed agent may still be completing some preliminary tasks within its manifest.

Locate CA Log File (qualys-cloud-agent.log)

You can use the Cloud Agent log file to monitor agent activity. You will find the log file for a Unix host in the /var/log/qualys directory.

7. **From a Terminal window, execute the following command:**

```
sudo cat /var/log/qualys/qualys-cloud-agent.log
```

CA Log Analysis & Troubleshooting

Visit the Qualys Training Video Library for more information and details on agent log analysis and troubleshooting:

- Introduction to Troubleshooting & Log Analysis (https://vimeo.com/412764672)

- Troubleshooting & Log Analysis – Common Errors (https://vimeo.com/412762742)

- Troubleshooting & Log Analysis – Unix/Linux Distribution (https://vimeo.com/418215691)

- Common Errors and Their Solutions – Unix/Linux Distribution (https://vimeo.com/418218290)

Appendix D: Qualys Technical Support

When contacting Qualys Technical Support to report observed agent issues or errors, you may be asked to provide the following information:

Windows Host

1. Make a copy of the following folder and all of its subfolders:

   `\ProgramData\Qualys\QualysAgent\`

2. Use Windows Explorer or your favorite archive utility to move the contents of this folder into a single compressed (.zip) file.

Linux/Unix/Mac Host

1. Make a copy of the following directory and all of its subdirectories:

   `/var/log/qualys/`

2. Use an archive utility to move the contents of this directory into a single compressed or tarball file.

Other Helpful Information

When possible, provide other log files (from other applications and services running on the suspect agent host) that correlate to the events recorded within the agent log file. This type of information is especially useful for identifying potential conflicts between Cloud Agent and other applications or services.