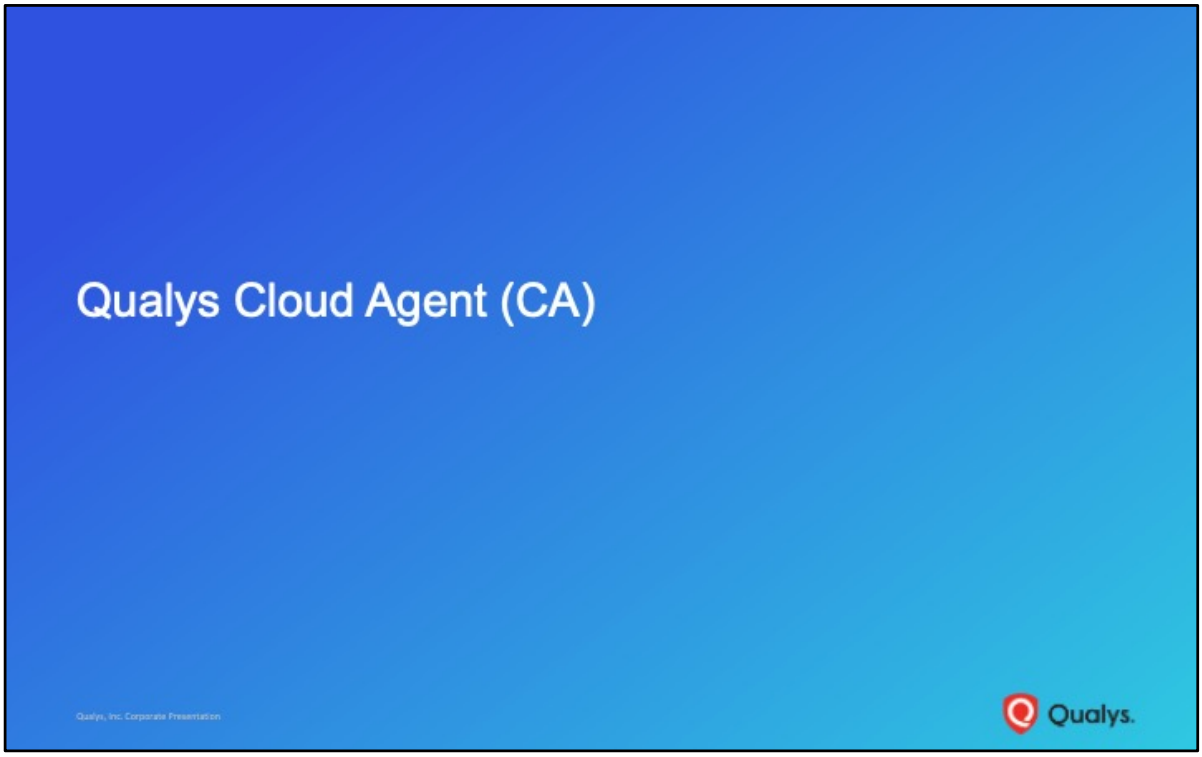
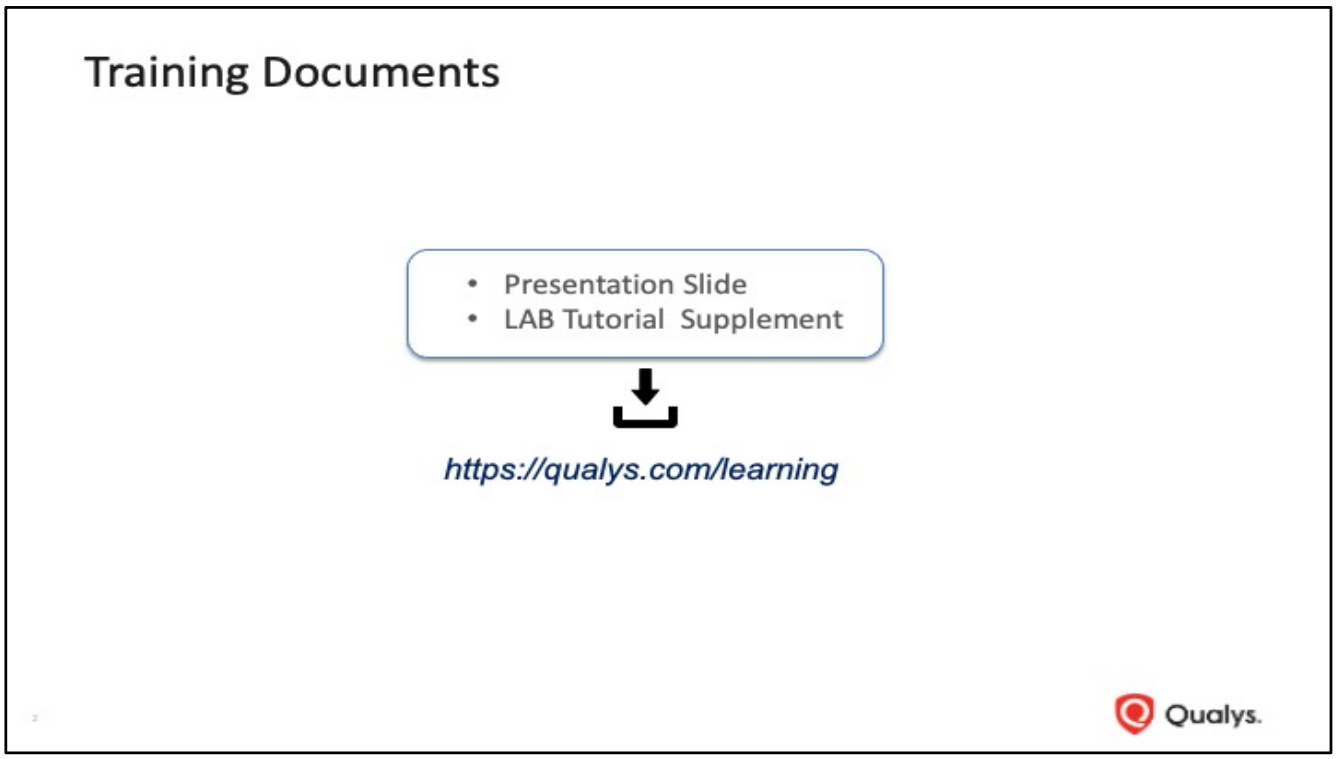
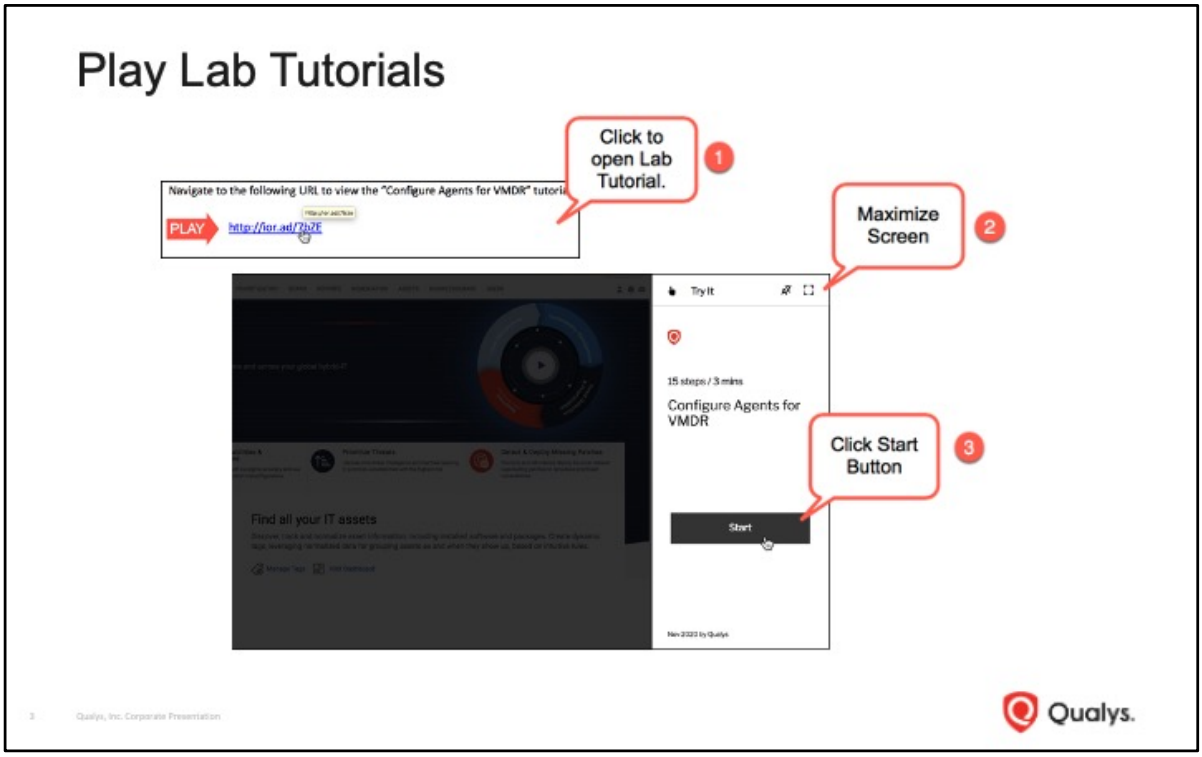



Welcome to Qualys Cloud Agent training.




You will need to download the training documents needed to complete the Container Security course from the Qualys learning portal qualys.com/learning.

Note that you will need a PDF reader like Adobe Acrobat to view these files.




1. When you click the link to open a lab tutorial, it will open-up in your default Web browser. If you would like to play the tutorial in a different browser, you can copy this link and paste it into the address field of another browser.

2. When the lab tutorial opens, click the icon in the upper-right corner, to maximize your screen size.

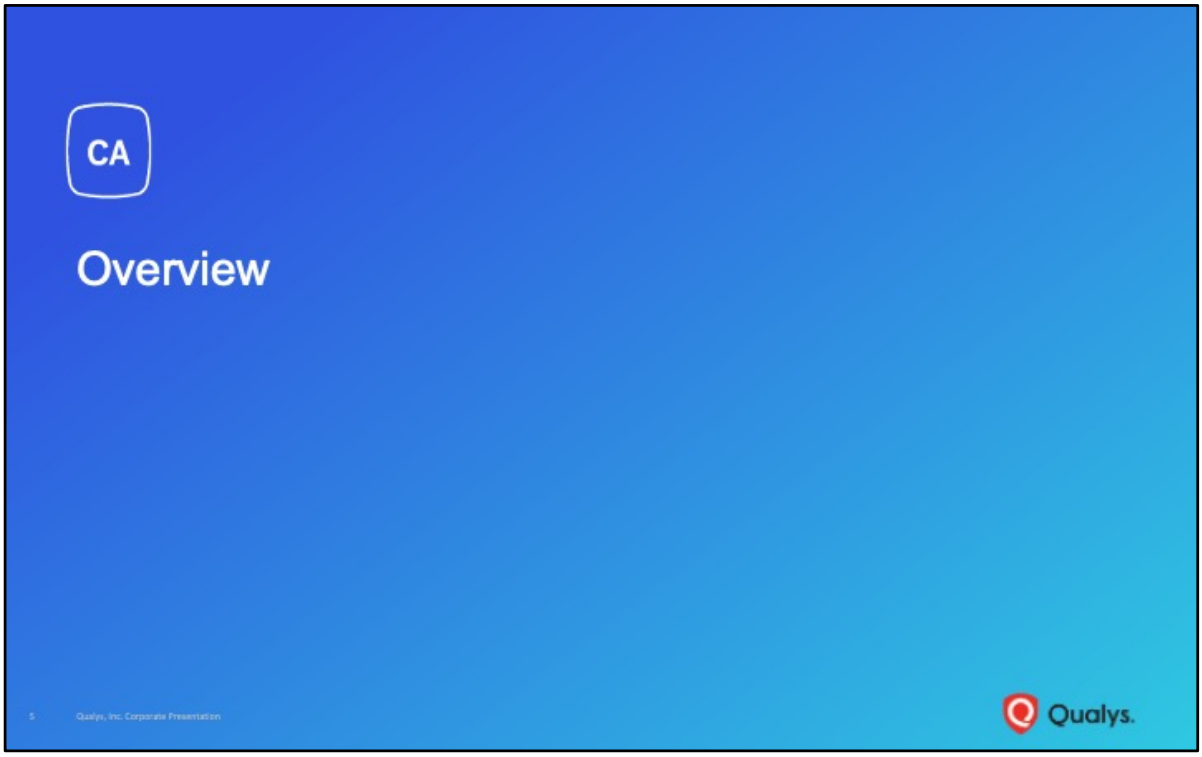
3. When your ready to play the tutorial, click the start button.

# Agenda

- **Cloud Agent Overview**
- **Cloud Agent Installation & Deployment**
  - **Agent Activation Key**
  - **Installation Components**
  - **Agent Installation Options**
- **Agent Asset Details**
- **Cloud Agent Lifecycle and Configuration**

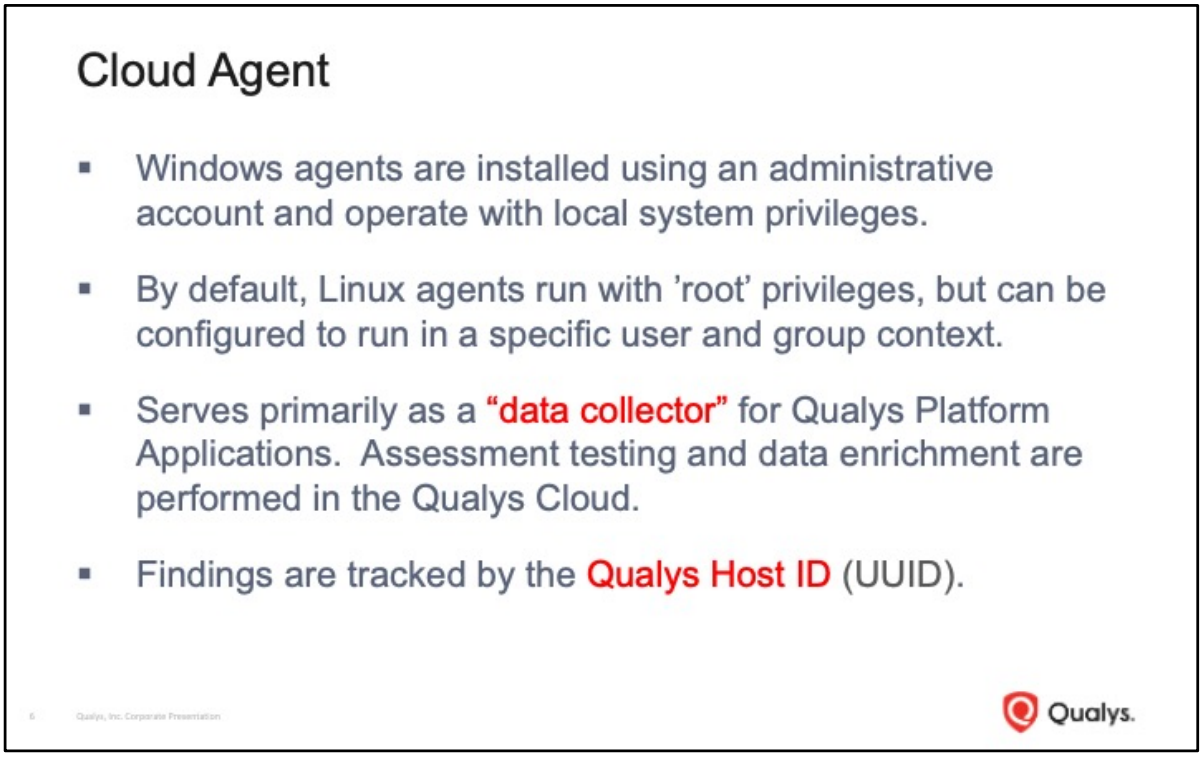


Qualys.




The objectives for this section are:

1. Provide a high-level overview of CA  behaviors and characteristics.
2. Identify operating systems and Qualys applications supported by CA.
3. New RedHat CoreOS feature

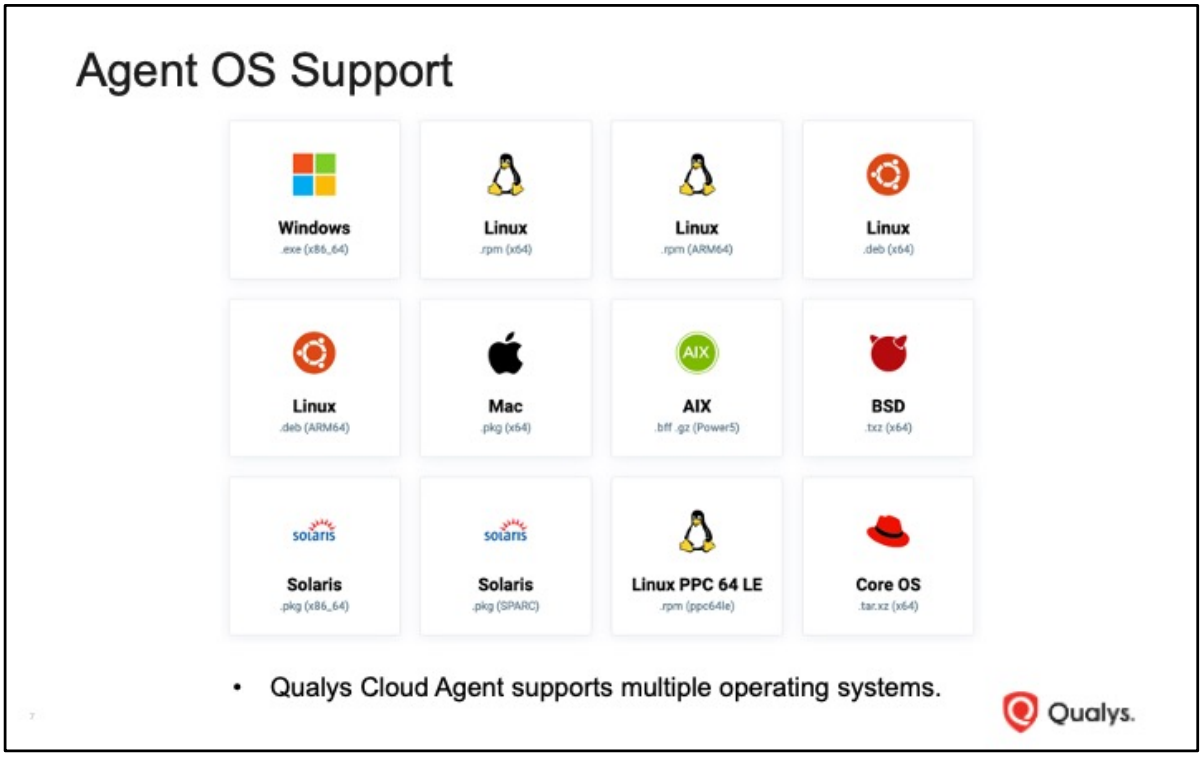



Windows agents must be installed using an administrative account and will operate with system level privileges.

The agent installation requires root level access on Unix and Linux systems (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. Caution: this limits the level of access of the Cloud Agent.

To optimize agent performance and keep its resource consumption low, agents focus primarily on data collection tasks (i.e., collecting host data and telemetry and then sending it to the Qualys Cloud). Assessment testing, data categorization, normalization, and enrichment are performed in the Qualys Cloud.

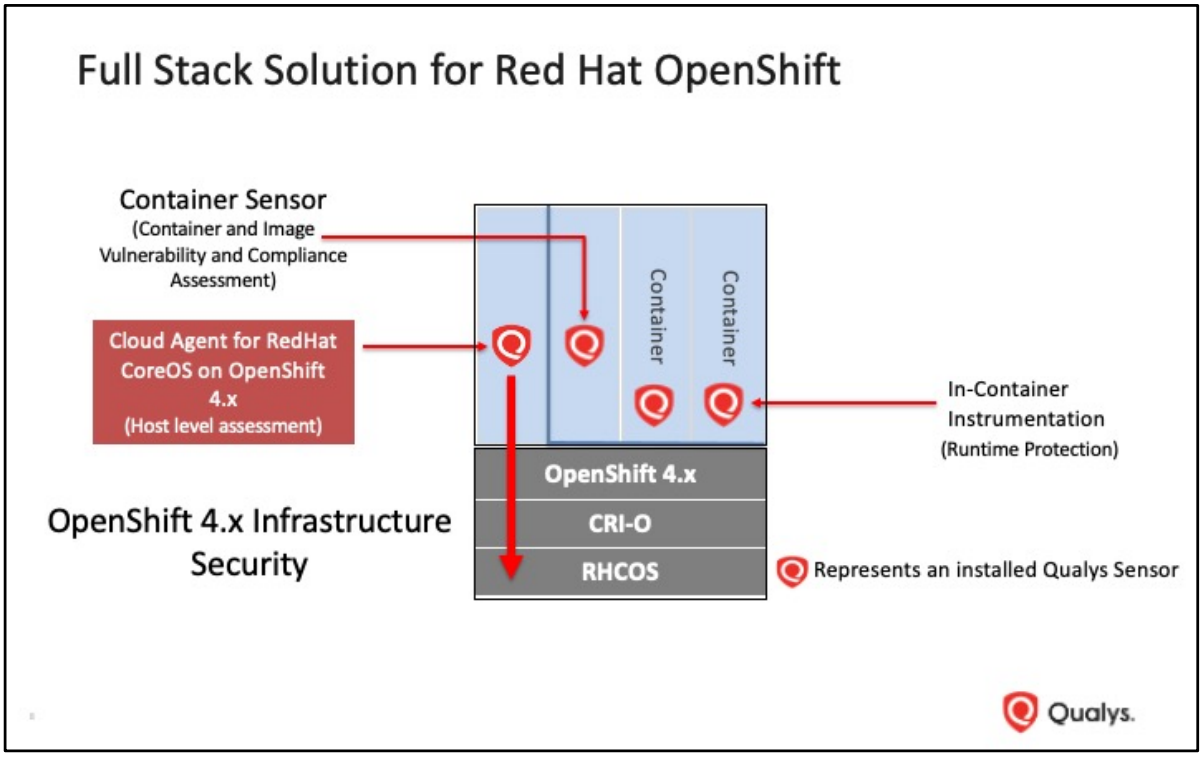
Agent findings are tracked by the Qualys Host ID, which uniquely identifies it agent host (UUID).




Cloud Agents can be installed on host assets running Cloud Agent supported operating systems, including:

- Windows XP SP3 or greater
- Apple Mac OS X
- Red Hat Enterprise Linux
- Oracle Enterprise Linux
- Amazon Linux
- SuSE Linux
- CentOS
- Fedora
- Debian
- Ubuntu
- FreeBSD
- IBM AIX
- Solaris
- Core OS

For a complete list of supported operating systems and version numbers, see the Cloud Agent Getting Started Guide: https://www.qualys.com/docs/qualys-cloud-agent-getting-started-guide.pdf




At Qualys, we have focused on delivering a full stack solution for Red Hat OpenShift. To do this, we utilize both Container Sensors and Cloud Agents.

As you can see in the diagram, our container sensor solution is deployed as its own container. It assesses images and running containers in your runtime environment.

This solution is technically independent from the Cloud Agent container and provides inventory, vulnerability, and compliance assessments;  with data merging and sharing between modules on the Qualys Cloud Platform.

Our Container Security Solution has been in the market for a while now and supports Docker, Container-D, and Crio runtimes.

But what about the Host OS? RHCOS does not permit modification of the host. This is a powerful security measure.

That does not mean it is impervious to attack, but it does provide a strong base for building excellent layered security solutions.

Our unique first to market solution, uses an agent-as-container approach.

Easily deployed, our containerized agent scans the Host OS to provide visibility, actionable intelligence, and auditing.

Qualys full-stack security for Red Hat OpenShift adds visibility, actionable intelligence, and security auditing for Red Hat Enterprise Linux CoreOS, the operating system that underpins OpenShift deployments for running containers securely. With this new offering, Qualys is now the first and only solution with the ability to scan directly into Red Hat Enterprise Linux CoreOS in Red Hat OpenShift, so you can manage and reduce risk at both the host OS and container levels. Built on the Qualys Cloud Platform, Qualys' solution seamlessly integrates with customers' vulnerability management workflows, reporting and metrics to help reduce risk.

# Cloud Agent for RedHat OpenShift

Qualys offers the first and only platform to identify and manage threats for Red Hat Enterprise Linux CoreOS in OpenShift.

This new capability enables:

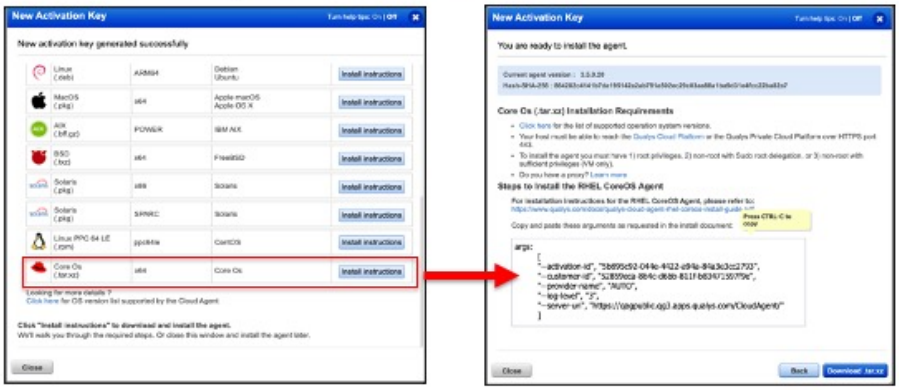
- Continuous visibility of installed software and packages, open ports, and Red Hat Security Advisories (RHSA)
- Vulnerability management and patch verification for Red Hat OpenShift
- Easy deployment via container to secure the host operating systems without requiring modifications to the host, opening ports, or dealing with credentials
- Seamless operation with Qualys Container Security to provide security from the host through the container level



Qualys.

## Cloud Agent for RedHat OpenShift Installation

Within the activation key, select install instructions for CoreOS from the list and follow the steps for installation.



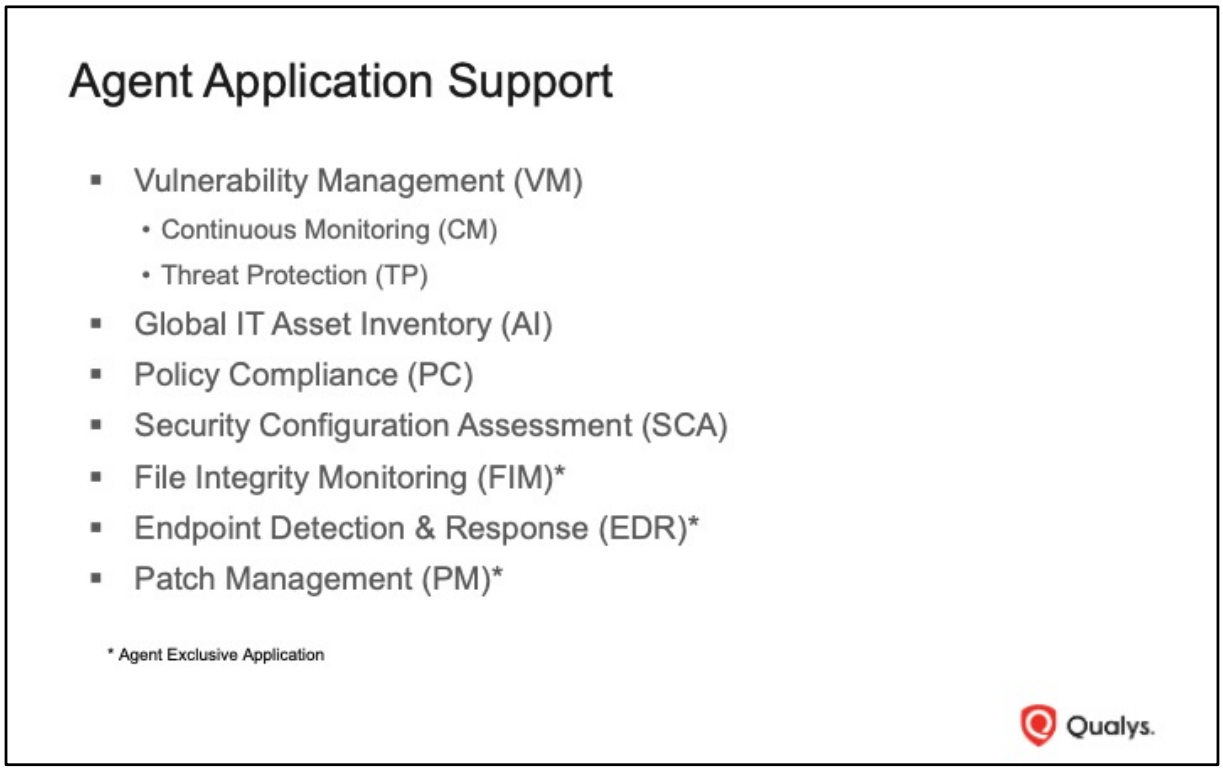



Qualys.

- Download the Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift Container image tar file from Qualys Cloud Platform.

Follow the steps in the below guide.

https://www.qualys.com/docs/qualys-cloud-agent-redhat-openshift-coreos-install-guide.pdf



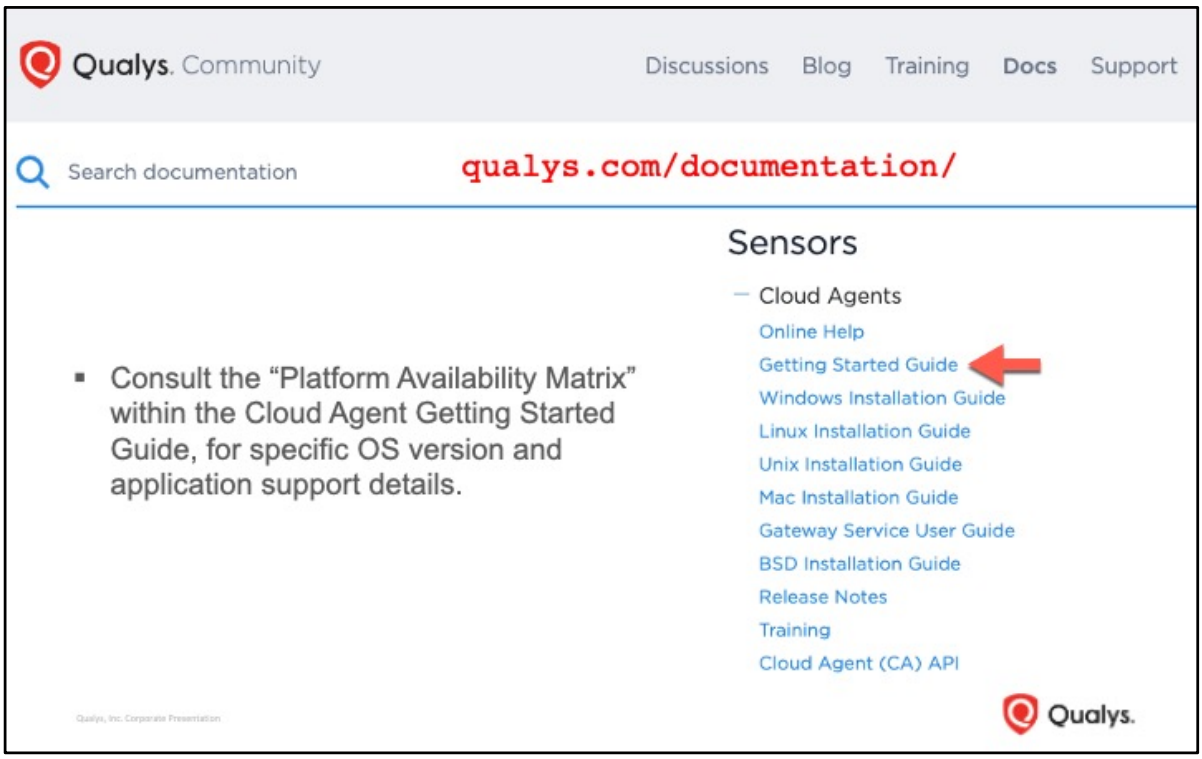

Qualys Cloud Agent supports multiple Qualys application modules.

Qualys Global IT Asset Inventory (AI) is automatically activated for all agents. When the VM module is activated for an agent, Continuous Monitoring (CM) and Threat Protection (TP) are included. You can activate Policy Compliance (PC) or Security Configuration Assessment (SCA) for an agent, but not at the same time.

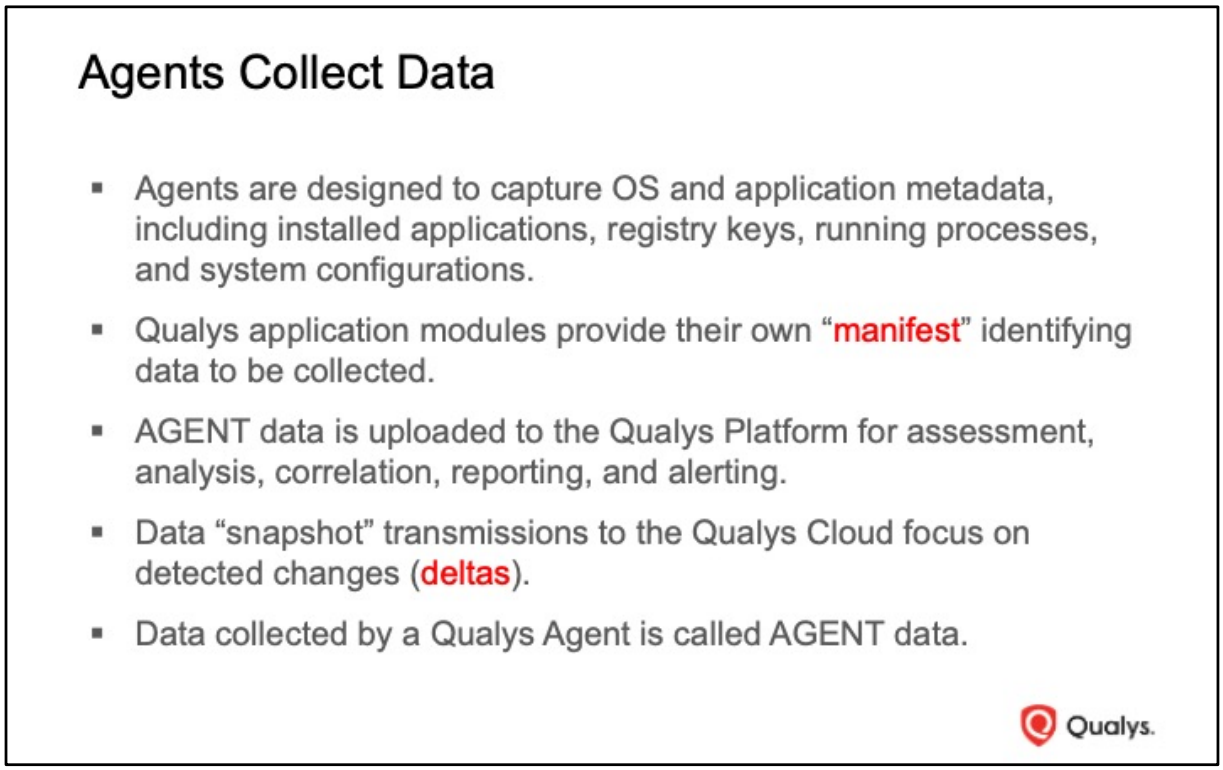
Qualys File Integrity Monitoring (FIM), Endpoint Detection & Response (EDR), and Patch Management are agent exclusive applications (i.e., they are not supported by other Qualys sensors).

Three options are provided for activating application modules:

1. Agent Activation Key
2. Host “Quick Actions” Menu
3. CA Application Program Interface (API)




For a complete list of supported operating systems and version numbers, see the Cloud Agent Getting Started Guide: qualys.com/documenttion

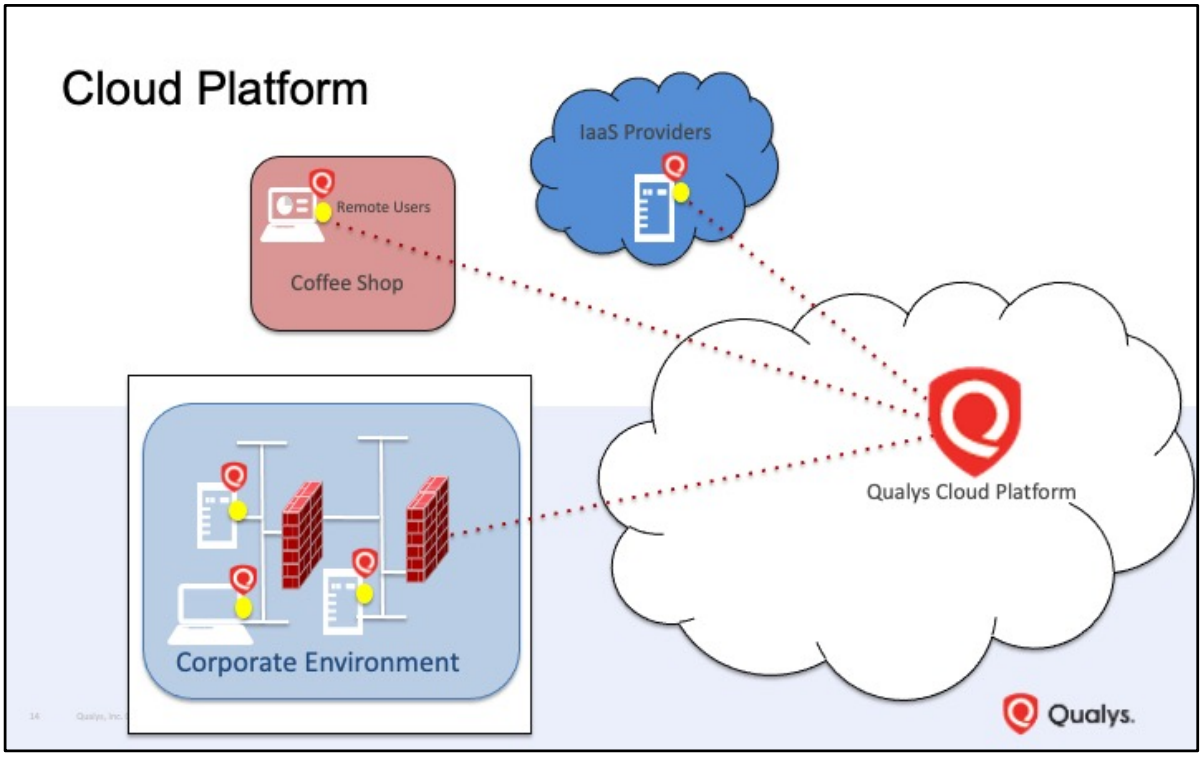



Functioning in the "data collector" role, agents collect everything needed by its activated Qualys application modules. Each agent supported application module identifies tasks to be performed and data to be collected, in a manifest. There are different manifests for each Qualys application module.

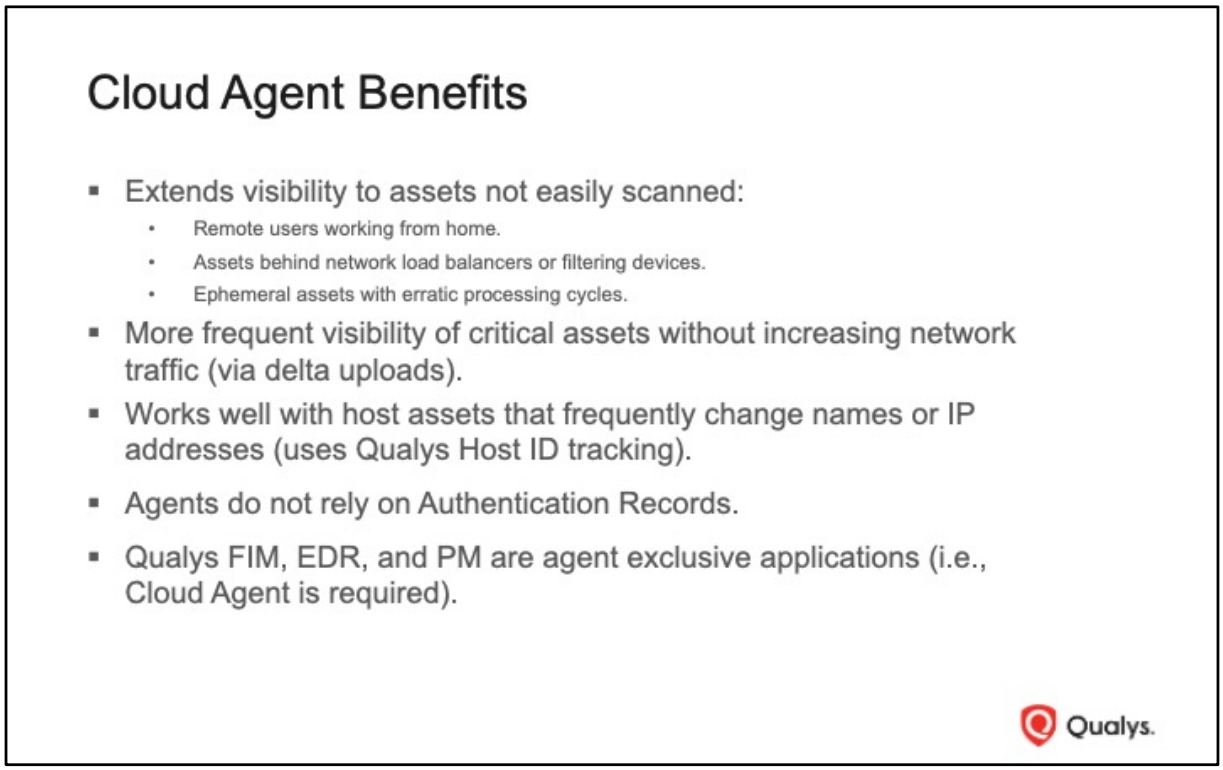
By design, the processing of agent data begins only after it is successfully transferred to the Qualys Platform. This helps to minimize the number of resources need by the agent.

Once the initial data "snapshot" has been successfully transferred to the Qualys Platform, all successive data transfers focus exclusively on the things that have changed (deltas).

Data collected by a Qualys Agent is referred to as AGENT data. This contrasts with the data collected by a Qualys Scanner Appliance, which is referred to as SCAN data.




1. To begin data collection an agent must be installed/deployed to a host.
2. Once the agent has successfully downloaded its application manifest(s), data will be collected to produce a host snapshot.
3. This “snapshot” is then sent to the Qualys Cloud for processing.



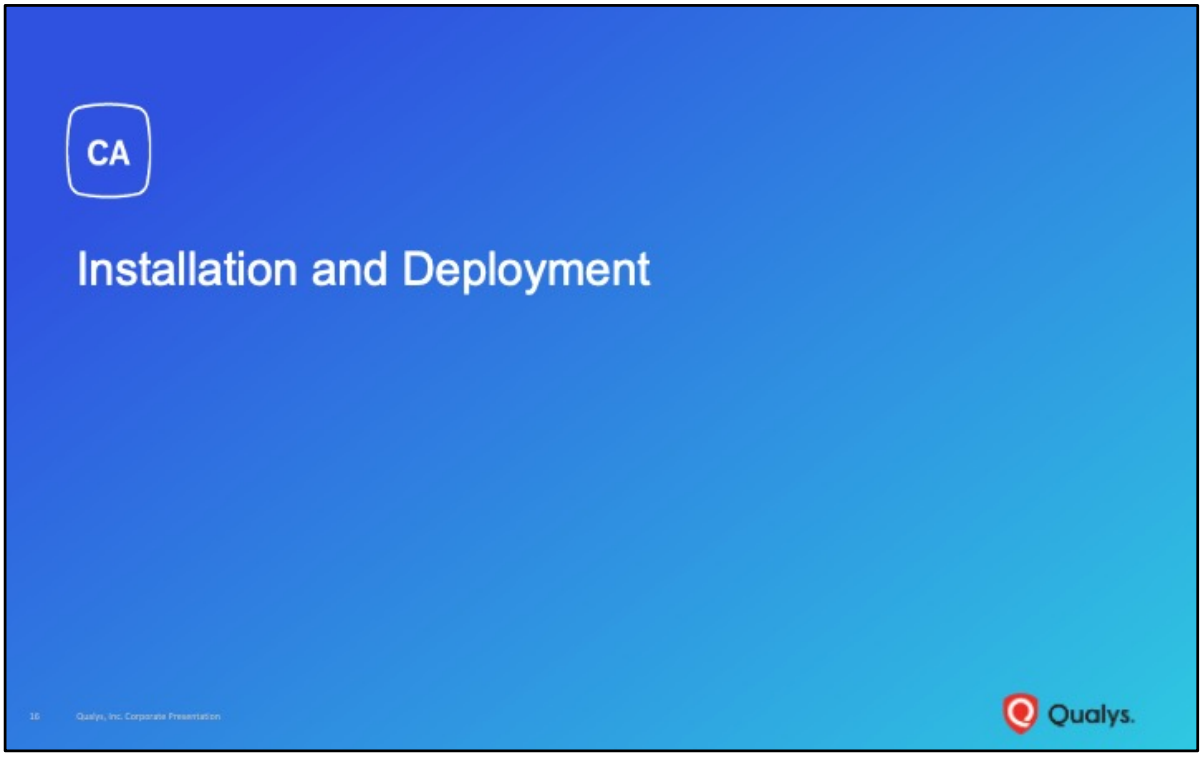

Cloud Agent extends visibility to assets not easily scanned, including roaming devices such as laptops, remote users working from home, ephemeral cloud instances that are not always online, and assets behind network filtering devices or load balancers.

Once the initial data “snapshot” has been successfully transferred to the Qualys Platform, all successive data transfers focus exclusively on the things that have changed (deltas). This can significantly reduce the amount of bandwidth typically consumed by traditional scanner appliances, allowing you to monitor critical hosts more frequently.

By default, agents track findings by the Qualys Host ID, making it ideal for hosts that frequently change names or IP addresses.

Cloud Agent installs as a local service with SYSTEM level privileges and does not require authentication records to access local system data and artifacts.

Cloud Agents are required by the Quays FIM, EDR, and PM applications.

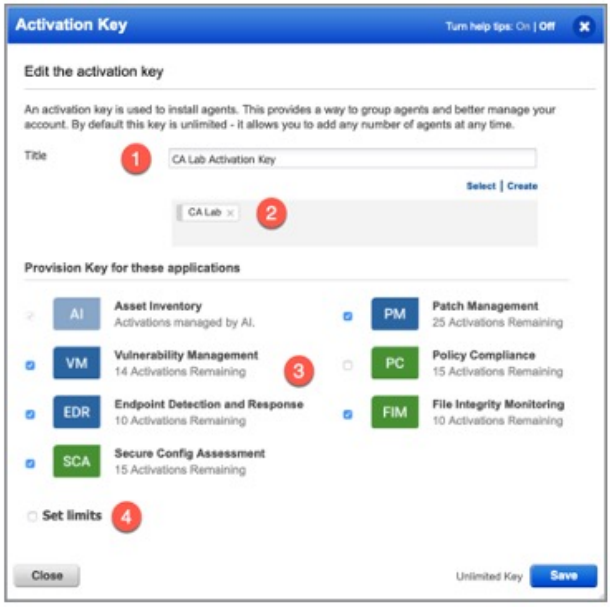



The objectives for this section are:

1. Identify and understand the steps to complete an agent installation.
2. Learn to build an Agent Activation Key and identify its components.
3. Understand the different agent deployment options.
4. Identify the signs of a successful agent installation
5. New MSI Extract Feature

# Agent Activation Key

1. Activation Keys allow you to manage and control the distribution of Cloud Agents.
2. Add a "static" tag to each key to label and track agent hosts deployed.
3. Application modules selected will be activated at agent deployment.
4. Create keys without limits or set limits by maximum number of agents or expiration date.



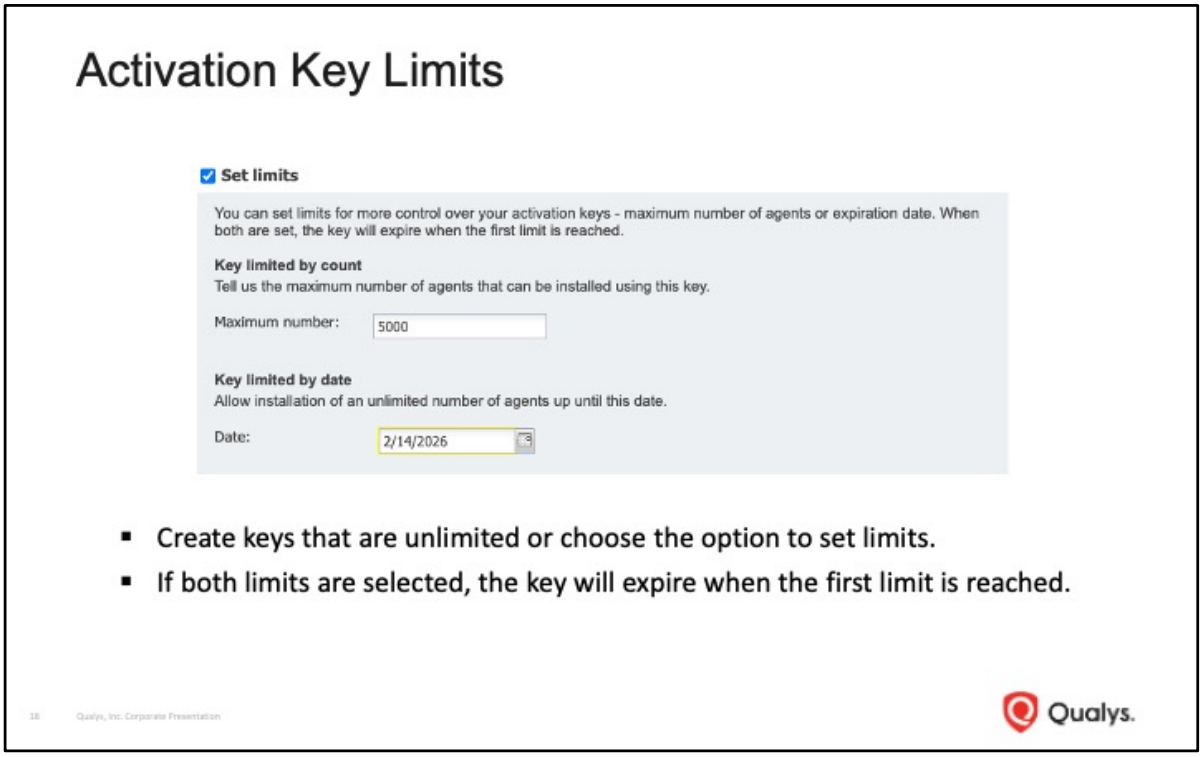

Qualys.

Activations Keys contain the components to successfully deploy agents. You must first create one or more Activation Keys, before installing an agent.

Qualys recommends adding a ”static” tag to an Activation Key, to easily identify the assets it deploys.

Any application module selected in the key will be activated at the time of deployment. Application modules not selected can always be activated later (after deployment).

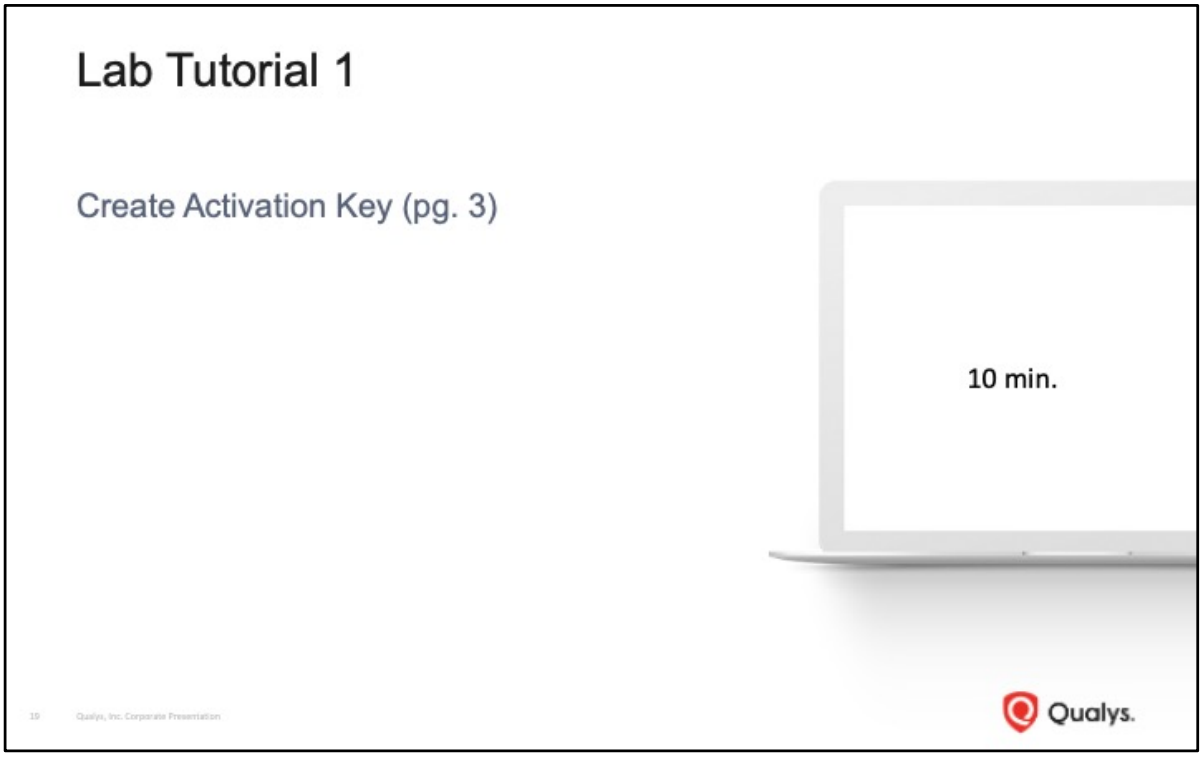
Options are available to limit the number of agents deployed with any key.




An Activation Key can deploy an unlimited number of agents, or you can set limits.

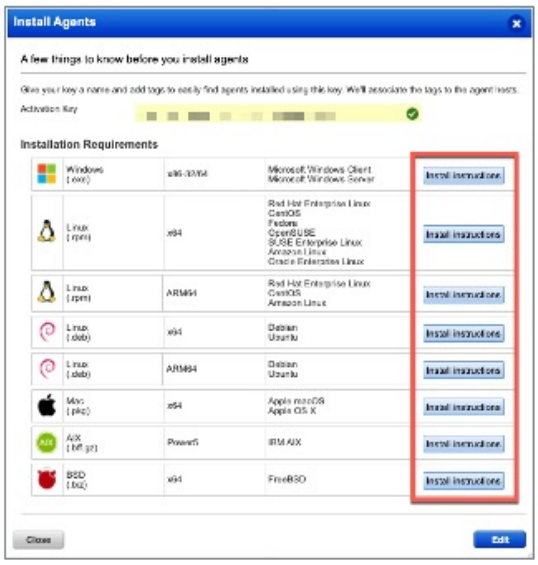
1. Specify the maximum number of agents deployed with a key.
2. Specify an expiration date for the key

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




1. Create CA Lab Activation Key
2. Create and add a static tag (CA Lab) to key
3. Add application modules to key
4. No restrictions or limits
5. Generate key

# Install Agents

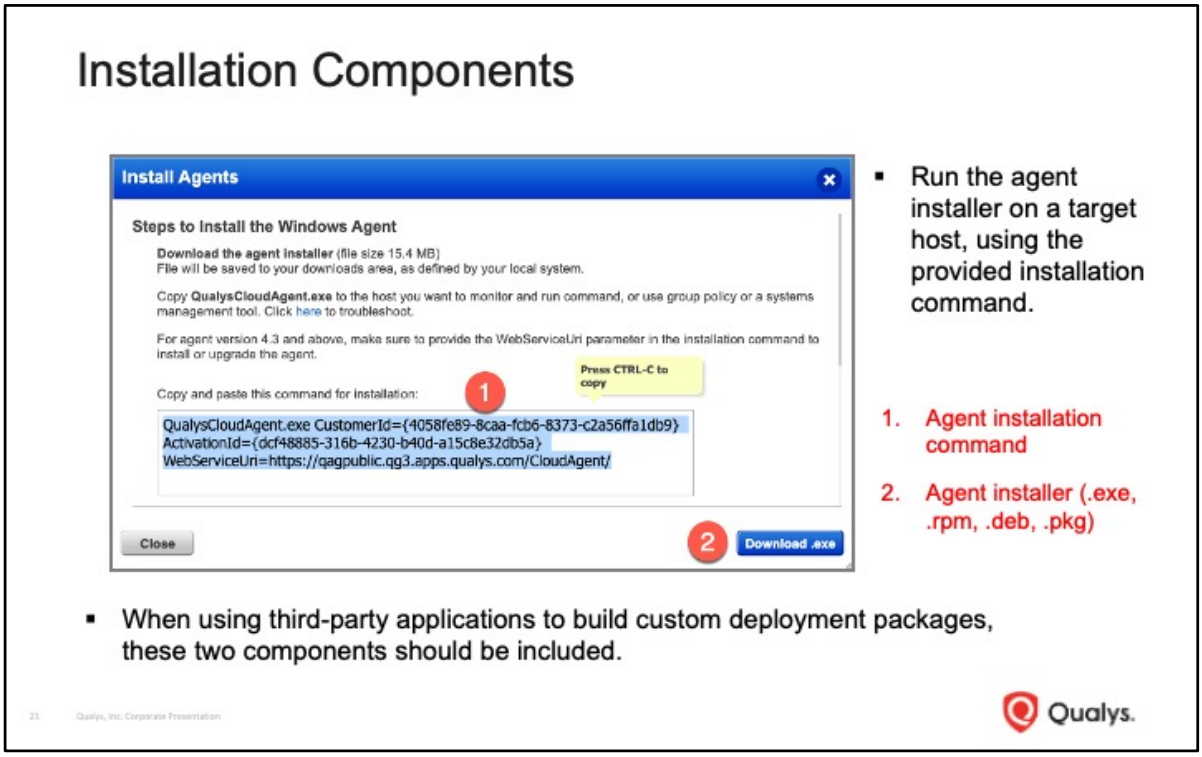



- Select the “Install Agent” option from the Quick Actions menu of any Activation Key.
- Each Activation Key contains installation instructions for agent supported operating systems.
- Click “Install Instructions” for any OS, to view its instructions and download the agent installation components.

Qualys.

To acquire the installation instructions and artifacts for an Activation Key, open its “Quick Actions” menu and select Install Agent.

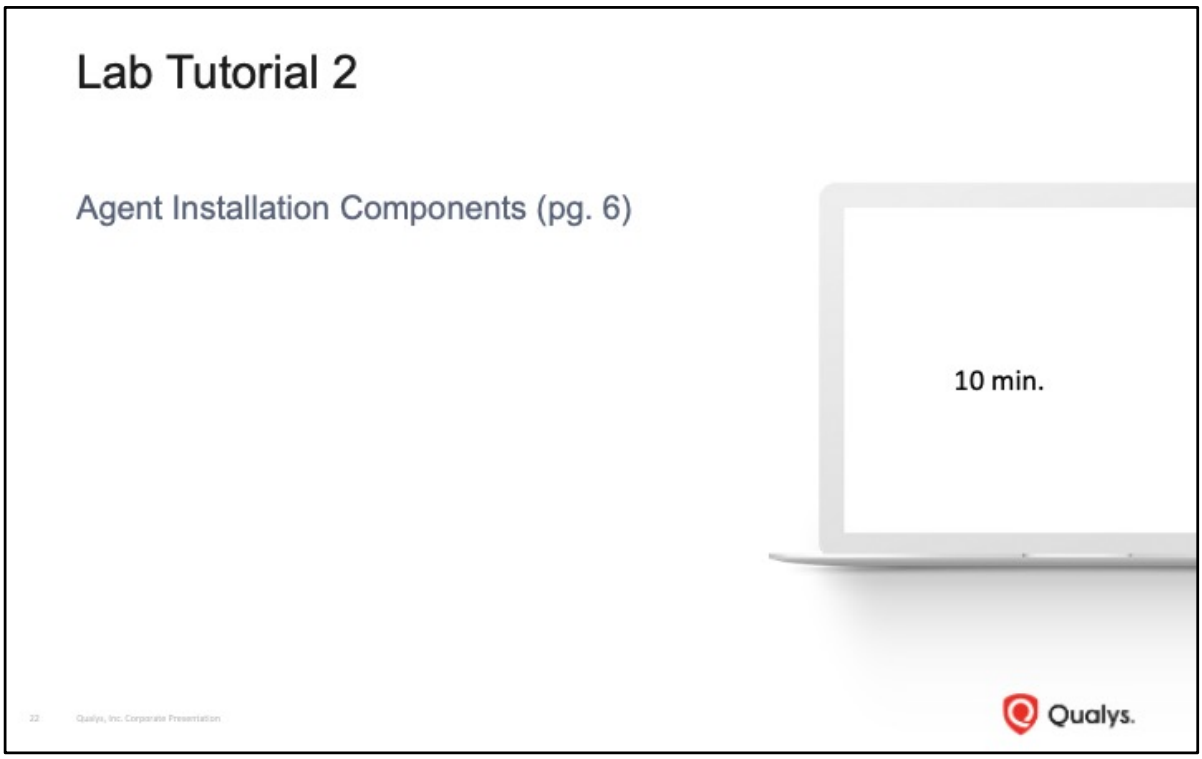
Click “Install Instructions” for any OS, to view its instructions and download its agent installation components.



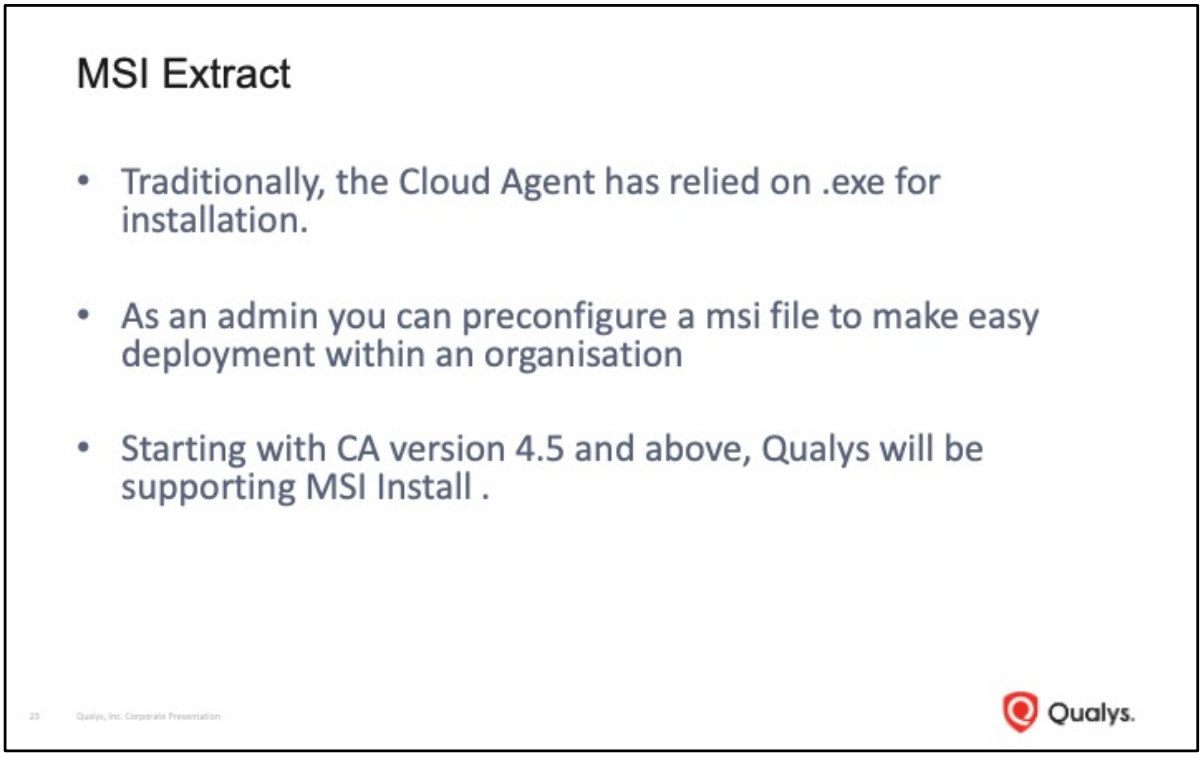

The primary agent installation components include:

1. Agent installation command
2. Agent installer

These two components must be included in your installation packages




1. Download installation components for Windows agent
2. Use CA Lab Activation Key to install agent
3. Download agent installer
4. Copy installation command




Use Case for MSI:

- It's relative easy to make a tree of msi files, and as an admin you can preconfigure a msi file to make easy deployment within an organisation
- You might want more precise control over how the installation is managed. An MSI has very specific rules about how it manages the installations, including installing, upgrading, and uninstalling.

From the high-level user's perspective, the new setup is an exe containing the setup components to install Qualys agent on the target machine. The exe contains two MSIs – one for 32-bit machines, and another one for 64-bit machines. The exe would extract the correct MSI and invoke the MSI engine to begin the installation process. The exe can also be instructed to only extract the MSI/MSI(s).

## MSI Extract

To extract MSI from the downloaded exe file, run the following command:

QualysCloudAgent.exe ExtractMSI=<*value*>

Any agent version above 4.5 will support MSI.

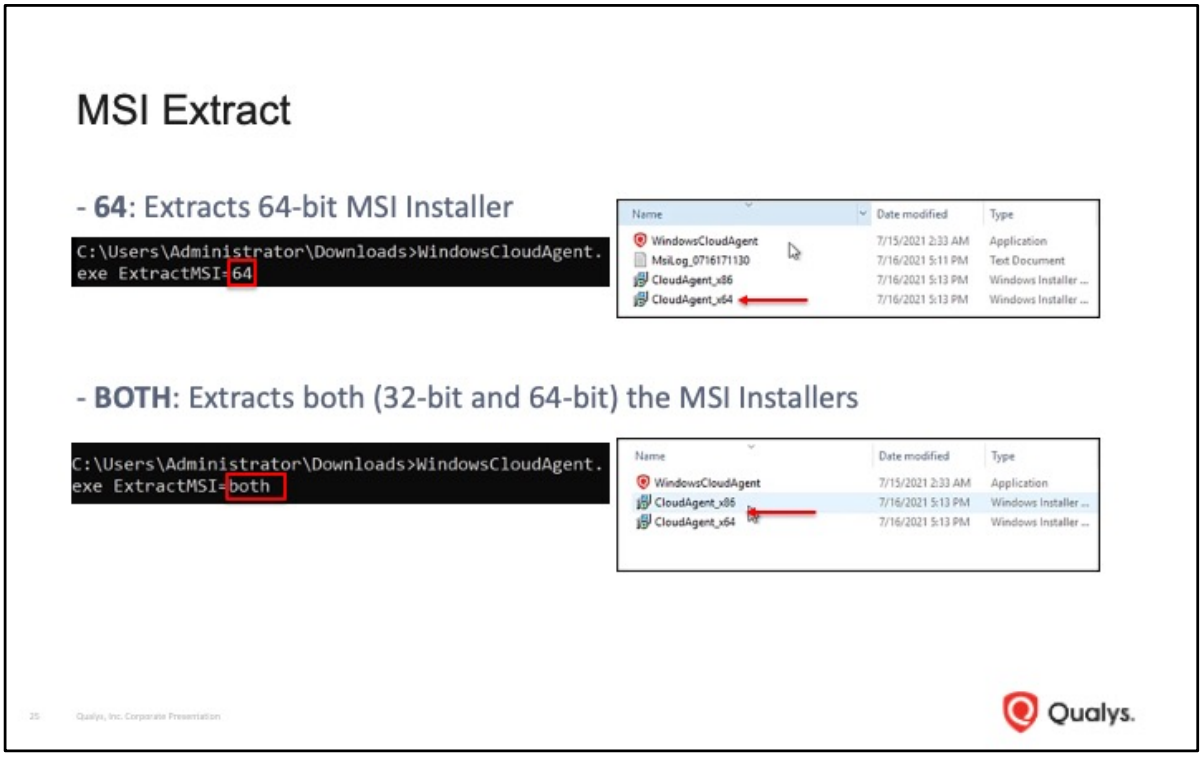
For ExtractMSI, use following values (*value*) as per host architecture.

For example, if you want to install cloud agent on 64-bit machine, you need to extract MSI package with value for ExtractMSI=32.



Qualys.

To extract MSI from the downloaded exe file, run the following command:
QualysCloudAgent.exe ExtractMSI=<*value*>
For ExtractMSI, use following values (*value*) as per host architecture.
For example, if you want to install cloud agent on 64-bit machine, you need to extract MSI package with value for ExtractMSI=64.
- **32**: Extracts 32-bit MSI Installer
- **64**: Extracts 64-bit MSI Installer
- **BOTH**: Extracts both (32-bit and 64-bit) the MSI Installers
- **AUTO**: Extracts the appropriate MSI based on the OS architecture. It extracts 32-bit MSI on a 32-bit machine and 64-bit MSI on a 64-bit machine

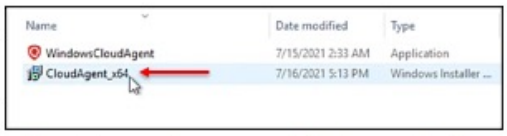



To extract MSI from the downloaded exe file, run the following command:
QualysCloudAgent.exe ExtractMSI=*<value>*
For ExtractMSI, use following values (*value*) as per host architecture.
For example, if you want to install cloud agent on 64-bit machine, you need to extract MSI package with value for ExtractMSI=64.
- **32**: Extracts 32-bit MSI Installer
- **64**: Extracts 64-bit MSI Installer
- **BOTH**: Extracts both (32-bit and 64-bit) the MSI Installers
- **AUTO**: Extracts the appropriate MSI based on the OS architecture. It extracts 32-bit MSI on a 32-bit machine and 64-bit MSI on a 64-bit machine

## MSI Extract

- **AUTO**: Extracts the appropriate MSI based on the OS architecture. It extracts 32-bit MSI on a 32-bit machine and 64-bit MSI on a 64-bit machine

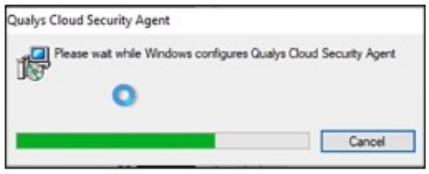
```
C:\Users\Administrator\Downloads>WindowsCloudAgent.
exe ExtractMSI=auto
```




The MSI file will be extracted in the same directory where exe file is available.

-Installing MSI Package

```
C:\Users\Administrator\Downloads>Msiexec.exe /i Clo
udAgent_x64.msi CustomerId={22d2b914-911d-432f-8010
-fa67b8421e70} ActivationId={df78bf6a-30e3-4ce2-853
0-8170d83c61b3} WebServiceUri=https://qagpublic.qg2
.apps.qualys.com/CloudAgent/
```




Qualys.

Copy the Qualys Cloud Agent installer onto the host where you want to install the agent, and run the command or use a systems management tool to install the agent as per your organization's standard process to install software. Following is the sample command for installing MSI package for 32-bit installer:
Msiexec.exe /i CloudAgent_x86.msi CustomerId={12345678-1234-1234- 1234-123456789012} ActivationId={12345678-1234-1234-1234- 123456789012}
Here CloudAgent_x86.msi is extracted MSI file for 32-bit installer.

## Pre-installation Checks

- Verify host OS is supported by Cloud Agent.
- Verify host OS patches and root certificates are up-to-date.
- Ensure you have acquired the agent installation components for the target OS:
  1. Agent Installer
  2. Installation Command
- Verify target host can access the Qualys Platform.

| Platform | Platform Identifier | Username Format | Platform URL |
|---|---|---|---|
| US1 | "_" (underscore) | quays_ab1 | https://qualysguard.qualys.com |
| US2 | "2" (the number 2) | quays2ab1 | https://qualysguard.qg2.apps.qualys.com |
| US3 | "3" (the number 3) | quays3ab1 | https://qualysguard.qg3.apps.qualys.com |
| EU1 | "-" (hyphen) | quays-ab1 | https://qualysguard.qualys.eu |
| EU2 | "5" (the number 5) or "!" (exclamation point) | quays5ab1 quays!ab1 | https://qualysguard.qg2.apps.qualys.eu |
| IN1 | "8" (the number 8) | quays8ab1 | https://qualysguard.qg1.apps.qualys.in |
| CA1 | "9" (the number 9) | quays9ab1 | https://qualysguard.qg1.apps.qualys.ca |
| AE1 | "7" (the number 7) | quays7ab1 | https://qualysguard.qg1.apps.qualys.ae |

`www.qualys.com/platform-identification/`

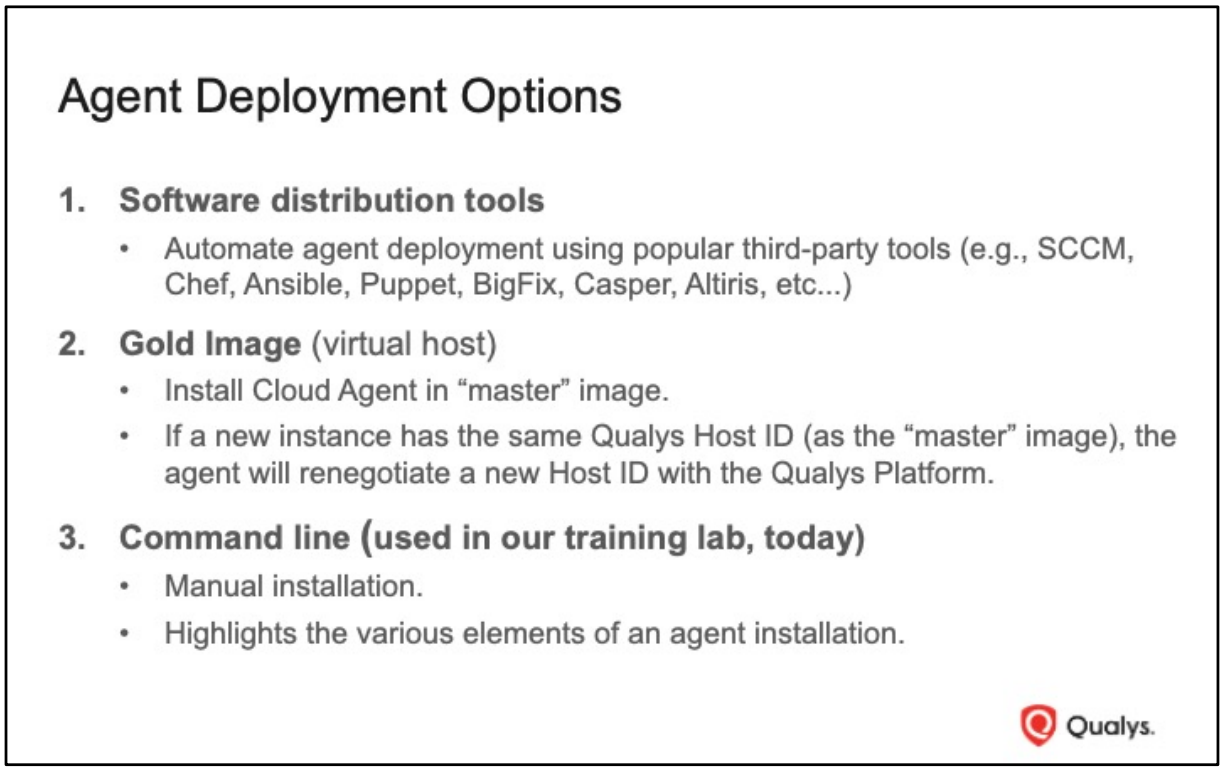
Qualys.

Before attempting to install or deploy agents, ensure the target OS is supported by Cloud Agent and that you have acquired the correct installation components.

Next, you want to verify you have connectivity between each target host and the Qualys Cloud Platform. There are test URLs for each public platform. Add these URLs to agent deployment packages (SCCM, BigFix, etc.) to test for successful connectivity, before installing the Cloud Agent.

Its a good idea to update OS patches and root certificates (on target hosts) before installing Cloud Agent.

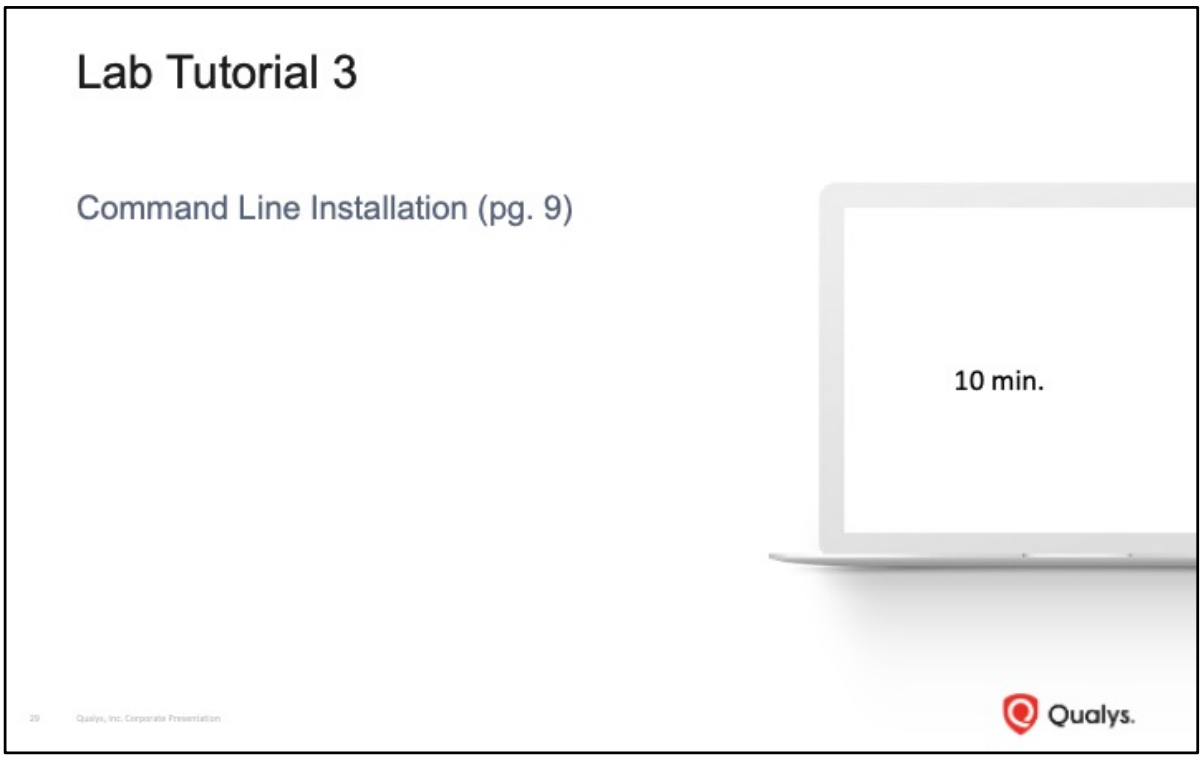
Starting with the Windows 1.6.0 agent version, the agent and installers are signed with an Extended Validation (EV) code-signing certificate. This requires the OS to validate the signed executables using certificates from the trusted root CA. You will encounter errors in the agent log file, if the appropriate root certificates are not installed.




Use third-party software management and distribution applications to perform large scale agent deployments.

You can also install the agent in a master or gold image. Each new instance created from the master image may potentially have the same Qualys Host ID as the "master" image. In this case, the agent will renegotiate its UUID with the Qualys Cloud Platform.

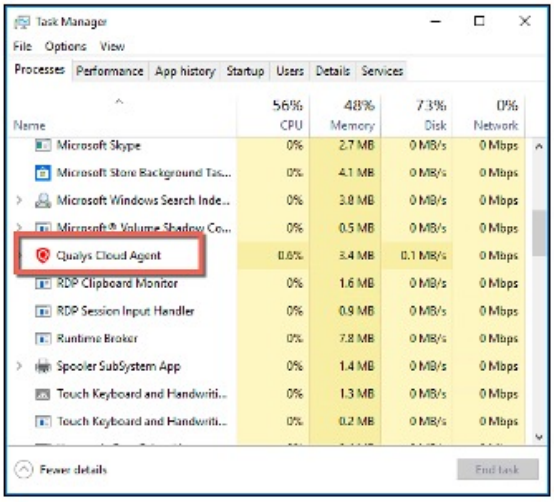
In this course you will manually install an agent from the command line. This will help to highlight the different components required for an agent installation.




1. Agent installer and installation command have been downloaded to Windows host
2. Verify the presence of the agent installer and execute the installation command
3. Open Task Manager and verify Qualys Cloud Agent process is running
4. Navigate to \ProgramData\Qualys\QualysAgent and display the contents of Log.txt

# Verify Agent Installation

## Qualys Cloud Agent Process




- Look for the Qualys Cloud Agent process in Windows Task Manager.
- List running processes on a Unix-based host:

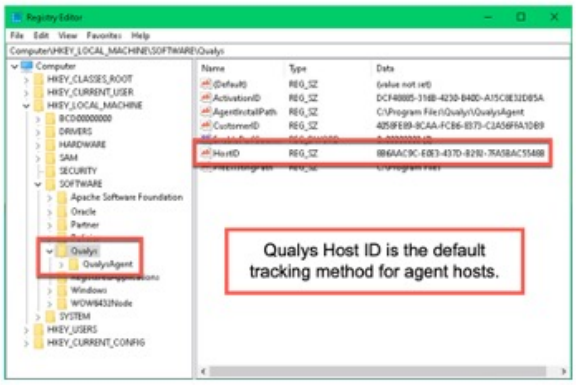
```
ps –e | grep qualys
```

Qualys.

Following a successful agent installation, the Qualys Cloud Agent process will appear in Windows Task Manager. View a list of running processes on a Unix or Linux host to view the Cloud Agent process (i.e., qualys-cloud-ag).

## Verify Agent Installation

Qualys Host ID




- Look for the Qualys Host ID in the Windows Registry:

  HKLM\SOFTWARE\Qualys

- Unix-based hosts store the Qualys Host ID in the 'hostid' file:

  `/etc/qualys/hostid`

- Provisioning tasks typically have not completed if Qualys Host ID is not present.
- **EXCEPTION**: "Gold Images" and hosts configured for Agentless Tracking may already have a Qualys Host ID.



Qualys.

The presence of a Qualys Host ID is a good indicator that the agent has successfully contacted the Qualys Cloud Platform. On Windows hosts the Host ID can be found under the Qualys registry key. On a Unix or Linux host the Host ID is stored in a plain text file (/etc/qualys/hostid).

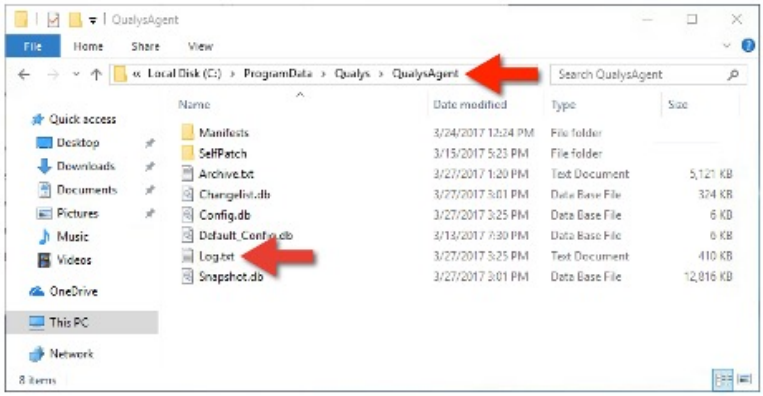
If an agent host has not acquired its Host ID, provisioning may still be in-progress or the agent was unsuccessful in contacting the Qualys Cloud Platform.

NOTE: Virtual hosts (created from a gold or master) image may potentially already have a Qualys Host ID. We'll examine a couple of solutions to this challenge, in the "Provisioning" discussion, later.

If the "Agentless Tracking" feature is enabled in Qualys VM, VMDR, or PC, a host may have already received Its Qualys Host ID, before an agent is installed. In this case, the agent will simply use the Qualys Host ID provisioned by the Agentless Tracking feature. For more information on the "Agentless Tracking" feature, please see the Qualys "Scanning Strategies & Best Practices" and "Reporting Strategies & Best Practices" training courses.

## Verify Agent Installation

Cloud Agent Log File




- **Windows**: `\ProgramData\Qualys\QualysAgent\Log.txt`
- **Unix**: `/var/log/qualys/qualys-cloud-agent.log`

Qualys.

Searching the CA log file will reveal agent connection attempts that are successful (return code 2xx) and unsuccessful (return code 4xx, 5xx). It is best to search the end of the CA log file for the most recent connections attempts.

On a Linux host search for the character string “Http request.” On a Windows host search for the character string “Http status.”

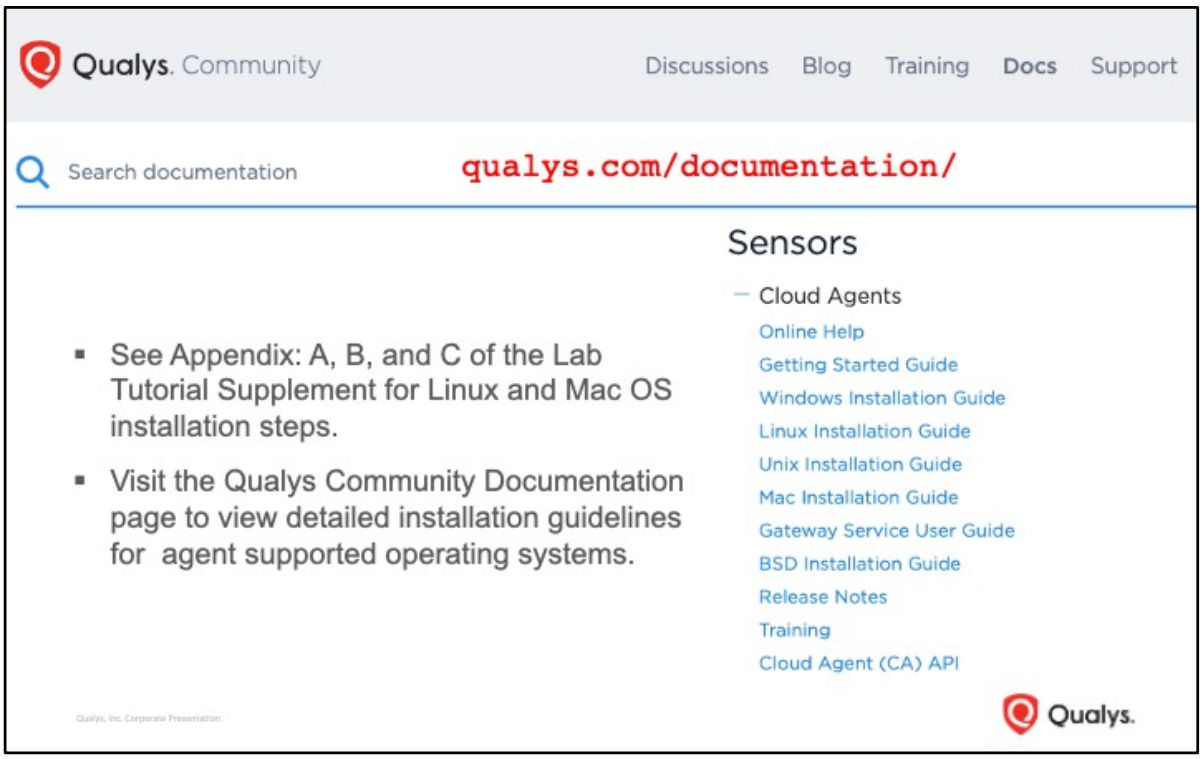
**HTTP Status Codes:**
1xx **Informational**.
**2xx Success**. ...
**3xx Redirection**. ...
4xx **Client Error**. ...
5xx **Server Error**.

Members of the Qualys Technical Support team will typically request a copy of your agent log file, when working on agent support calls:

- Unix/Linux: var/log/qualys/qualys-cloud-agent.log
- Windows: \ProgramData\Qualys\QualysAgent\Log.txt

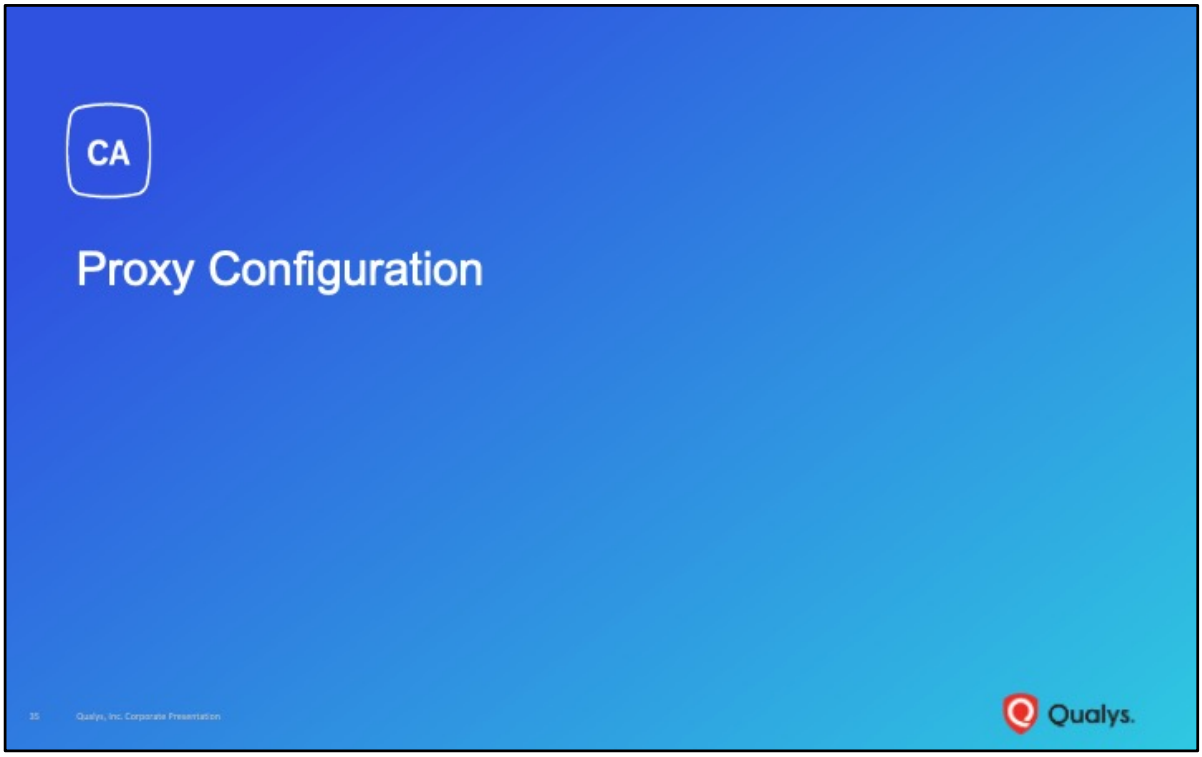
See Lab Appendix D, to learn about the information that is useful when working with the Qualys Technical Support Team.


- Introduction to Cloud Agent Log Analysis - https://vimeo.com/412764672
- Cloud Agent Troubleshooting – Common Errors - https://vimeo.com/412762742
- Cloud Agent Log Analysis – Unix/Linux Distribution - https://vimeo.com/418215691
- Common Errors and Their Solutions – Unix/Linux Distribution - https://vimeo.com/418218290




While the lab tutorials in this course illustrate a Windows agent installation, you'll find Linux and Mac OS examples in Appendix A, B, and C of the Cloud Agent Lab Tutorial Supplement.

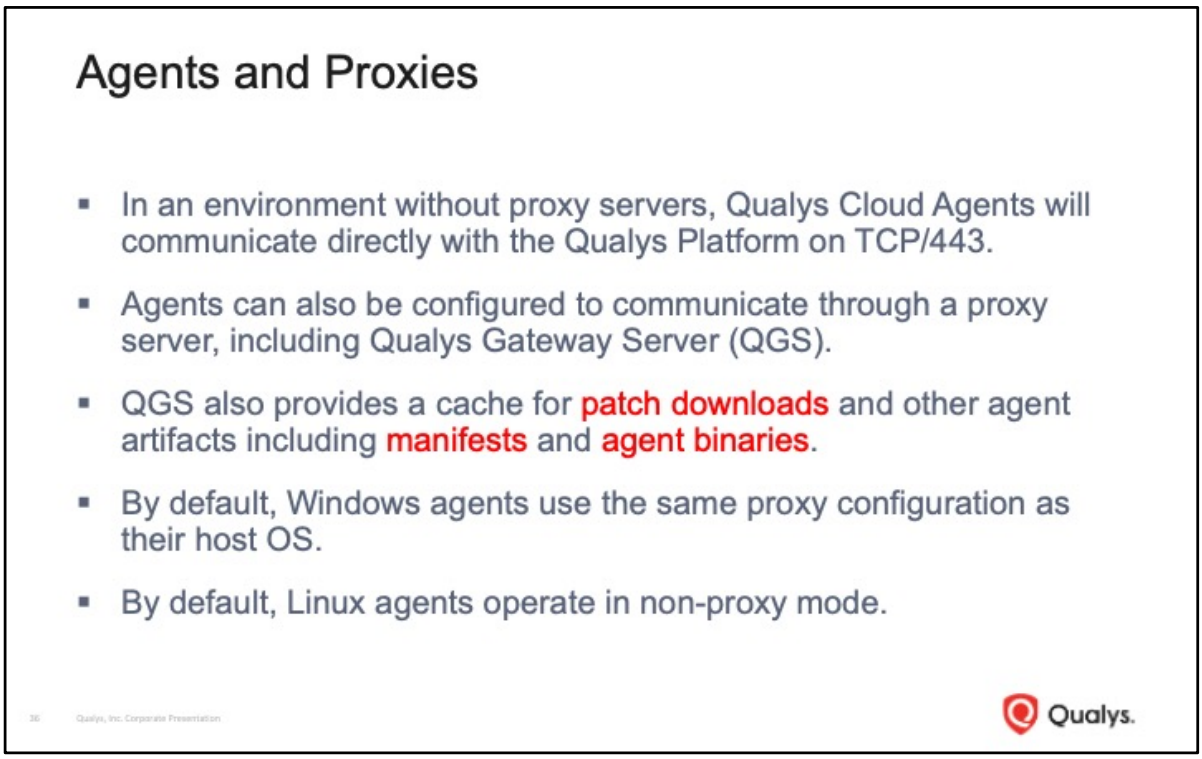
For the most current agent installation information, consult the Agent OS Installation Guides found on the Qualys Community (qualys.com/documentation).




The objectives of this section are:

1. Outline the need for proxy servers or Qualys Gateway Servers.
2. Provide a comparison of Windows and Linux proxy options.

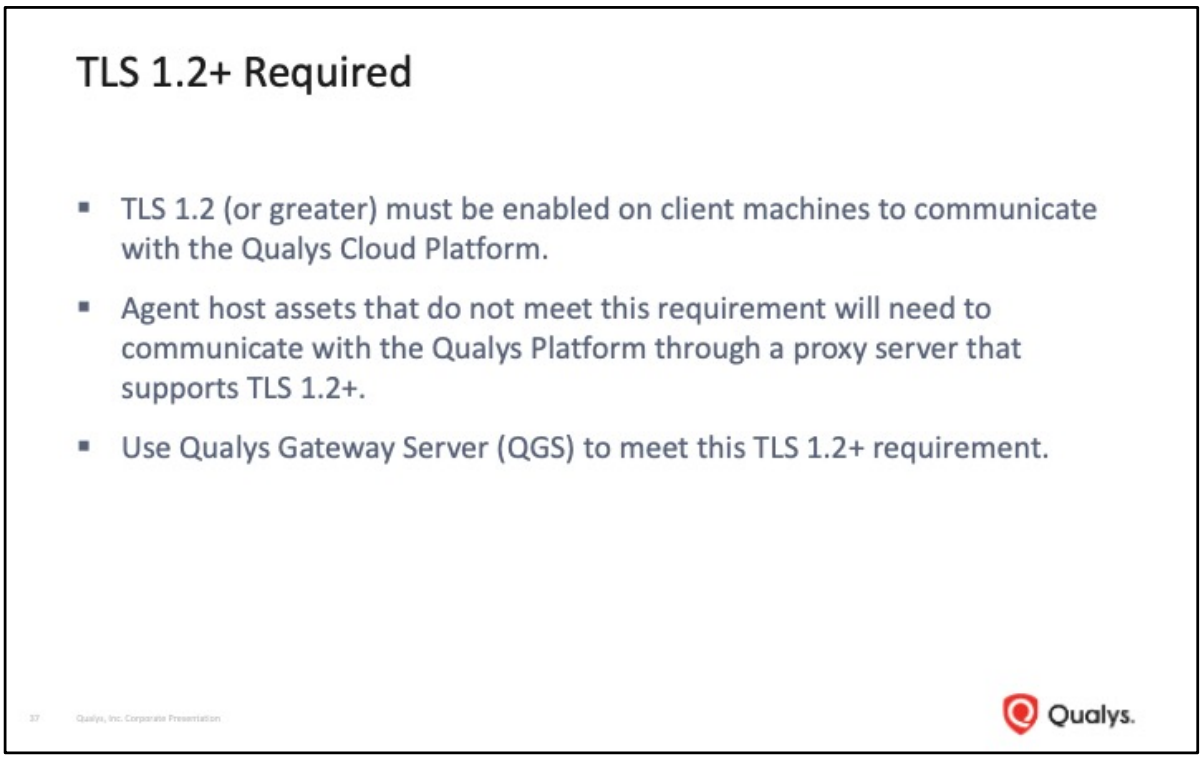
See “Proxy Configuration” in the lab tutorial supplement for this course for more proxy configuration details.




In an environment without proxy servers, Qualys Cloud Agents will communicate 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 cache for patch downloads and other agent artifacts including manifests and agent binaries.

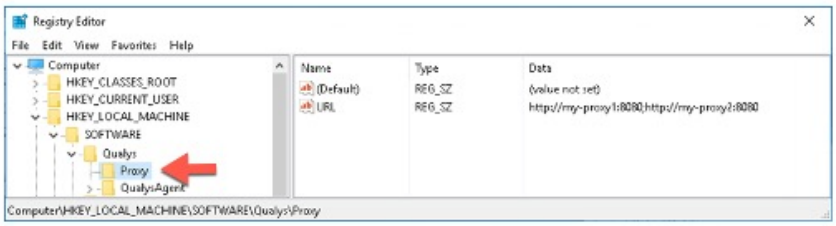



TLS 1.2 (or greater) is a host requirement, for communicating with the Qualys Cloud Platform.

Any agent host that does not meet this requirement (e.g., Windows XP and Windows Server 2003) will need to communicate with the Qualys Platform through a proxy server that supports TLS 1.2+. Qualys Gateway Server meets this requirement.

## Proxy Configuration

- Windows agent proxy settings are stored under the Qualys registry key (`HKLM\SOFTWARE\Qualys\Proxy`).




- Linux agents can be configured to use an HTTPS proxy, using the following configuration files:
  1. `/etc/sysconfig/qualys-cloud-agent (.rpm)`
  2. `/etc/default/qualys-cloud-agent (.deb)`
  3. `/etc/environment (.rpm and .deb)`

Qualys.

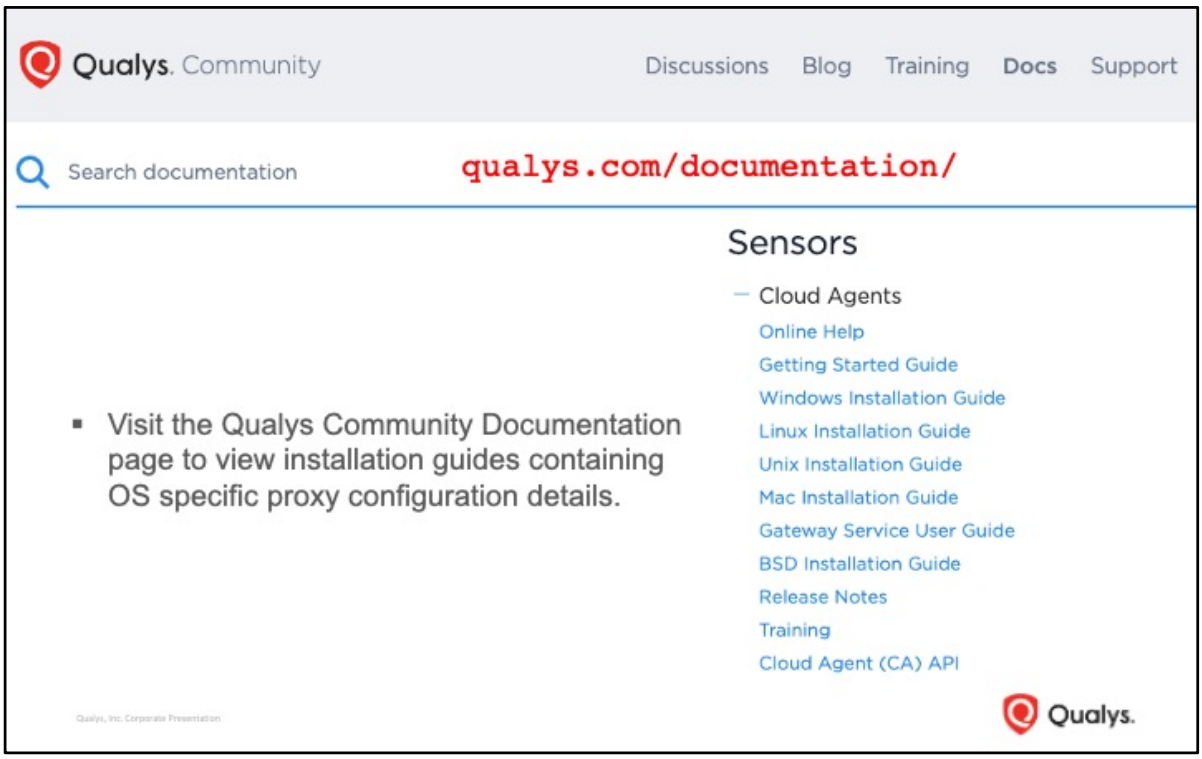
Windows agent proxy configuration can be accomplished by creating and editing the Qualys Proxy registry key (HKLM\SOFTWARE\Qualys\Proxy). The Qualys Proxy utility (QualysProxy.exe) will automatically create this key, if it is not already present.

Any application that can access the Remote Registry Service (including GPMC, Group Policy, WMI, etc...) can create or modify agent proxy configuration settings.

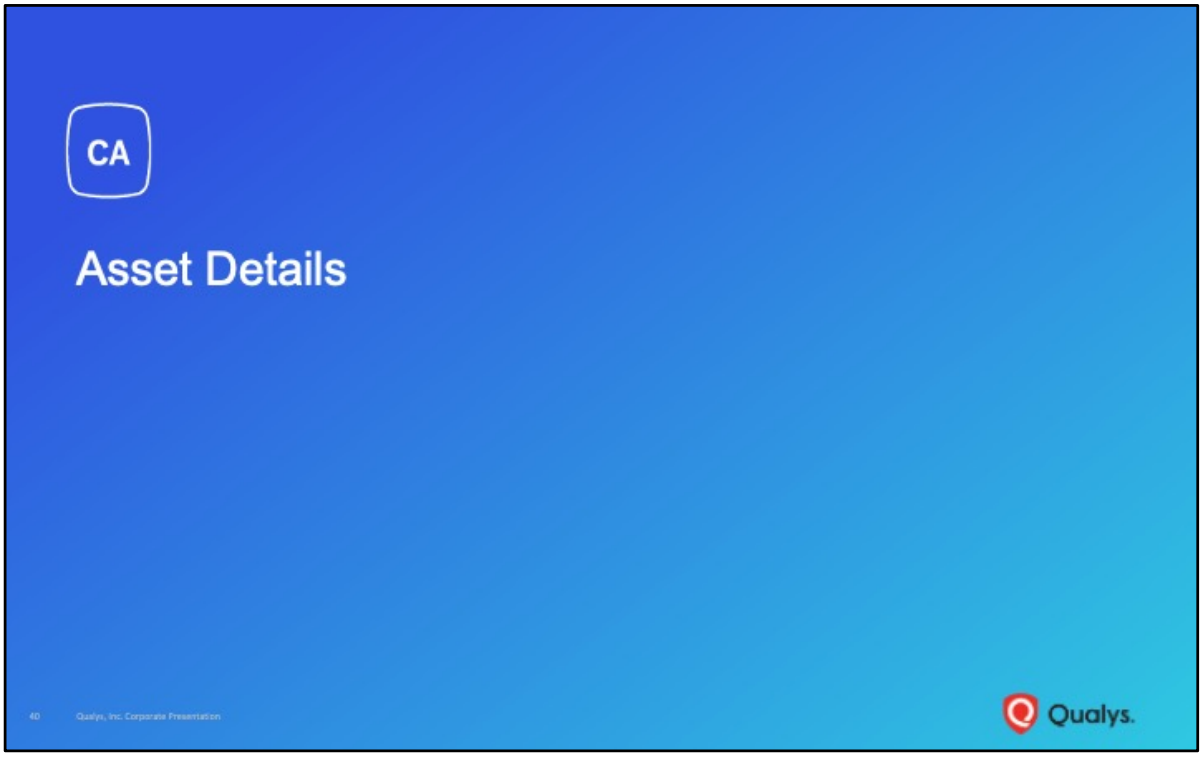
By default, Linux agents operate in non-proxy mode. Agents can be configured for proxy communications using the 'qualys-cloud-agent' proxy configuration file:

- `/etc/sysconfig/qualys-cloud-agent (.rpm)`
- `/etc/default/qualys-cloud-agent (.deb)`

If this file does not already exist, you must create it. `Both .rpm and .deb environments support file /etc/environment.`

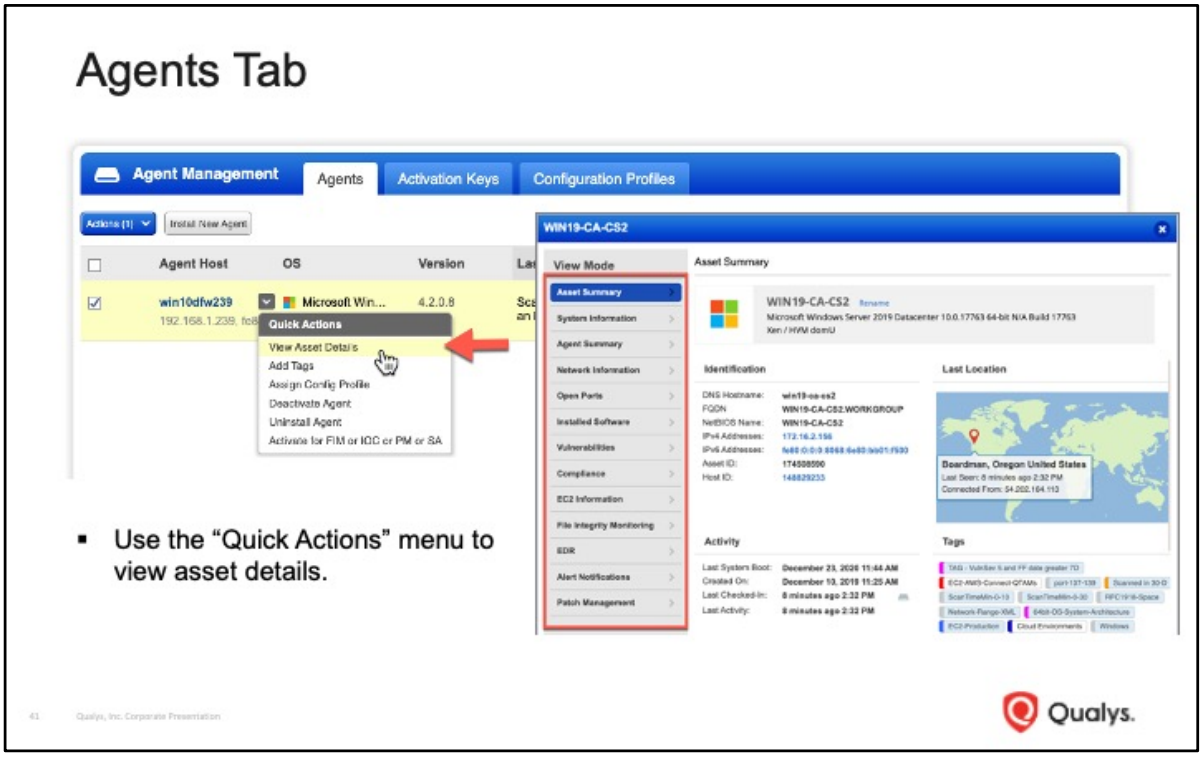



For the most current agent installation information, consult the Agent OS Installation Guides found on the Qualys Community (qualys.com/documentation).




The objectives for this section are:

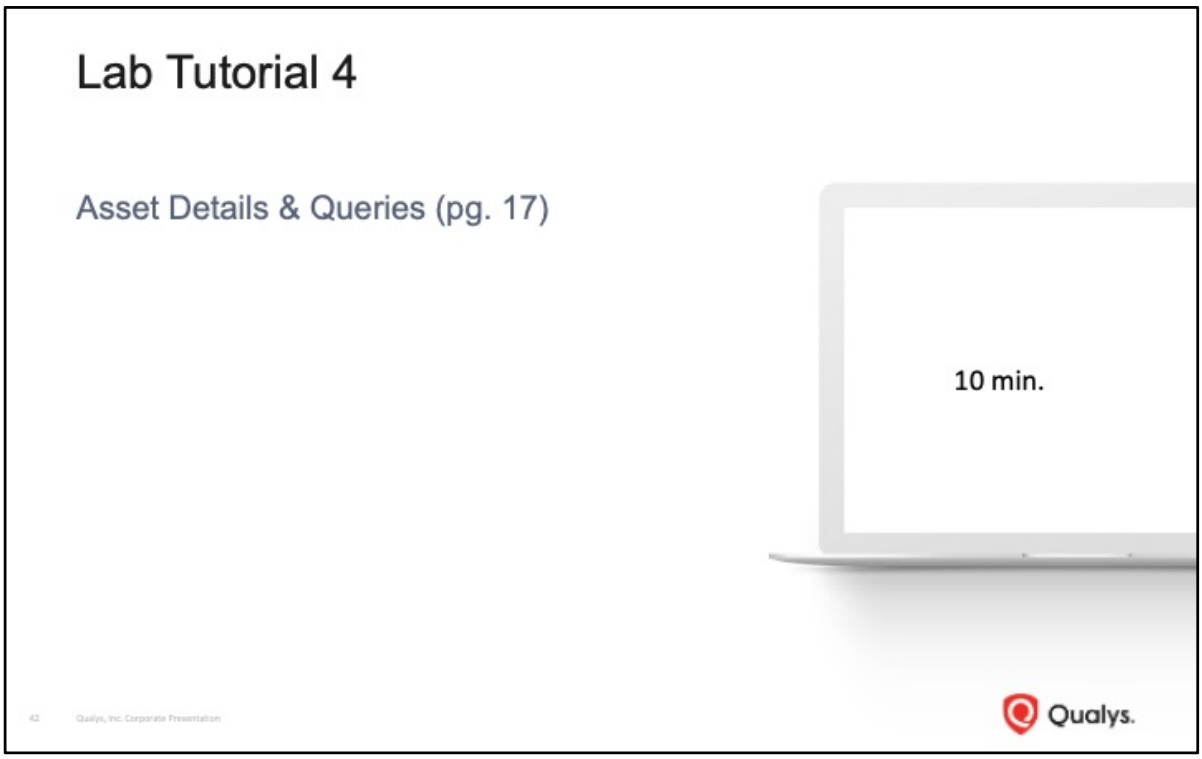
1. Identify the agent asset details provided by the Cloud Agent application and other Qualys applications.
2. Learn to use the Qualys Query Language (QQL) and Query Tokens, to search for agent assets.



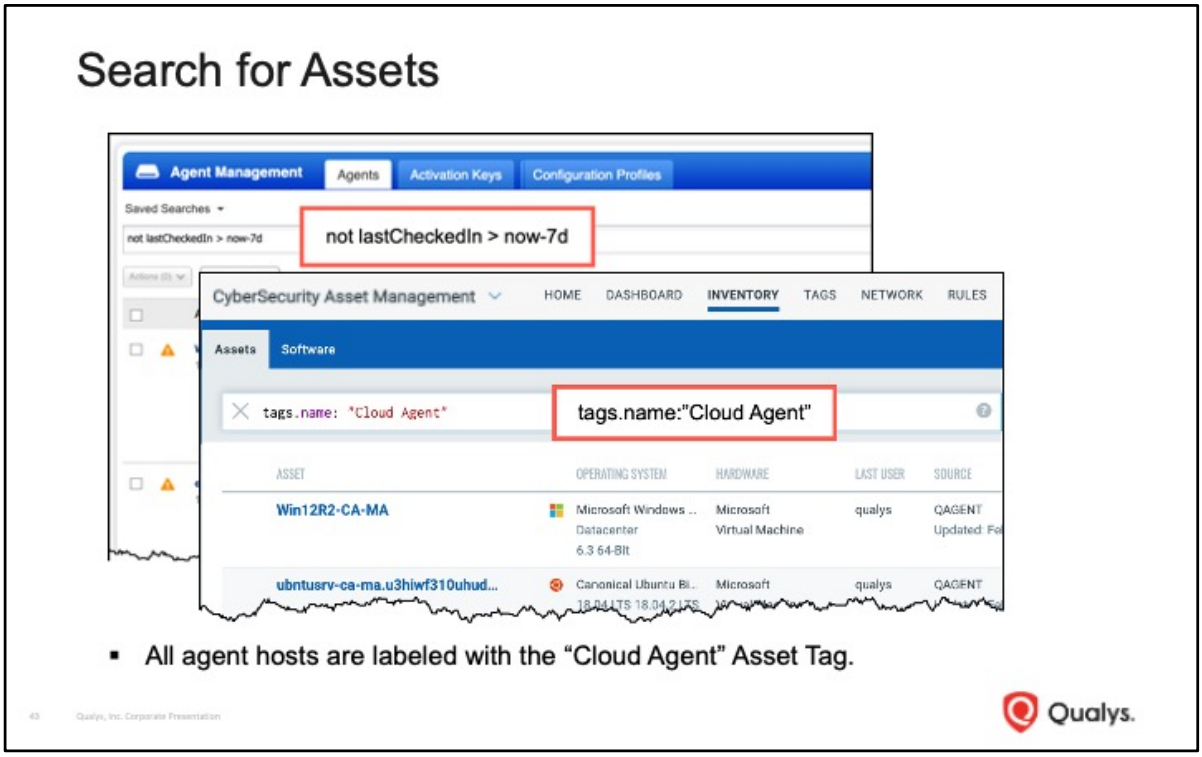

Use the "Quick Actions" menu for any agent host listed in the Cloud Agent application, to view specific asset details.

The Asset Summary displays host OS details, geolocation information, names and addresses, activity updates, and Asset Tags.

The very next lab tutorial provides a quick tour of the various asset detail components.



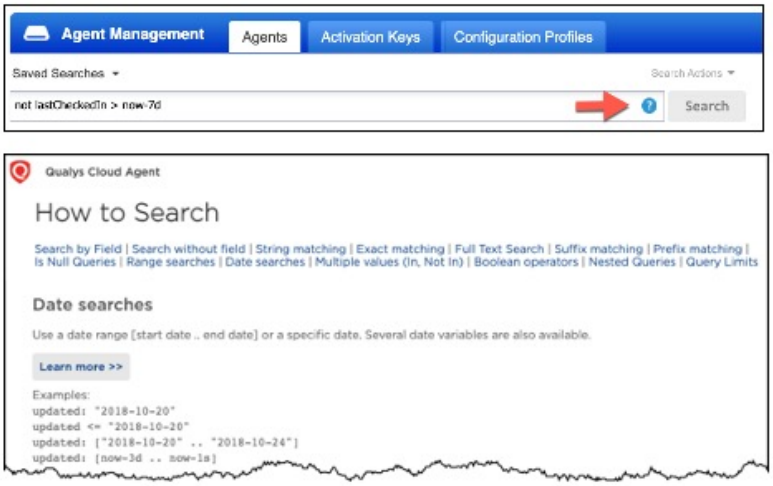

1. View asset details for host with all agent modules activated
2. Display all ”View Mode” options including GCP Instance Information
3. Use lastCheckedIn query token find agent host that have not checked-in for seven days
4. Download the result set into a spreadsheet (.csv) file.




One of the more useful queries (when searching for agent hosts) uses the "lastcheckedIn" query token, which can help you to identify agents that are failing to communicate with the Qualys Platform. For example, if someone manually uninstalls an agent from its host (without using the Qualys UI or API), a stale host record will remain in your account, until you remove it. Use the "lastCheckedIn" token to help you find stale agent hosts, using a timeframe of your choice.

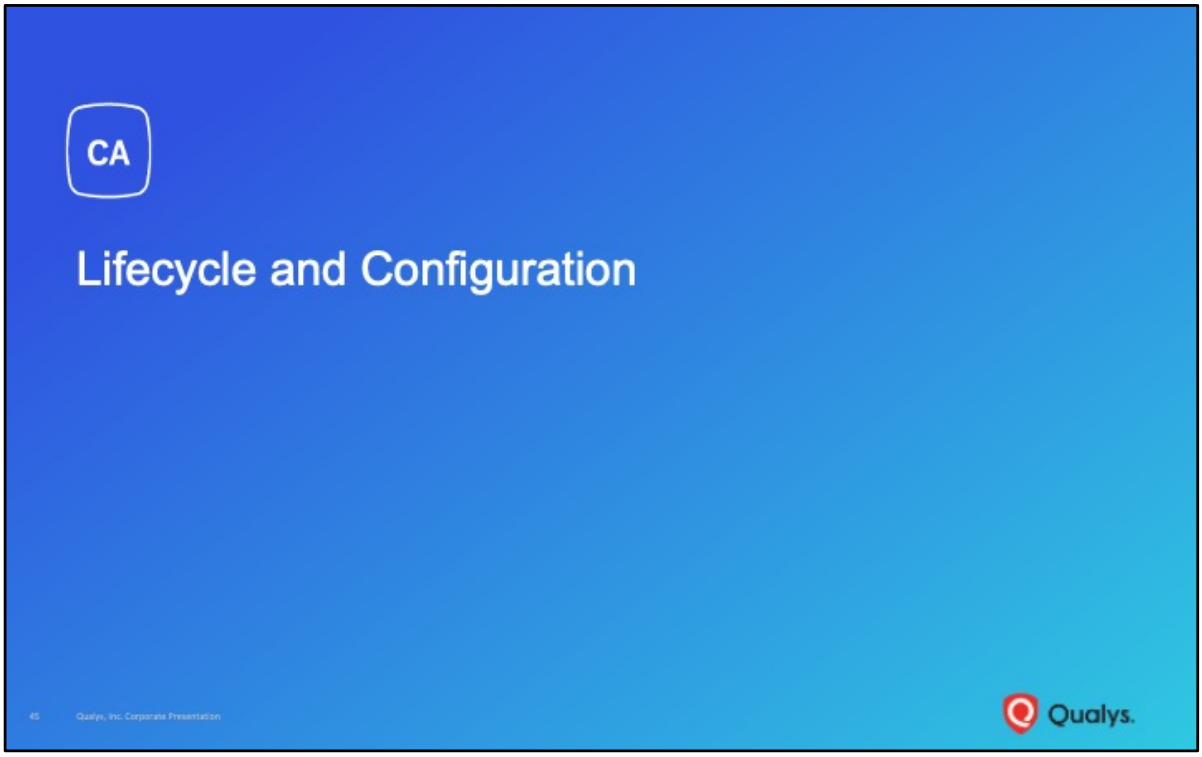
All agent host assets are labeled with the "Cloud Agent" tag. Using the "tags.name" token (with a value of "Cloud Agent") will help you to find agent host assets from the search field of any Qualys application.

# How To Search




- Click the “Help” icon inside the “Search” field for more information on building queries and using the Qualys Query Language (QQL).

Information and examples for using Qualys Query Language (QQL) to build effective queries can be found by clicking the “Help” icon, inside the “Search” field.




The objectives of this section are:

1. Identify and define the Cloud Agent lifecycle of events, including:
    - Agent Provisioning
    - Download Agent Configuration Profile
    - Agent Upgrades
    - Agent Status Interval
    - Agent Data Collection
    - Download Application Manifests
    - Agent – Platform Synchronization
    - Activate, Deactivate, Uninstall Agents
2. Learn to build and configure a CA Configuration Profile.
3. Understand the different agent data collection methods.


Throughout its life, an agent will go through a series of events or workflow. Agent provisioning was demonstrated in the first part of this course.

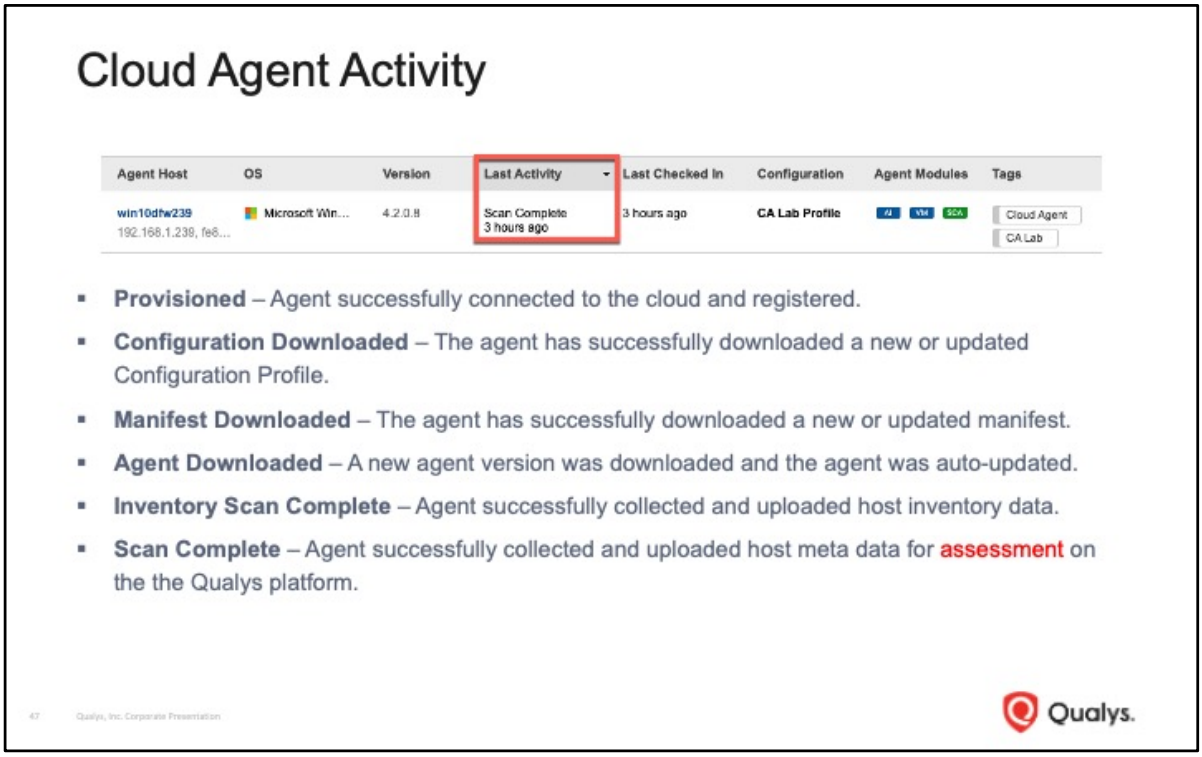
When provisioning is successful an agent will download its configuration profile. A configuration profile specifies various agent behaviors and characteristics. Other lifecycle events are controlled by settings in the downloaded configuration profile, including: 1) Agent Status Interval, 2) Agent Version Upgrades, and 3) Data Collection Methods.

A manifest is downloaded for each activated agent application module. Data collection will begin immediately, following the download of a new or updated application manifest.

Once an agent has successfully transferred its first data “snapshot” to the Qualys Platform, it will regularly perform synchronization checks, to ensure data on both sides is accurate and consistent.

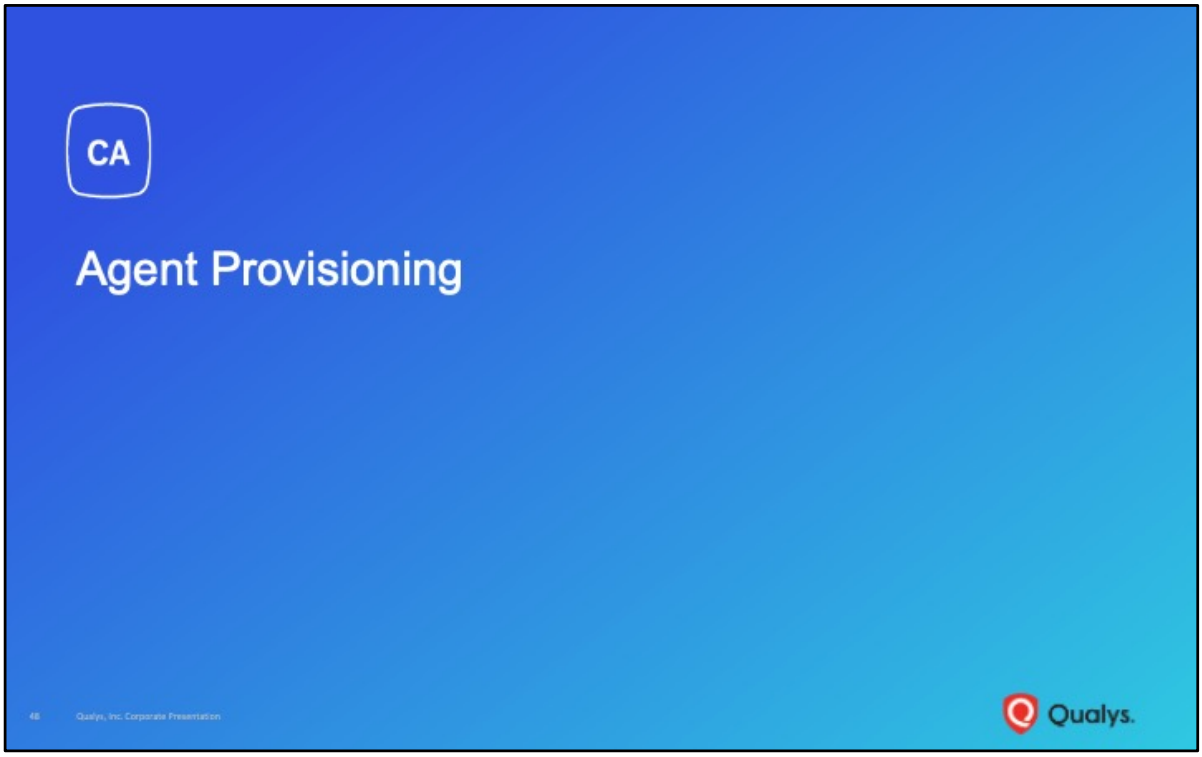
Application modules can be activated or deactivated for individual or entire groups of agents.

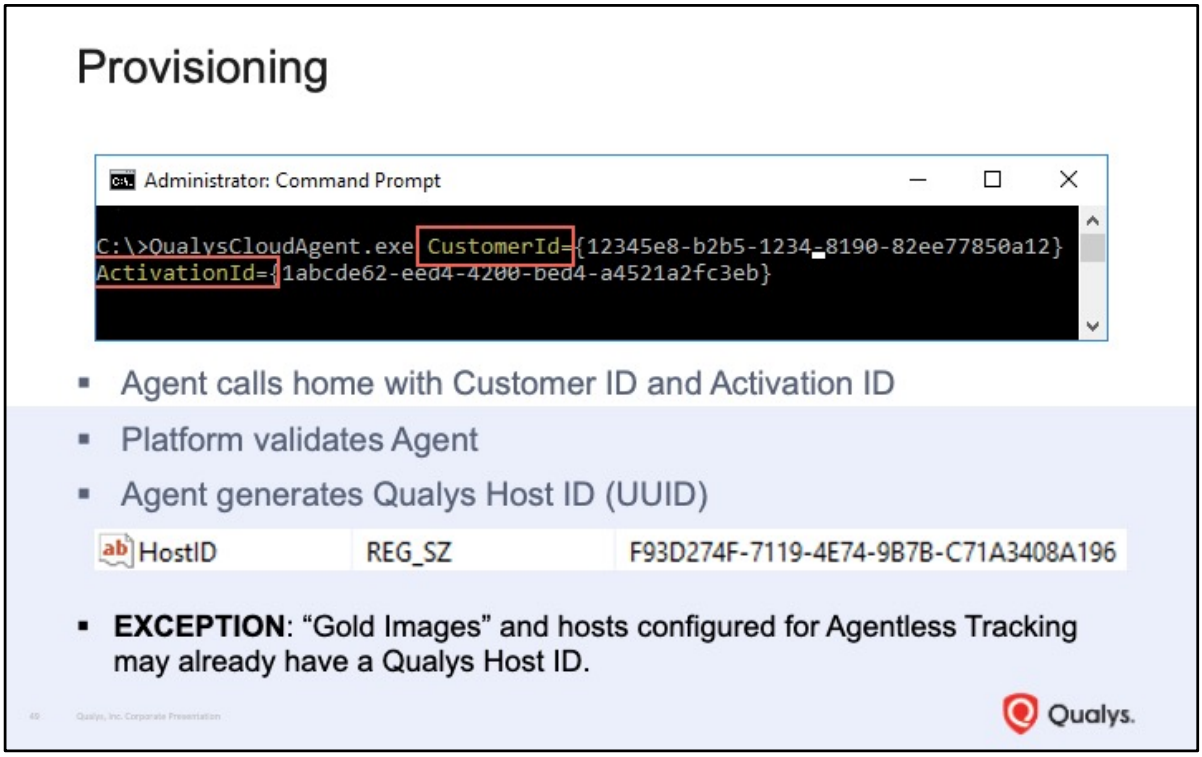
Uninstalling an agent will free its license for use elsewhere.




As agents complete various lifecycle events, an event message is displayed in the host's "Last Activity" column.

To view a comprehensive list of events for any agent host, refer to the agent log file.

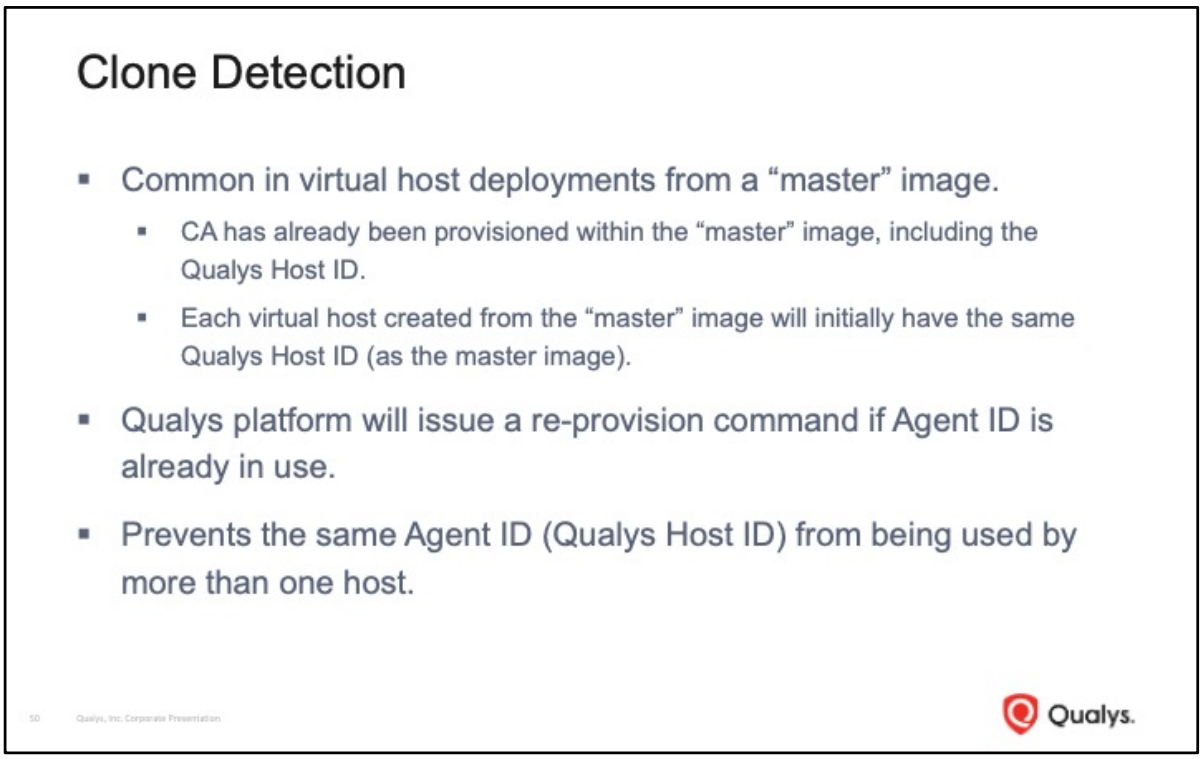

CA
Agent Provisioning
48
Qualys, Inc. Corporate Presentation
Qualys.




Provisioning is the first request an agent performs, following a successful installation. The provisioning step requires a valid Customer ID and Activation ID to be successful. When verified, the agent generates its Qualys Host ID (UUID) and submits it to the platform.

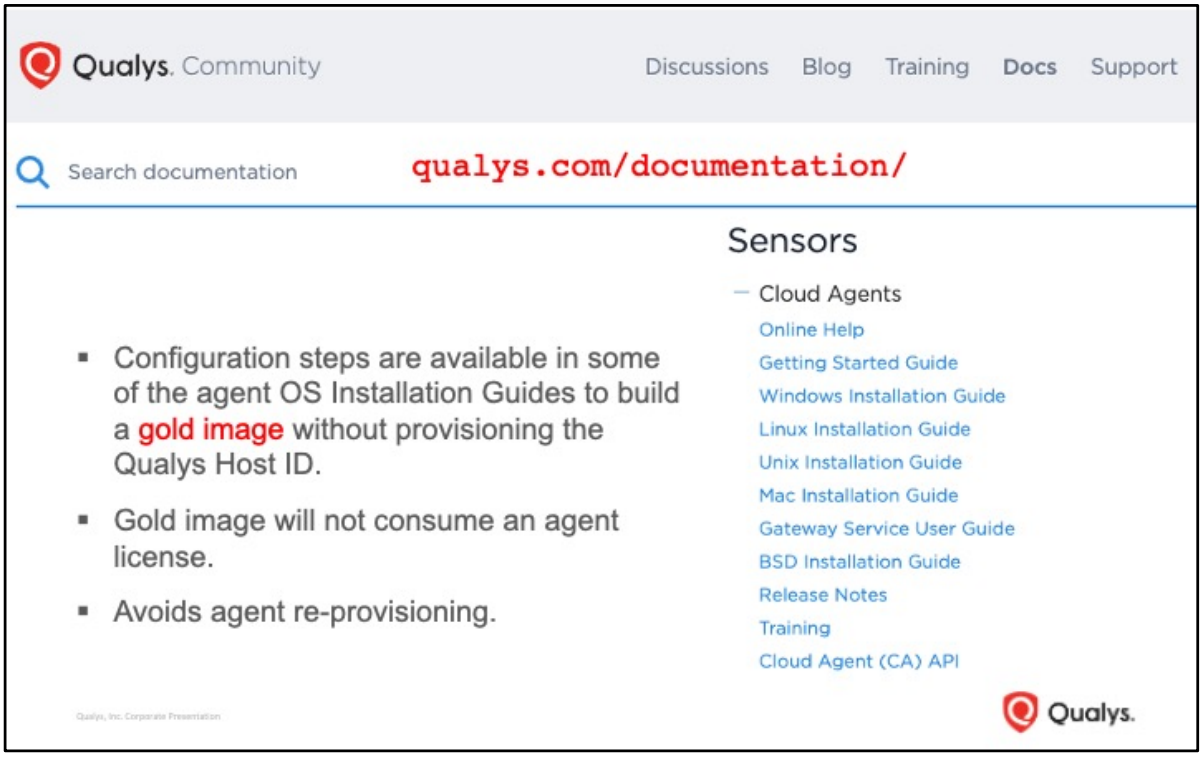
At the completion of provisioning, the agent does not perform any subsequent provisioning methods except in the case of duplicate agent UUIDs. Agents that cannot communicate to the platform for provisioning will keep retrying with an exponential backoff algorithm (current interval * 1.5 = next interval). The initial current interval is 60 seconds.

If the "Agentless Tracking" feature is enabled in Qualys VM, VMDR, or PC, a host may have already received Its Qualys Host ID, before an agent is installed. In this case, the agent will simply use the Qualys Host ID provisioned by the Agentless Tracking feature. For more information on the "Agentless Tracking" feature, please see the Qualys "Scanning Strategies & Best Practices" and "Reporting Strategies & Best Practices" training courses.

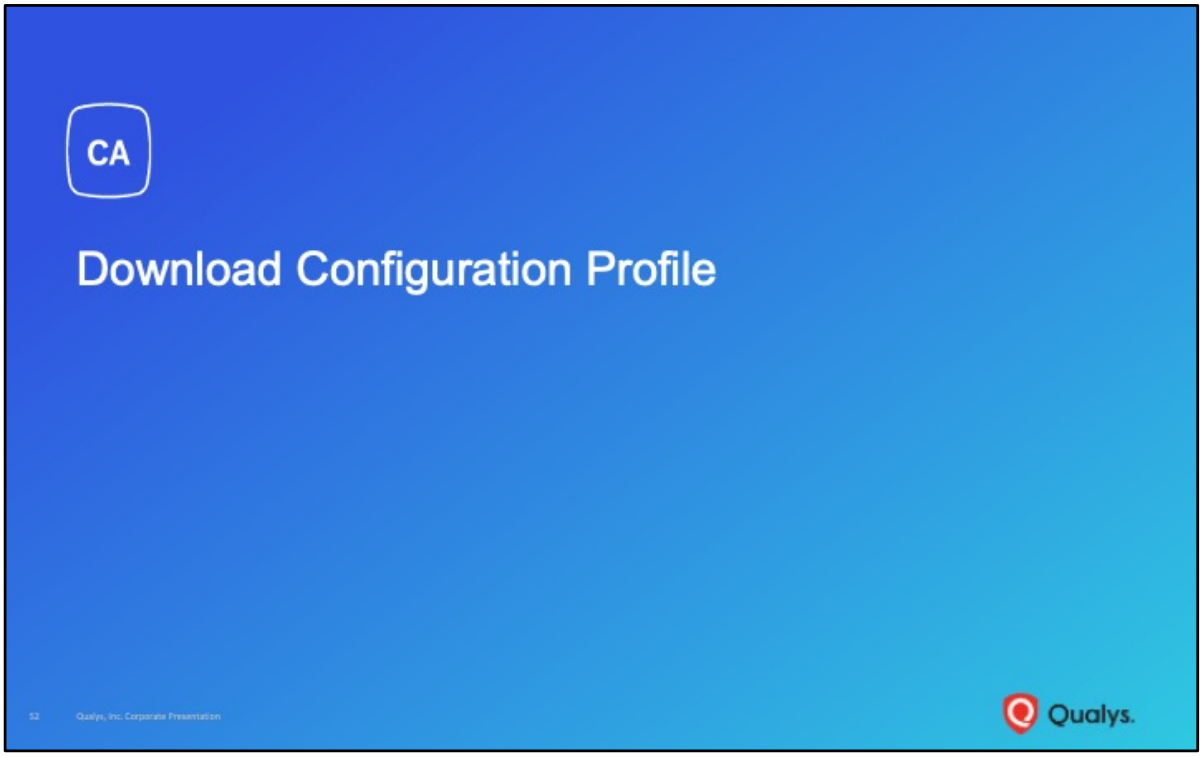


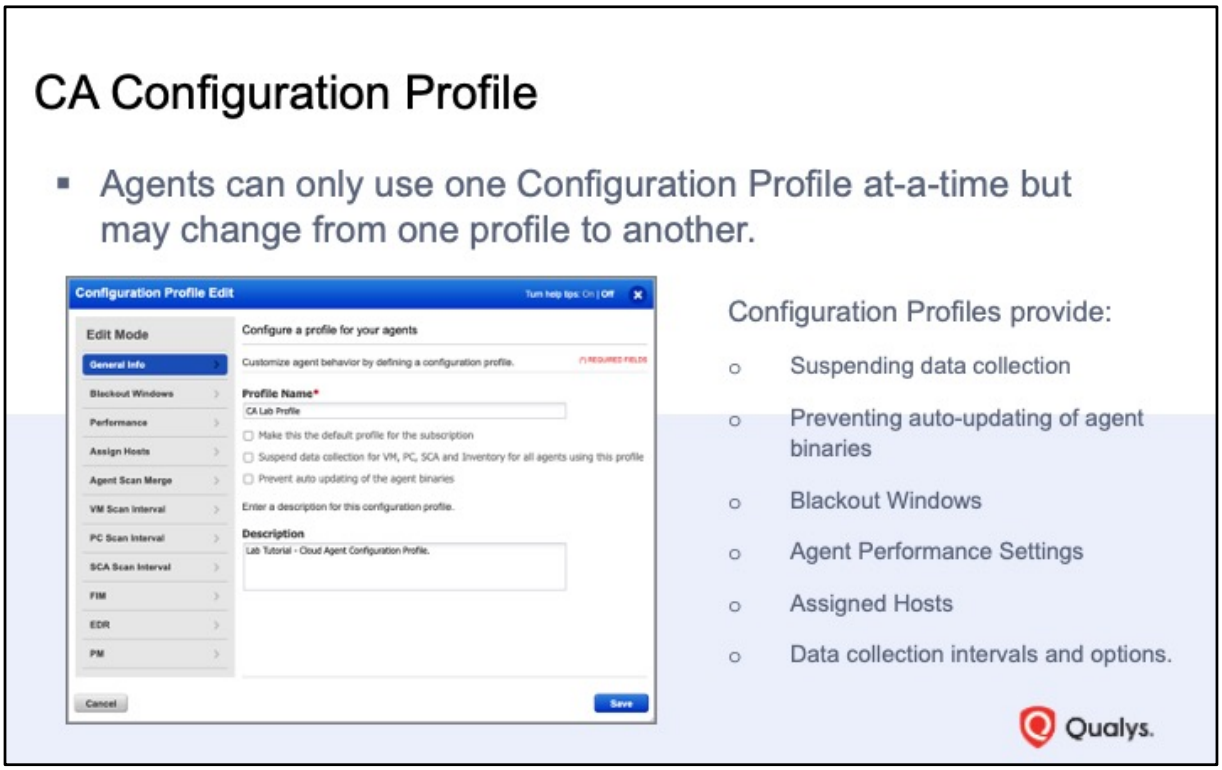

The platform has a feature to detect duplicate agent IDs and trigger the agent to reprovision with a newly generated agent ID. This feature is always enabled and not exposed as a configurable setting.

The most common case where duplicate agent IDs are created is when an agent is provisioned in a gold image that is used to create clones. In this case, cloned agents will have the same UUID as the agent in the gold image thus creating duplicate agent IDs in the platform when the cloned agents connect.




When building a master image, avoid renegotiation by deploying agent on host that is disconnected from the network (i.e, prevent the agent from provisioning).

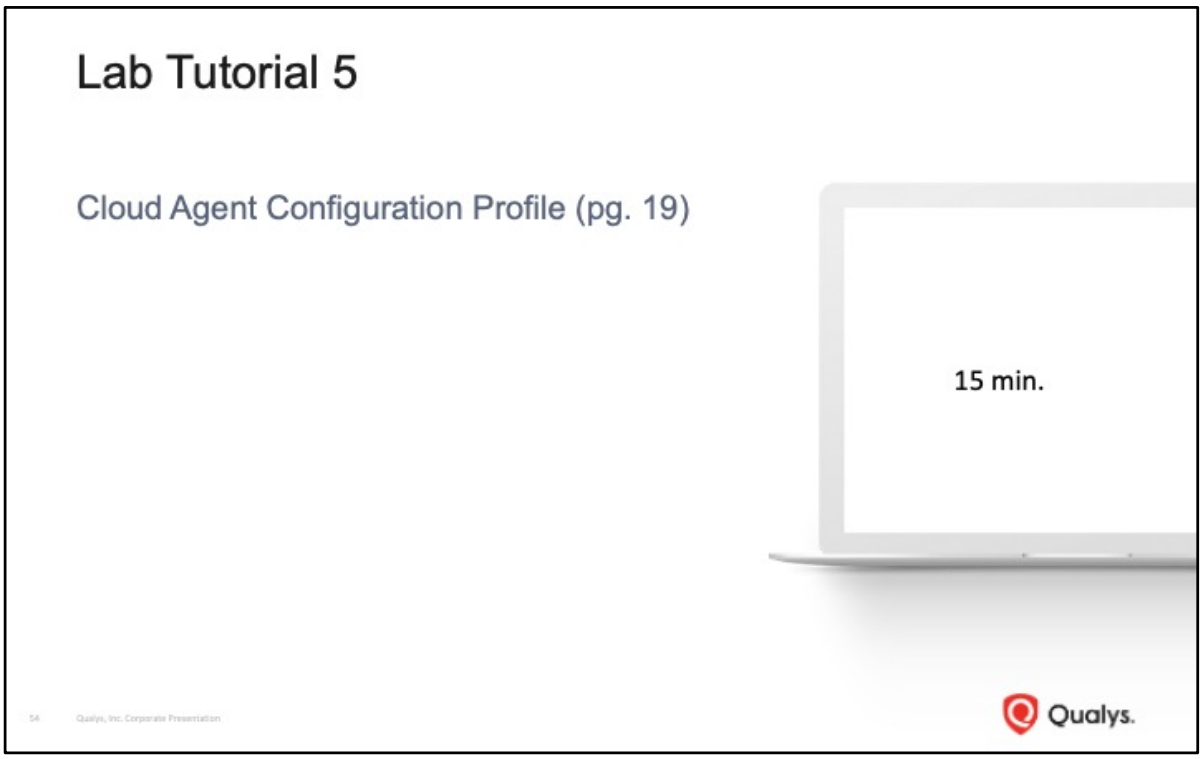

CA
Download Configuration Profile
52
Qualys, Inc. Corporate Presentation
Qualys.




Agents can only use one Configuration Profile at-a-time but may change from one profile to another.

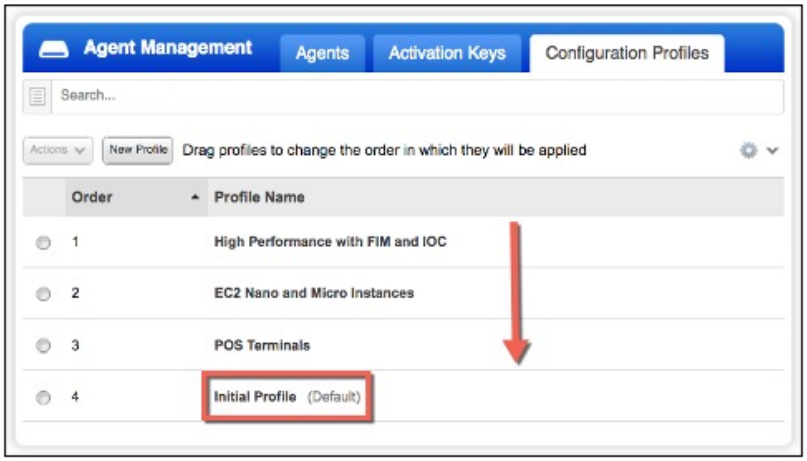
Each Configuration Profile contains settings for:

- Suspending data collection
- Preventing auto-updating of agent binaries
- Blackout Windows
- Agent Performance
- Assigned Hosts
- Agent Scan Interval
- Data collection options




1. Create the CA Lab Configuration Profile
2. Complete all Configuration Profile Creation steps:
    - Define General Info settings
    - Define Blackout Windows
    - Customize agent performance and select the LOW presets
    - Define Agent Status Interval
    - Define Delta Upload Interval and Chunk sizes for file fragment uploads
    - Define Logging Level
    - Define CPU Limit and CPU Throttle
    - Add “CA Lab” tag to Assigned Hosts
    - Briefly define Agent Scan Merge. The lab tutorial supplement provides more details on agent scan merge (pages 23 – 25)
    - Define VM, PC, SCA scan intervals
    - FIM and EDR are defined but not enabled
    - PM is enabled by default
3. Explain Configuration Profile precedence

## Configuration Profile Precedence

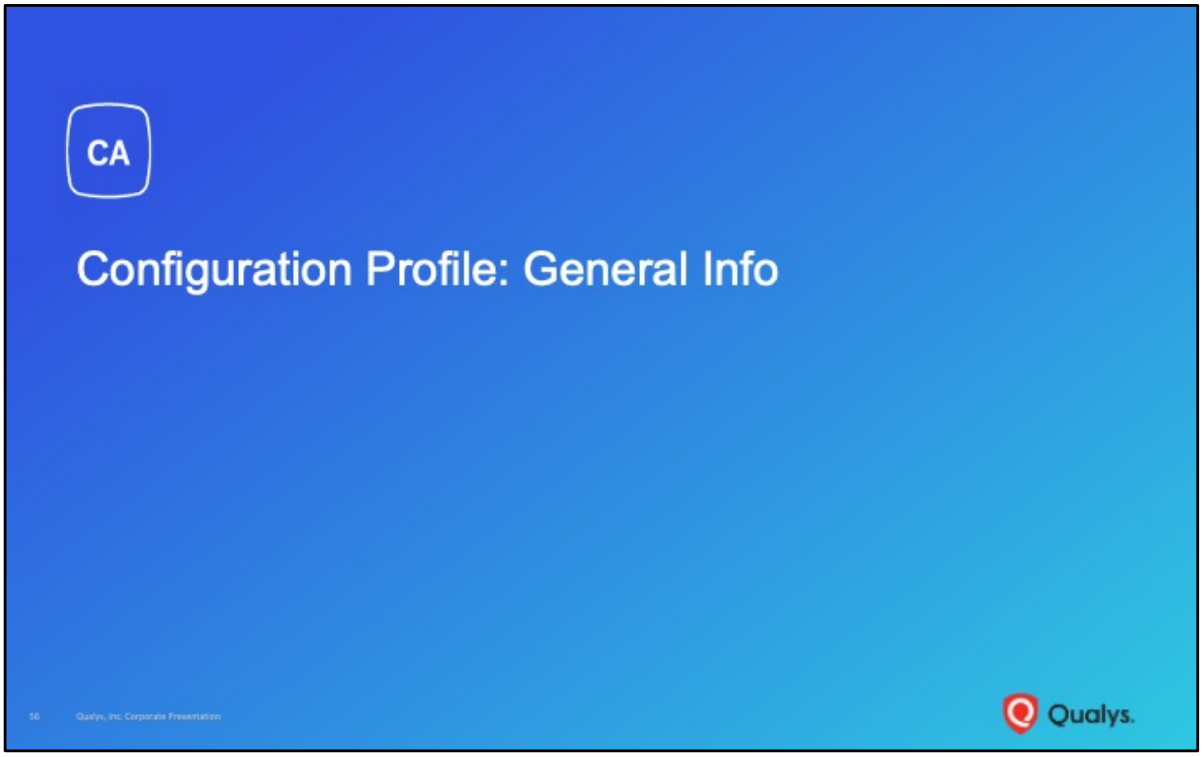



- The "Default" profile will be used for any agent host not assigned to a Configuration Profile.
- If an agent host is assigned to more than one profile, the profile closest to the top of the list will take precedence (top-down).

Qualys.

You can create multiple Configuration Profiles for your needs. There is a precedence that occurs. If an agent is assigned to more than one profile; the highest priority profile will be assigned to the host.

A Default profile also exist for hosts that do not have one assigned explicitly.


CA
Configuration Profile: General Info
56
Qualys, Inc. Corporate Presentation
Qualys.

## Suspend Data Collection


- Although not commonly used, selecting this option will stop agents from performing VM, PC, SCA, and Inventory scans.
- Agents will continue to get manifest updates, configuration updates, and even agent version updates.



Qualys.

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.

## Cloud Agent Upgrades

- By default, Cloud Agents will automatically upgrade to the latest version
- ~80% of all agents have the auto-upgrade option enabled.

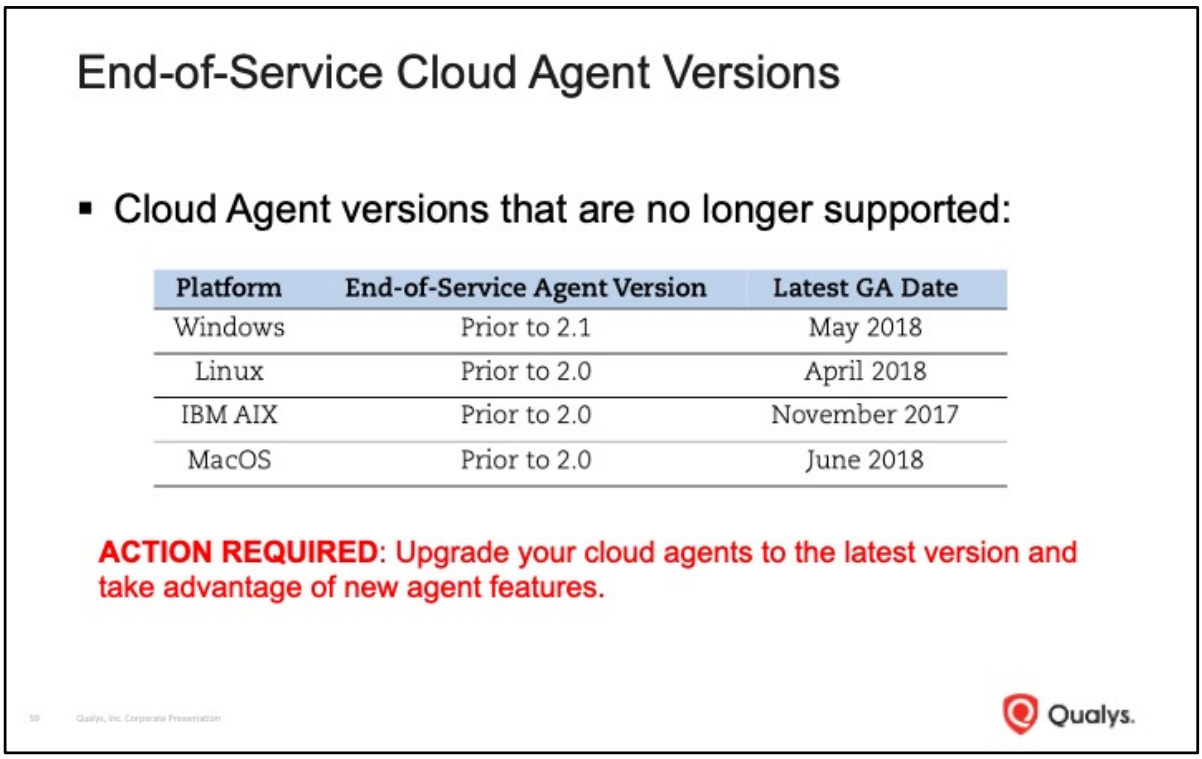

- To certify and upgrade agents via a third-party software manager, click the "Prevent auto updating of the agent binaries" check box.



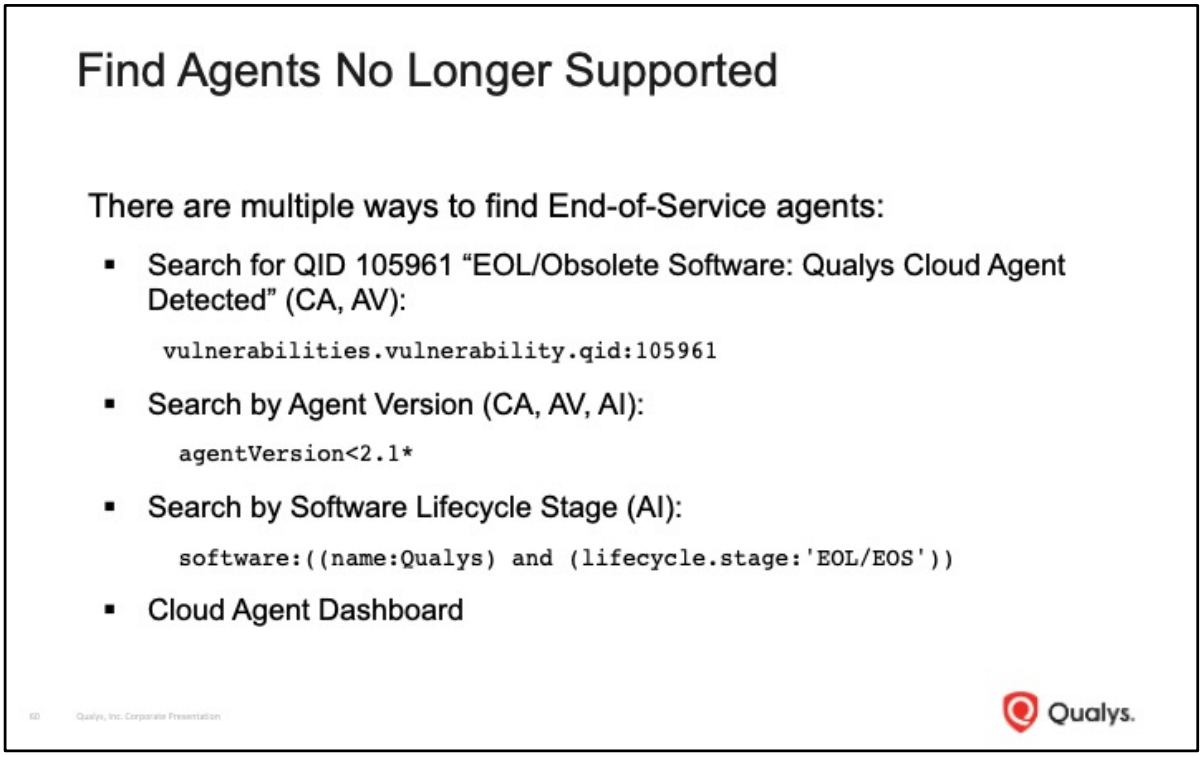
Qualys.

By default, agents will automatically upgrade to the latest agent version. It is very common to find agents configured in the “auto-upgrade” mode.

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. This feature supports an organization’s change management policies, allowing for testing and certifying new agent versions before they they are released into production environments.




Some older version of Cloud Agent have reach end-of-support and should be upgraded to the latest version to take full advantage of new features and benefits.




Here are a few ways to find end-of-service agents:

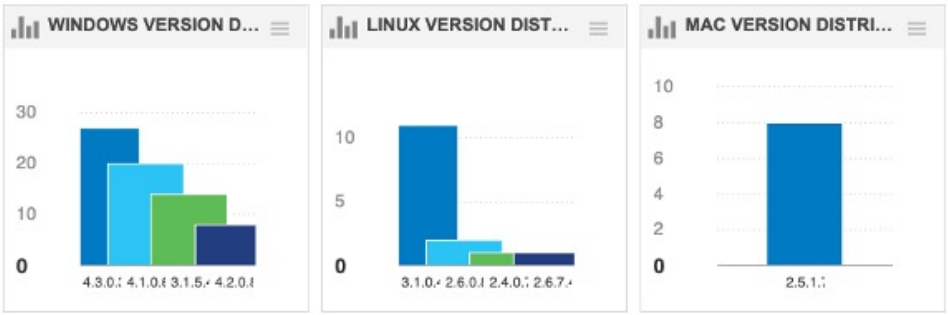
Search for QID 105961 "EOLObsolete Software: Qualys Cloud Agent Detected." The "`vulnerabilities.vulnerability.qid:" token`, is presently supported in the Cloud Agent and AssetView applications.

Seach for EOS agent versions. The "agentVersion:" token is supported in CA, AV, and AI.

Seach for 'EOL/EOS' software lifecycle stage. The "software:(name:)" and "software:(lifecycle.stage:)" tokens are supported in the Asset Inventory application.

Use the "Agent Version Distribution" widgets in the CA Dashboard.

# Cloud Agent Dashboard

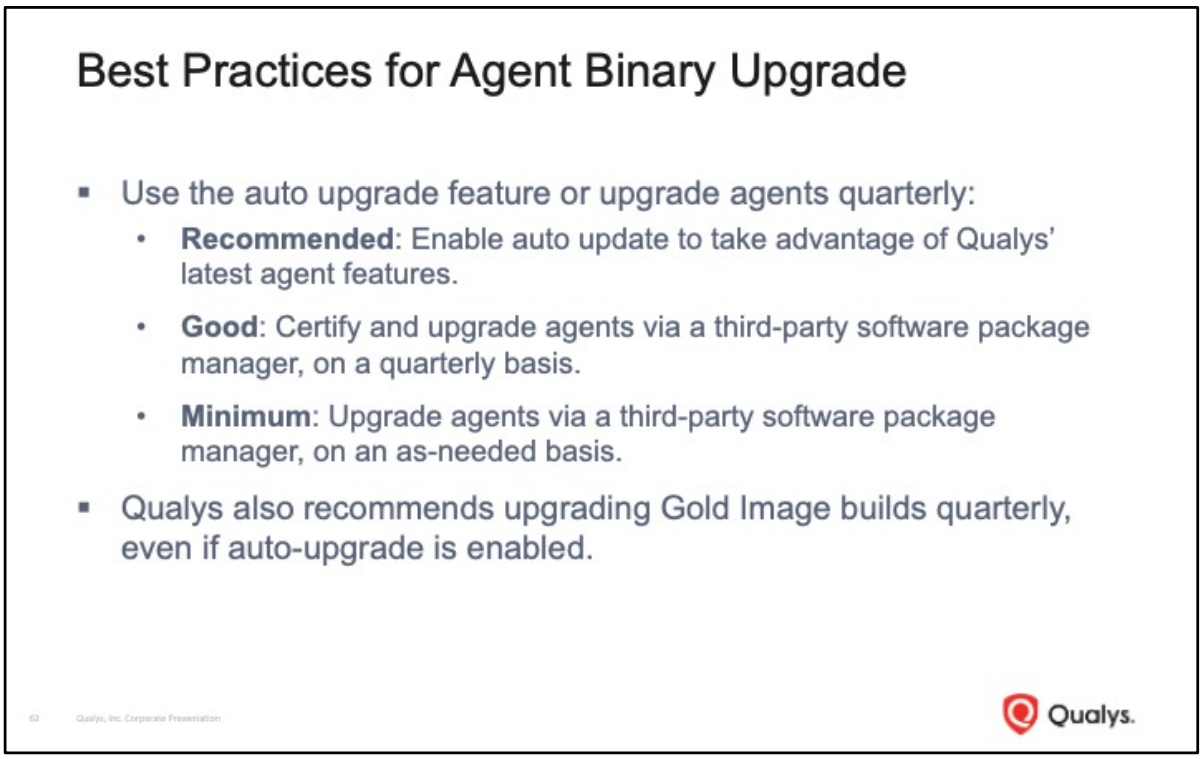



- Click on any version distribution to display its agent hosts.



Qualys.

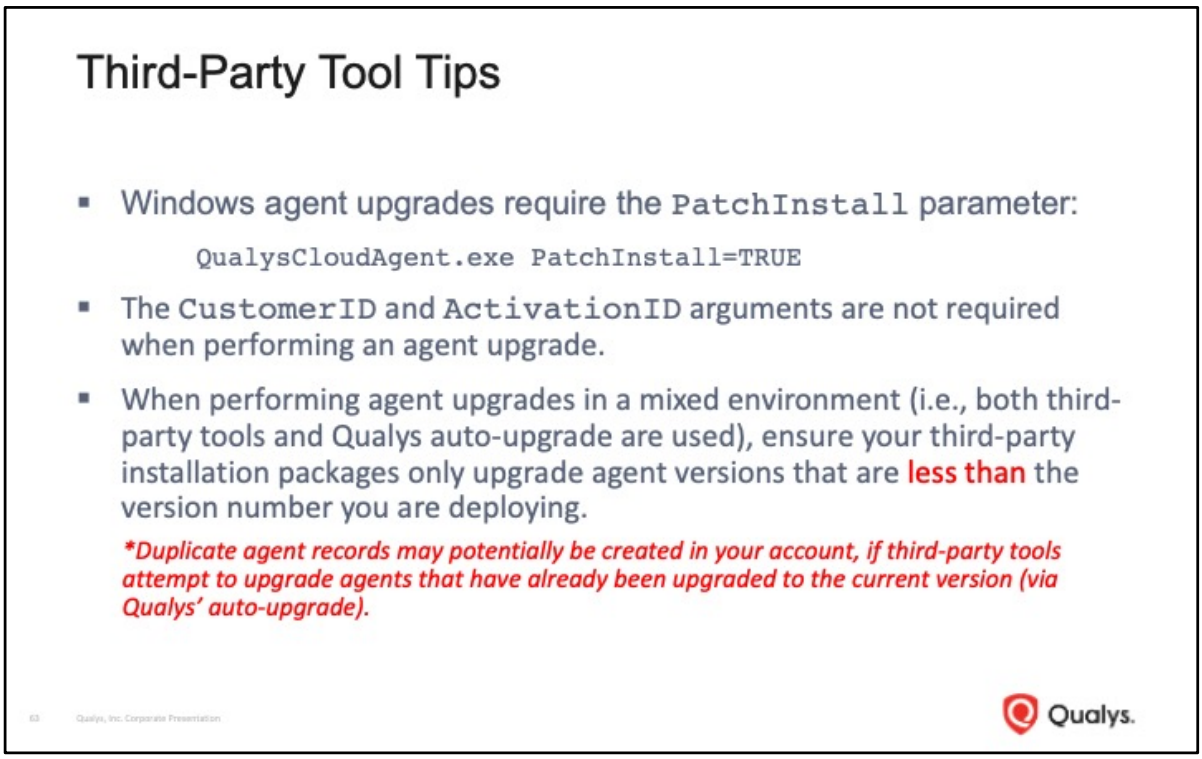
Click on any version number in the bar chart to display its agent hosts.




Although not all hosts are candidates for the agent auto-upgrade feature, Qualys recommends using this option wherever possible to take advantage of the latest agent features.

When using third-party software distribution tools to upgrade agents, Qualys recommends performing agent upgrades quarterly. At a minimum, upgrade all EOS agents and continue to keep agents upgraded on an as-needed basis.

Qualys recommends updating Gold Image builds quarterly, even if auto-upgrade is enabled.

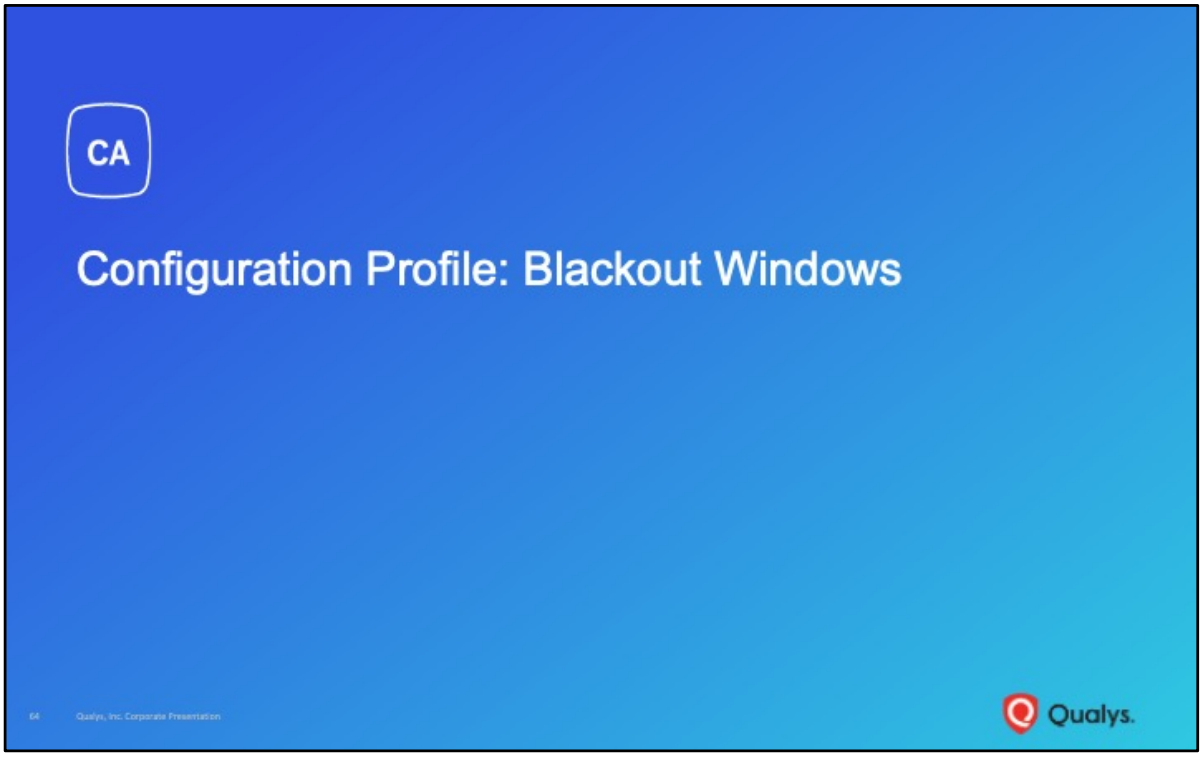



Here are a couple of tips when upgrading agents:

Windows agent upgrades must be performed using the PatchInstall parameter.

Do not attempt to use the CustomerID and ActivationID parameters when upgrading agents.

Ensure your third-party installation packages are designed to upgrade agent versions that are less than the version number you are deploying. This will help to prevent adding duplicate agent host records to your account.


CA
Configuration Profile: Blackout Windows
64
Qualys, Inc. Corporate Presentation
Qualys.

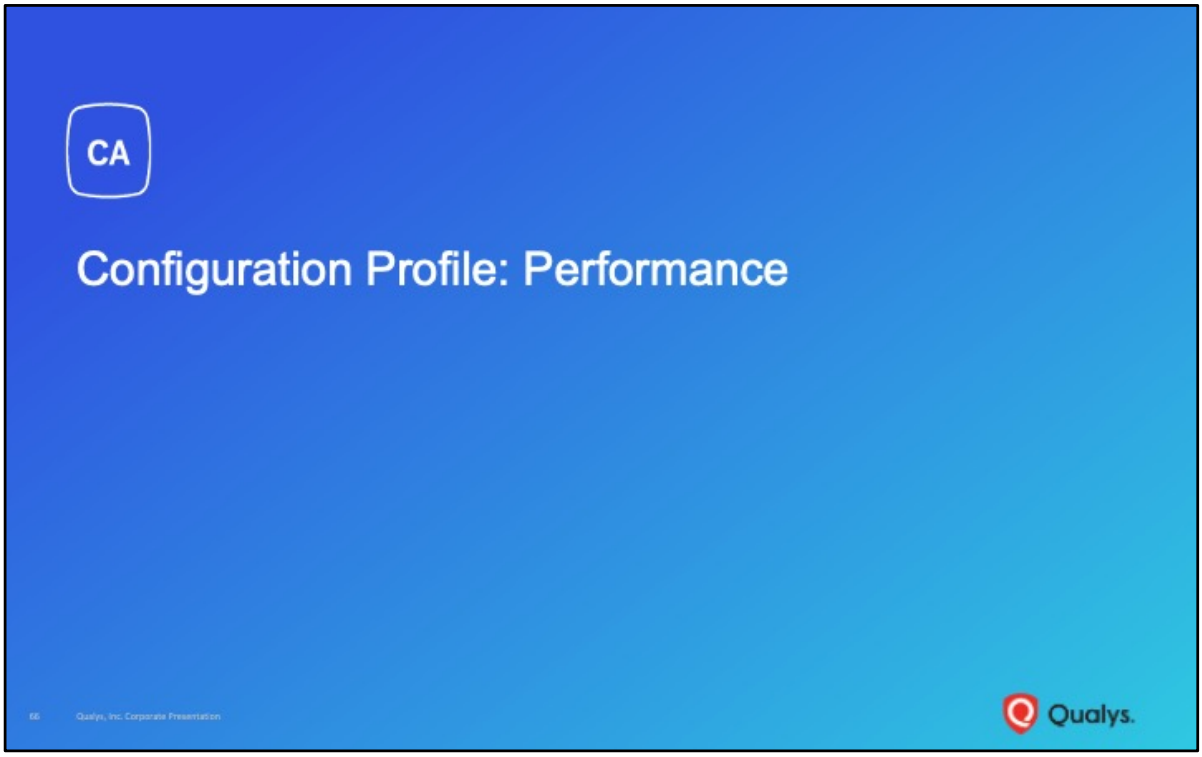
# Blackout Windows


- Prevent communication between agents and the Qualys Platform at specified times of the week.
- This is useful if you want your agents to stop communicating during expected times of heavy or increased network traffic.

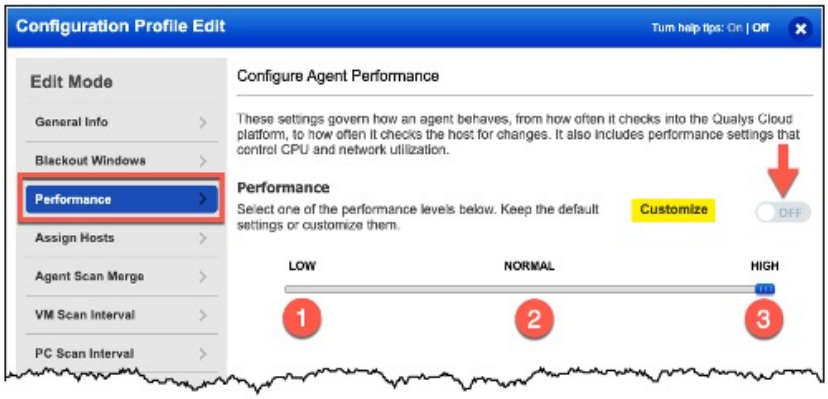


Qualys.

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.


CA
Configuration Profile: Performance
66
Qualys, Inc. Corporate Presentation
Qualys.

# Performance

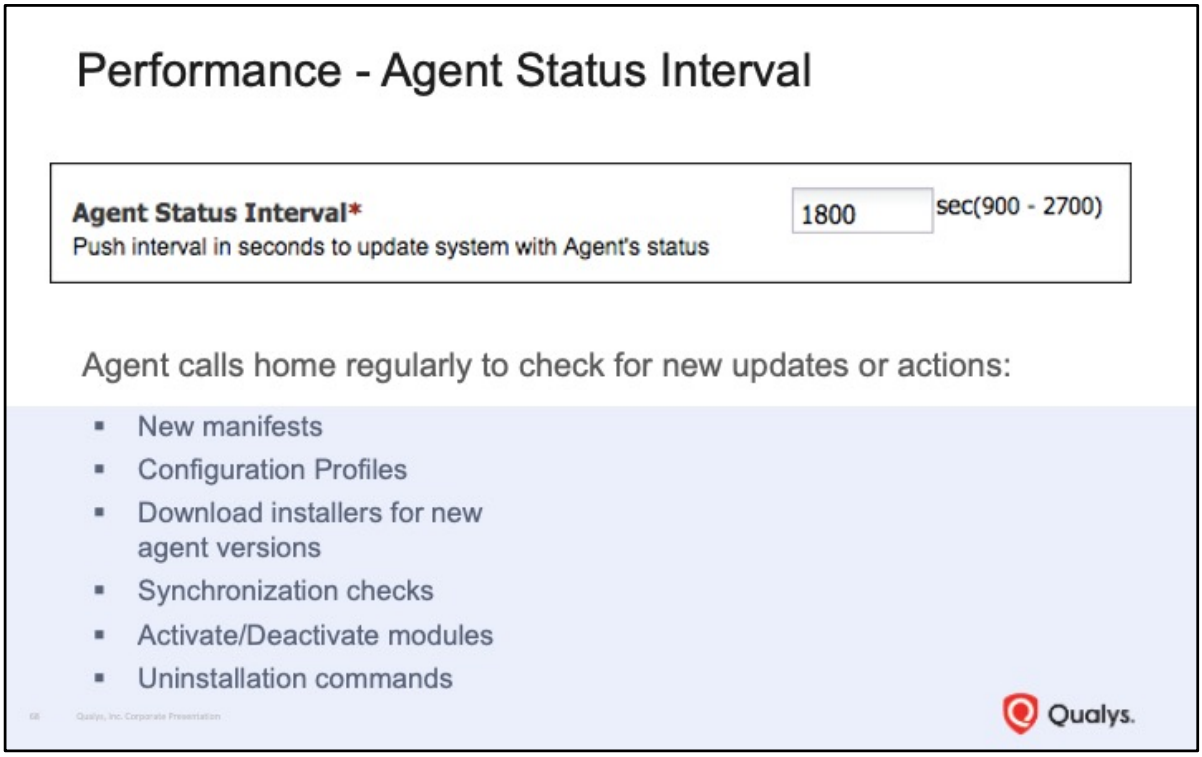



- Select default preset levels (LOW, NORMAL, or HIGH) or turn-on the “Customize” toggle switch.



Qualys.

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.

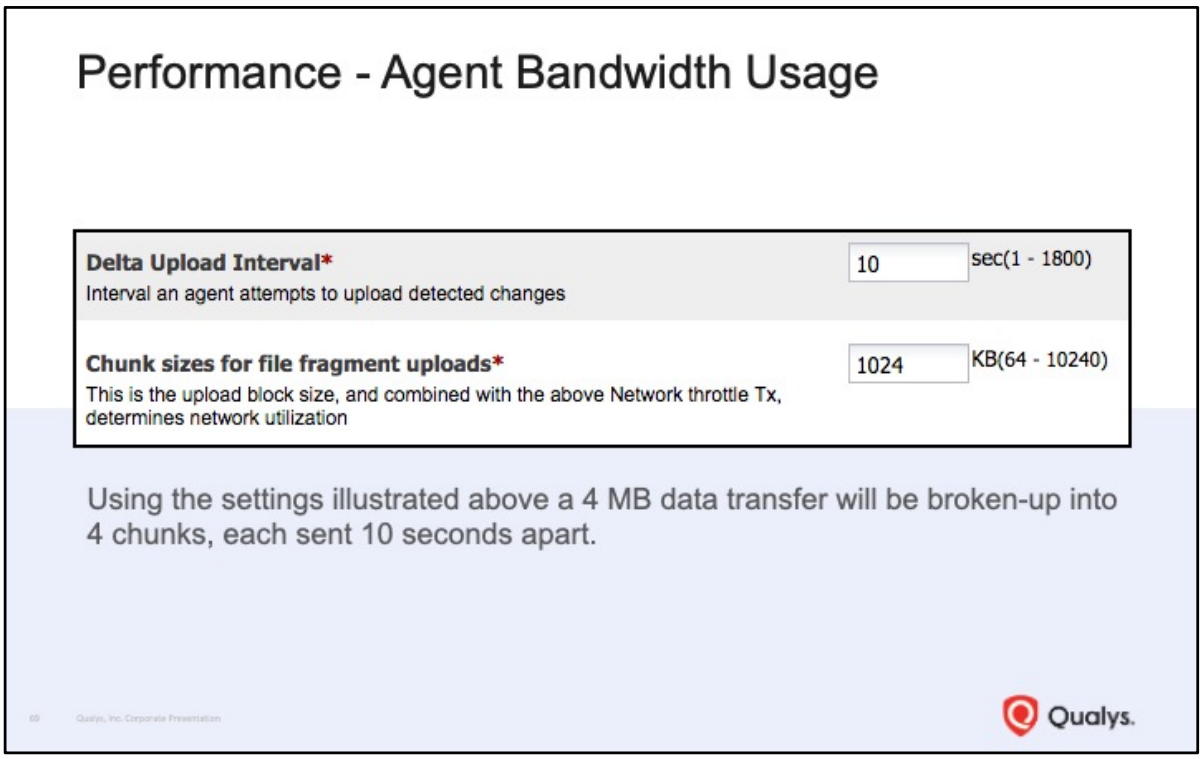



All communication between an agent and the Qualys Platform must be initiated by the agent.

The agent communicates to the Qualys platform at regular, configurable intervals (15 - 45 min.) to receive any new content or actions to perform. The request/reply is typically small in size (usually less than 1 KB).

The content or actions received through the Status Update include:

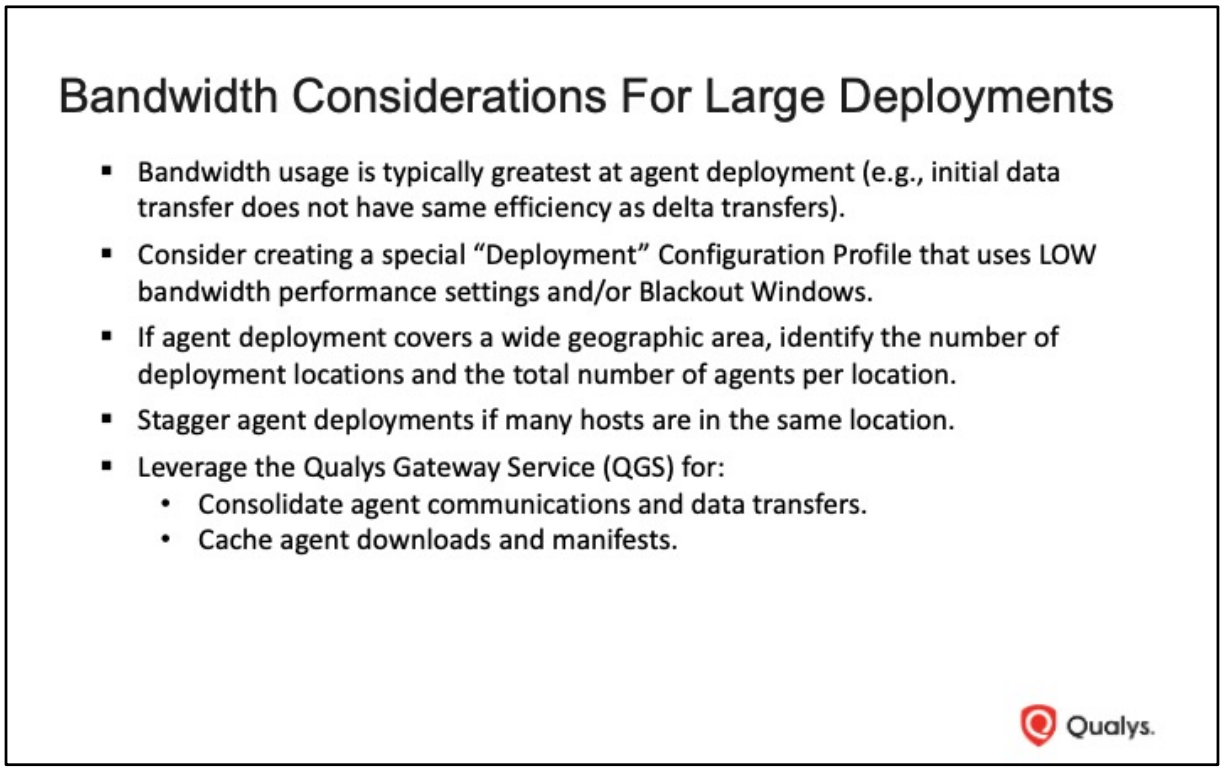
- New manifests
- Configuration Profiles
- Download installers for new agent versions (if configured)
- Re-provisioning commands
- Re-synchronization commands
- Activate/Deactivate application modules
- Uninstallation commands




When an agent is ready to transmit a “snapshot” to the Qualys Cloud Platform, the “Chunk sizes for file fragment uploads” setting will determine whether the “snapshot” file will be broken-up into smaller fragments or chunks.

If more than one “chunk” is to be sent to the Qualys Cloud Platform, the “Delta Upload Interval” setting determines the amount of time between individual “chunk” transmissions.

Data collections are compared to latest snapshot and only changes (deltas) are uploaded to the Qualys Platform.




Bandwidth usage is typically greatest at agent deployment (e.g., initial data transfer does not have same efficiency as delta transfers). When deploying agents in an enterprise (large) environment, consider spacing out your deployment over time and wide geographic areas. Consider creating a special "Deployment" Configuration Profile that uses LOW bandwidth performance settings and/or Blackout Windows.

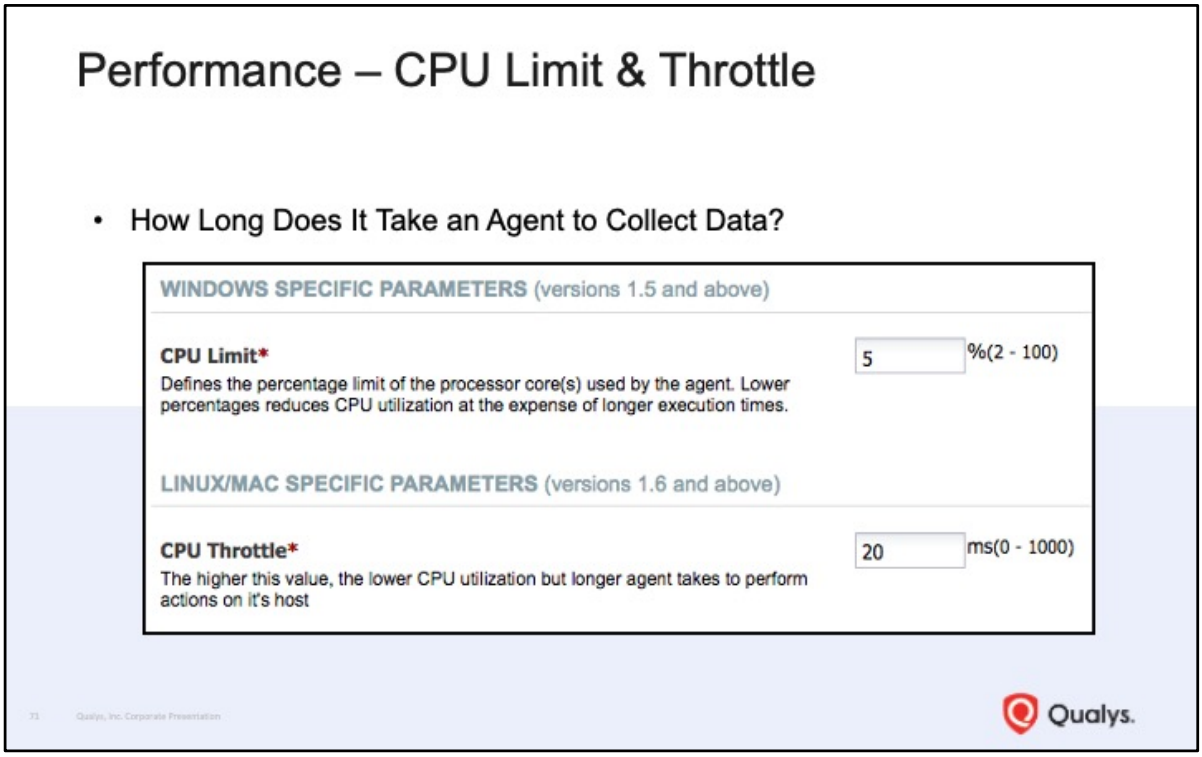
If agent deployment covers a wide geographic area, identify the number of deployment locations and the total number of agents per location. You likely do not want all your agents calling home at the same time. Stagger your deployment over hours or days if located in the same location.

Qualys Gateway Server provides proxy services for cloud agents. It an be used for assets that don't have direct internet access or when you want to optimize bandwidth.

Leverage the Qualys Gateway Service (QGS) to:

Consolidate agent communications and data transfers.

Cache agent downloads and manifests.

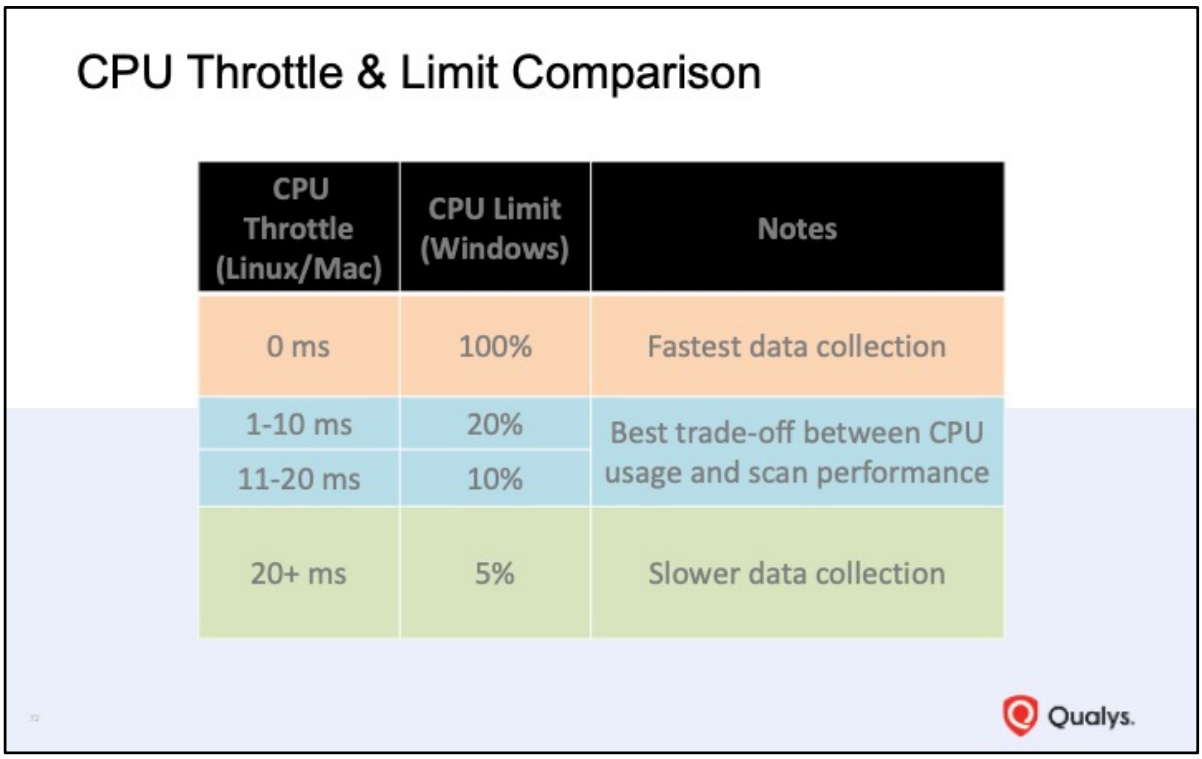



While the agent "Data Collection Interval" setting determines how often or frequently an agent collects assessment and inventory data, the CPU Performance settings determine how quickly or slowly the agent goes about the task of data collection.

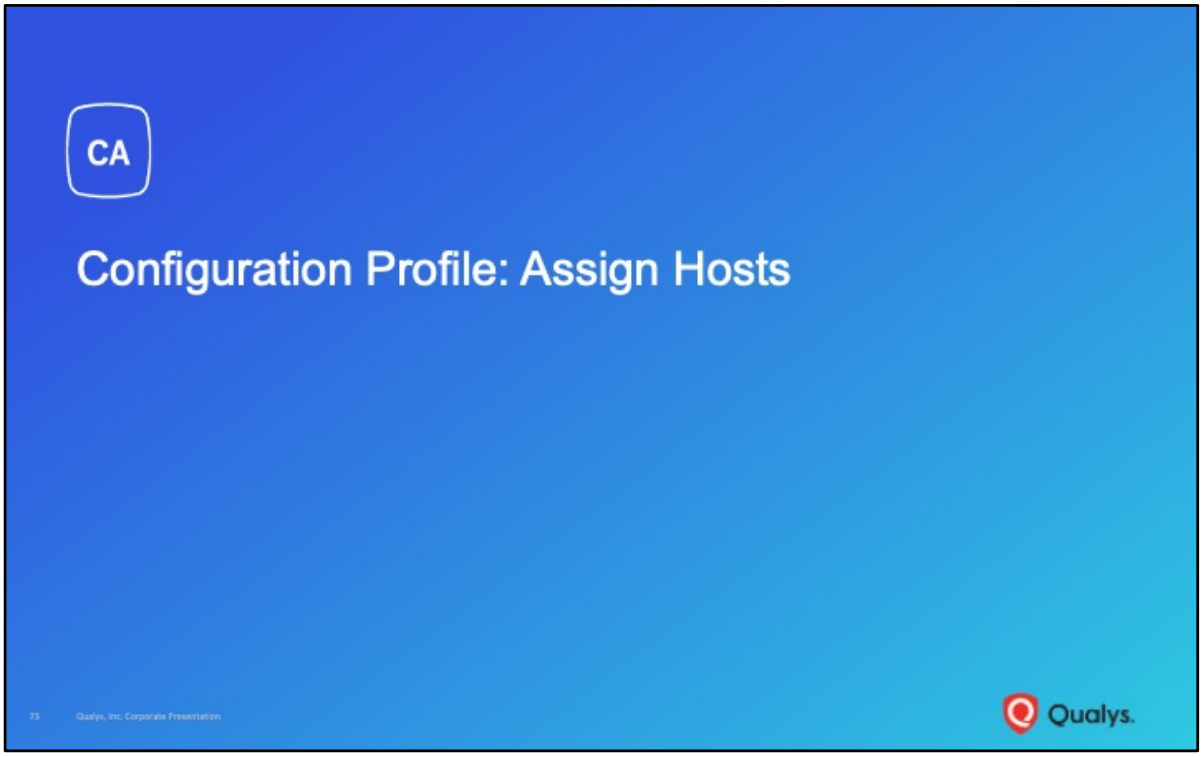
For Windows, faster data collections speeds are associated with higher "CPU Limit" percentages and slower data collection speeds are associated with lower "CPU Limit" settings.

For Unix/Linux, faster data collection speeds are associated with lower "CPU Throttle" values and slower data collection speeds are associated with higher "CPU Throttle" values.

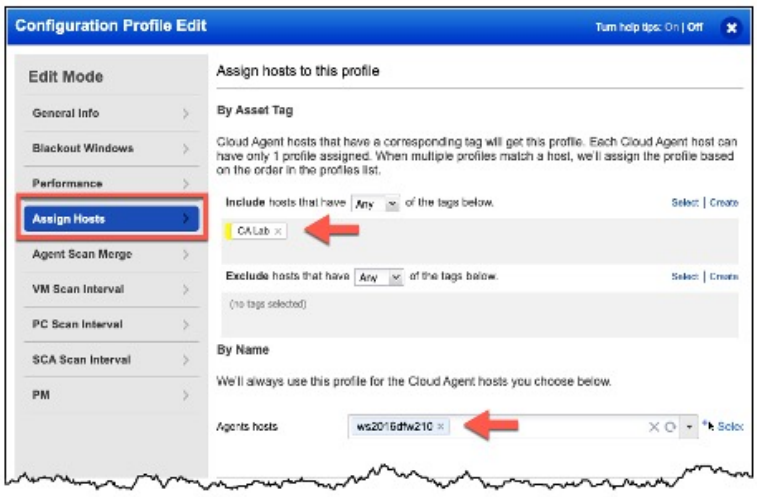
Windows agents are single threaded, and only consume a single CPU core--to calculate the real CPU usage on a four core system, divide the CPU Limit percentage by 4. On an eight core system, divide the CPU Limit percentage by 8.




The middle (blue) rows in this table represent the agent performance sweet spot. This is a good place to start and attempts to balance agent performance with CPU usage. Adjustments should then be made higher or lower, according to available resources and performance needs.


CA
Configuration Profile: Assign Hosts
73
Qualys, Inc. Corporate Presentation
Qualys.

# Assign Hosts




- Assign host assets to a Configuration Profile by Asset Tag or Host Name.
- **BEST PRACTICE**: Rely on Asset Tags to assign hosts.

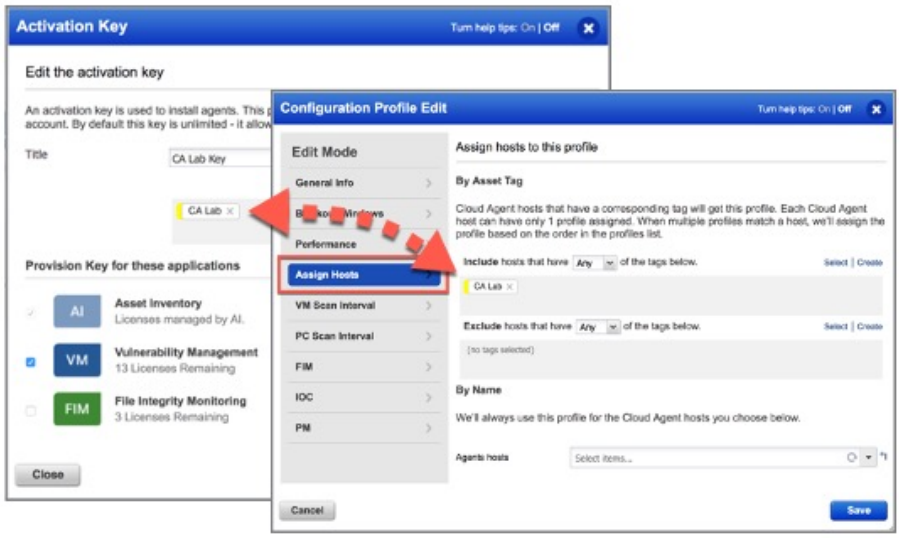
Qualys.

Agent hosts can be assigned to a configuration profile by Asset Tag or explicitly by name.

BEST PRACTICE: Rely on Asset Tags to assign hosts.

## Activation Key Tag Strategy

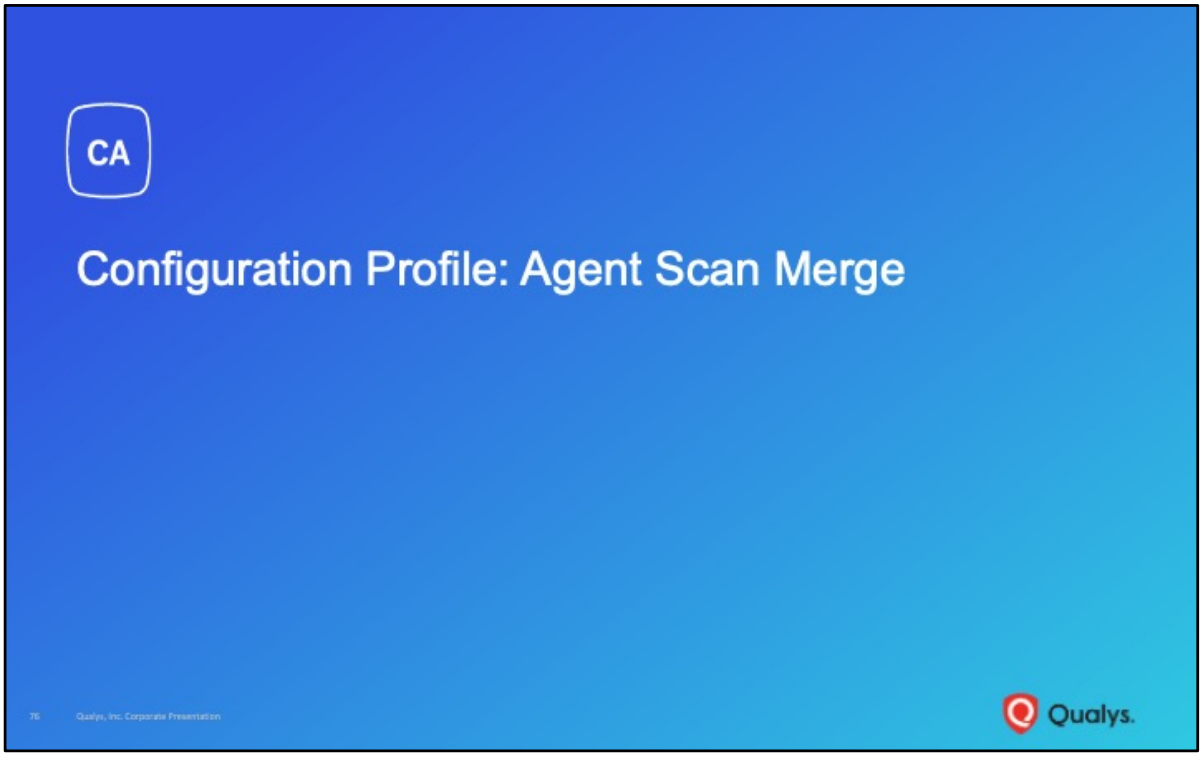
- **BEST PRACTICE**: Assign "static" tags to agent Activation Keys and use them to ensure agent hosts receive their appropriate performance settings, patching licenses, and patch job assignments.



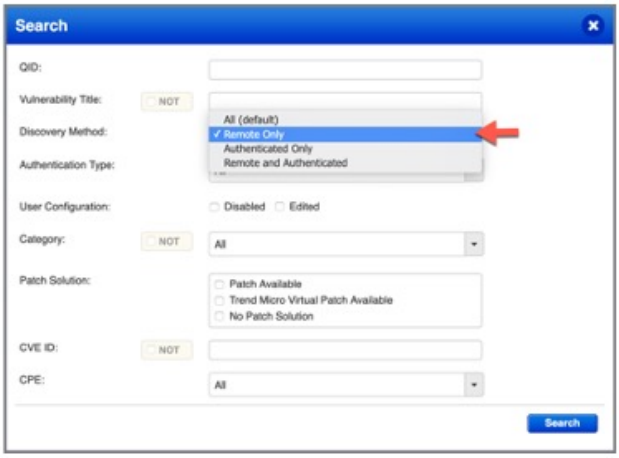

Qualys.

Assign a "static" tag to each agent Activation Key to easily locate the agent hosts it deploys. You can then use the same "static" tag to assign these hosts to their Configuration Profile

BEST PRACTICE: Use this strategy to assign agent host assets to their appropriate profiles, licenses, and jobs (at the time of agent deployment).


CA
Configuration Profile: Agent Scan Merge
76
Qualys, Inc. Corporate Presentation
Qualys.

# Remote Only QIDs




- A Qualys Scanner's "remote" perspective is required to detect "Remote Only" QIDs.
- Perform supplemental scans for agent hosts that are impacted by "Remote Only" QIDs.
- These hosts will have both SCAN data and AGENT data.

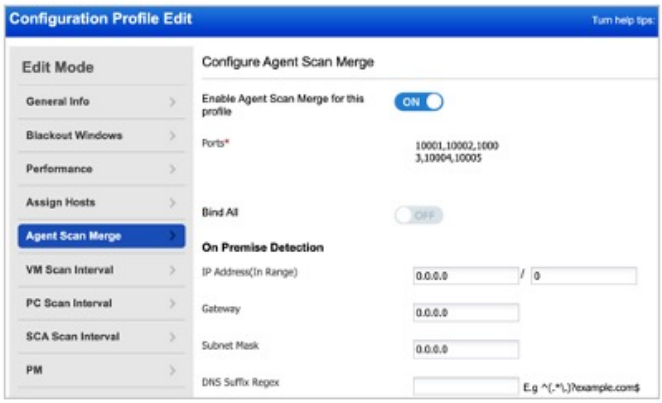
77

Qualys.

Supplemental scans (using a Qualys Scanner Appliance) may be performed on agent hosts, to provide coverage for "Remote Only" QIDs.

# Agent Scan Merge

- Enable Agent Scan Merge in the agent Configuration Profile to expose the Agent Correlation Identifier.
- The agent will attempt to bind to the lowest available TCP port, in the range of 10001 through 10005.
- Use the "Bind All" option to bind on all ports simultaneously.




- Configure "On Premise Detection" to expose the Agent Correlation Identifier only when on a trusted network.

Qualys.

Qualys Scanner Appliances produce SCAN data. Qualys Agents produce AGENT data. When a Qualys Scanner is used to scan a host that already has a Qualys Agent installed, both SCAN data and AGENT data records are collected and stored.

SCAN data and AGENT data can be successfully merged, when both types of records contain a common field or attribute. The Agent Correlation Identifier provides this common attribute.

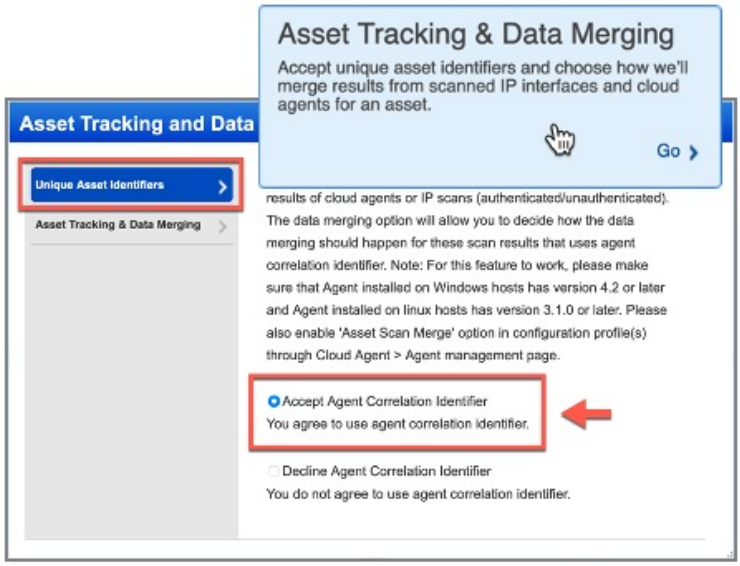
When Agent Scan Merge is enabled in a Configuration Profile, the Agent Correlation Identifier is exposed on TCP ports 10001-10005. By default the lowest available port number will be used. Use the "Bind All" option to bind on all five ports simultaneously.

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.

Once Agent Scan Merger is enabled, the 'agentid-service' can be viewed from Windows Task Manager or within a Unix/Linux process list. Use the netstat command to view its assigned port number(s).

# Unique Asset Identifiers

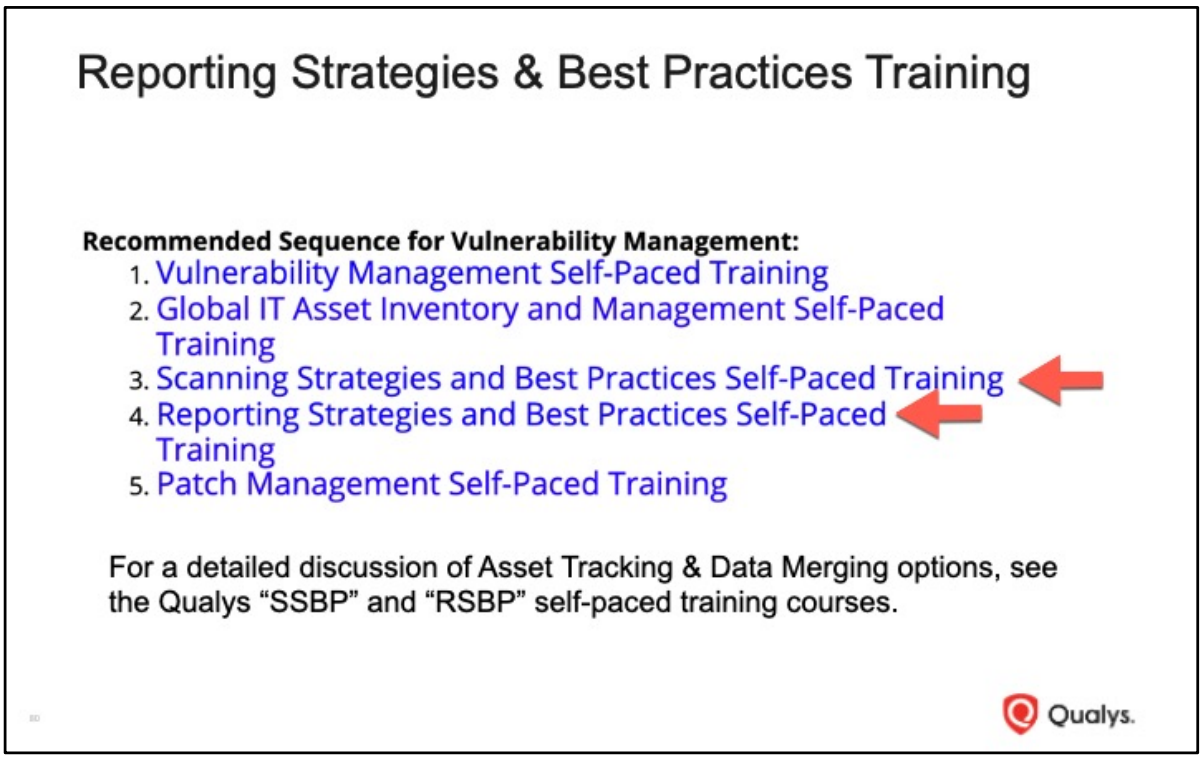
- From Qualys VM or VMDR, accept the "Agent Correlation Identifier" option (Assets > Setup > Asset Tracking & Data Merging).
- Qualys Scanner Appliances will attempt to read the correlation identifier when scanning agent hosts, allowing the SCAN data to be linked to its associated agent.



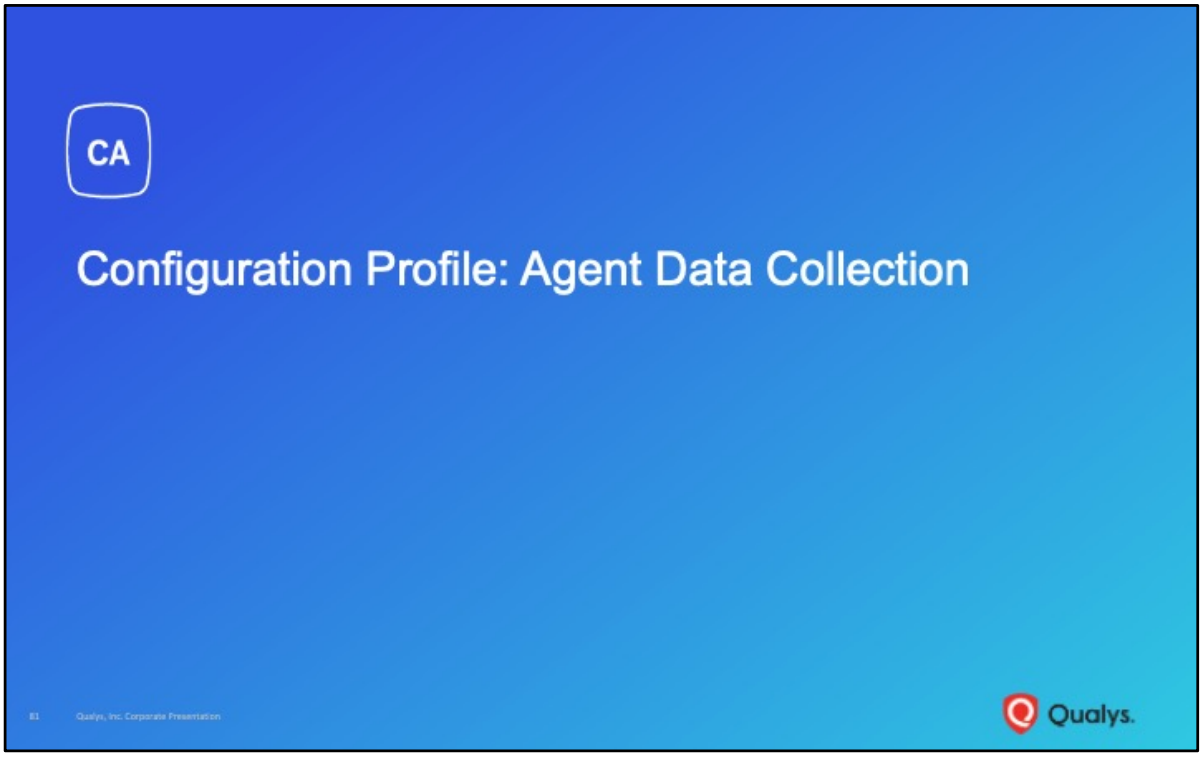

Qualys.

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.

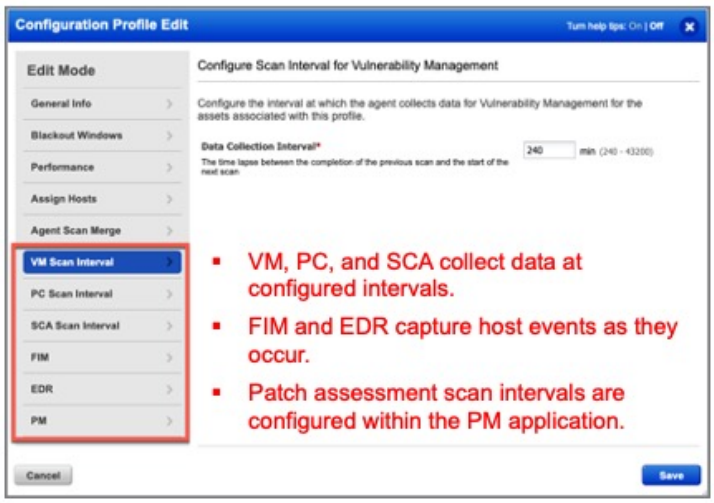
AGENT data and SCAN data can be successfully merged using the Agent Correlation Identifier attribute.




For a complete description of the different Data Merging options in Qualys VM and VMDR, please enroll in the Qualys "Scanning Strategies & Best Practices" self-paced training course.


CA
Configuration Profile: Agent Data Collection
81
Qualys, Inc. Corporate Presentation
Qualys.

## Interval vs. Event-Driven Data Collection



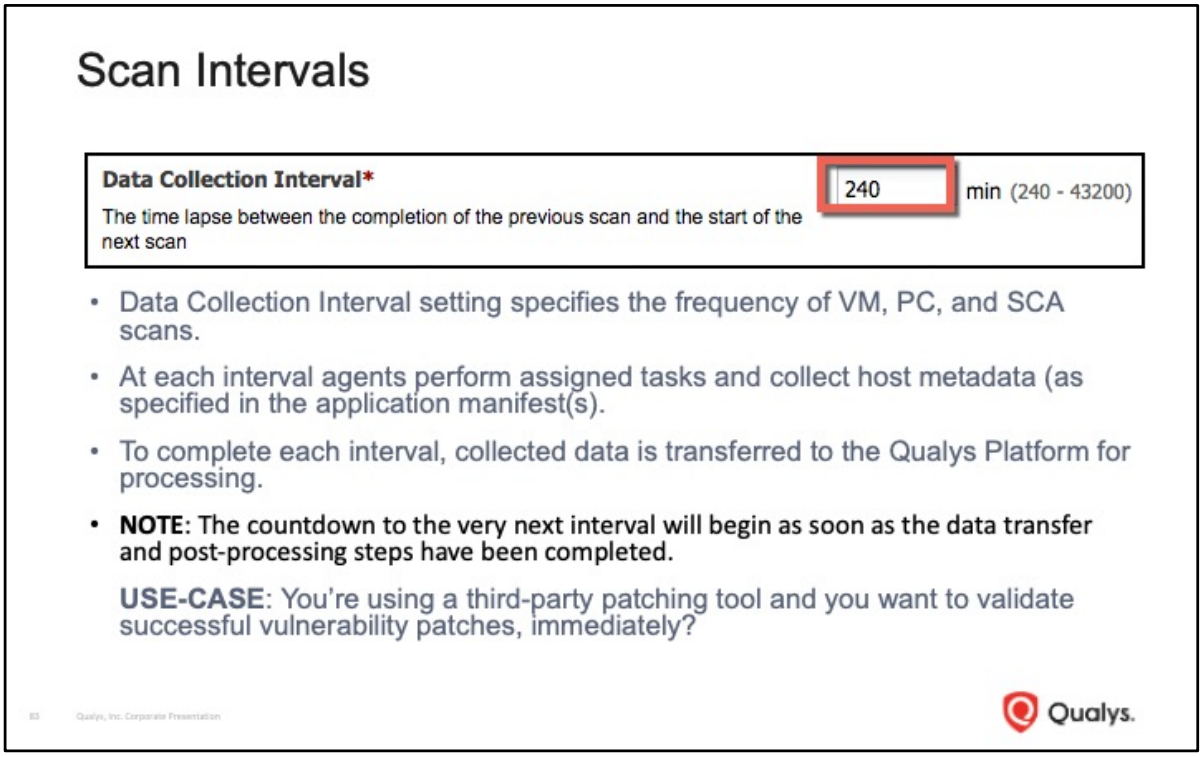



Qualys.

The remaining options, allow you to customize the data collection methods used by agent hosts. Some Qualys applications collect data at user-defined intervals and other applications capture events as they occur on the host.

Focusing on data collection allows the agent to remain relatively lightweight, while sending the collected data to the Qualys platform for assessment and enrichment.

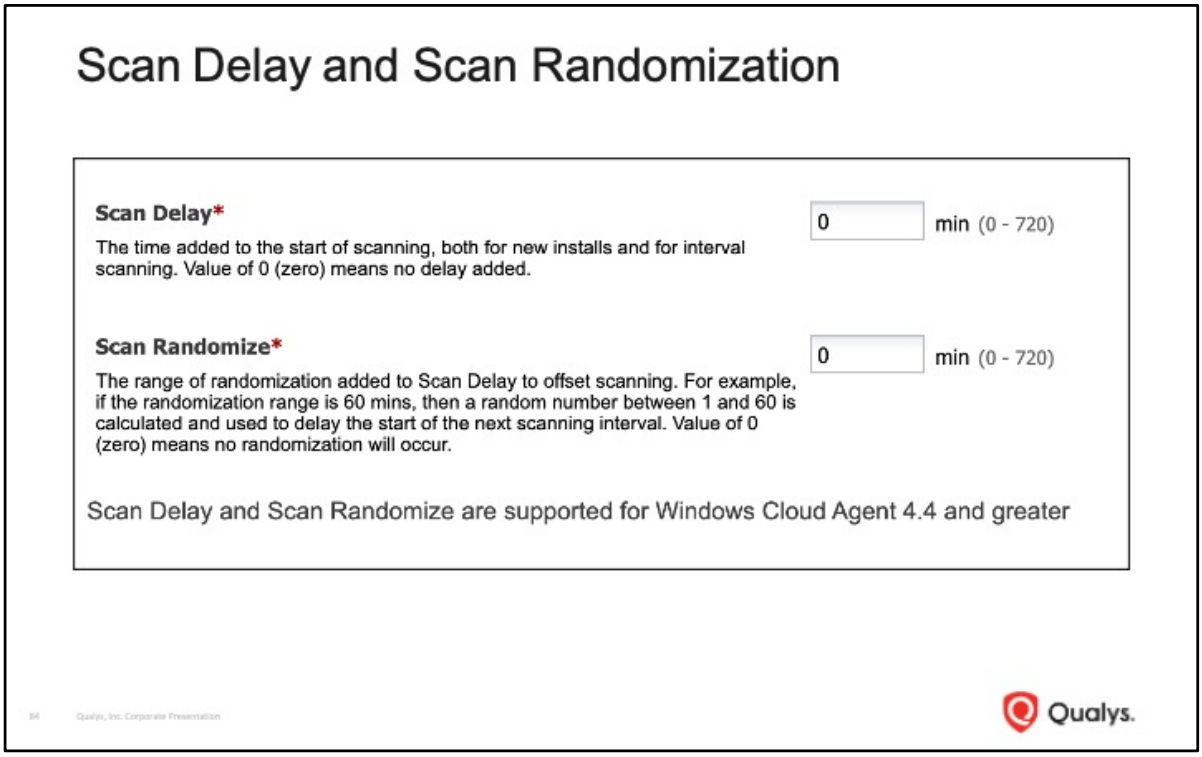
VM, PC, and SCA provide user-defined intervals for data collection, while FIM and EDR use event-driven techniques. Although Patch Management (PM) provides user-defined intervals for its patch assessment scans, this setting must be configured within the PM application.




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.

NOTE: The countdown to the very next interval will begin as soon as the data transfer and post-processing steps have been completed. The countdown to the next interval begins at the END of the previous interval (i.e., it does NOT begin at the START of the previous interval).

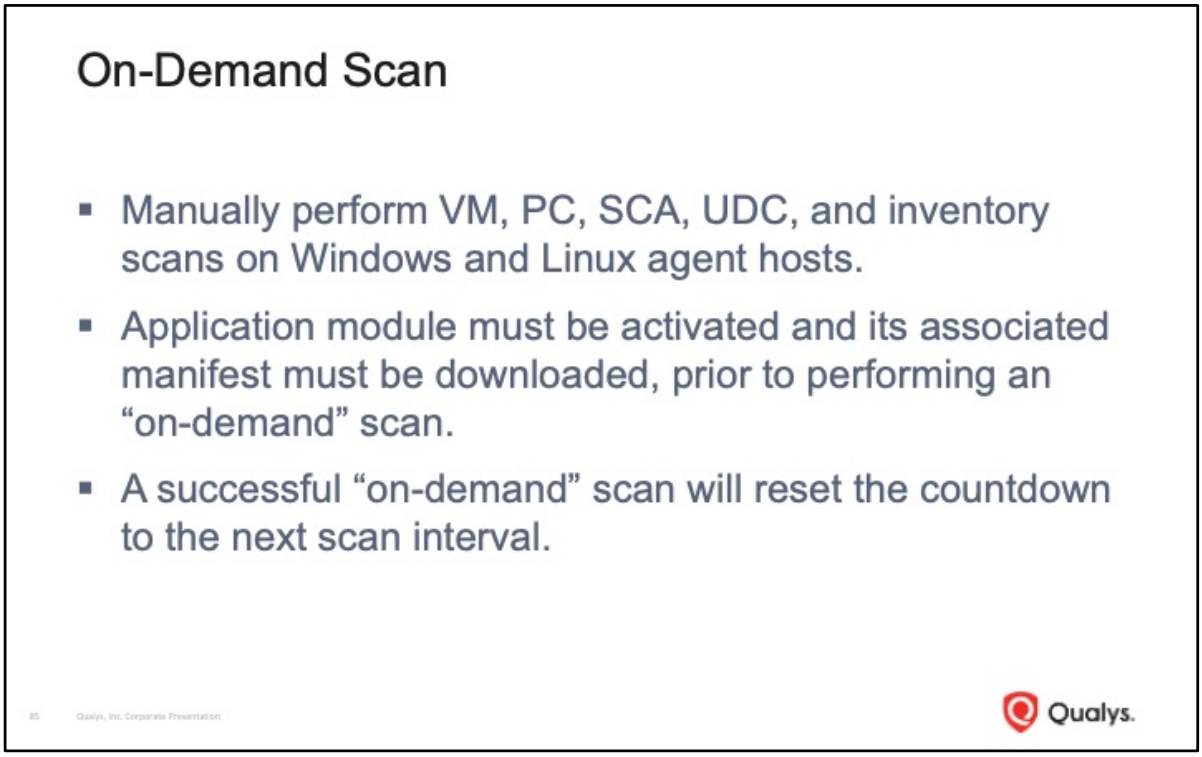
The solution to the use-case in this slide calls for the ability to run "on-demand" agent scans.




The use case for this would be to make sure that all agents don't send the data to platform at the same time. It can be seen as a means to stagger the communication, so that impact on the network is reduced.

Additional Use cases for this:

Client VDI all starting at 9am when employees start working
Elastic cloud when 1000s of assets are deployed at the same time
Agent assets in Blackout Windows all start processing at the same time
When new manifests come out, especially for remote office locations and slow links
When new agent installer versions come out



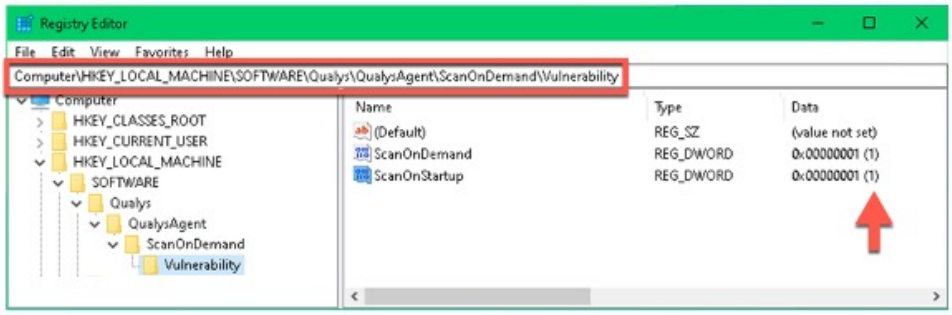

You can run an On Demand Scan to instruct the agent to immediately scan as long as the agent is not already scanning.

The target application module must be activated and its associated manifest must be downloaded, prior to performing an “on-demand” scan.

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.

## On-Demand Scan Examples

- On-demand scans for Windows are configured in the Windows Registry.




- On-demand scans for Linux are executed from the command line.

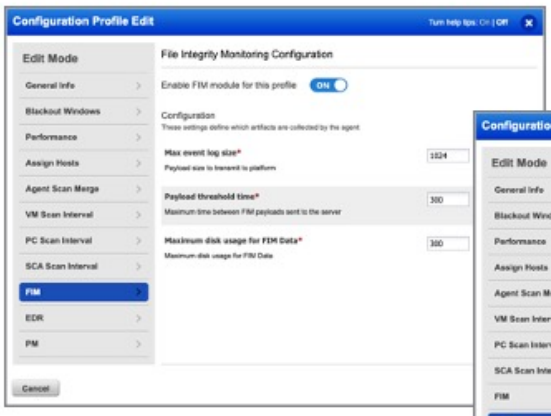
```
>#  ./cloudagentctl.sh action={demand} type=vm
```

Qualys.

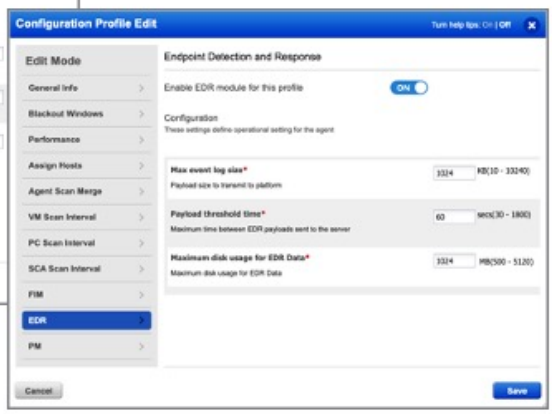
On-demand scans for Windows are configured in the Windows Registry and on-demand scans for Linux are executed from the command line. Please see the lab tutorial supplement for this course for more examples and details for running on-demand scans for Windows and Linux.

The same command of LinuxOS can even be used for MacOS.

# Event-Driven Data Collection




- Events are captured and logged as they occur for FIM and EDR.

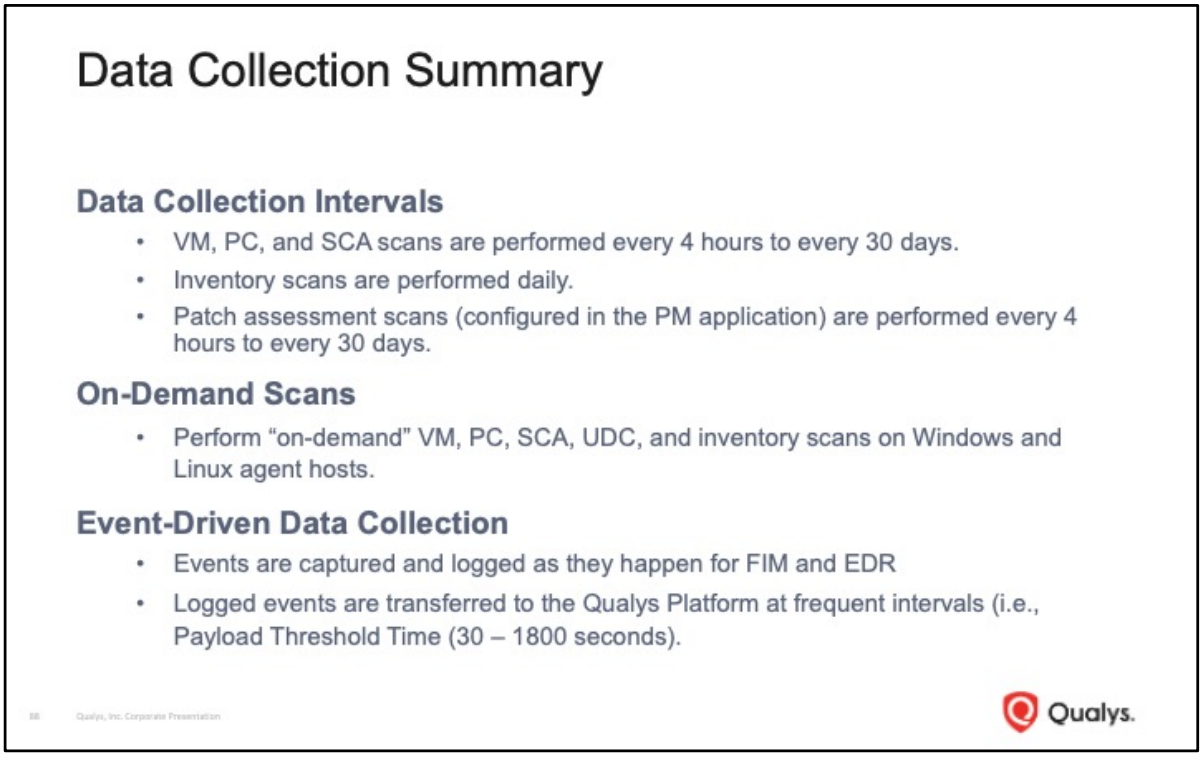



- Event log payloads are transferred to the Qualys Platform at frequent intervals.

87 Qualys, Inc. Corporate Presentation

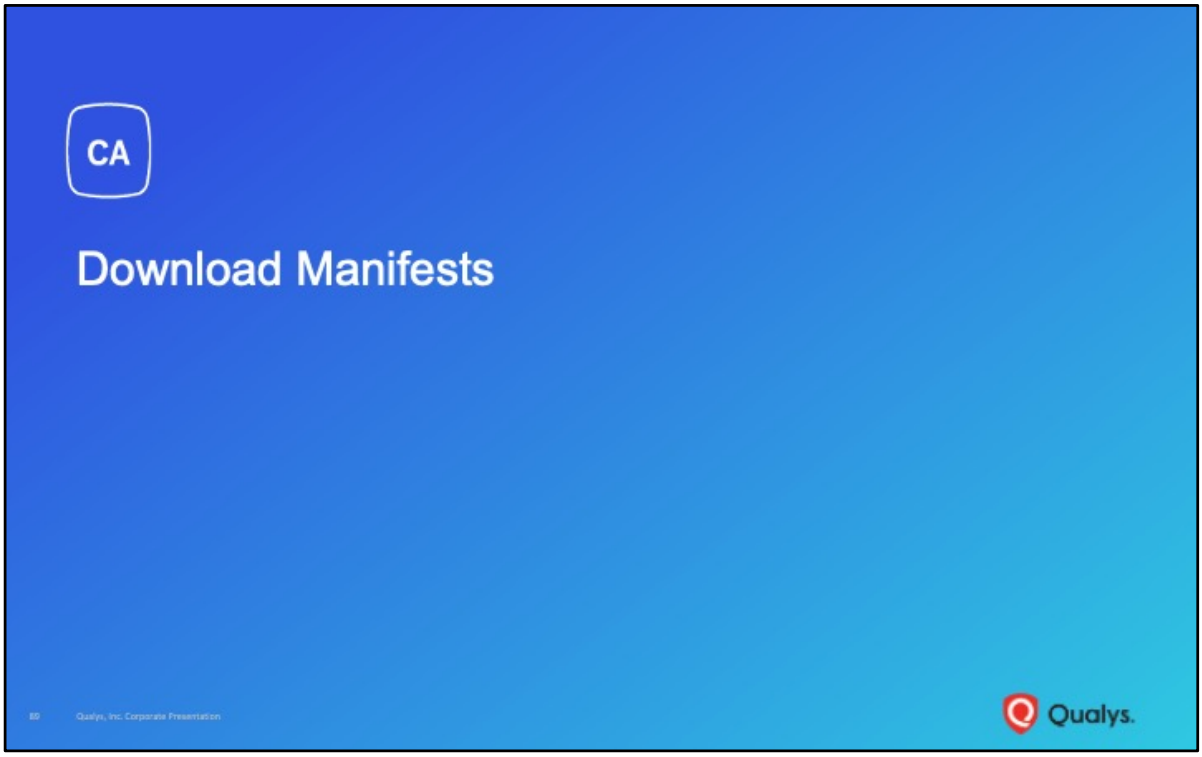
Qualys.

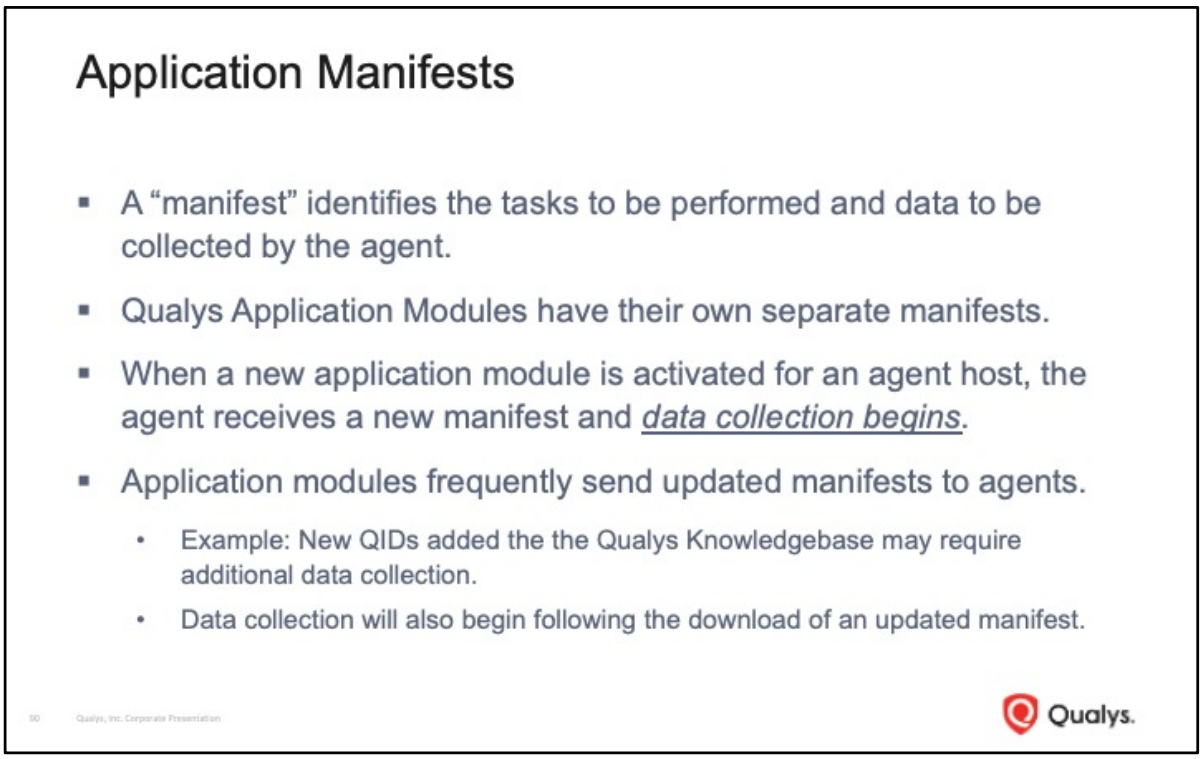
Kernel drivers allow agents to collect event data for FIM and EDR, as the events occur on the agent host. The “Payload Threshold Time” setting specifies the frequency of event log transmissions to the Qualys Platform (anywhere from 30 to 1800 seconds).




This slide provides a summary of the various agent data collection methods.

Agent data collection methods are dependent on the Qualys application module.


CA
Download Manifests
89
Qualys, Inc. Corporate Presentation
Qualys.




A manifest identifies the metadata an agent will collect from its host for a given application. Qualys Application Modules have their own separate manifests.

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.

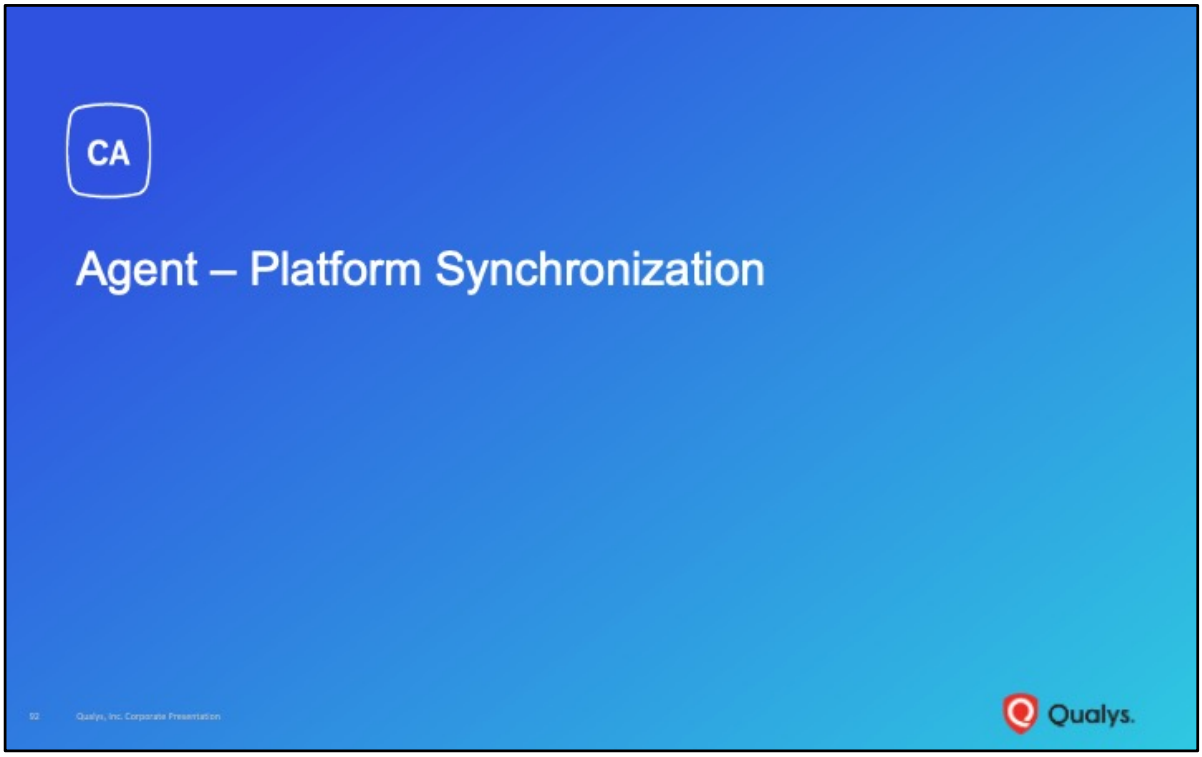
Manifests get updated regularly, especially in the case of VM where Qualys is continually adding new vulnerability signatures to our KnowledgeBase.

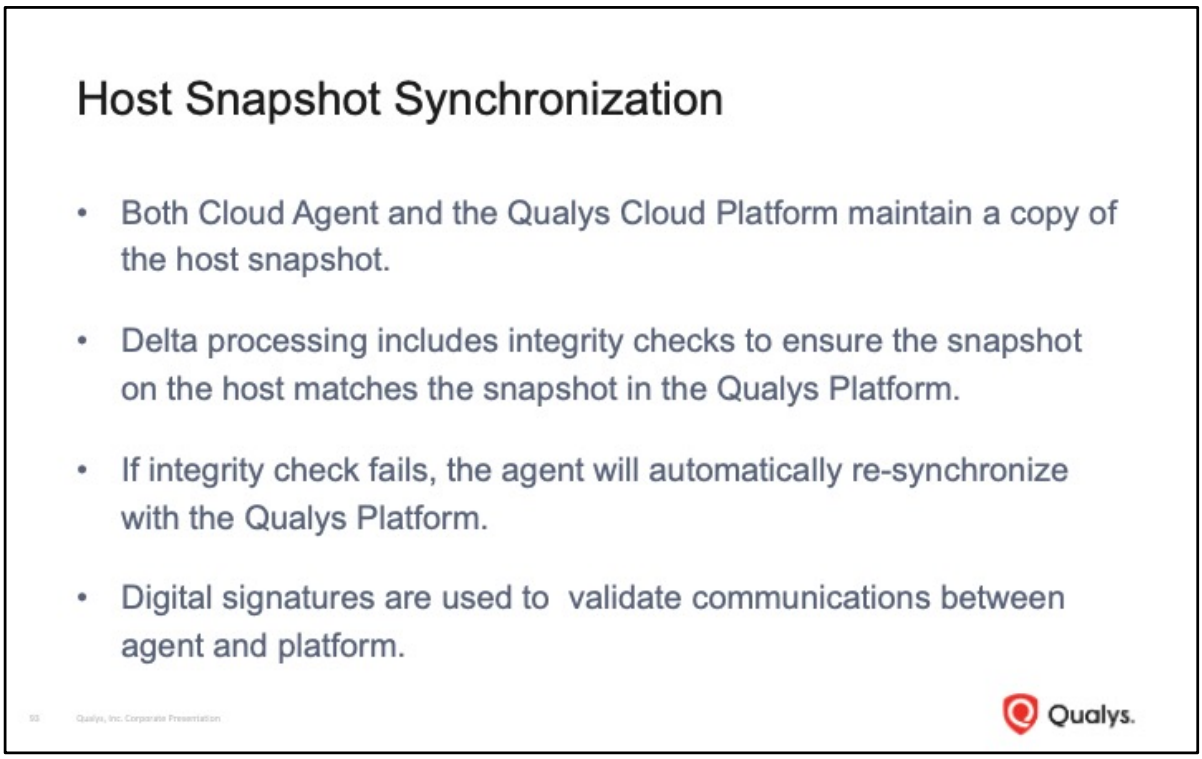
| Manifest Type | Description | Data Collection |
|---|---|---|
| Inventory | Collects asset inventory such as hardware, software, active services, etc... | Daily Intervals |
| Vulnerability | Collects data defined by QIDs in the Qualys Vulnerability KnowledgeBase. | User-Defined Intervals (240 - 43200 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.) |



Qualys.

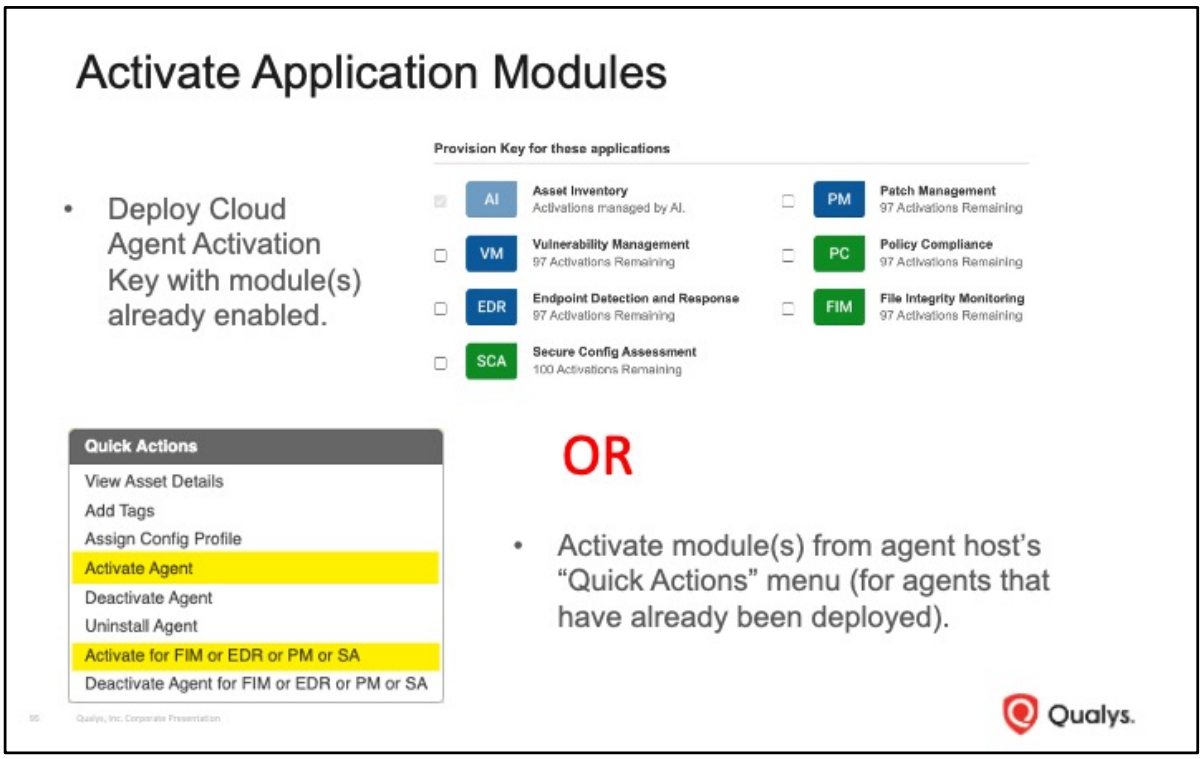
This table provides a summary of manifest types along with their respective data collection methods.


CA
Agent – Platform Synchronization
92
Qualys, Inc. Corporate Presentation
Qualys.

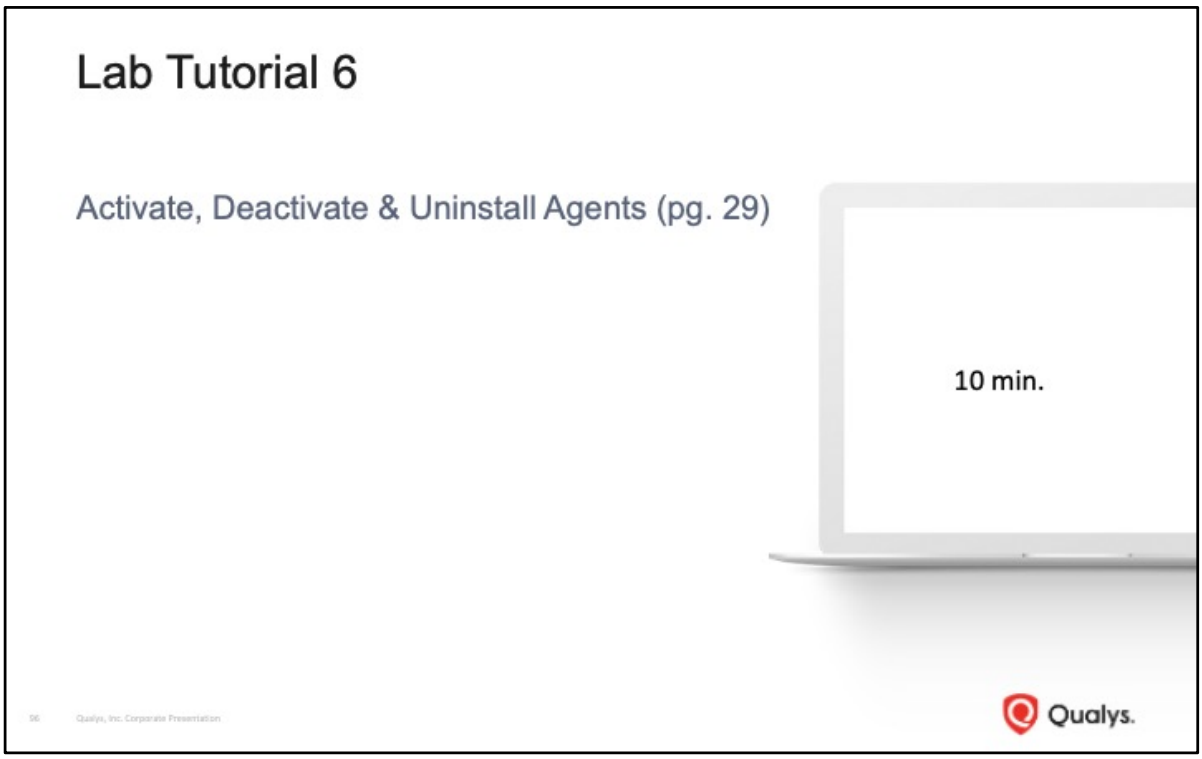



The delta processing feature of the Cloud Agent includes a synchronization mechanism that guarantees that local snapshot files and the data processed by the platform are the same. If the integrity check fails on either side, the agent will re-synchronize (called “scorch” internally) where both the agent and the platform delete existing snapshot data and start as if a newly provisioned agent. This process is performed automatically, if synchronization checks fail.


CA
Activate, Deactivate & Uninstall Agents
94
Qualys, Inc. Corporate Presentation
Qualys.

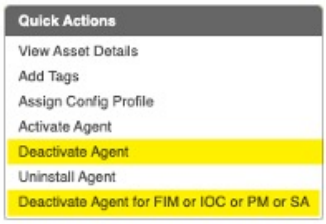



Qualys application modules (selected within an agent Activation Key) are activated at the time of agent deployment. Application modules can also be activated from the "Quick Actions" Menu of any agent hosts.

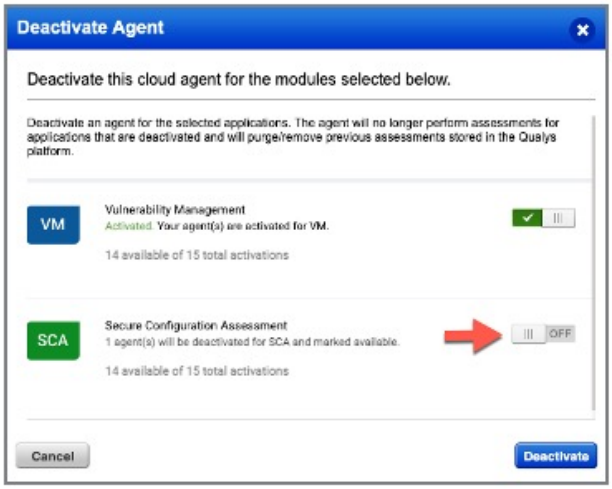



1. Deactivate the PC application module for an agent host
2. From the “Agents” tab, uninstall agents from three hosts, using the “Actions” button in the Cloud Agent UI

# Deactivate Application Module



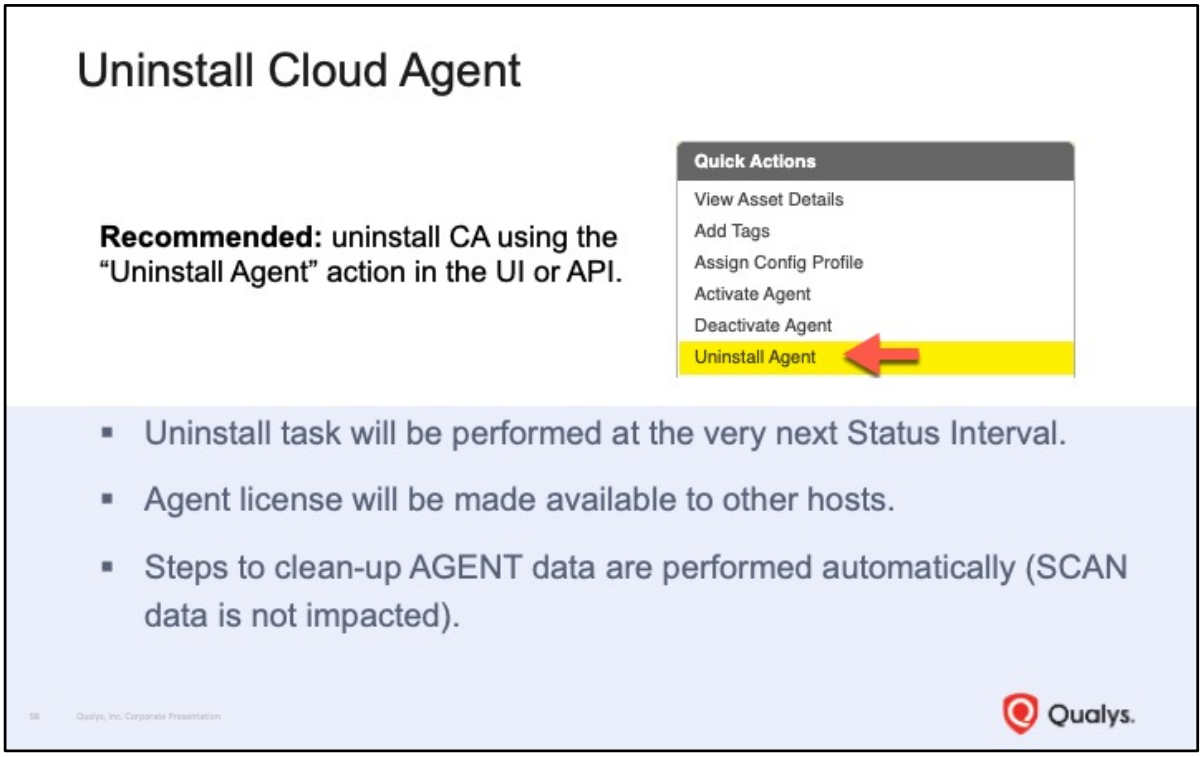

- Deactivate individual application modules for agent host assets.




Application modules can be deactivated for one agent host and then activated for another.

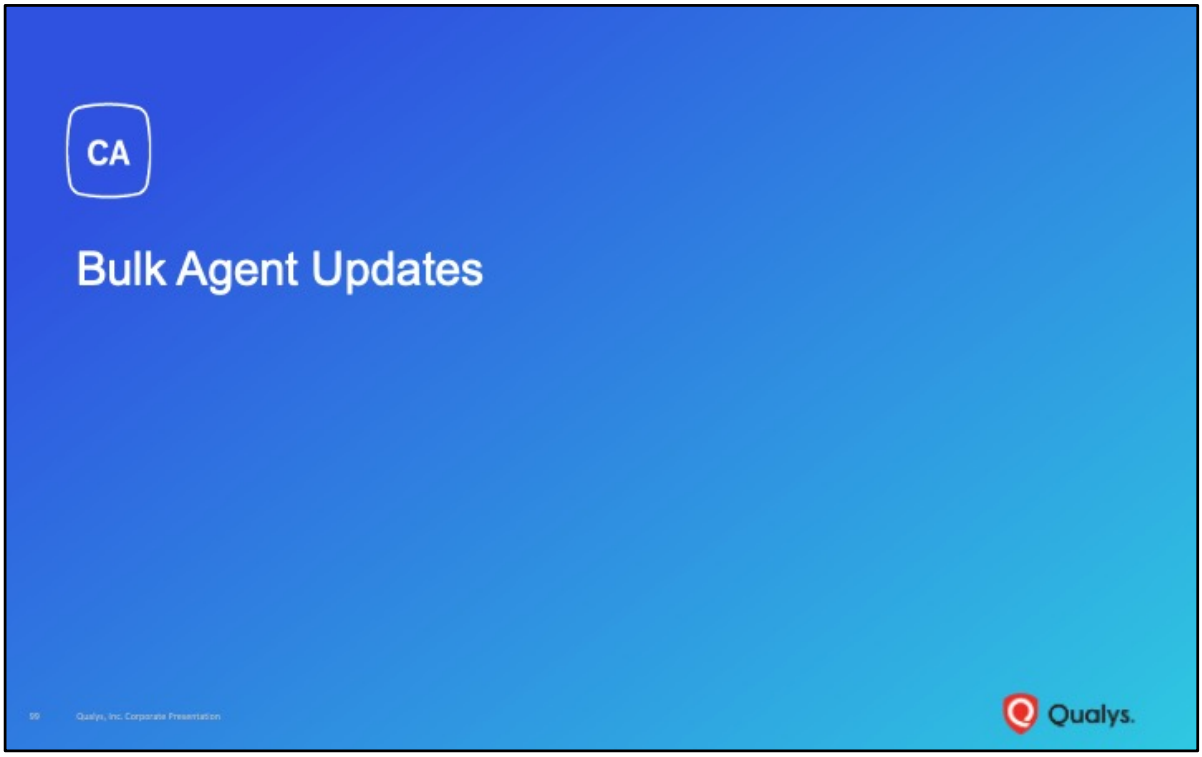
To deactivate an Agent Module, select “Deactivate Agent” from the “Quick Actions” menu. Then turn-off the targeted module, before clicking the “Deactivate” button.

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



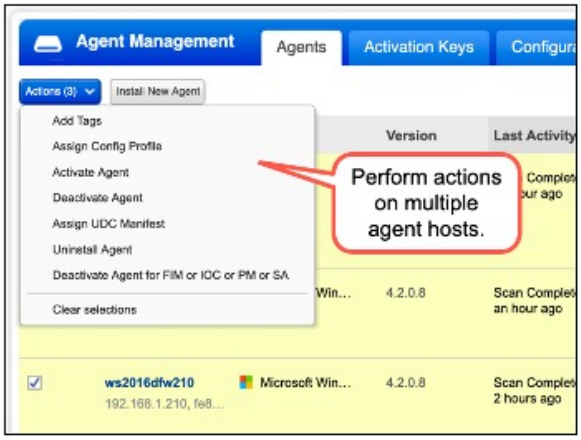

Selecting the "Uninstall Agent" option from the "Quick Actions" menu of any agent, will remove the agent from its host the very next time it checks-in. Any asset inventory, vulnerability, or policy compliance data is purged from the platform.

Agents must be uninstalled from the Qualys UI of API to ensure appropriate data clean-up measures are performed.




The objective of this section is to understand the different option for updating agents in bulk.

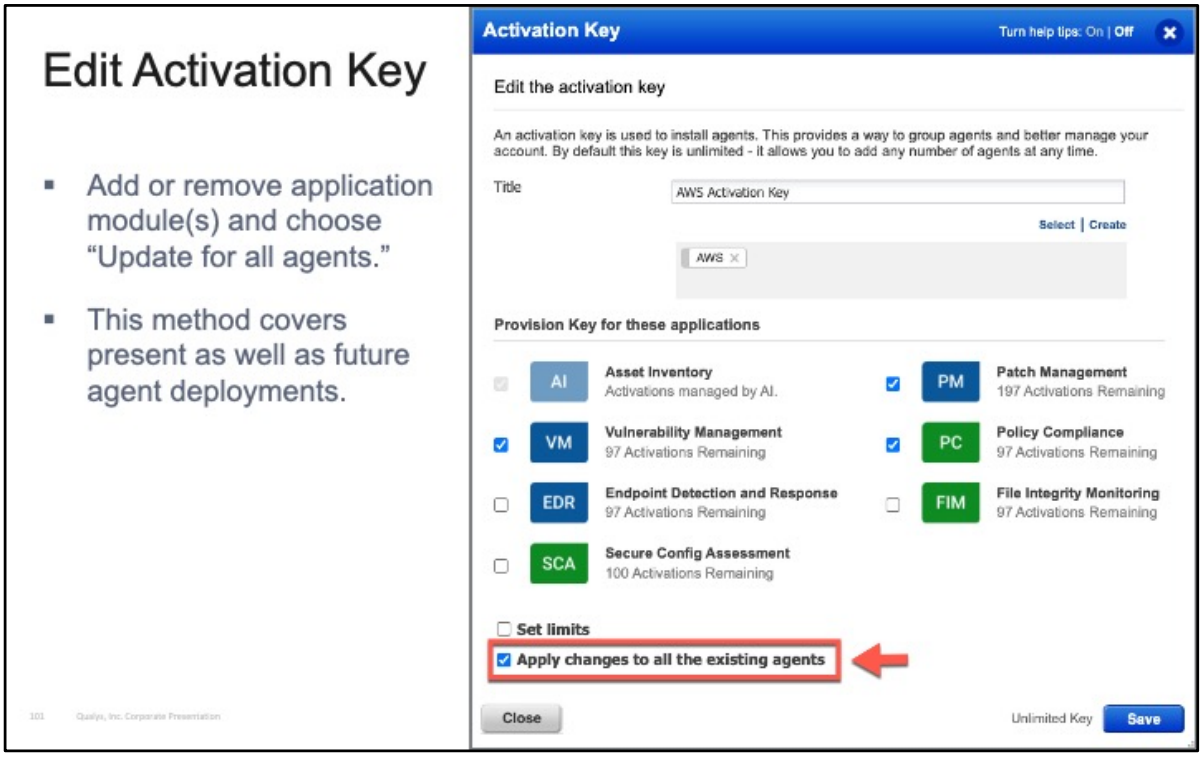
# Actions Button



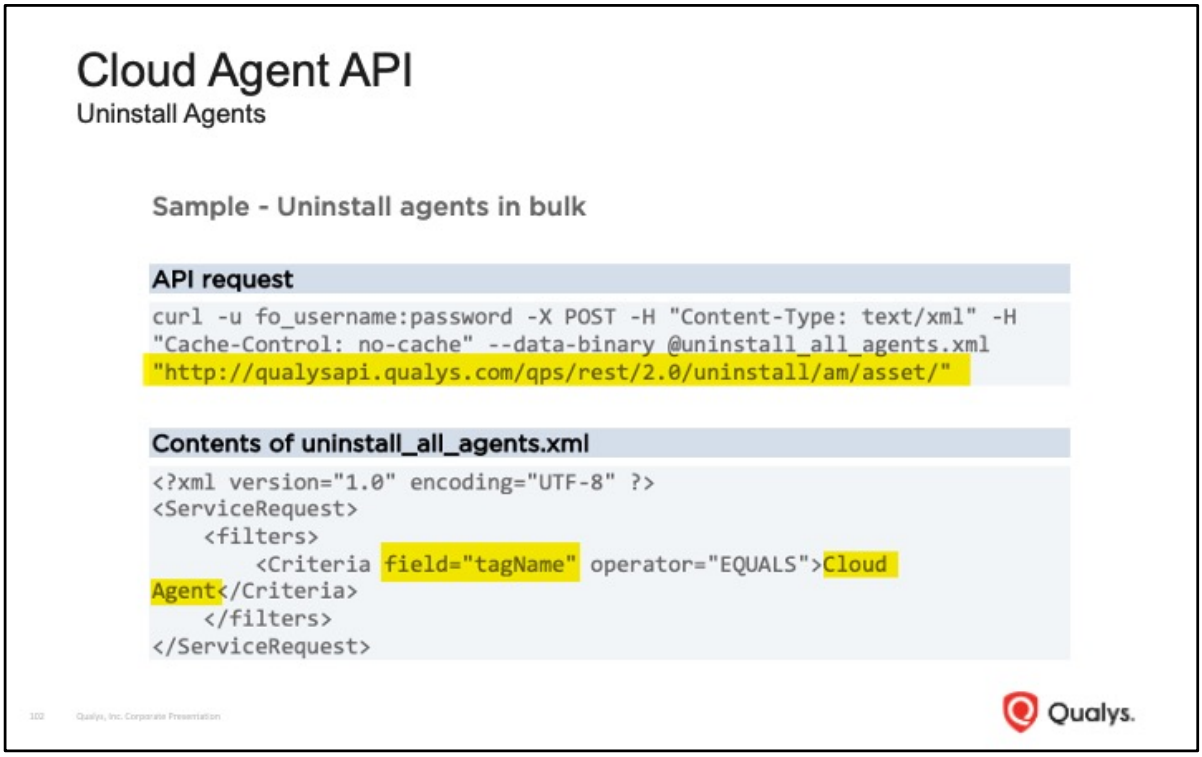

- Within the Cloud Agent application, select multiple agent hosts and use the “Actions” button to perform tasks in bulk.
- Execute queries to help filter agents for selection.

Qualys.

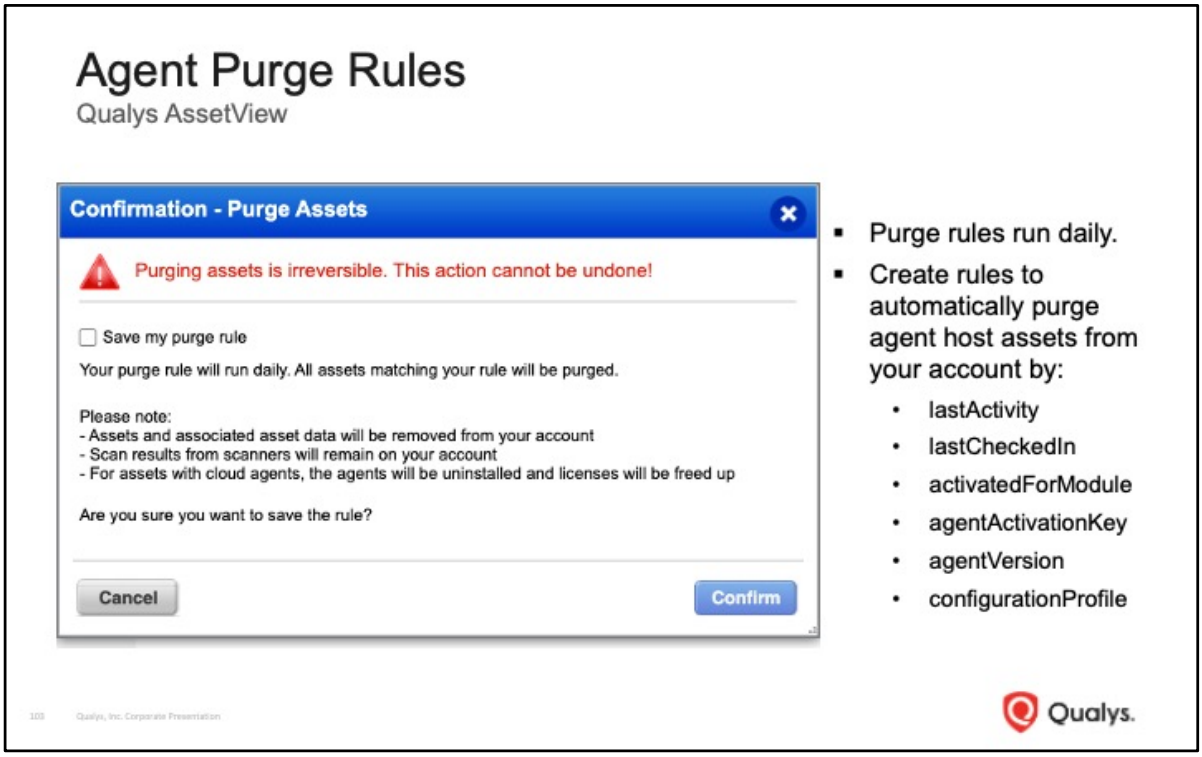
Select multiple agent hosts from the Cloud Agent UI and then use the “Actions” button to perform updates in bulk.




Adding and removing application modules can be performed for all existing agents using their associated Activation Key. Simply select the "Apply Changes to all existing agents" option. Future agent deployments will receive the updated module configuration.

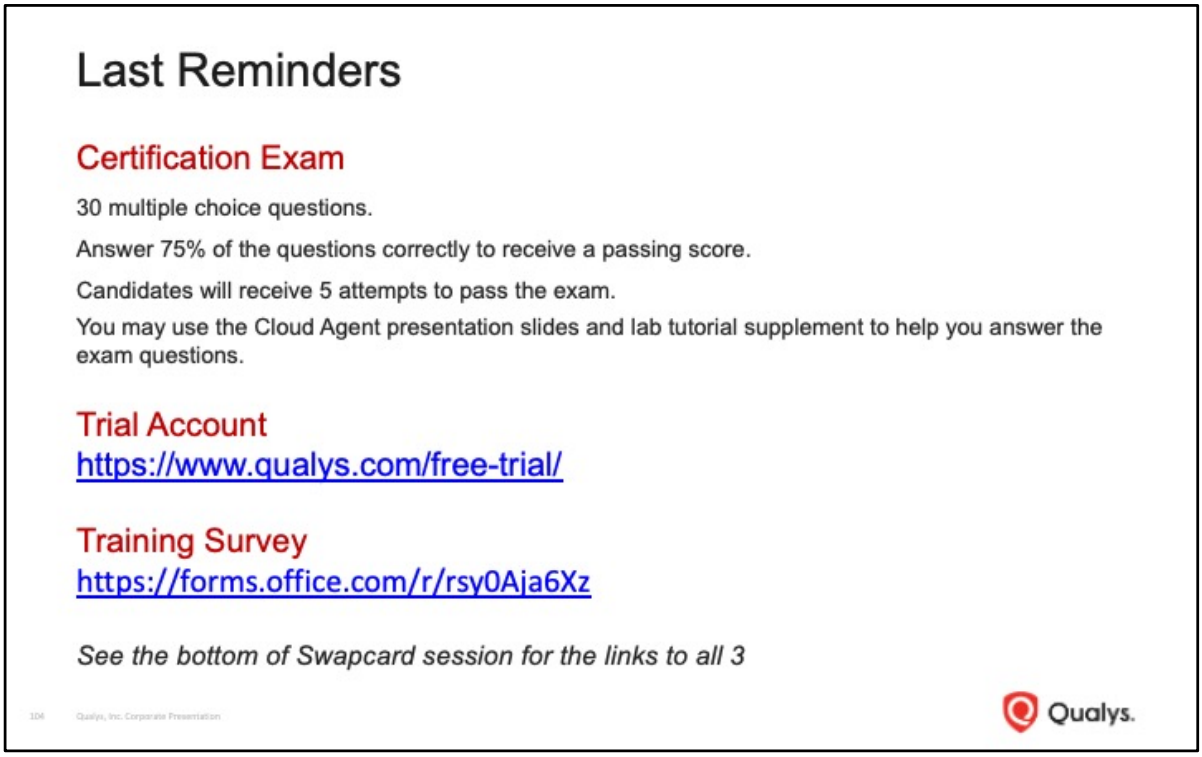



Agents can be uninstalled in bulk using the Cloud Agent API.




Purge Rules (provided in the AssetView application) will remove agent assets from your account, based upon various agent statuses and configurations:

- lastActivity
- lastCheckedIn
- activatedForModule
- agentActivationKey
- agentVersion
- configurationProfile




The link to enrol for the course and the certification exam is https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?&id=22511237821

Please consult the Lab Tutorial Supplement for information regarding registration for the Cloud Agent course certification exam.
*NOTE: We recommend that you take this certification exam at the earliest possible convenience.*

You can request a free Qualys limited trial account by submitting a request on this link https://www.qualys.com/free-trial/


Qualys.
Thank You
training@qualys.com
105
Qualys, Inc. Corporate Presentation