

# **Cloud Agent**

Lab Tutorial Supplement

### **Table of Contents**

CLOUD AGENT DEPLOYMENT	
AGENT ACTIVATION KEY	
Add a Static Tag	4
Application Module Support	4
Activation Key Limits	5
AGENT INSTALLATION COMPONENTS	
Command Line Installation	9
Validate CA Installation	
Locate Host ID	
View CA Log File (Log.txt)	
CA Log Analysis & Troubleshooting	
Cloud Agent Installation Guides	
AGENT PROXY CONFIGURATION	
TLS 1.2+ Requirement	
Windows Agent Proxy Configuration	
Linux Agent Proxy Configuration	
Cloud Agent Installation Guides	
Asset Details & Queries	
CONFIGURATION AND TUNING	
CLOUD AGENT CONFIGURATION PROFILE	
General Info	
Blackout Windows	
Agent Performance Settings	
Assign Hosts	
Agent Scan Merge	
VM, PC, and SCA Scan Intervals	
Scan On-Demand	
FIM and EDR	
РМ	
Configuration Profile Precedence	
Download Manifest	
ACTIVATE, DEACTIVATE & UNINSTALL AGENTS	
Activate & Deactivate Application Modules	
Uninstall Agents	
APPENDIX A: MAC OS AGENT INSTALLATION	
APPENDIX B: RPM-BASED AGENT INSTALLATION	
APPENDIX C: DEBIAN/UBUNTU AGENT INSTALLATION	
APPENDIX D: QUALYS TECHNICAL SUPPORT	

# **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**



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:



LAB 1 - http://ior.ad/7fyC

Edit the act	ivation key				
An activation I account. By de	key is used to install age efault this key is unlimite	nts. This provides and it allows you to	a way to grou add any num	ip ager	its and better manage your agents at any time.
ſitle	CA Lab Ac	tivation Key			
					Select   Create
	CA Lat	∞ 2	Add a "sta hosts de	itic" tag ployed	to label agent with this key.
Provision Ke	ey for these applicati	ons			
AI	Asset Inventory Activations managed	l by Al.		РМ	Patch Management 25 Activations Remaining
VM	Vulnerability Manage 14 Activations Remain	gement ining	0	PC	Policy Compliance 15 Activations Remaining
EDR	Endpoint Detection 10 Activations Rema	and Response	٥	FIM	File Integrity Monitoring 10 Activations Remaining
SCA	Secure Config Ass 15 Activations Rema	essment Ap	oplication mo activated at	dules s the time	selected in the key will be e of agent deployment.
🗆 Set limit	s 🚺				

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 (<u>https://www.qualys.com/docs/qualys-cloud-agent-getting-</u><u>started-guide.pdf</u>)

## **Activation Key Limits**

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

Set limits	
You can set limits for both are set, the key	more control over your activation keys - maximum number of agents or expiration date. When will expire when the first limit is reached.
Key limited by coun	t
Tell us the maximum	number of agents that can be installed using this key.
Maximum number:	5000
Key limited by date Allow installation of a	n 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:



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.

ve you	r key a name and a	dd tags to easily find age	nts installed using this key. We'll associa	ate the tags to the agent ho
tivatior	n Key			0
stalla	ition Requirem	ents		
	Windows (.exe)	x86-32/64	Microsoft Windows Client Microsoft Windows Server	Install instructions
۵	Linux (.rpm)	x64	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Enterprise Linux Amazon Linux Oracle Enterprise Linux	Install instructions
۵	Linux (.rpm)	ARM64	Red Hat Enterprise Linux CentOS Amazon Linux	Install instructions
0	Linux (.deb)	x64	Debian Ubuntu	Install instructions
0	Linux (.deb)	ARM64	Debian Ubuntu	Install instructions
Ć	Mac (.pkg)	x64	Apple macOS Apple OS X	Install instructions
AIX	AIX (.bff.gz)	Power5	IBM AIX	Install instructions
	BSD (tyz)	x64	FreeBSD	Install instructions

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	8
You are ready to install the agent.	
Current agent version : 4.2.0.8 Hash-SHA-256 : c29848099fcedce7b57f027514c9ecf5e3f4b8a8d79c983	33c00b4ea2c9a23b0c
Deploying in Azure Cloud	
Windows Installation Requirements	
Click here for the list of supported operation system versions.	
<ul> <li>To install the agent you must have local administrator privileges</li> </ul>	on your host.
<ul> <li>Your host must be able to reach the Qualys Cloud Platform or th 443.</li> </ul>	e Qualys Private Cloud Platform over HTTPS port
<ul> <li>Do you have a proxy? Learn more</li> </ul>	
Steps to Install the Windows Agent	
<b>Download the agent installer</b> (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 management tool. Click here to troubleshoot.	I run command, or use group policy or a systems
For agent version 4.3 and above, make sure to provide the WebSe install or upgrade the agent.	erviceUri parameter in the installation command to
	Press CTRL-C to
Copy and paste this command for installation:	сору
QualysCloudAgent.exe CustomerId={4058fe89-8caa-fcb6 ActivationId={dcf48885-316b-4230-b40d-a15c8e32db5a WebServiceUri=https://qagpublic.qg3.apps.qualys.com/C	5-8373-c2a56ffa1db9} } CloudAgent/ 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:





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.

Processes	Performance	App history	Startup	Users	Details	Services			
	~			56%	4	8%	73%	0%	
Name				CPU	Mem	ory	Disk	Network	
🔳 Mi	crosoft Skype			0%	2.7	MB	0 MB/s	0 Mbps	
💼 Mi	crosoft Store Ba	ackground Tas		0%	4.1	мв	0 MB/s	0 Mbps	
> 🔒 Mi	crosoft Windov	vs Search Inde		0%	3.8	мв	0 MB/s	0 Mbps	
> 🖬 Mi	crosoft® Volun	ne Shadow Co		0%	0.5	мв	0 MB/s	0 Mbps	
🛛 🧿 Qu	alys Cloud Age	ent		0.6%	3.4	мв	0.1 MB/s	0 Mbps	
RD	P Clipboard M	onitor		0%	1.6	мв	0 MB/s	0 Mbps	
🔳 RD	P Session Input	t Handler		0%	0.9	мв	0 MB/s	0 Mbps	
🔳 Ru	ntime Broker			0%	7.8	мв	0 MB/s	0 Mbps	
> 🖶 Sp	ooler SubSyster	n App		0%	1.4	мв	0 MB/s	0 Mbps	
📖 To	uch Keyboard a	ınd Handwriti.		0%	1.3	мв	0 MB/s	0 Mbps	
🔳 То	uch Keyboard a	ınd Handwriti.		0%	0.2	мв	0 MB/s	0 Mbps	

**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.

→ * ↑	« Loc	al Disk (C:) > ProgramData > Qualys	> QualysAgent	Search QualysAge	nt .
- Quick access		Name	Date modified	Туре	Size
		Manifests	3/24/2017 12:24 PM	File folder	
Desktop	R	SelfPatch	3/15/2017 5:23 PM	File folder	
Downloads	A	Archive.txt	3/27/2017 1:20 PM	Text Document	5,121 KI
Documents	A	Changelist.db	3/27/2017 3:01 PM	Data Base File	324 KI
Pictures	#	Config.db	3/27/2017 3:25 PM	Data Base File	6 KI
Music		Default_Config.db	3/13/2017 7:30 PM	Data Base File	6 KI
Videos		Log.txt	3/27/2017 3:25 PM	Text Document	410 KI
		Snapshot.db	3/27/2017 3:01 PM	Data Base File	12,816 KI
OneDrive	_				
This PC					

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)

Qualys. Community	Disc	ussions	Blog	Training	Docs	Suppor	
Search documentation	qualys.com/d	locum	enta	tion/	+		
		Ser	nsors				
		- CI	oud Age	ents			
		Or	Online Help				
Bloase refer to the insta	llation quido for	Ge	Getting Started Guide				
= Flease feler to the first	mation guide for	W	Windows Installation Guide				
your agent 03, for the r	nosi complete and	Lir	Linux Installation Guide				
up-to-date agent installa	ation and	Unix Installation Guide					
configuration steps.		Mac Installation Guide					
		Ga	teway Se	rvice User Gu	uide		
		BS	D Installa	tion Guide			
		Re	lease Not	tes			
		Tra	ining				
		Clo	oud Agen	t (CA) API			
Gealps, Int. Estiporate Preservation					00	ualys.	

# **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.

📑 Registry Editor X File Edit View Favorites Help 🗸 🛄 Computer Name Data Type HKEY CLASSES ROOT (Default) REG\_SZ (value not set) HKEY\_CURRENT\_USER ab URL REG\_SZ http://my-proxy1:8080;http://my-proxy2:8080 HKEY\_LOCAL\_MACHINE SOFTWARE V Qualys Proxy QualysAgent Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Qualys\Proxy

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://mypacfile-server/QualysAgent.pac

### **Linux Agent Proxy Configuration**

- 1. Create file /etc/sysconfig/qualys-cloud-agent (or /etc/default/qualys-cloudagent) 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.

<b>Qualys</b> . Community	Discuss	sions	Blog	Training	Docs	Support
<b>Q</b> Search documentation	qualys.com/do	cum	enta	tion/	-	
		Ser	sors			
		<ul> <li>Cloud Agents</li> </ul>				
		Online Help				
Diagon refer to the install	ation quido for	Getting Started Guide				
- Flease feler to the mistalia	atton guide for	Windows Installation Guide				
your agent OS, for the mo	ost complete and	Linux Installation Guide				
up-to-date proxy configur	ation details and	Unix Installation Guide				
examples.		Mac Installation Guide				
		Ga	teway Se	rvice User Gu	uide	
		BS	D Installa	tion Guide		
		Re	lease Not	es		
		Tra	ining			
		Clo	oud Agen	t (CA) API		
Quality, Int. Corporata Preservation					00	ualys.

# **Cloud Agent Installation Guides**

# **Asset Details & Queries**

It typically takes a few minutes for a new Agent Host to appear under the "Agents" tab.

-	Agent wanagen	Agents	Activation Keys	Configuration Profiles					
tions (1)	Install New Agent								\$
]	Agent Host	OS	Version	Last Activity	•	Configuration	Agent Modules	Tags	
l .	win10dfw239 192.168.1.239, fe	Microsoft Win	4.2.0.8	Scan Complete an hour ago		Initial Profile	AJ VM SCA	Cloud Agent CA Lab	
		View Asset Details Add Tags							
		Assign Config Profile Deactivate Agent							
		Uninstall Agent	PM or SA						

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:



\_

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.

Saved Searches - not lastCheckedIn > now-7d			not lastCh	eckedIn >	now-7d		
Action	ns (0) 🛩	Install New Agent	os	Version	Last Activity	•	Last Checked In
	<b>A</b>	WIN7-32BIT 10.0.1.227, 2600:8	Microsoft Win	4.1.0.67	Manifest Downloaded Jan 31, 2021 4:09:15 PM		Jan 31, 2021 4:09:15 PM
	<b>A</b>	ec2-54-185-121-19	Microsoft Win	4.2.0.8	Manifest Downloaded Jan 27, 2021 9:56:27 PM		Jan 27, 2021 9:56:27 PM

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.

Saved Searches 🔹				save save as undo	Search Actions *
last	<	type your sear	ch term here >		3 Search
lasiCheckedin lasiFullScan	Synt	ax Help CheckedIn			
lastinventory	Use a date range or specific date to define when agents last checked in to the platform.				
last LoggedOnUser	Examples Show findings with last check in within certain dates				
system.astBoot	lastCheckedIn: [2016-01-01 2016-01-10]				
vulnerabilities.lasiFound	Show findings with last check in starting 2015-10-01, ending 1 month ago				
	la	stCheckedIn: [2015-10-	-01 now-1M]		
	Show	v findings with last check in s	tarting 2 weeks ago, ending 1 se	cond ago	

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.

CyberSecurity Ass	et Man	agement	~		ŀ	HOME DASHBOARD	INVENTORY	TAGS NETWORK	RULES RESPONSES
Managed		Assets	Software						
		×	tags.name:"Cloud	agent"	tags.na	me:"Cloud	Agent"		
179		TOP HAP	RDWARE CATEGORIES	<b></b>				TOP OPERAT	ING SYSTEMS CATEGORIES
Total Assets		Q	Victorilized	Internet		Unidentified	Comparison		Windows
MANUFACTURER VMware Amazon Web Ser	56 34		Actions (0) V	Group Assets by 🗸	CRITICALITY	OPERATING SYSTEM		HADDWADE	LAST LISER
Google Microsoft Unknown	28 22 21	-	WIN-HB2C14TBNP 172.31.0.18,35.176.25	P 51,187	4	Microsoft Window Standard6.3 64-E	ws Server 201	Amazon Web Services Cloud Instance	Administrator

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.



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.

e Lun	Tum	help tips: On   Off	×
	Configure a profile for your agents		
>	Customize agent behavior by defining a configuration profile.	(*) REQUIRED	FIELD
>	Profile Name*		
>	CA Lab Configuration Profile	-	
>	Suspend data collection for VM, PC, SCA and Inventory for all agents using the second seco	his profile	
>	Prevent auto updating of the agent binaries		
>	Enter a description for this configuration profile.		
>	Description		
>	Cloud Agent Configuration Profile Lab Tutorial		
>			
	<b>&gt; &gt; &gt; &gt; &gt; &gt; &gt; &gt; &gt; &gt;</b>	Configure a profile for your agents         Customize agent behavior by defining a configuration profile.         Profile Name*         CA Lab Configuration Profile         Make this the default profile for the subscription         Suspend data collection for VM, PC, SCA and Inventory for all agents using the prevent auto updating of the agent binaries         Prevent auto updating of the agent binaries         Enter a description         Cloud Agent Configuration Profile Lab Tutorial	Configure a profile for your agents Customize agent behavior by defining a configuration profile. (*) REQUIRED  Profile Name*  CA Lab Configuration Profile Make this the default profile for the subscription Make this the default profile for the subscription Suspend data collection for VM, PC, SCA and Inventory for all agents using this profile Prevent auto updating of the agent binaries Enter a description Cloud Agent Configuration Profile Lab Tutorial Cloud Agent Configuration Profile Lab Tutorial

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



## **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.

Blackout windows									
You can create any numbe during any of these window	r of black vs.	out	windows	for thi	s cont	iguratio	on. The a	agent will	not operate
1. Blackout window								- Ren	nove window
Blackout days*		IN	Mon		ie (	Wed	🗆 Thu	🗆 Fri	🗆 Sat
Blackout time	From	Sele	ect	~	То	Select		~	

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).

Ste	p 3 of 8		Configure Agent Perform	ance		
1	General Info	~	These settings govern how a	in agent behaves, from how often i	t checks into the Qualys	
2	Blackout Windows	~	control CPU and network util	lization.	iddes performance setti	nga t
0	Performance		Performance			
	Assign Hosts		Select one of the performance settings or customize them.	ce levels below. Keep the default	Customize	6
Ĩ	Assign nosts		LOW	NORMAL		HIGH
5	VM Scan Interval		<u></u>			
6	PC Scan Interval					
7	FIM					
8	IOC					

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).

Delta Upload Interval*	1	sec
Interval an agent attempts to upload detected changes		
Chunk sizes for file fragment uploads*	4096	KB(64 - 10240)
This is the upload block size, and combined with the above Network throttle Tx, determines network utilization	-	

**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*	100	%(2 - 100)
Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times.		
LINUX/MAC SPECIFIC PARAMETERS (versions 1.6 and above)		
LINUX/MAC SPECIFIC PARAMETERS (versions 1.6 and above) CPU Throttle*	0	ms(0 - 1000

**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.

Ste	ep 4 of 9		Assign hosts to	this profile	
1 2 3 4 5	General Info Blackout Windows Performance Assign Hosts VM Scan Interval	1 1 1	By Asset Tag Cloud Agent hos have only 1 prot on the order in t Include hosts th CA Lab X	ts that have a corresponding tag will get le assigned. When multiple profiles matc le profiles list. It have Any v of the tags below.	this profile. Each Cloud Agent host or ch a host, we'll assign the profile base Seignt   Crea Select   Crea
7	FIM		(no tags selected		
8	IOC		By Name		
9	PM		We'll always use	this profile for the Cloud Agent hosts yo	u choose below.
			Agents hosts	Select items	O 💌 🍾 Sele

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.

Edit Mode		Configure Agent Scan Merge			
General Info	>	Enable Agent Scan Merge for this profile			
Blackout Windows	$\rightarrow$	Ports*	10001,10002,1000		
Performance	×		3,10004,10005		
Assign Hosts	×	Bind All	OFF		
Agent Scan Merge		On Premise Detection			
VM Scan Interval	5	IP Address(In Range)	0.0.0.0	/ 0	1
PC Scan Interval	>	Gateway	0.0.0.0	1	
SCA Scan Interval	$\rightarrow$	Subnet Mask	0.0.0.0		
FIM	×	DNS Suffix Regex			23
EDR	>	Note: To enable this feature, please of	rovide values to at least or	E.g ~(.~), rexample.com	*
PM	×	parameters. If you would like the mer	ging feature to always be e	nabled on all Agents with th	hi

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 enables this feature for all agent hosts.

Processes Performance Users Details	Services			
^ Name	<b>1%</b> CPU	32% Memory		
Apps (2)				^
> 🙀 Task Manager	0%	8.2 MB		
> 💽 Windows Command Processor	0%	0.5 MB		
Background processes (20)				
agentid-service	0%	4.9 MB		
> III Antimalware Service Executable	0%	100.2 MB		
🏷 Apache Commons Daemon Ser	0%	1.0 MB		
Application Frame Host	0%	4.1 MB		
둸 Google Crash Handler	0%	0.4 MB		
🐝 Google Crash Handler (32 bit)	0%	0.4 MB		
Host Process for Windows Tasks	0%	2.3 MB		
Host Process for Windows Tasks	0%	2.6 MB		
Java Update Checker (32 bit)	0%	2.6 MB		
Java Update Scheduler (32 bit)	0%	2.6 MB		~

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).

Admir	nistrator: Command Prompt				
C:\Users	\Administrator≻nets	tat -p tcp -ano			
Active C	connections				
Proto	Local Address	Foreign Address	State	PID	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	684	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	828	
TCP	0.0.0.0:10001	0.0.0.0:0	LISTENING	3380	
TWF	0.0.0.0.4/001	0.0.0.0.0	CT01CH1H0	-	
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	472	
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	564	
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	904	
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	728	
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	1932	
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	552	
TCD	0.0.0.0.40570	0.0.0.0.0	LISTENIAN	1940	

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.

Unique Asset Identifiers	agent installed on Windows and/or Unix hosts, to correlate the scan results of cloud agents or IP scans (authenticated/unauthenticated).
Asset Tracking & Data Merging >	The data merging option will allow you to decide how the data merging should happen for these scan results that uses agent correlation identifier. Note: For this feature to work, please make sure that Agent installed on Windows hosts has version 4.2 or later and Agent installed on linux hosts has version 3.1.0 or later. Please also enable 'Asset Scan Merge' option in configuration profile(s) through Cloud Agent > Agent tagget page.
	Accept Agent Correlation Identifier You agree to use agent correlation identifier.
	Decline Agent Correlation Identifier

When Qualys Scanner Appliances scan agent hosts (that have the Agent Correlation Identifier enabled), they return QID 48143 – Qualys Correlation ID Detected.

First Detected: 02	/03/2021 at 03:49:59 PM (GMT+0000)	Last Detected:	02/03/2021 at 07:1
QID:	48143		
Category:	Information gathering		
CVE ID:	-		
Vendor Reference	-		
Bugtraq ID:			
Service Modified:	12/15/2020		
User Modified:			
Edited:	No		
PCI Vuln:	No		
THREAT:			
Qualys correlation ID QID Detection Logic: This QID sends GET	is a unique value - a binary array of a spe (Unauthenticated) request to /correlation-id to retrieve correl	ecific size, which will be ation id.	e used to merge age

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 CpuLimit	<b>Type</b> REG_DWORD (decimal)	<b>Data</b> 2 - 100	Description Sets the CPU Limit (%) for the execution. Key is not required	HKEY_LOCAL_MACHINE SOFTWARE QualysAgent QualysAgent ScanOnDemand Inventory
			Default value is 100 if no value exists or the data is not valid.	CpuLimit ScanOnDemand ScanOnStartup
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.	Vulnerability CpuLimit ScanOnDemand ScanOnStartup PolicyCompliance CpuLimit
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.	ScanOnDemand ScanOnStartup UDC CpuLimit ScanOnDemand ScanOnStartup SCA CpuLimit

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.

ScanOnStartup

#### 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.

Actions	lew Profile Dra	ag profiles to change the order in which they will be applied
Order	*	Profile Name
1 (B)		CA Lab High Performance
2		Initial Profile (Default)

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 <u>data collection begins</u>. 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:



#### **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.

An activatio	on key is used to install agents. This provides a	way to group a	gents and better manage your
account. By	/ default this key is unlimited - it allows you to a	idd any number	of agents at any time.
nue	AWS Activation Key		Salast   Creata
	AWS		Select   Create
	AND A		
Provision	Key for these applications		
A	Asset Inventory Activations managed by AI.	PN	Patch Management 197 Activations Remaining
	Vulnerability Management 97 Activations Remaining	PC	Policy Compliance 97 Activations Remaining
ED	R Endpoint Detection and Response 97 Activations Remaining	FIN	File Integrity Monitoring 97 Activations Remaining
sc	A Secure Config Assessment 100 Activations Remaining		
🗌 Set lin	nits		
Annly	changes to all the existing agents		

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 Agent	8
🛕 Uninstall Agent?	
This step will remove the agent and revoke license(s) data for this agent will not be removed. You will need to clear the related data.	for all applications.Please note that any VM or PC to also purge that asset from the respective module
Cancel	Confirm

Uninstall agents in bulk using the CA Application Program Interface (API) or create Agent Purge Rules within the Qualys AssetView application.

	p 2 of 4		Rule Definition			
1	Rule Details	4	Add criteria to permanen	tly remove cloud based assets	(*)	REQUIRED F
2	Rule Definition	1	All matching assets will be pure	Jed		Ren
3	Purge Limits		Cloud Agent Based Fil	ter 🖊		
4	Review And Confin	n	Assets match all of the follo	wing conditions for		
				Select Operator. 👻		0
			lastActivity	OLDER THAN		
			- lastCheckedIn	IN LAST		

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.

Y	Quarys. Haining & Certificatio
	qualys.com/learning
	Login
	Please log in to the Qualys training site. First time users need to create an account.
	*Required Field *Username:
	*Password:
	Sign In
	Forget your password? Bequest a new 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=22 511237821

my nome+ cearrier	Information +								÷-
Course Catalog: Class D	etails								
Course: Qualys Cloud Agen	t - QSC 2021								Close Record
To see how a class below fits	into your sch	edule, click View N	Ay Class Schedule.						
CLASS DETAILS: CLOUD A	GENT - QSC 2	021							
Course Name:	Qualys Clou	d Agent - QSC 202	21						
Class Name:	Cloud Agent	t - QSC 2021							
Class Code:	2250729076	552021091712525	0						
Contact Name:	Vibhu Gupta	a ()							
Private Class:	Yes								
Maximum Class Capacity:	5000								
Class Cost:	\$0.00								
Session Name 🔺	Location	Classroom	Address 1	Address 2	City	State	Postal Code	Times	Instructor(s)
Session 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Tuesday, November 16, 2021 9:00 AM to 1:00 PM (America/Los_Angeles) (UTC -07:00)	Vibhu Gupta
								View My I	Enroll

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.

Qualys Cloud Agent - QSC 2021							Close Record
Progress: Not Attempted Status: Enrolled R	Jequired: No Duration: 4 hours						
Notice: Enrollment Successful You have been successfully enrolled in t	the class.						
							Drop Class Drop Course
- Activities							
Class Sessions							
Class Name	Date				Location	Classroom	Instructor(s)
Cloud Agent - QSC 2021	Tuesday, November 16, 2021 9:00 AM	d to 1:00 PM (Americ	a/Los_Angeles) (UTC -07:00)		N/A	N/A	Vibhu Gupta
To access a learning activity, select the activi	ity name and click Launch or Open.						
Activity Name 🛓	Туре	Score	Progress	Last Accessed	Time Taken	Attempts	Action
Cloud Agent Lab Tutorial Supplement	🛅 pdf	N/A	N/A	9/17/2021 12:11:17 PM	N/A	2	Open
Cloud Agent Slides for QSC 2021	[T] pdf	N/A	N/A	N/A	N/A	0	Open
Qualys Cloud Agent Exam 2.0	Actual Test	N/A	Not Attempted	N/A	N/A	N/A	Launch

Each candidate is provided five attempts to pass the exam.

Qualys. Trainin	ng & Certification			
My Home   Learner Information	1*			۵
Qualys Cloud Agent - QSC 202 Progress: Completed Status: Enrolled Ro	11 aquired: No Duration: 4 hours			Close Record
- Activities				Print Certificate
Class Sessions				
Class Name	Date	Location	Classroom	Instructor(s)
Cloud Agent - QSC 2021	Tuesday, November 16, 2021 9:00 AM to 1:00 PM (America/Los_Angeles) (UTC -07:00)	N/A	N/A	Vibhu Gupta
To access a learning activity, select the ac	thirty name and click Launch or Open.			

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 - <u>https://forms.office.com/r/rsy0Aja6Xz</u>

# **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 툑 "Mac (.pkg)" option.

Install Agents	8
You are ready to install the agent.	
Current agent version : 1.6.1.26 Hash-SHA-256 : 00395e343a31dd2bdf4074040b571cf3e1b77342019c22a3d6	ac587e1a860292
Mac (.pkg) Installation Requirements	
Click here for the list of supported operation system versions.	
<ul> <li>Your host must be able to reach the Qualys Cloud Platform or the Qua Platform over HTTPS port 443.</li> </ul>	alys Private Cloud
<ul> <li>To install the agent you must have 1) root privileges, 2) non-root with 3) non-root with sufficient privileges (VM only).</li> </ul>	Sudo root delegation, or
Do you have a proxy? Learn more	
Steps to Install the Mac Agent	
Download the agent installer (file size 3.5 MB) File will be saved to your downloads area, as defined by your local syste	em.
Copy <b>qualys-cloud-agent.x86_64.pkg</b> to the host you want to monitor Click here to troubleshoot.	and run commands.
Copy and paste this command for installation (sudo access required):	Press Cmnd + C to copy
sudo installer -pkg ./qualys-cloud-agent.x86_64.pkg -target / sudo bash -c " if [[ -f /usr/local/qualys/cloud-agent/bin/qualys ]]; then /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent ActivationId=	s-cloud-agent.sh .sh
Close	ack Download .pkg

- 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 왿 "Linux (.rpm)" option.

Install Agents
You are ready to install the agent.
Current agent version : 2.0.2.79 Hash-SHA-256 : 89001da9caed3736e157df99e58a62ad20212cc5db51a4c1822898b53d6f7f8a
Deploying in Azure Cloud
Linux (.rpm) Installation Requirements
Click here for the list of supported operation system versions.
Your host must be able to reach the Qualys Cloud Platform or the Qualys Private Cloud Platform over HTTPS port 443.
<ul> <li>To install the agent you must have 1) root privileges, 2) non-root with Sudo root delegation, or 3) non-root with sufficient privileges (VM only).</li> </ul>
Do you have a proxy? Learn more
Steps to Install the Linux Agent
Download the agent installer (file size 3.5 MB) File will be saved to your downloads area, as defined by your local system.
Copy qualys-cloud-agent-2.0.2.79.rpm to the host you want to monitor and run commands. Click here to troubleshoot.
Copy and paste this command for installation (sudo access required):
sudo rpm -ivh qualys-cloud-agent-2.0.2.79.rpm sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId= CustomerId=
Close Back Download .rpm

- 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).



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 6987	? ?	Type "ps -e" from the command line.
6988 8404	pts/1 pts/2	00:00:00 bash 00:00:00 gualvs-cloud-ag
8420	pts/1	00:00:00 ps
24375 26814	?	00:00:14 java 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 <sup>O</sup> "Linux (.deb)" option.

Install Agents	8
You are ready to install the agent.	
Current agent version: 2.1.0.91 Hash-SHA-256:3979670e28b702242017a3ed362c9d9af224459dfabcb2de8e	c8d3a1ed785936
Linux (.deb) Installation Requirements	
Click here for the list of supported operation system versions.	
<ul> <li>Your host must be able to reach the Qualys Cloud Platform or the Qu Platform over HTTPS port 443.</li> </ul>	alys Private Cloud
<ul> <li>To install the agent you must have 1) root privileges, 2) non-root with 3) non-root with sufficient privileges (VM only).</li> </ul>	Sudo root delegation, or
Do you have a proxy? Learn more	
Steps to Install the Linux Agent	
Download the agent installer (file size 3.5 MB) File will be saved to your downloads area, as defined by your local syste	em.
Copy qualys-cloud-agent-2.1.0.91.deb to the host you want to monitor Click here to troubleshoot.	and run commands.
Copy and paste this command for installation (sudo access required):	Press CTRL-C to copy
sudo dpkginstall qualys-cloud-agent-2.1.0.91.deb sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=e2bce151-4a3f-4012-b27e-3d156d4ed8ba CustomerId=b48c8fb6-6b92-d0c7-804e-1e20fe1af1ea	
Close	Download .deb

- 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-	-ul	bu1604:	~\$ 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-rr	1	ubuntu	ubuntu	220	Aug	31	2015	.bash logout
-rw-rr	1	ubuntu	ubuntu	3771	Aug	31	2015	.bashrc
drwx	2	ubuntu	ubuntu	4096	Aug	7	21:39	.cache
-rw-rr	1	ubuntu	ubuntu	655	May	16	2017	.profile
-rw-rr	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-rr	1	ubuntu	ubuntu	0	Aug	7	21:41	.sudo as admin successful
-rw	1	root	root	2935	Aug	29	15:12	.viminfo
ubuntu@ec2-	-ul	bu1604:	~\$					

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.