



Qualys Gateway Service

User Guide

Version 2.1.0

July 27, 2022

Copyright 2021-22 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



Table of Contents

About this Guide	4
About Qualys	4
Qualys Support	4
Overview	5
Virtualization Server Requirements and Virtual Machine File Formats	6
Qualys Gateway Service User Interface Module	9
Qualys Gateway Service Module User Interface	15
Virtual Appliance Local Configuration	18
Configuration Screens	19
Appendix - Things to Remember	33

About this Guide

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Overview

Qualys Gateway Service (QGS) is a packaged virtual appliance developed by Qualys that provides proxy services for Qualys Cloud Agent deployments that require proxy connectivity to connect agents to the Qualys Cloud Platforms.

Qualys Gateway Service is managed using a new module user interface on the Qualys platform. From this interface, one can create, register, monitor, and manage QGS virtual appliance deployments.

The QGS virtual appliance is separate and different from the virtual scanner appliance that is used for Vulnerability Management and Policy Compliance scanning. The QGS virtual appliance only provides proxy services for Cloud Agent deployments.

The following features and capabilities are available in QGS virtual appliance:

- A virtual appliance image downloaded, registered, and managed from the Qualys platform user interface using the **QGS** module
- Support for any Cloud Agent version that supports HTTP/HTTPS proxy (all agents since 2016)
- Explicit forward proxy
- SSL/TLS pass-through bypass
- Can be deployed in High-Availability failover using external 3rd party load balancers
- Connection Security – the QGS proxy only will provide connections to the Qualys platform from where it is registered. It is not possible to use QGS to proxy connections to any other destination.
- Shared Platform support (Private Cloud Platforms require coordination with Qualys Operations)
- **Enabling Allowed Domains:** We have added an option which will help you to allow traffic for required domains.
 - Default Domains Allowed: qualys.eu, qualys.ca, qualys.com, qualys.in

Virtualization Server Requirements and Virtual Machine File Formats

Virtual Server	Supported Versions	File Format
VMware vSphere / ESXi	5.5, 6.0, 6.5, 6.7, 7.0	VMDK, OVA, OVF
Microsoft Hyper-V	2012, 2012 R2, 2016	VHD

Virtual Machine Configuration

- 2 vCPUs
- 16 GB RAM minimum
- 30 GB Disk minimum (For QGS primary disk only)
 - For Patch Mode, a second disk of 250GB minimum is required.
- One network adapter
 - IP address configured with a Default gateway
 - QGS Proxy listening port for Cloud Agents: 1080 (can be changed)
 - QGS Cache listening port for Cloud Agent: 8080 (can be changed)
- Available support to connect QGS to upstream proxy server, if required
 - IP/DNS name and port of upstream proxy
 - Optional username/password proxy credentials
 - Support for upstream proxy domain-based filtering
 - This is a method for adding the static host to IP mapping to the QGS appliance. Similar to an entry in the/etc/hosts file, this is a way to add a FQDN<-->IP mapping to the QGS service.

Network Configuration

QGS requires connectivity to five (5) URLs on the Qualys Platform for full functionality. The appropriate network routing, firewall rules, and upstream proxy configurations (if used) must be configured correctly to allow QGS to connect to these URLs.

- One URL is for Cloud Agents to connect through QGS to the Qualys Platform
- Three URLs are for QGS to connect to Qualys Platform for management functions
- One URL is for operating system updates as this appliance is based on Flatcar Linux
- For any Windows Cloud Agents where falling back to a direct connection to the platform is required, those Cloud Agents will require the relevant qagpublic URL to be enabled in a separate firewall rule

Platform	Cloud Agent	Qualys Gateway Service
US 1	qagpublic.qg1.apps.qualys.com	qagpublic.qg1.apps.qualys.com camspublic.qg1.apps.qualys.com camspm.qg1.apps.qualys.com camsrepo.qg1.apps.qualys.com update.release.flatcar-linux.net
US 2	qagpublic.qg2.apps.qualys.com	qagpublic.qg2.apps.qualys.com camspublic.qg2.apps.qualys.com camspm.qg2.apps.qualys.com camsrepo.qg2.apps.qualys.com update.release.flatcar-linux.net
US 3	qagpublic.qg3.apps.qualys.com	qagpublic.qg3.apps.qualys.com camspublic.qg3.apps.qualys.com camspm.qg3.apps.qualys.com camsrepo.qg3.apps.qualys.com update.release.flatcar-linux.net
US 4	qagpublic.qg4.apps.qualys.com	qagpublic.qg4.apps.qualys.com camspublic.qg4.apps.qualys.com camspm.qg4.apps.qualys.com camsrepo.qg4.apps.qualys.com update.release.flatcar-linux.net
EU 1	qagpublic.qg1.apps.qualys.eu	qagpublic.qg1.apps.qualys.eu camspublic.qg1.apps.qualys.eu camspm.qg1.apps.qualys.eu camsrepo.qg1.apps.qualys.eu update.release.flatcar-linux.net
EU 2	qagpublic.qg2.apps.qualys.eu	qagpublic.qg2.apps.qualys.eu camspublic.qg2.apps.qualys.eu camspm.qg2.apps.qualys.eu camsrepo.qg2.apps.qualys.eu update.release.flatcar-linux.net

Platform	Cloud Agent	Qualys Gateway Service
IN 1	qagpublic.qg1.apps.qualys.in	qagpublic.qg1.apps.qualys.in camspublic.qg1.apps.qualys.in camspm.qg1.apps.qualys.in camsrepo.qg1.apps.qualys.in update.release.flatcar-linux.net
CA 1	qagpublic.qg1.apps.qualys.ca	qagpublic.qg1.apps.qualys.ca camspublic.qg1.apps.qualys.ca camspm.qg1.apps.qualys.ca camsrepo.qg1.apps.qualys.ca update.release.flatcar-linux.net
AE 1	qagpublic.qg1.apps.qualys.ae	qagpublic.qg1.apps.qualys.ae camspublic.qg1.apps.qualys.ae camspm.qg1.apps.qualys.ae camsrepo.qg1.apps.qualys.ae update.release.flatcar-linux.net
UK1	qagpublic.qg1.apps.qualys.co.uk	qagpublic.qg1.apps.qualys.co.uk camspublic.qg1.apps.qualys.co.uk camspm.qg1.apps.qualys.co.uk camsrepo.qg1.apps.qualys.co.uk update.release.flatcar-linux.net
AU 1	qagpublic.qg1.apps.qualys.com.au	qagpublic.qg1.apps.qualys.com.au camspublic.qg1.apps.qualys.com.au camspm.qg1.apps.qualys.com.au camsrepo.qg1.apps.qualys.com.au update.release.flatcar-linux.net

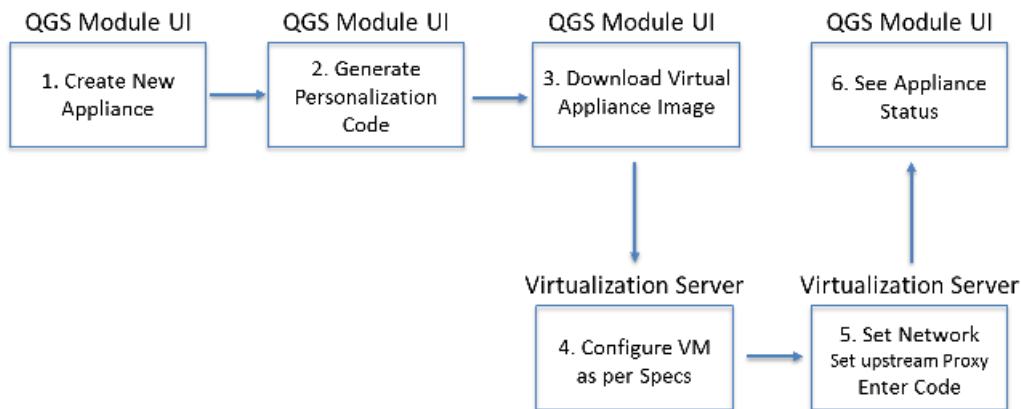
Qualys Gateway Service User Interface Module

Qualys Gateway Service has a user interface module on the Qualys Platform. Customers with purchased or trial accounts see the QGS module in the module picker.

Use the QGS UI to create, configure, monitor, disable, and delete QGS appliances deployed in your organization.



In order to deploy a QGS virtual appliance, log into the Qualys Platform, select the QGS module, and follow the steps below. By default, QGS is configured as a proxy server only when deployed. Cache Mode and Patch Cache Mode are additional explicit configuration options to be performed to enable this functionality.



- 1) Create a New Appliance. Give the appliance a name and enter a location, if desired.
- 2) Generate a Personalization Code. Similar to the virtual scanner, you will need to enter this Personalization Code in the QGS virtual appliance local user interface to fully configure the appliance.
- 3) Select Download Image and chose the appropriate file format for your environment
- 4) Download/copy the virtual appliance image to your virtualization server.

- Configure the Virtual Machine properties following the specified resources.

Important: Enabling Patch Mode so that QGS can cache patches requires a second virtual hard drive to be added to the virtual appliance before Patch Mode can be enabled.

- A minimum disk size of 250GB is required.
- Only a single secondary virtual hard drive will be recognized as available capacity; extending the second QGS volume via multiple virtual hard drives is not supported.

5) Start the image.

Note: Console access to the running image is required to configure the appliance.

6) Use the console-based user interface to configure the virtual appliance for networking, DNS, time server, and optional upstream proxy configuration (see instructions below).

7) Validate that the appliance can successfully communicate with the Qualys Platform.

8) Register the Appliance with the Qualys Platform.

The QGS Appliance supports a Diagnostic mode to help accelerate Qualys Customer Support troubleshooting and problem resolution, primarily for initial network setup and registration issues. Refer to the section below on Diagnostics Mode.

Changing the Proxy Port

After successful appliance deployment and registration, you can change the proxy port from default 1080 to any allowable port number.

- 1) Use the Quick Action menu to select Configuration (hover over the appliance name in the appliance list until the Quick Action down-arrow menu appears)
- 2) In the first configuration step (Proxy), enter the new proxy port.
- 3) Click **Next** to the menu, then **Finish** to save the configuration.

The screenshot shows a web interface for configuring the proxy port. At the top, there is a blue header bar with a back arrow and the word 'Configuration'. Below this, on the left, is a sidebar titled 'STEPS 1/3' with three steps: '1 Proxy' (highlighted with a blue circle), '2 Modes', and '3 TLS Protocols'. The main content area is titled 'Configure the Proxy Port' and includes the subtitle 'Cloud Agents connects to Qualys Cloud Platform using proxy port while using Qualys Gateway Service'. There is a text input field labeled 'Proxy Port' with the value '1080'. Below the input field, a note states: 'Note: Valid Port values are 1 – 65535 (integers only), excluding 22, 23, 2379, 2380, 4001, 5514, 7001, 48081, 48082, 48083, 48084, 48085, 48086.' At the bottom of the form, there are two buttons: 'Cancel' and 'Next'.

Note: Valid Port values are 1 – 65535 (integers only), excluding 22, 23, 2379, 2380, 4001, 5514, 7001, 48081, 48082, 48083, 48084, 48085, 48086.

On the next appliance check-in, the appliance will download the configuration and use the new proxy port.

Cache Mode and Patch Mode Configuration

Cache Mode is an optional feature used to optimize the download network bandwidth used by Cloud Agents whereby the QGS appliance caches downloaded Cloud Agent artifacts (installers for platform-initiated upgrades and manifest files).

Files downloaded by the first-connecting agent will be cached on the QGS appliance to be served to any subsequent configured agents requesting the same content. This will save Internet download bandwidth from the Qualys cloud platform to the on-premise network as only one copy of unique files will be downloaded. For environments with a large number of Cloud Agents deployed, this can save a significant amount of download bandwidth.

File Type	Interval	Number of Agents	Bandwidth without Caching	Bandwidth with Caching
VM Manifest	Daily	1,000	2 GB	2 MB
VM Manifest	Daily	5,000	10 GB	2 MB
VM Manifest	Daily	10,000	20 GB	2 MB
VM Manifest	Daily	25,000	50 GB	2 MB

Patch Mode extends the caching capability to cache patch files for Cloud Agents activated with the Qualys Patch Management application. Similar to Cache Mode where the gateway appliance caches the downloaded Cloud Agent artifacts, Patch Mode will cache the patch files downloaded by the first requesting Cloud Agent in order to serve patch files locally to subsequent download request. Patch Mode uses the same port and connection as Cache Mode.

Note: When Patch Mode is enabled, the default Connection Security that only allows outbound connections from the gateway appliance to Qualys platform domains is disabled. Cloud Agents with Patch Management application need to download patch files from the software vendor's website thus the gateway appliance allows for connections to any Internet resource. In Patch Mode, Connection Security is configured to only allow client connections from Cloud Agent clients as an additional protection method.

Cache Mode and Patch Mode are not enabled by default. Additional configuration is required to enable caching and patch file caching, both on the gateway appliance itself (using the QGS module UI) and on the host that runs the Cloud Agent.

Qualys Gateway Appliance Configuration

To enable Cache Mode or Patch Cache Mode on an existing QGS appliance:

- 1) For a specific appliance, use the Quick Action menu to select Configuration (hover over the appliance name in the appliance list until the Quick Action menu appears)
- 2) Click **Next** through the menu until **Caching Modes**
- 3) To enable Cache Mode, toggle the On/Off slider to **On**
- 4) The default cache port is **8080**. You may accept or change the cache port to an allowable port number.

Note: Valid Port values are 1 – 65535 (integers only), excluding 22, 23, 2379, 2380, 4001, 5514, 7001, 48081, 48082, 48083, 48084, 48085, 48086.

- 5) To enable Allowed Domains, toggle the On/Off slider to **On**

Allowed Domains: This option will allow traffic to required domains. You can add the domain names manually.

Default Domains Allowed: qualys.eu, qualys.ca, qualys.com, qualys.in

Note: While adding domains in the allowed domain section you should not add a prefix like **http(s)://www**. For instance, if you want to allow traffic to Microsoft then you should enter only microsoft.com and not https://www.microsoft.com

← Configuration

STEPS 2/3

- 1 Proxy
- 2 Modes
- 3 TLS Protocols

Configure Modes

Cache Mode

Enable Cache Mode to cache Cloud Agent artifacts including version installers and manifests. Cache port is used when Cache Mode is enabled

Requires Cache Certificates to be installed on all Cloud Agent assets

☒

Cache Port

8080

Note: Valid Port values are 1 – 65535 (integers only), excluding 22, 23, 2379, 2380, 4001, 5514, 7001, 48081, 48082, 48083, 48084, 48085, 48086.

Allowed Domains

Enable to allow the traffic to required domains

☒

Default Domains Allowed: qualys.eu, qualys.ca, qualys.com, qualys.in

Enter domain without 'www' prefix. You can add maximum 10 domains

Type domain name here

☐ Actions (0)

DOMAINS	ACTIONS
hetzner.de	

PM Patch Mode

Enable Patch Mode to cache patch files when using Patch Management app for Cloud Agent. Patch Mode uses the Cache Mode port configuration.

Note: A second disk with required minimum free disk space must be attached to the virtual appliance first. Patch Mode can not enabled if the disk is not attached.

☒

6) To enable Patch Mode, toggle the On/Off slider to **On**

Note: A second disk with required minimum free disk space must be attached to the virtual appliance first. Patch Mode can not be enabled if the disk is not attached.

7) Click **Next** through the menu until **TLS Protocols**

8) Select the Minimum TLS Protocol Version allowed for agent connections. To support older operating systems that only support TLS, select TLS 1.0 as the minimum protocol version. (Default setting is TLS 1.2 and higher.)

The screenshot shows the 'Configuration' screen with a blue header. On the left, a sidebar indicates 'STEPS 3/3' with three steps: 1 Proxy, 2 Modes, and 3 TLS Protocols (the current step). The main content area is titled 'TLS Protocols' and contains the text: 'Allow Cloud Agent connection to the gateway on enabled protocols. (Connections from the gateway to Qualys platform always only use the highest TLS protocol available and is not configurable.)'. Below this, there is a dropdown menu labeled 'Minimum TLS Protocol Version' with 'TLS 1.0' selected. At the bottom of the main area are three buttons: 'Cancel', 'Previous', and 'Finish'.

Note: To enable this mode, a second virtual disk drive, minimum capacity 250 GB, is required to be added to the virtual appliance prior to enabling Patch Mode.

Cloud Agent Configuration

Refer to the Cloud Agent Install Guide to know more about each supported operating system for the appropriate proxy configuration and certificate installation instructions.

Configure Cloud Agents to use the IP or DNS name of the QGS as the agent's proxy is similar to any other proxy server configuration.

- For Cloud Agent for Windows v3.1, or higher / Cloud Agent for Linux, AIX & Mac v2.5, or higher:

- Cloud Agent supports up to five (5) proxy servers or QGS appliances (semi-colon separated) and uses them for connection in the order defined.
- If the agent can't connect to the proxy server, the agent will try to connect to the next one in the defined list.
- Once all listed proxy servers or QGS appliances have been tried, Cloud Agent will fall back to attempting a direct connection, if this is supported by network routing and firewalls.
- Proxy server or QGS appliances can be aliased using DNS aliases or abstracted via Network Load Balancer Virtual FQDNs/IPs.

If using QGS appliance(s) behind one or more load balancers, define a compound keepalive configuration that is checking the availability of both QGS proxy + cache ports, periodically, in each case, and marking any QGS appliance that fails the keepalive check as unavailable.

- QGS appliances can be nested to provide two layers of proxy communication:
 - The QGS immediately upstream from the Cloud Agent connection can be in Proxy, Cache, or Patch mode.
 - The second QGS layer must be in Proxy mode only.
 - The second QGS layer sizing must anticipate the overall number of agent communications that need to navigate this second layer and connect to the platform.
 - In Patch Mode, QGS behaves as an open proxy, with no content or category filtering, so there should always be a general-purpose proxy server, suitable for internet browsing, with the appropriate filters, upstream from QGS.

Cloud Agent Cache Mode and Patch Mode Configuration

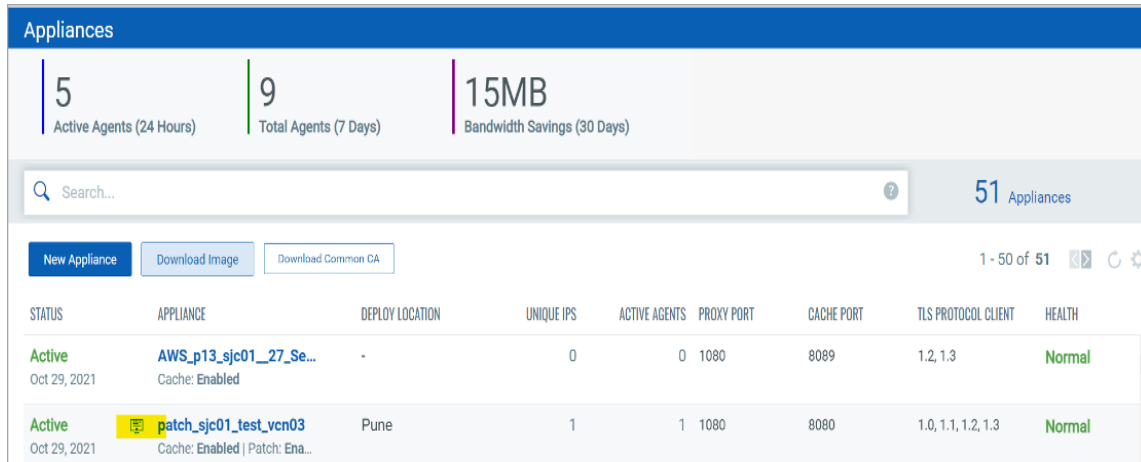
Cloud Agents deployed in Cache and Patch Mode require the public certificate of each QGS appliance installed on the host that runs the Cloud Agent.

There are two certificate deployment options available in the QGS User Interface:

- 1) Certificate File in PEM file format for any operating system
 - Use any supported software distribution tool to deploy the certificate PEM to the host certificate store
- 2) MSI Certificate File installer for Windows operating systems
 - Use any supported software distribution tool (SCCM, GPO, BigFix, etc.) to deploy the certificate by installing the Win.MSI file
 - Install the certificate manually on a single host


```
C:\>msiexec -I <location_to_file\WIN.msi
```

Qualys Gateway Service Module User Interface



The Activity Summary widgets provide aggregate activity information for all QGS appliances in the subscription. Active Agents and Total Agents count the number unique agent IPs connecting through all appliances. Bandwidth Savings is calculated in cache mode.

- **Status:** This column shows the current status of your appliance. Appliances with common CA certificate enabled will be shown an icon (Highlighted) on the appliance list page.

- **Unique IPs:** This column shows the count of unique IPs which have communicated through the QGS appliance proxy port during the last 60 minutes.

- **Active Agents:** This column shows the number of active agents which have communicated via the QGS appliance cache port during the last 60 minutes, with QGS and Cloud Agent configured to use **Cache** mode.

In **Proxy** mode, you'll see only unique IPs count on QGSUI, while in **Cache** mode you'll see count of active agent and unique IPs on QGSUI.

Create New Appliance / Generate Personalization Code / Use Common Certificate

New Appliance

← Create Appliance

Registration

Enter Appliance Name (Max 100 characters)

Deployment Location

Deployment Location (Max 255 characters)

Personalization Code
Generate the personalization code and keep it handy to register the appliance once you download the image.

Generate Code Copy

Advanced Settings

☒ **Use Common Certificate**
Use a common certificate while registering the appliance. We recommend using the common certificate for all appliances.

Cancel Save

The appliance can be created with a Common CA certificate enabled. It can help you to deploy a single certificate across all the cloud agents meant for the particular appliance.

If you want to use a common certificate while registering the appliance, then click **Use Common Certificate** checkbox.

Note: We recommend to use the Common CA certificate for all the appliances.

View List of Appliances and their Status

Appliances

5 Active Agents (24 Hours) | 9 Total Agents (7 Days) | 15MB Bandwidth Savings (30 Days)

Search... 51 Appliances

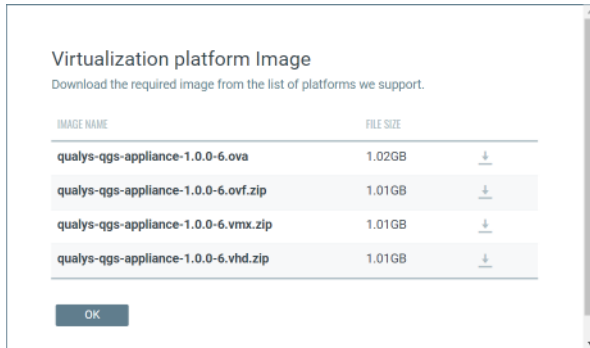
New Appliance Download Image Download Common CA 1 - 50 of 51

STATUS	APPLIANCE	DEPLOY LOCATION	UNIQUE IPS	ACTIVE AGENTS	PROXY PORT	CACHE PORT	TLS PROTOCOL CLIENT	HEALTH
Active Oct 29, 2021	AWS_p13_sjc01_27_Se... Cache: Enabled	-	0	0	1080	8089	1.2, 1.3	Normal
Active Oct 29, 2021	patch_sjc01_test_vcn03 Cache: Enabled Patch: Ena...	Pune	1	1	1080	8080	1.0, 1.1, 1.2, 1.3	Normal

A single Subscription certificate will be available instead of appliance specific certificate on the appliance list if appliances are registered with the common CA certificate option.

Appliances with common CA certificate enabled will be shown an icon (Highlighted) on the appliance list page.

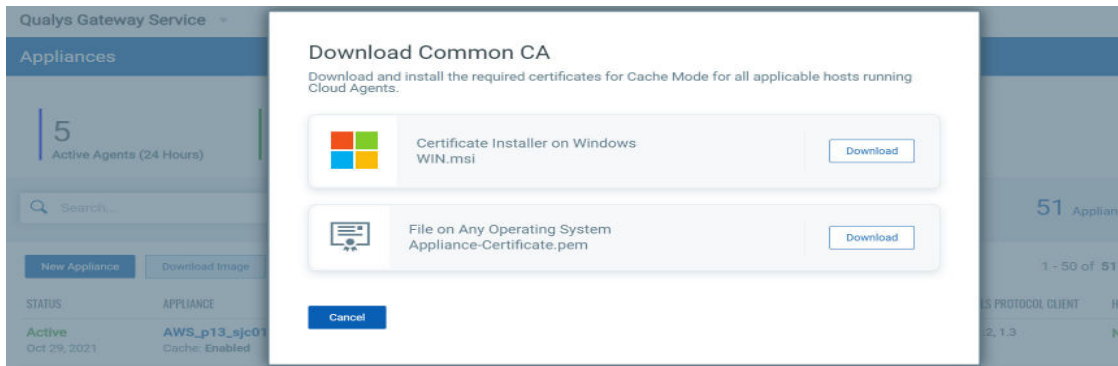
Download Image of the Virtual Appliance



Download Common CA

You can download the common CA certificate from the appliance details page or the appliance list page.

Note: To download the common CA Certificate, you must create and register a new appliance with the common CA certificate option enabled. After registering the appliance with a common CA certificate, it takes about 15 to 20 minutes to generate the common CA certificate.



After Successful Setup and Registration, the Appliance has Active Status

Appliances

5

Active Agents (24 Hours)

9

Total Agents (7 Days)

15MB

Bandwidth Savings (30 Days)

Search...

?

51 Appliances

New Appliance

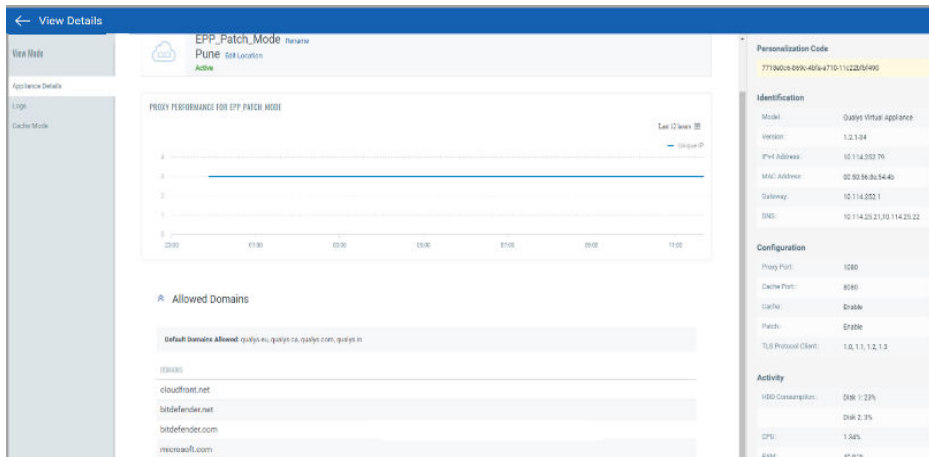
Download Image

Download Common CA

1 - 50 of 51

STATUS	APPLIANCE	DEPLOY LOCATION	UNIQUE IPS	ACTIVE AGENTS	PROXY PORT	CACHE PORT	TLS PROTOCOL CLIENT	HEALTH
Active Oct 29, 2021	AWS_p13_sjc01__27_Se... Cache: Enabled	-	0	0	1080	8089	1.2, 1.3	Normal
Active Oct 29, 2021	<div><div></div>patch_sjc01_test_vcn03 Cache: Enabled Patch: Ena...</div>	Pune	1	1	1080	8080	1.0, 1.1, 1.2, 1.3	Normal

View Details, Stats, and Logs of an Active Appliance



The Performance graph shows connection counts by unique agent IP addresses over the time period selected.

Allowed Domains: This option displays your allowed domain's information.

Virtual Appliance Local Configuration

The Qualys Gateway Service virtual appliance utilizes a text-based user interface available from the appliance console to configure, set networking, view status, perform diagnostics, and reset the appliance.

Local Configuration Menu Structure

- ❖ Registration
- ❖ System
 - Network
 - First
 - DNS
 - Proxy
 - Time
- ❖ Info
- ❖ Diagnostics
 - Containers
 - Images
 - Units
 - Logs
 - Stats
- ❖ Commands
 - Ping
 - Reboot
 - Shutdown
 - Reset

Configuration Screens

Next we'll document the screens used to configure & manage the Qualys Gateway Service.

QGS virtual appliance starting up

```

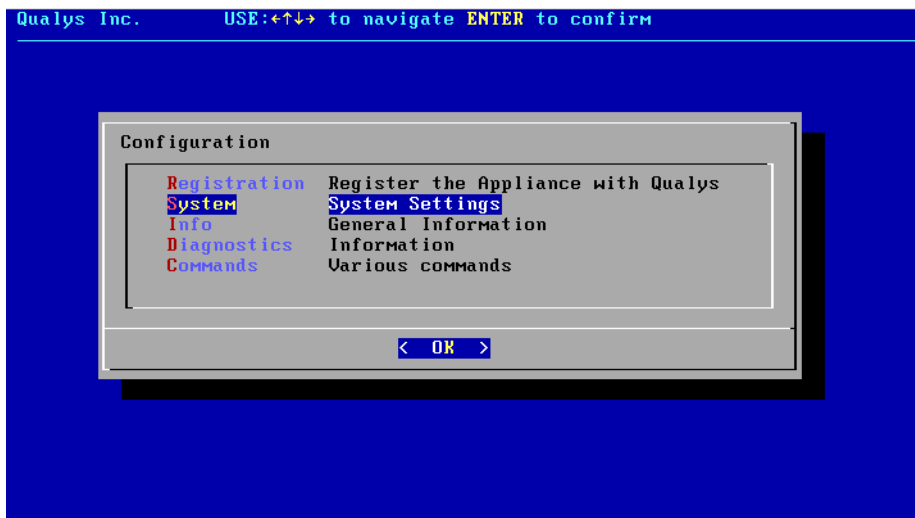
11.458732] SELinux: Class iucv_socket not defined in policy.
11.458780] SELinux: Class rxrpc_socket not defined in policy.
11.458827] SELinux: Class isdn_socket not defined in policy.
11.458873] SELinux: Class phonet_socket not defined in policy.
11.458921] SELinux: Class ieee802154_socket not defined in policy.
11.458971] SELinux: Class caif_socket not defined in policy.
11.459019] SELinux: Class alg_socket not defined in policy.
11.459065] SELinux: Class nfc_socket not defined in policy.
11.459295] SELinux: Class vsock_socket not defined in policy.
11.459344] SELinux: Class kcm_socket not defined in policy.
11.459391] SELinux: Class qipcrtr_socket not defined in policy.
11.459440] SELinux: Class smc_socket not defined in policy.
11.459486] SELinux: Class infiniband_pkey not defined in policy.
11.459536] SELinux: Class infiniband_endpoint not defined in policy.
11.459586] SELinux: the above unknown classes and permissions will be allowe

11.459655] SELinux: policy capability network_peer_controls=1
11.459715] SELinux: policy capability open_perms=1
11.459757] SELinux: policy capability extended_socket_class=0
11.459804] SELinux: policy capability always_check_network=0
11.459851] SELinux: policy capability cgroup_seclabel=0
11.459896] SELinux: policy capability nnp_nosuid_transition=0
11.486879] systemd[1]: Successfully loaded SELinux policy in 94.115ms.
11.528438] systemd[1]: Relabelled /dev, /run and /sys/fs/cgroup in 9.065ms.

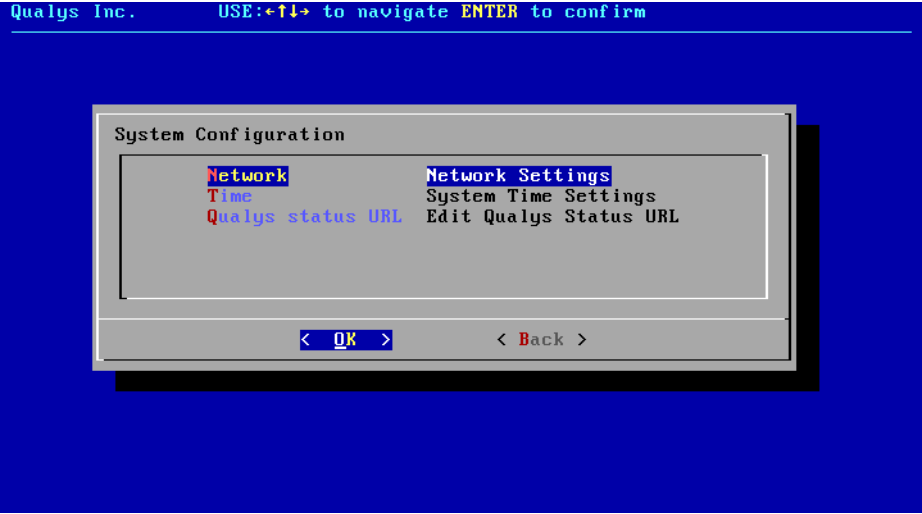
```

Main Configuration Menu

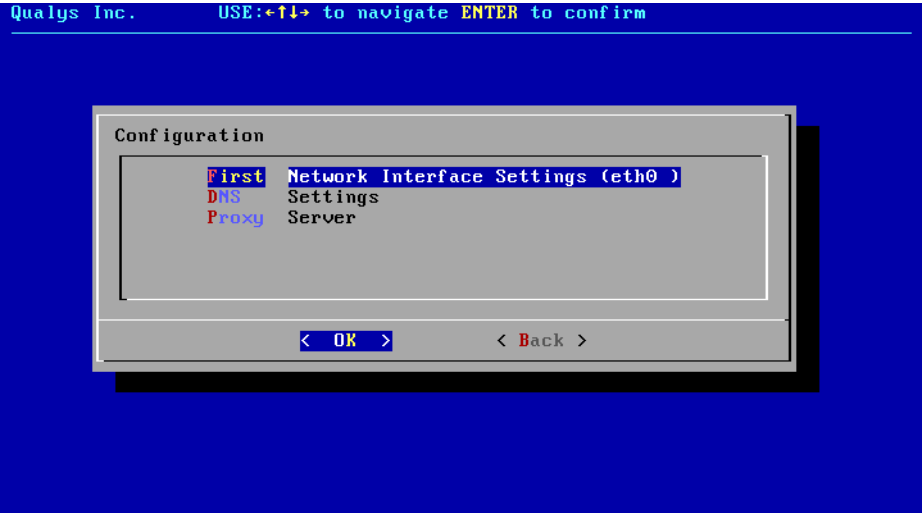
Under System menu, configure Network Settings



Network Configuration



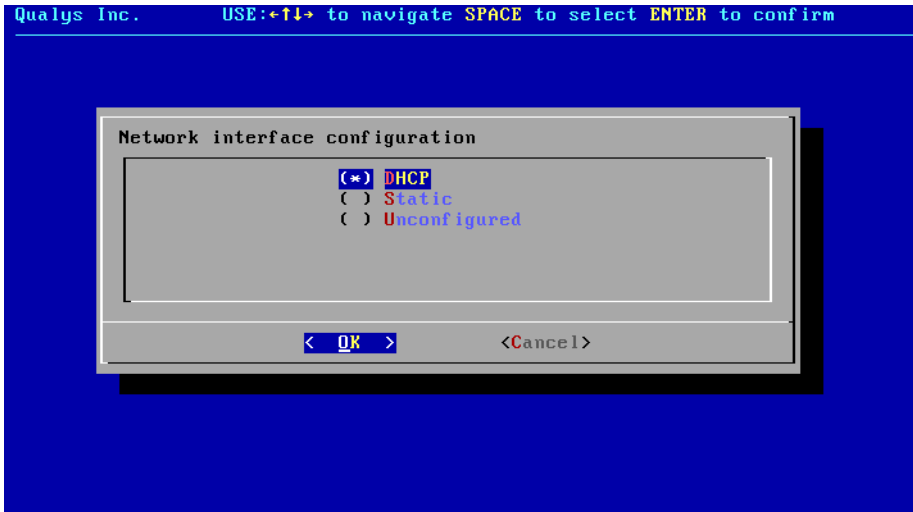
First ethernet interface



DHCP

If using DHCP, configure the virtual appliance network interface to use DHCP.

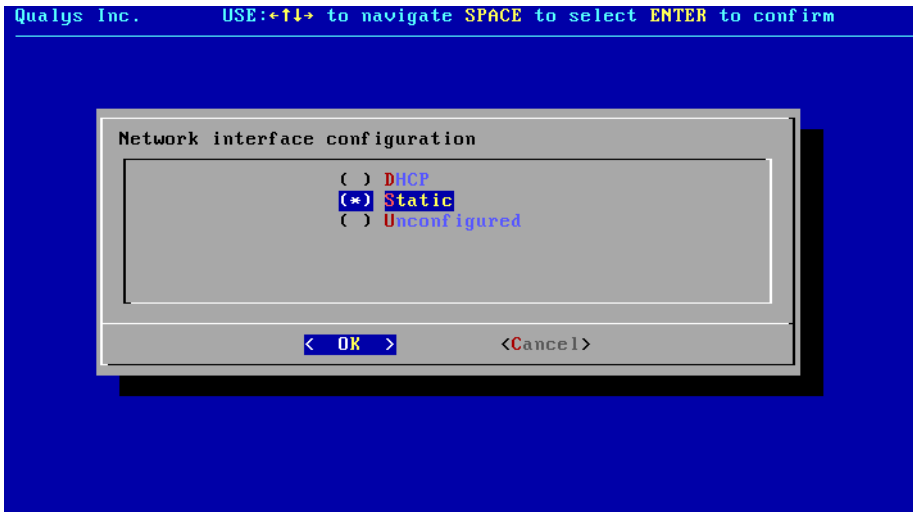
This is the IP of the QGS proxy that Cloud Agents will connect running on port 1080.



Static

If using Static IP, configure the virtual appliance network interface to use Static IP Address.

Cloud Agents connect to the Static IP Address on port 1080.



Set static IP address, if used.

IP address uses a 32-bit netmask, e.g. "/24" for 255.255.255.0

Specify the Default Gateway IP address.

Qualys Inc. USE:↑↓ to navigate TAB to focus ENTER to confirm

eth0:

IP (CIDR):

Gateway:

< OK > < Back >

DNS Servers

Set DNS servers for the virtual appliance to resolve the Qualys URLs.

Qualys Inc. USE:↑↓ to navigate TAB to focus ENTER to confirm

DNS Servers:

DNS:

DNS:

Search domain:

< OK > < Back >

Proxy Servers

Configure upstream Proxy Server, if using proxy chaining.

Proxy Settings:

Proxy URL:	<input type="text" value="http://10.10.10.10"/>
Proxy Port:	<input type="text" value="3128"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
DNS Host:	<input type="text"/>
DNS IP:	<input type="text"/>

< **OK** > < **Back** >

Info

Qualys Inc. USE:↑↓→ to navigate ENTER to confirm

Configuration

Registration	Register the Appliance with Qualys
System	System Settings
Info	General Information
Diagnostics	Information
Commands	Various commands

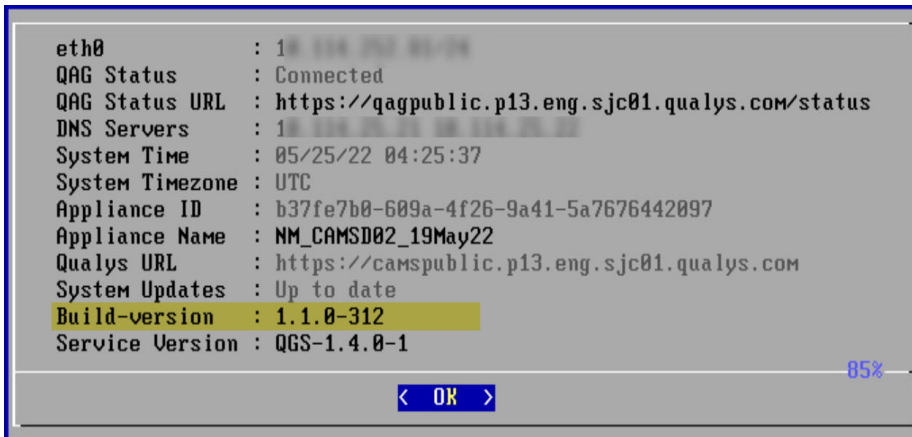
< **OK** >

QAG Status: Connected

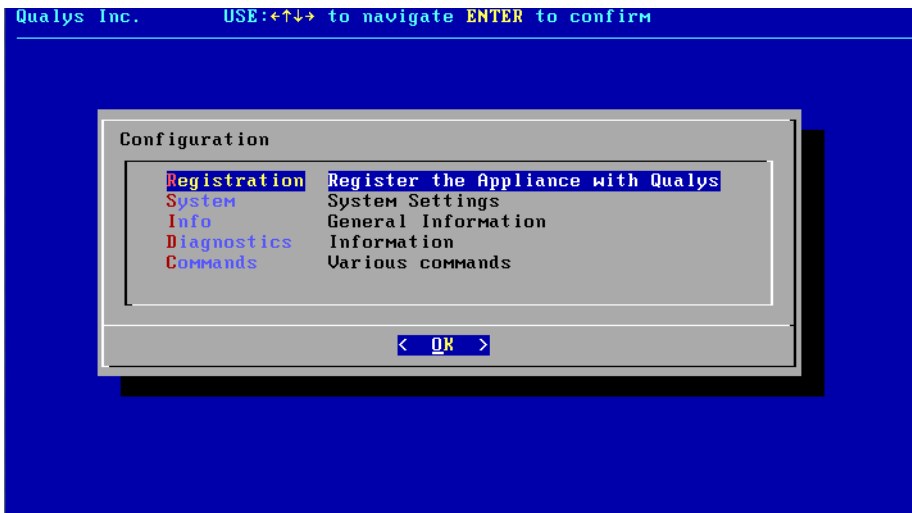
QAG Status: Connected shows that QGS can connect to the Qualys POD.

If the status is not **Connected**, verify network connectivity and firewall settings.

Note: As of QGS v2.1.0 release, the appliance TUI now display the service version on the Info tab, as shown in the following screenshot.



Registration



Enter the Personalization Code generated in the QGS User Interface module.

Qualys Inc. USE:↑↓→ to navigate ENTER to confirm

Enter lookup code in *lowercase*

CHANGE_ME

< OK > < Back >

Here's an example of a redacted Personalization Code.

Qualys Inc. USE:↑↓→ to navigate ENTER to confirm

Enter lookup code in *lowercase*

0123a17a-46dc-669-0db

< OK > < Back >

Registration in process

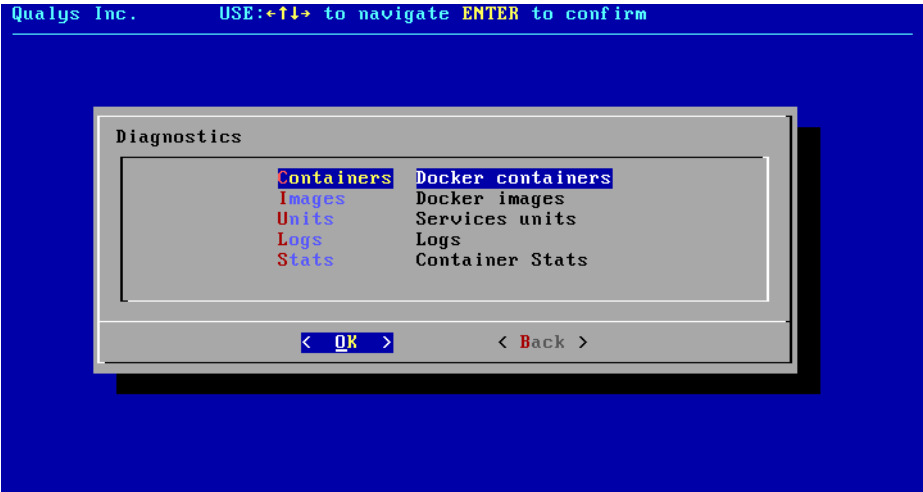
Please wait while appliance registration is being verified. This may take few minutes.

WARNING: Do not interact with the appliance during this time.

Successful Registration



Diagnostics



Containers

Qualys Inc. USE:↑↓ to scroll ENTER to exit

NAMES	STATUS	COMMAND
HAPROXY	Up 17 minutes	"/entrypoint.sh"
CONFD-HAPROXY	Up 17 minutes	"/usr/local/bin/confd -wat
cams-logstash	Up 17 minutes	"/usr/share/logstash/bin/l
squid-2	Up 17 minutes	"/docker-entrypoint.sh"
CAMSD	Up 17 minutes	"/sbin/init"

63%

< EXIT >

Images

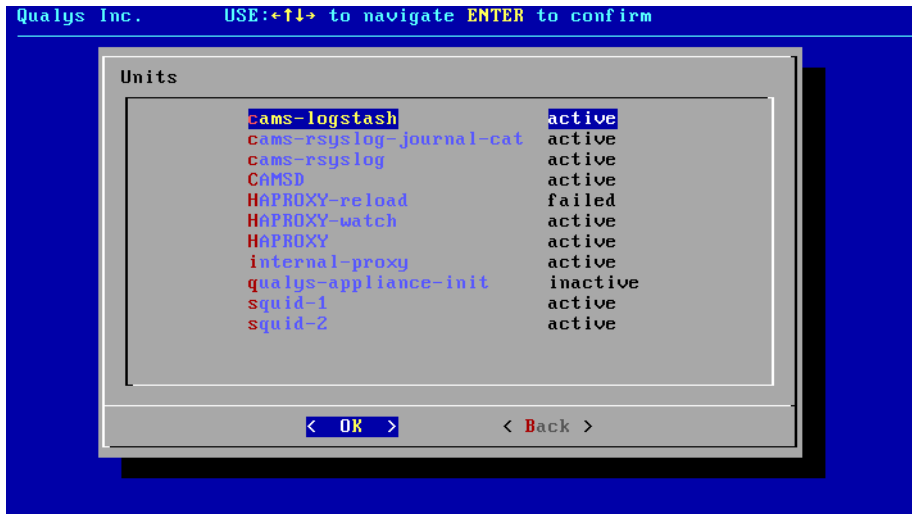
Qualys Inc. USE:↑↓ to scroll ENTER to exit

REPOSITORY	TAG	IMAGE ID
cams-haproxy	0.1.0-47	a397bd13a1
camslocal:443/cams-haproxy	0.1.0-47	a397bd13a1
camslocal:443/cams-keepalived	0.1.0-47	8cd941c6d3
cams-keepalived	0.1.0-47	8cd941c6d3
camslocal:443/cams-squid	0.1.0-47	9042e180e2

35%

< EXIT >

Units

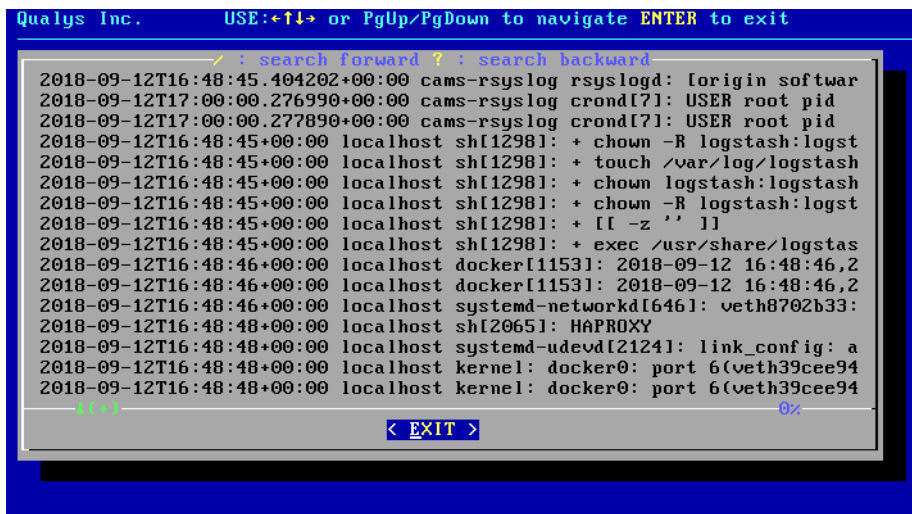


Logs

View log file of the virtual appliance. (Logs are also uploaded to the QGS UI Module.)

Logs are sorted with most recent descending.

Navigation and search commands are defined in the UI.



Don't worry to delete or archive logs! The QGS appliance will automatically clean up its logs and disk space as it reaches capacity.

Proxy

Executes a network connection test through a configured upstream proxy.

Stats

View utilization of the virtual appliance services.

Qualys Inc. USE:↑↓ to scroll ENTER to exit

CONTAINER ID	NAME	CPU %	MEM USAGE /
960eb4df3552	HAPROXY	0.02%	2.285MiB /
1e480d9ab0f3	CONFD-HAPROXY	0.00%	1.656MiB /
f5459536ba9a	cams-logstash	2.45%	501.1MiB /
ffe47a1b904e	squid-2	0.01%	160.4MiB /
f18fac5251ac	CAMSD	0.00%	7.055MiB /

66%

< EXIT >

Commands

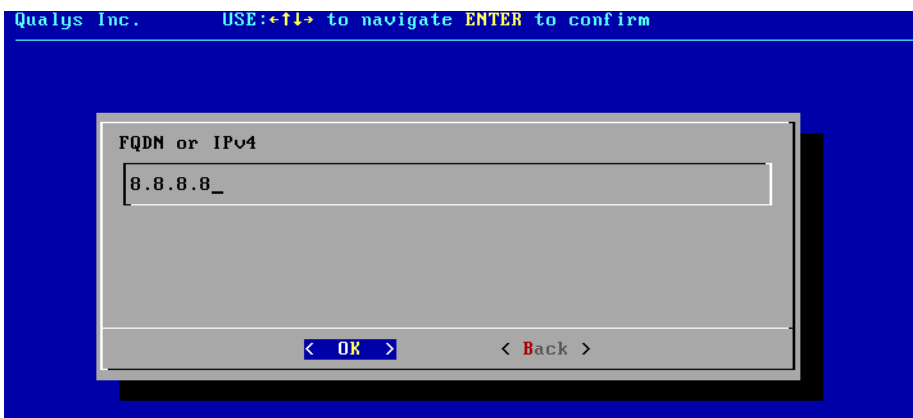
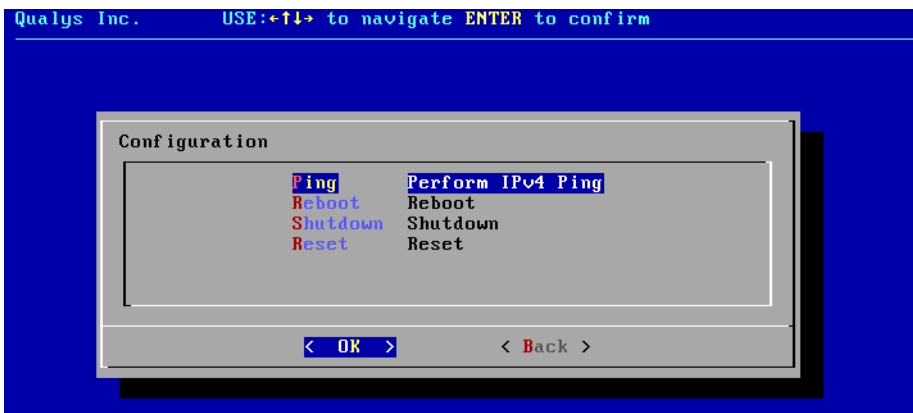
Qualys Inc. USE:←→ to navigate ENTER to confirm

Configuration	
Registration	Register the Appliance with Qualys
System	System Settings
Info	General Information
Diagnostics	Information
Commands	Various commands

< OK >

Ping

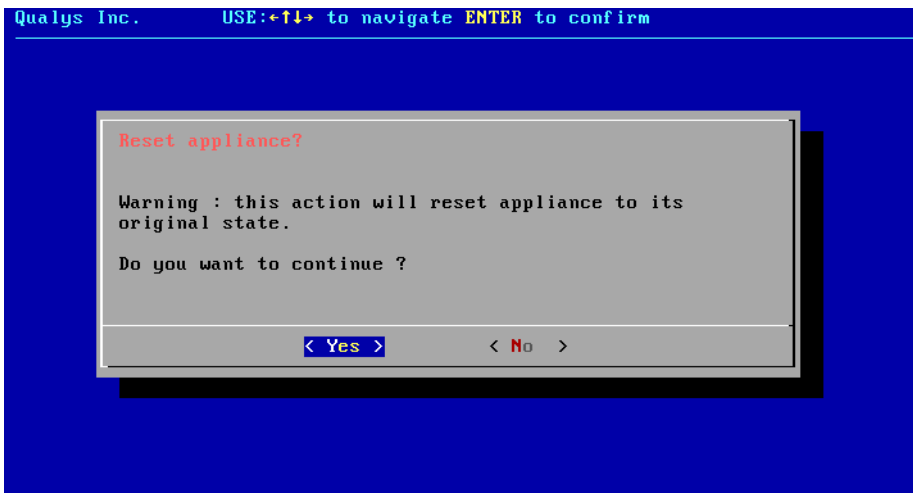
Ping is required to perform the connectivity checks. So, make sure that ping is enabled for IPs/URLs mentioned in [Network Configuration](#) section.



Reset appliance

Reset appliance to its original unconfigured state.

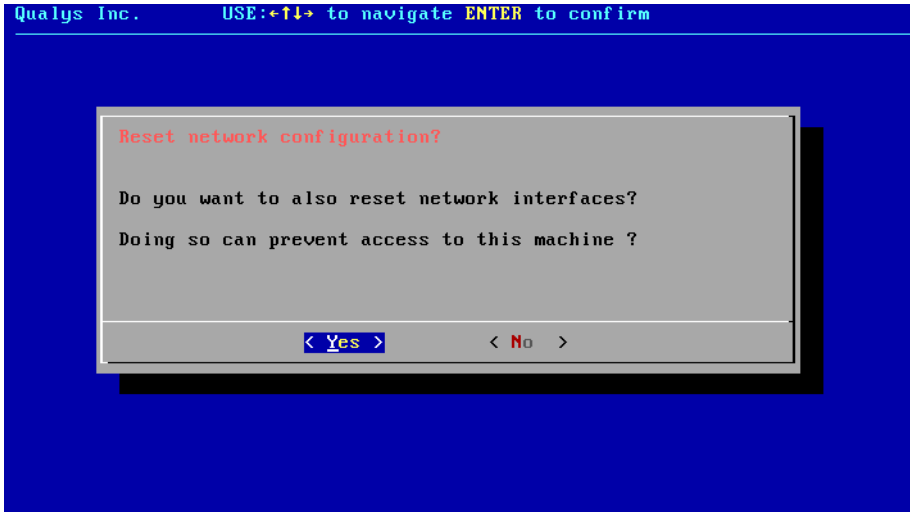
Warning: All configurations and log files will be deleted.



Reset network interface

Reset network interface of virtual appliance.

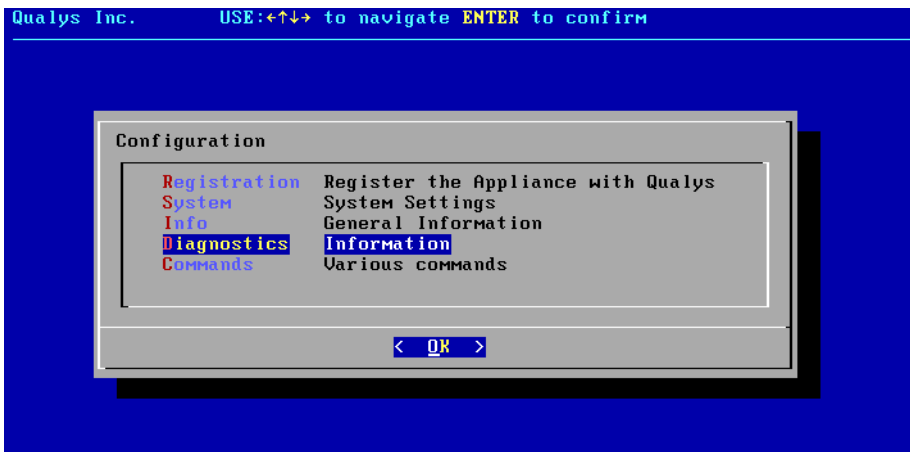
Note: This only resets the network configuration of the appliance.



Diagnostics Mode

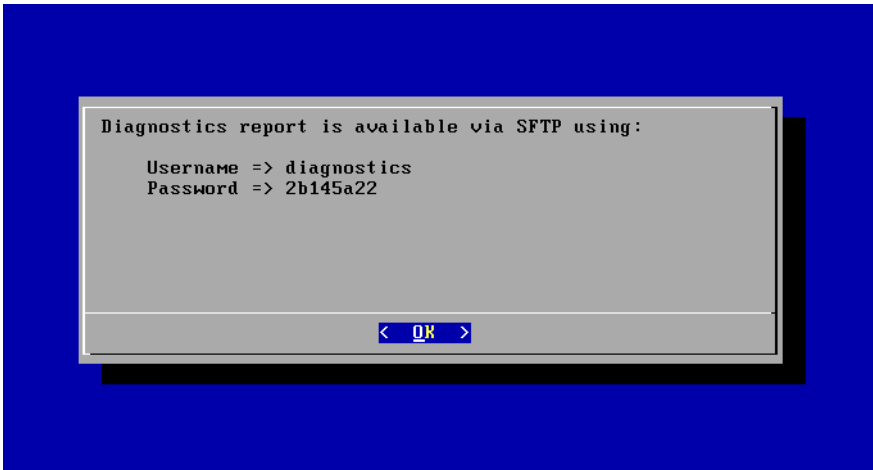
The QGS Appliance supports a Diagnostic mode to help accelerate Qualys Customer Support troubleshooting and problem resolution, primarily for initial network setup and registration issues. The Diagnostic mode is a user-initiated command that creates an encrypted report archive for the customer to collect and submit to Qualys Customer Support. The Diagnostics command creates a one-time generated password to download the encrypted report archive from the QGS appliance using SFTP.

1) On the local console-based user interface, select the Diagnostics menu



2) Executing the Diagnostics mode will trigger the appliance to create the encrypted report archive and generate a one-time random password to access the appliance to copy the diagnostics archive.

3) Connect to the appliance using SFTP using the diagnostics username and one-time random password.



4) Download the encrypted report archive from the appliance to a system of your choosing.

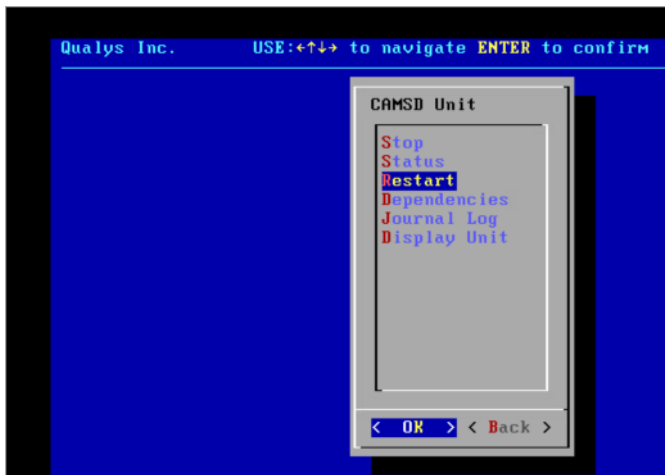
5) Upload/attach the encrypted report archive to a Qualys customer support case.

Appendix - Things to Remember

- Qualys Gateway Service detects only one secondary hard disk.
- To retain more logs, you can extend the primary hard disk.
- To retain more patches, you can extend the secondary hard disk.
- Extending any QGS hard disks must be done from your hypervisor console with appropriate permissions with the QGS in question, powered off.
- You can only have a maximum of 5 proxies, QGS appliances, DNS aliases, or Load Balancer VIP entries.
- The direct connection from a cloud agent will be attempted after all proxy/QGS/DNS/VIP options have been attempted and will work only if the firewall rules allow it.
- You can nest QGS appliances, but only the QGS device that the cloud agent communicates directly with can be used in proxy, cache, or patch mode. Any QGS above the first QGS must be defined as the upstream proxy for the first QGS, using only the proxy port on the second QGS.
- Restart the CAMSD service unit if you see your appliance is inactive on the UI.

The following are the steps to restart the CAMSD service unit to active your appliance on the UI:

1. Connect to the appliance **Text** user interface.
2. Go to the **Diagnostics** and select **Units**.
3. Go to the **CAMSD** unit and click **Restart**.



4. Wait at least 45 minutes to 1 hour for the appliance to become active on the UI.