



# **Qualys Gateway Service**

User Guide  
Version 3.5.0

December 29, 2023

Copyright 2022-23 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

<b>About this Guide .....</b>	<b>5</b>
About Qualys .....	5
Qualys Support .....	5
<b>Overview .....</b>	<b>6</b>
Virtualization Server Requirements and Virtual Machine File Formats .....	7
Virtual Machine Configuration .....	7
Network Configuration .....	8
<b>Qualys Gateway Service User Interface Module .....</b>	<b>10</b>
Qualys Virtual Appliance Configuration .....	11
Qualys Gateway Service Module User Interface .....	12
Create a New Appliance .....	13
View List of Appliances and their Status .....	14
Download Image of the Virtual Appliance .....	15
Download Qualys Signed Certificate .....	15
After Successful Setup and Registration, the Appliance has Active Status .....	16
Identifying the Appliance Certificate .....	17
View Details, Stats, and Logs of an Active Appliance .....	18
Upload Certificates .....	19
Assign Certificates .....	23
Things to Remember: .....	23
Downloading Cache Certificates to Configure on the Agents .....	24
Changing the Proxy Port .....	25
Understanding Cache Mode and Patch Mode .....	26
QGS Appliance Cache and Patch Mode Configuration .....	27
Cloud Agent Configuration .....	29
Cloud Agent Cache Mode and Patch Mode Configuration .....	30
Virtual Appliance Local Configuration .....	31
Local Configuration Menu Structure .....	31
Configuration Screens .....	32
QGS virtual appliance starting up .....	32
Main Configuration Menu .....	32
Network Configuration .....	33
First ethernet interface .....	33
DHCP .....	33
Static IP .....	34
DNS Servers .....	35
Proxy Servers .....	35
NTP Servers .....	36
Info .....	37

Registration .....	38
Personalization Code .....	38
Registration-in-progress .....	39
Successful Registration .....	39
Diagnostics .....	40
Containers .....	40
Images .....	41
Units .....	41
Logs .....	42
Proxy .....	42
Stats .....	42
Diagnostics Mode .....	43
Generate Upstream PCAP File .....	44
Commands .....	44
Ping .....	45
Reset appliance .....	46
Reset network interface .....	46

<b>Appendix - Things to Remember.....</b>	<b>47</b>
<b>Frequently Asked Questions .....</b>	<b>48</b>

# 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](http://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/](http://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 provides caching and proxy services for Cloud Agent deployments. It also provides proxy services for Qualys Scanner and Qualys Network Passive Sensor.

The QGS virtual appliance provides proxy services for Cloud Agent deployments, Qualys Scanner, and Qualys Network Passive Sensor and caching service 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, 2019 (Disk type IDE)	VHD

### Virtual Machine Configuration

- 4 vCPUs.
- 16 GB RAM minimum.
- 40 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.
- QGS caching limit is dynamic. The caching limit is based on the RAM assigned to QGS. Caching consumes 40% of the total allocated RAM.

#### Note:

- Cloud agents on Windows Server 2008 Standard R1 may face connectivity issues. This is because TLS1.0 is not supported with the upgraded OpenSSL library. Connect with the Qualys Support team in case of connectivity issues with Windows Server 2008 Standard R1 cloud agents.
- The QGS installable may occupy lesser space than the minimum space requirements. However, we recommend that the VM must meet the minimal requirements of 40 GB of disk space and 16 GB RAM.

## 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.
- The Content Delivery Network URLs (cask urls) are necessary for SwCA functionality of cloud agents connecting to the Qualys Cloud Platform using QGS.

Platform	Cloud Agent	Qualys Gateway Service	Platform URL
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 cask.qg1.apps.qualys.com	qg1.apps.qualys.com
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 cask.qg2.apps.qualys.com	qg2.apps.qualys.com
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 cask.qg3.apps.qualys.com	qg3.apps.qualys.com
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	qg4.apps.qualys.com
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 cask.qg1.apps.qualys.eu	qg1.apps.qualys.eu

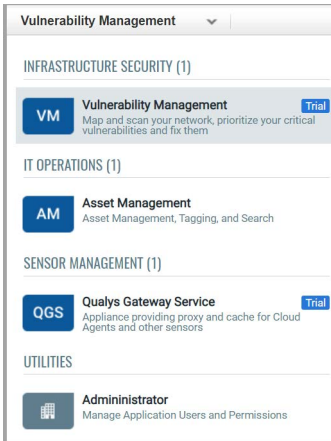


<b>Platform</b>	<b>Cloud Agent</b>	<b>Qualys Gateway Service</b>	<b>Platform URL</b>
EU 2	qagpublic.qg2.apps.qualys.eu	qagpublic.qg2.apps.qualys.eu camspublic.qg2.apps.qualys.eu camspm.qg2.apps.qualys.eu camsrepo.qg2.apps.qualys.eu update.release.flatcar-linux.net cask.qg2.apps.qualys.eu	qg2.apps.qualys.eu
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 cask.qg1.apps.qualys.in	qg1.apps.qualys.in
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 cask.qg1.apps.qualys.ca	qg1.apps.qualys.ca
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 cask.qg1.apps.qualys.ae	qg1.apps.qualys.ae
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 cask.qg1.apps.qualys.co.uk	qg1.apps.qualys.co.uk
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 cask.qg1.apps.qualys.com.au	qg1.apps.qualys.com.au
KSA 1	qagpublic.qg1.apps.qualysksa.com	qagpublic.qg1.apps.qualysksa.com camspublic.qg1.apps.qualysksa.com camspm.qg1.apps.qualysksa.com camsrepo.qg1.apps.qualysksa.com update.release.flatcar-linux.net	qg1.apps.qualysksa.com

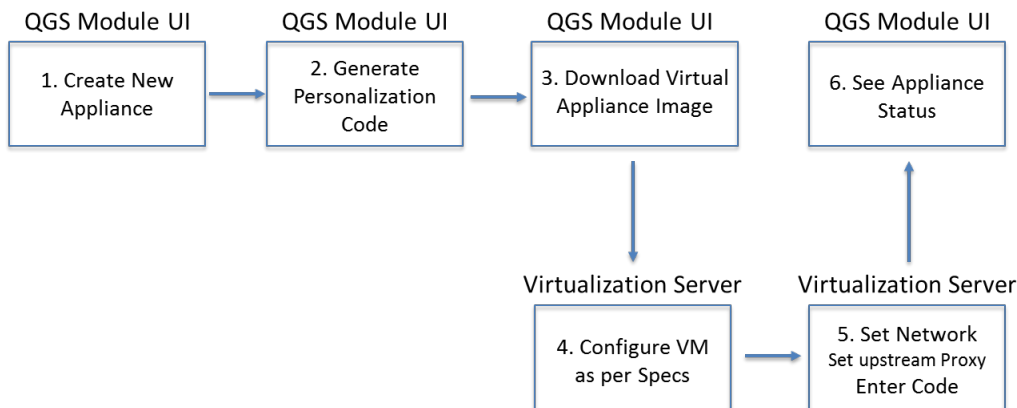
# Qualys Gateway Service User Interface Module

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.



## Qualys Virtual Appliance Configuration

- 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.

**Note:** The third hard disk is not supported and would not be recognized on the CAMS/QGS appliance to use the patch mode. We recommend using only one extra hard disk of 250GB or more to use the patch mode.

- 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.

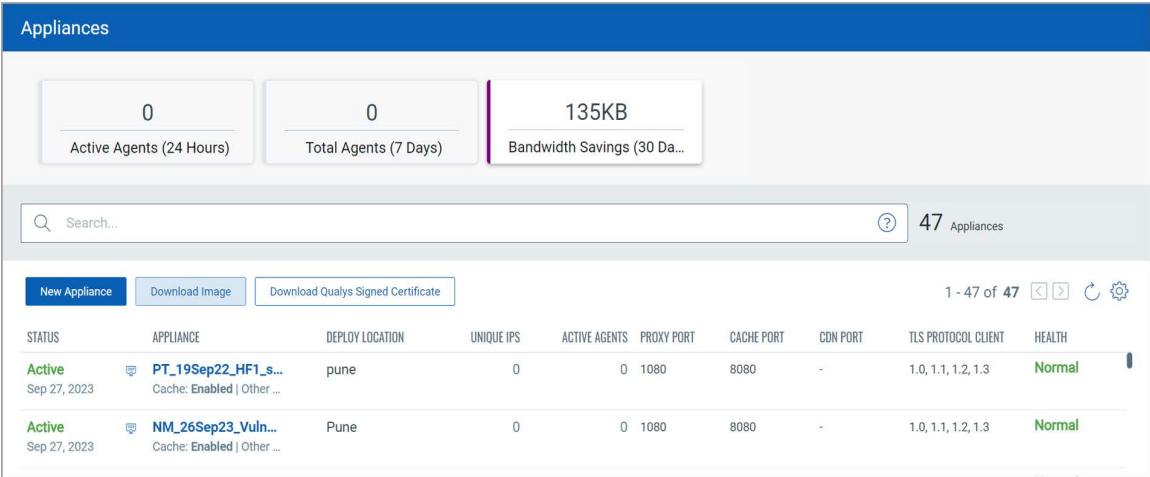
- 5) Start the image.

**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.

# 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.

To create a new appliance, click **New Appliance**.

## Create a New Appliance

← New Appliance

Create Appliance

Registration

### Registration

Provide the appliance name, deployment location and generate the personalization code to register the appliance.

#### Appliance Details

Appliance Name \*

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

#### Assign Certificate

Appliance Level **Qualys Signed** Customer Signed

Cancel Save

While creating a new appliance/personalization code, you can choose the appliance certificate type from the "Assign certificate" section.

A Qualys Signed certificate is a common certificate. It can help you to deploy a single certificate across all the cloud agents meant for the particular appliance.

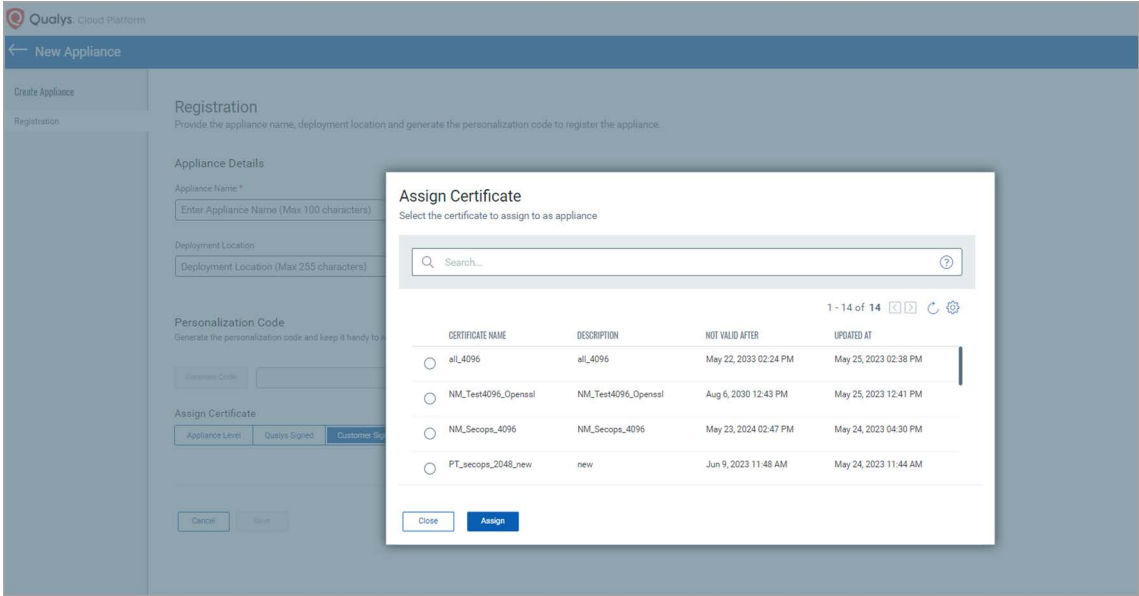
If you want to use a common certificate while registering the appliance, then click **Use Common Certificate** checkbox.

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

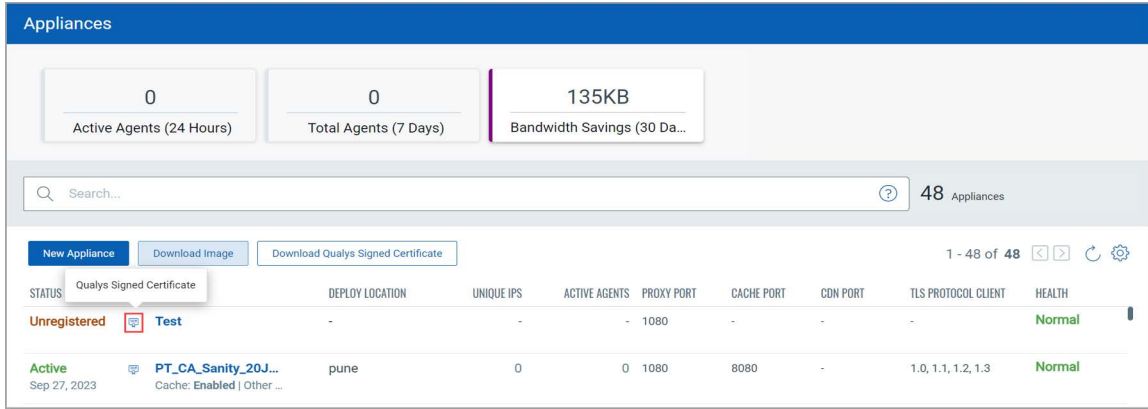
An Appliance Signed certificate is a certificate specific to that appliance.

A Customer Signed certificate is signed by the customer from the **Certificates** tab of the QGS UI. Read more about creating Customer Signed certificates at [Upload Certificates](#).

When you select the customer-signed certificate, you can see the below window to assign the custom certificate while generating the personalization code.



View List of Appliances and their Status



The newly created appliance status is shown as **Unregistered** until you follow the registration steps. Refer to [Virtual Appliance Local Configuration](#) to learn more.

A subscription-level common CA is available instead of appliance specific certificate on the appliance list if appliances are registered with the Qualys Signed certificate option.

Appliances with Qualys Signed or Customer Signed certificate enabled will be shown an icon as highlighted on the appliance list page. Appliance-level certificates do not have the icon displayed.

## Download Image of the Virtual Appliance

### Virtualization Platform Image

Download the required virtualization platform image from the supported list.

IMAGE NAME	FILE SIZE	
qualys-qgs-appliance-2.1.0-55.ova	1.50GB	<a href="#">↓</a>
qualys-qgs-appliance-2.1.0-55.ovf.zip	1.47GB	<a href="#">↓</a>
qualys-qgs-appliance-2.1.0-55.vmx.zip	1.46GB	<a href="#">↓</a>

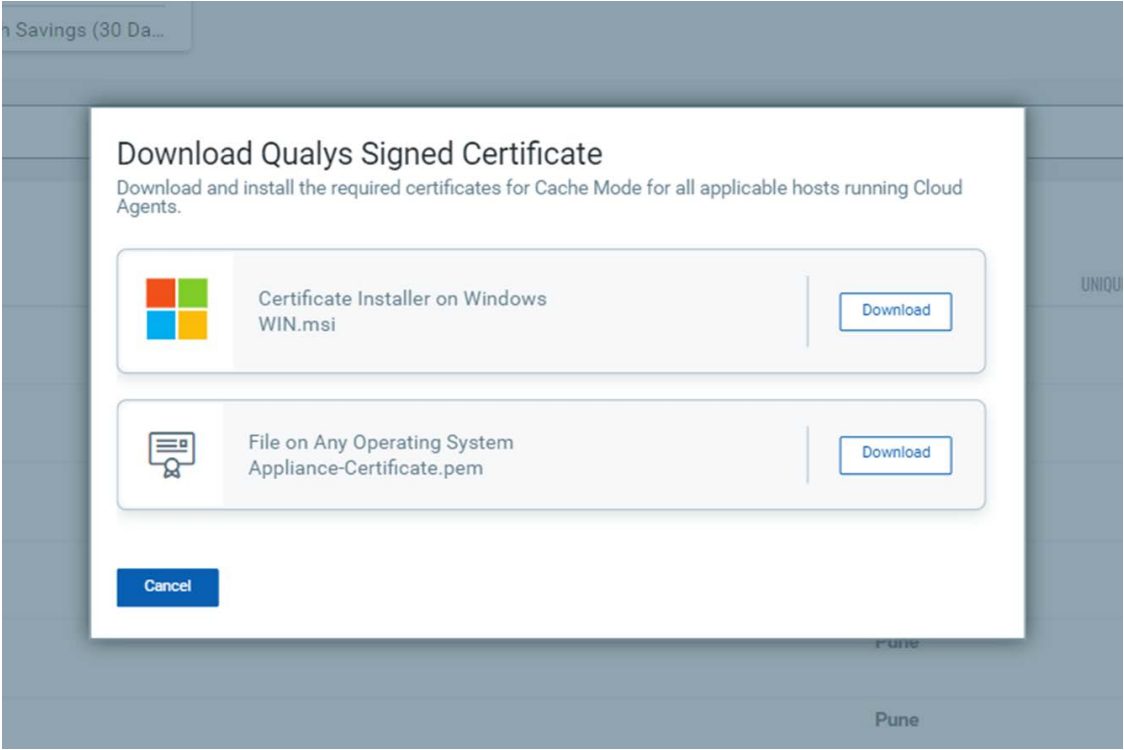
OK

Download the virtualization platform image for the appliance from the given list.

### Download Qualys Signed Certificate

You can download the Qualys Signed certificate from the appliance details page or the appliance list page.

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



**After Successful Setup and Registration, the Appliance has Active Status**

To know more about registering your appliance, refer to [Virtual Appliance Local Configuration](#).

Appliances

0Active Agents (24 Hours)

0Total Agents (7 Days)

135KBBandwidth Savings (30 Da...

Search...

47Appliances

New ApplianceDownload ImageDownload Qualys Signed Certificate

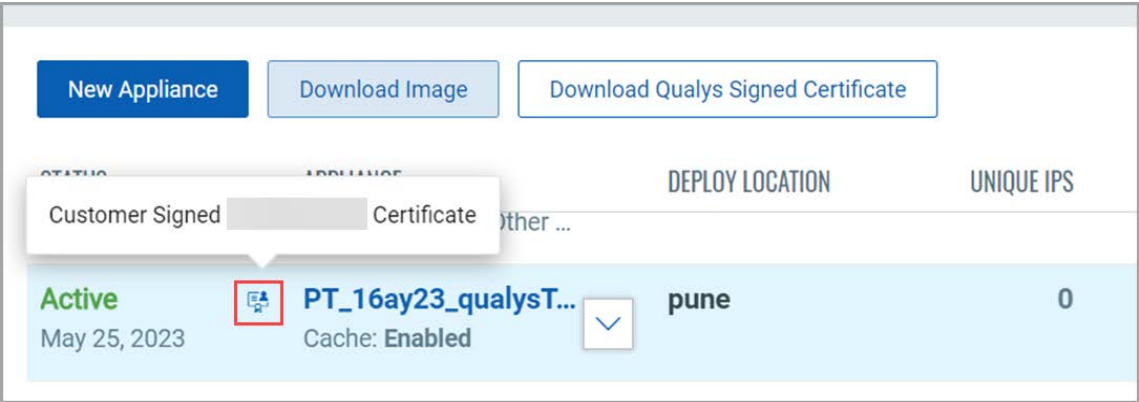
1 - 47 of 47

STATUS	APPLIANCE	DEPLOY LOCATION	UNIQUE IPS	ACTIVE AGENTS	PROXY PORT	CACHE PORT	CDN PORT	TLS PROTOCOL CLIENT	HEALTH
Active Sep 27, 2023	PT_19Sep22_HF1_s... Cache: Enabled   Other ...	pune	0	0	1080	8080	-	1.0, 1.1, 1.2, 1.3	Normal
Active Sep 27, 2023	NM_26Sep23_Vuln... Cache: Enabled   Other ...	Pune	0	0	1080	8080	-	1.0, 1.1, 1.2, 1.3	Normal

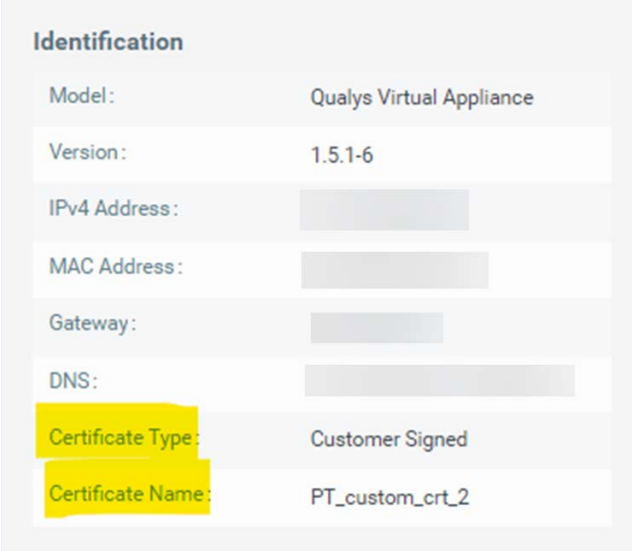


Identifying the Appliance Certificate

The appliances registered with custom certificate displays a different icon on the appliance list page.



Click the appliance name to identify the Certificate Name and Certificate Type associated with it.

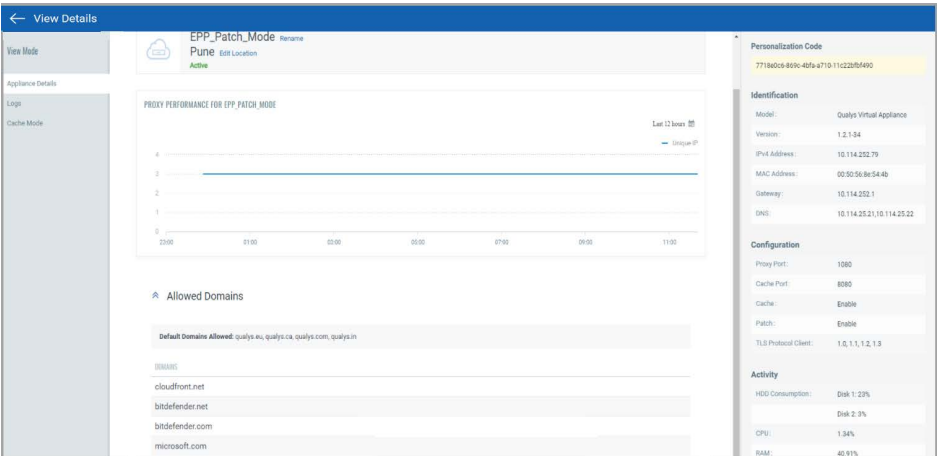


Appliances with Qualys Common CA will display the certificate type as “Qualys Signed”.  
Appliances with Appliance level certificate shows the certificate type as “Appliance level”.

### Identification

Model:	Qualys Virtual Appliance
Version:	1.5.1-6
IPv4 Address:	
MAC Address:	
Gateway:	
DNS:	
Certificate Type:	Qualys Signed

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.

## Upload Certificates

You can also choose to add your own certificates to the appliance instead of using the Qualys Common CA or appliance-level certificates. The QGS UI offers the Certificates tab, which allows you to upload your organizational chain (including root certificates, intermediate certificates, and issuing certificates) and your private key, which is required to decrypt the traffic encrypted with your public key.

Qualys Cloud Platform

Qualys Gateway Service

APPLIANCESCONNECTED IPSCERTIFICATES

35 Certificates

1 - 35 of 35

Upload Certificate

COMMON NAME	DESCRIPTION	ASSOCIATED APPLIANCES	VALID NOT AFTER	VALID NOT BEFORE	UPDATED AT	CREATED AT
S...		1	Jun 9, 2023 11:48 AM	May 10, 2023 11:48 AM	Jun 5, 2023 01:17 PM	Jun 5, 2023 01:17 PM
m...		0	Aug 6, 2030 12:43 PM	May 5, 2023 12:43 PM	Jun 2, 2023 05:01 PM	Jun 1, 2023 04:13 PM
P...		0	Jun 9, 2023 11:48 AM	May 10, 2023 11:48 AM	Jun 2, 2023 03:40 PM	Jun 2, 2023 03:40 PM
P...		0	Aug 9, 2030 10:54 AM	May 8, 2023 10:54 AM	Jun 2, 2023 03:39 PM	Jun 2, 2023 03:39 PM
P...		0	Aug 6, 2030 12:43 PM	May 5, 2023 12:43 PM	Jun 2, 2023 03:38 PM	Jun 2, 2023 03:38 PM

To upload the certificates to the QGSUI, click the **Upload Certificate** button on the certificates page.



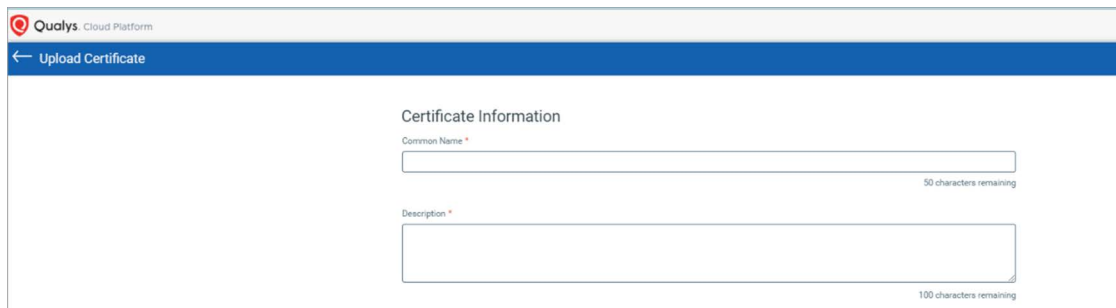
The **Upload Certificate** screen appears. You can upload the intermediate certificate's Root, Intermediate, and Private keys in the respective upload sections.

You can find the list of uploaded certificates listed on the **Certificates** tab.

Provide the following values:

**Common name** - A unique name given to the certificate to identify the certificate.

**Description** - Provide the description of the certificate.



**Upload Certificate** - You can upload the Root, Intermediate and Private Keys certificate on the Upload Certificate section.

← Upload Certificate

100 characters remaining

Upload Certificate

Make sure private key is not password protected. The X.509 certificate (PEM format) should look like as per below format.

-----BEGIN CERTIFICATE-----  
Your certificate content here  
-----END CERTIFICATE-----

Root Certificate

Drag and drop to upload or [Browse](#)  
(Max file size 3 MB) | Supported file: .pem

Intermediate Chain

Drag and drop to upload or [Browse](#)  
(Max file size 3 MB) | Supported file: .pem

Private Key

Drag and drop to upload or [Browse](#)  
(Max file size 3 MB) | Supported file: .pem

[Cancel](#)

[Save](#)

Click on **Save** to save the uploaded certificate. You can find the list of uploaded certificates listed on the **Certificates** tab.

Qualys Cloud Platform

Qualys Gateway Service

APPLIANCESCONNECTED IPS**CERTIFICATES**

14 Certificates

1 - 14 of 14

COMMON NAME	DESCRIPTION	ASSOCIATED APPLIANCES	VALID NOT AFTER	VALID NOT BEFORE	UPDATED AT	CREATED AT
	atl_4096	0	May 22, 2033 02:34 PM	May 25, 2023 02:34 PM	May 25, 2023 02:38 PM	May 25, 2023 02:38 PM
	NM_Tests4096_Opened	0	Aug 6, 2030 12:43 PM	May 5, 2023 12:43 PM	May 25, 2023 12:41 PM	May 25, 2023 12:41 PM
	NM_Secops_4096	1	May 23, 2024 02:47 PM	May 24, 2023 02:47 PM	May 24, 2023 04:30 PM	May 24, 2023 04:30 PM

You can edit the certificate from the quick actions menu.

The screenshot shows the 'Certificates' page in the Qualys Cloud Platform. At the top, there's a search bar and a '14 Certificates' indicator. Below the search bar is a table with columns: COMMON NAME, DESCRIPTION, ASSOCIATED APPLIANCES, VALID NOT AFTER, VALID NOT BEFORE, UPDATED AT, and CREATED AT. The first row shows a certificate with a common name 'aL4096', description 'aL4096', 0 associated appliances, and validity dates from May 22, 2023 to May 25, 2023. A 'Quick Actions' menu is open for the first row, showing options: 'Edit' (highlighted in yellow), 'Delete', and 'Assign to appliances'.

**Note:** When uploading your certificate, ensure that a new valid set of CA certs is uploaded before the existing ones have expired. Failure to do this results in the agents being unable to communicate with the platform via QGS.

You can only edit the common name and description of the uploaded certificates.

The screenshot shows the 'Edit Certificate' form. It has a title 'Certificate Information'. There are two text input fields: 'Common Name' and 'Description'. The 'Common Name' field has a placeholder and a '42 characters remaining' indicator. The 'Description' field has a placeholder and a '92 characters remaining' indicator.

You can also delete the certificates from the quick action menu.

The screenshot shows the 'Certificates' page in the Qualys Cloud Platform. At the top, there's a search bar and a '14 Certificates' indicator. Below the search bar is a table with columns: COMMON NAME, DESCRIPTION, ASSOCIATED APPLIANCES, VALID NOT AFTER, VALID NOT BEFORE, UPDATED AT, and CREATED AT. The first row shows a certificate with a common name 'aL4096', description 'aL4096', 0 associated appliances, and validity dates from May 22, 2023 to May 25, 2023. A 'Quick Actions' menu is open for the first row, showing options: 'Edit', 'Delete' (highlighted in yellow), and 'Assign to appliances'.

## Assign Certificates

Once you have successfully uploaded your certificates, you can assign them to any appliance. The Uploaded certificates can be assigned to the Qualys-signed, Appliance-level appliances from the **Assign to appliances** option of the Quick Action menu.

CERTIFICATE NAME	DESCRIPTION	ASSOCIATED APPLIANCES	VALID NOT AFTER	VALID NOT BEFORE	UPDATED AT	CREATED AT
...	...	0	May 25, 2023 02:24 PM	May 25, 2023 02:24 PM	May 25, 2023 02:28 PM	May 25, 2023 02:28 PM
...	NM_TestK096_Opened	0	Aug 5, 2020 12:43 PM	May 5, 2023 12:43 PM	May 25, 2023 12:41 PM	May 25, 2023 12:41 PM
...	NM_Secops_A096	1	May 23, 2024 02:47 PM	May 24, 2023 02:47 PM	May 24, 2023 04:30 PM	May 24, 2023 04:30 PM

After clicking **Assign to appliances**, a list of the appliances with the cert\_type as Qualys-signed and Appliance-level certificate are listed on the appliance.

APPLIANCE	DEPLOY LOCATION	STATUS	CERTIFICATE TYPE
PT_18May23_app_run_qualys	Pune	Active	Appliance Level
AKBUILD-45-SINGLE-IMAGE-14	Pune	Active	Qualys Signed
AKSingle_Image_DVF-175	Pune	Active	Qualys Signed
AKSSHTESTREN116	Pune	Active	Qualys Signed
NM_24May23_A096DtgCert	Pune	Active	Customer Signed

You can select multiple appliances for assigning a single set of custom certificates together.

**Note:** Custom certificates can be assigned/modified on the appliance which is configured with another custom certificate with the same steps as above.

## Things to Remember:

- You must manage your Root, Intermediate, and private key per your requirements.
- No passphrase should be assigned to the certificates while creating the CSR or any certificate.

- The multiple QGS appliances can be configured to receive the customer signing chain instead of the appliance level or common CA signing chain from Qualys.
- The QGS feature does not validate the certificate chain, so you must upload a valid one.
- Only the PEM format is supported while uploading the certificates on the Certificates tab.
- A certificate size over 3MB cannot be uploaded in the Certificate section.
- Assign a maximum of two agents at the start with a QGS appliance registered/configured with a customer-signed certificate instead of moving all the agents at once.
- Ensure to complete and validate the agent communication flow successfully before moving all the agents to a QGS proxy with a customer-signed certificate to avoid agent failure.

## Downloading Cache Certificates to Configure on the Agents

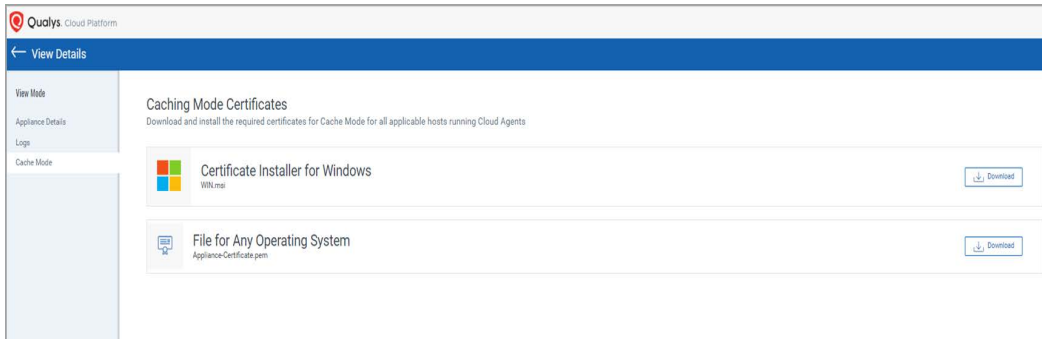
To download the cache certificates to be configured on the agents, click **View Details** on the quick action menu of the appliance.

The screenshot shows the 'Appliances' section of the Qualys Gateway Service User Interface. At the top, there are three summary boxes: 'Active Agents (24 Hours)' with 0, 'Total Agents (7 Days)' with 0, and 'Bandwidth Savings (30 Da...)' with 135KB. Below these is a search bar and a 'Quick Actions' dropdown menu. The dropdown menu is open, showing options: 'View Details' (highlighted with a red box), 'Configuration', 'Assign Customer Signed Certificate', and 'Delete'. Below the menu is a table of appliances. The table has columns: STATUS, DEPLOY LOCATION, UNIQUE IPS, ACTIVE AGENTS, PROXY PORT, CACHE PORT, CDN PORT, TLS PROTOCOL CLIENT, and HEALTH. The first appliance is 'pune' with 0 unique IPs, 0 active agents, proxy port 1080, cache port 8080, and health 'Normal'. The second appliance is 'NM\_26Sep23\_Vuln...' with 0 unique IPs, 0 active agents, proxy port 1080, cache port 8080, and health 'Normal'.

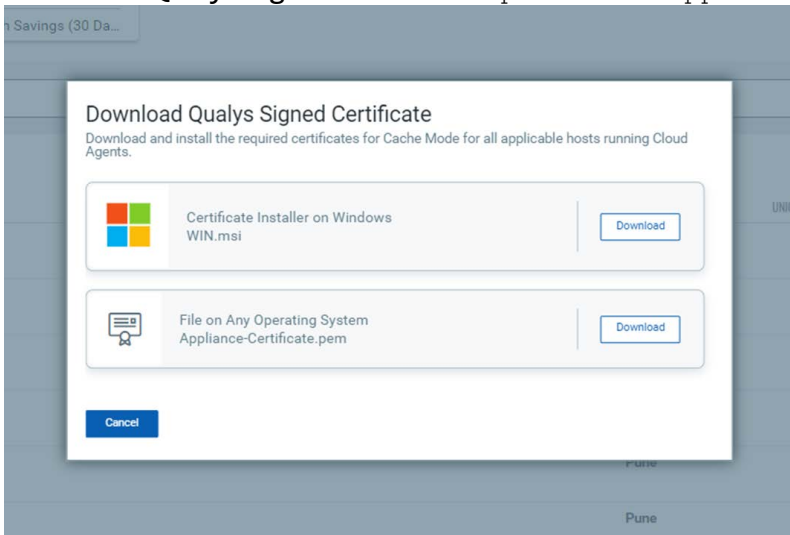
STATUS	DEPLOY LOCATION	UNIQUE IPS	ACTIVE AGENTS	PROXY PORT	CACHE PORT	CDN PORT	TLS PROTOCOL CLIENT	HEALTH
Active Sep 27, 2023	pune	0	0	1080	8080	-	1.0, 1.1, 1.2, 1.3	Normal
Active Sep 27, 2023	NM_26Sep23_Vuln...	0	0	1080	8080	-	1.0, 1.1, 1.2, 1.3	Normal



For appliances registered with either the Custom certificate or the Appliance-level certificate, the cache certificate (MSI,PEM) is available for download in the **Cache Mode** tab.



For appliances registered with Qualys signed certificate (Common CA), the cache certificate (MSI,PEM) is available for download in either the Cache Mode tab or the **Download Qualys signed Certificate** option on the Appliance listing page.



## 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.

**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.

## Understanding Cache Mode and Patch Mode

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 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. When allowing QGS to communicate with third-party vendor patch repositories, these connections must be allowed through customer firewalls. For more details, refer to the "URLs to be added to the Allowlist for Patch Download" section of the [Patch Management Getting Started Guide](#).

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 the runs the Cloud Agent.

## QGS Appliance Cache and Patch Mode 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

The screenshot shows the 'Configuration' page with a sidebar on the left indicating 'STEPS 2/3' with steps: 1 Proxy, 2 Modes (active), and 3 TLS Protocols. The main content area is titled 'Configure Modes' and contains two sections: 'Cache Mode' and 'Patch Mode'.

**Cache Mode** (toggle is On):

- 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 (toggle is On): Enable to allow the traffic to required domains.
- Default Domains Allowed: qualys.eu, qualys.ca, qualys.com, qualys.in.
- Input field: Enter domain without 'www' prefix. You can add maximum 10 domains. Type domain name here. Add button.
- Table with 2 columns: DOMAINS, ACTIONS. One row: hetzner.de, with edit and delete icons.

**Patch Mode** (toggle is On):

- 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.

At the bottom are buttons: Cancel, Previous, Next.

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

Important: 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.

**Note:** The third hard disk is not supported and would not be recognized on the CAMS/QGS appliance to use the patch mode. We recommend using only one extra hard disk of 250GB or more to use the patch mode.

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' page with a left sidebar indicating 'STEPS 3/3' and three steps: 1 Proxy, 2 Modes, and 3 TLS Protocols (which is the active step). The main content area is titled 'TLS Protocols' and includes a note: '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 for 'Minimum TLS Protocol Version' currently set to 'TLS 1.0'. At the bottom of the form 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.

**Note:** A Minimum 16GB of RAM is recommended for CAMS/QGS appliances. A total of 3000 concurrent cloud agent requests are supported by a QGS appliance. In case of more than 3000 agents communicating simultaneously, customers should deploy a new appliance instead of increasing RAM on the existing appliance.

## 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

## 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

```

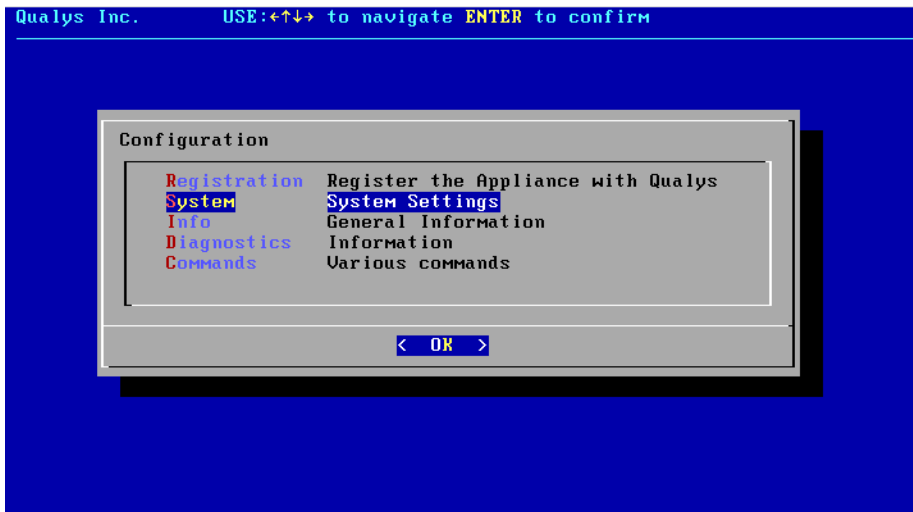
11.458732] SELinux: Class iucv_socket not defined in policy.
11.458780] SELinux: Class rxrpc_socket not defined in policy.
11.458827] SELinux: Class isdn_socket not defined in policy.
11.458873] SELinux: Class phonet_socket not defined in policy.
11.458921] SELinux: Class ieee802154_socket not defined 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 qipctr_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_endport 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.

```

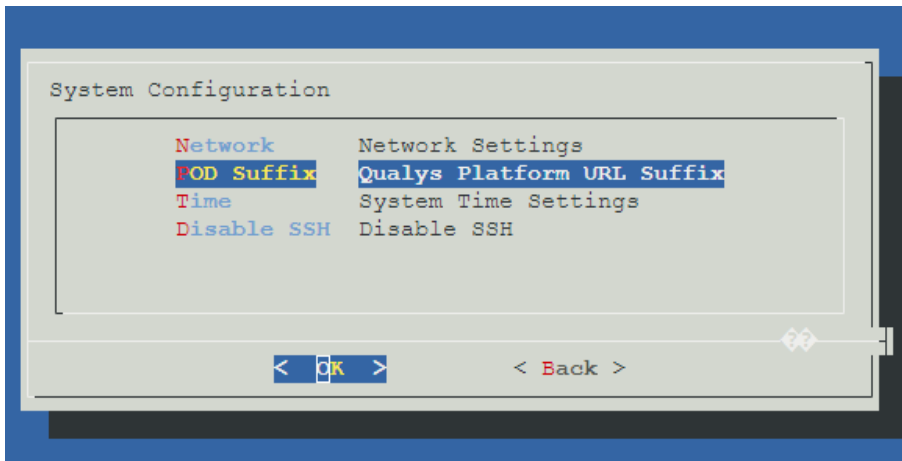
### Main Configuration Menu

Under System menu, configure Network Settings

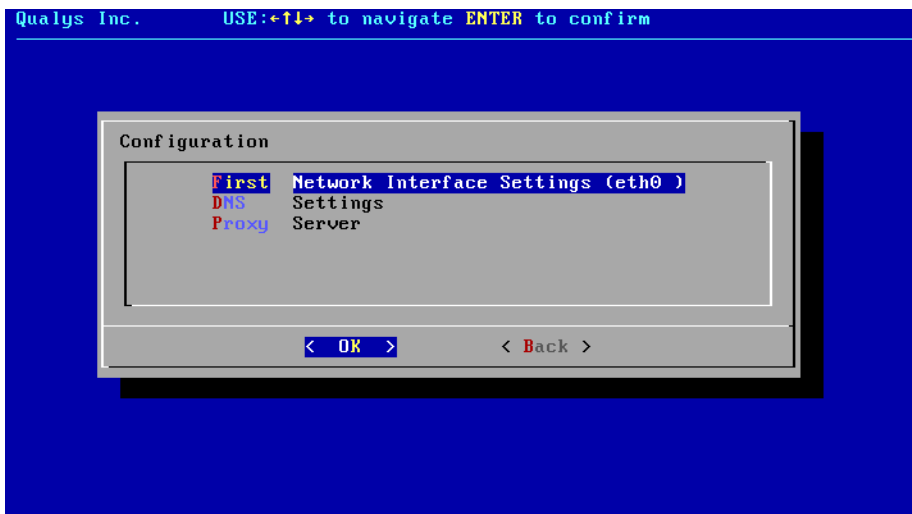




## Network Configuration



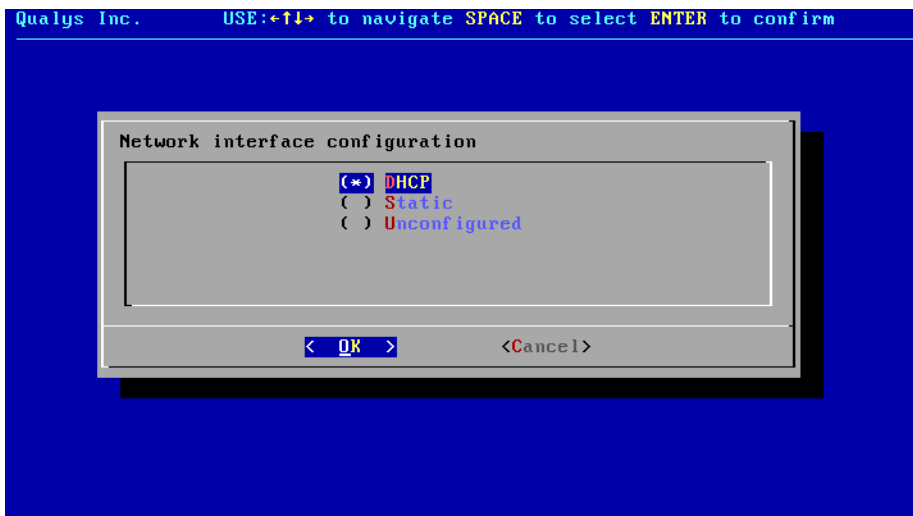
### First ethernet interface



### DHCP

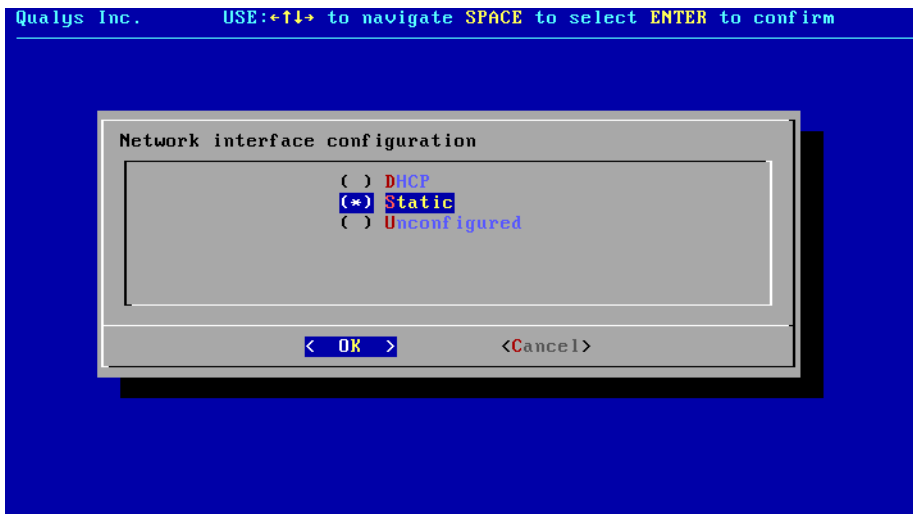
If using DHCP, configure the virtual appliance network interface to use DHCP.

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



### Static IP

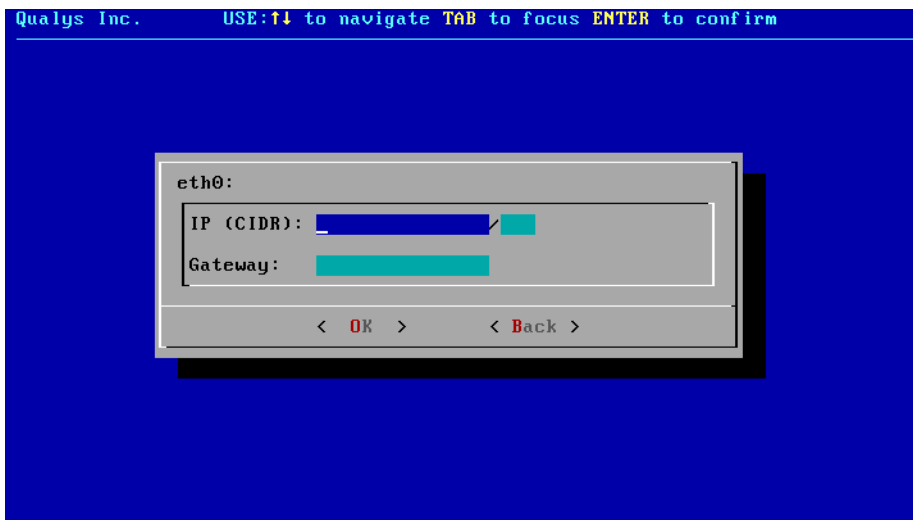
If using Static IP, configure the virtual appliance network interface to use Static IP Address. Cloud Agents connect to the Static IP Address on port 1080.



Set static IP address, if used.

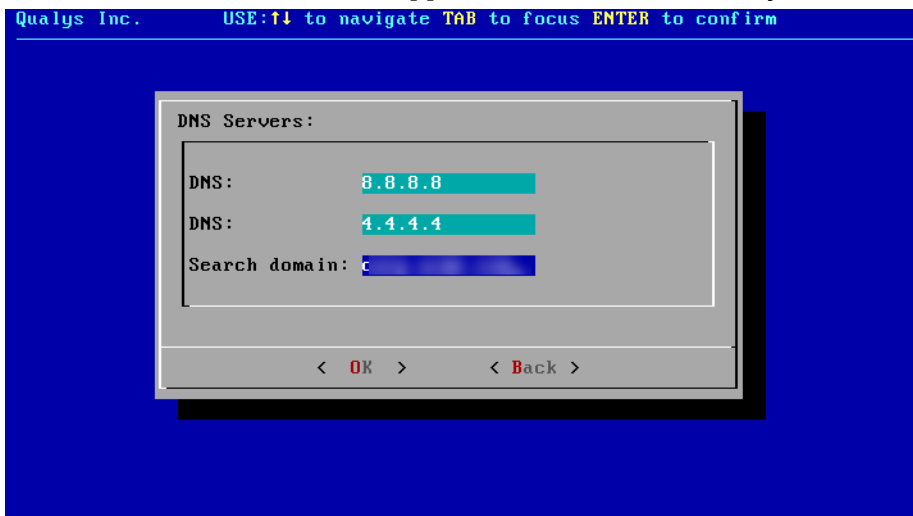
IP address uses a 32-bit netmask, e.g. "/24" for 255.255.255.0

Specify the Default Gateway IP address.



## DNS Servers

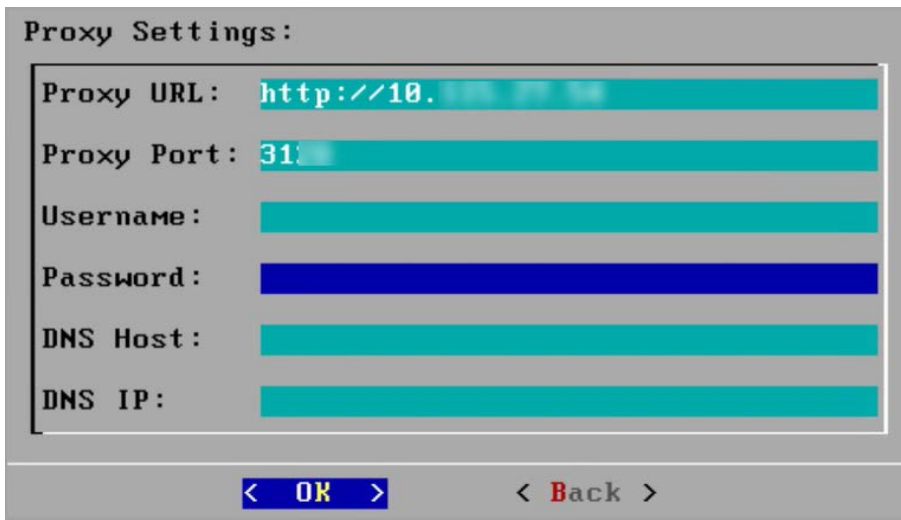
Set DNS servers for the virtual appliance to resolve the Qualys URLs.



We have used Google internet DNS servers as example. Please point to your internal corporate DNS servers. If these are only accessible through a firewall, ports 53/tcp and 53/udp will need to be opened for successful DNS resolution.

## Proxy Servers

Configure upstream Proxy Server, if using proxy chaining.



**Proxy Settings:**

Proxy URL:

Proxy Port:

Username:

Password:

DNS Host:

DNS IP:

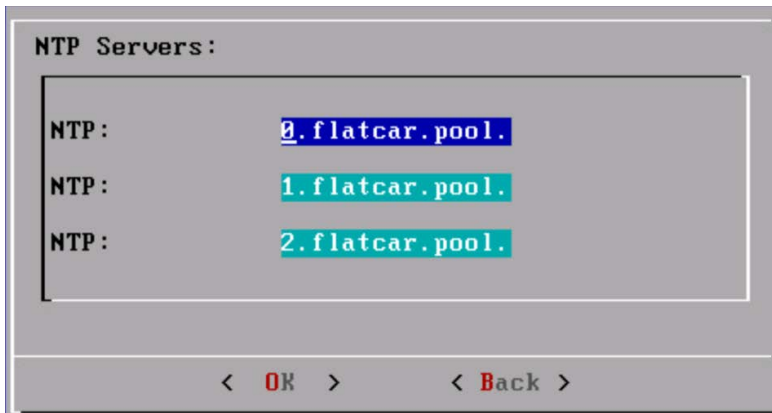
< **OK** >      < **Back** >

### NTP Servers

The NTP service's behavior has changed as follows:

- If NTP servers are not specified, the QGS appliance will use default flatcar NTP servers to sync the time. The default flatcar NTP servers are listed as follows:

- 0.flatcar.pool.ntp.org
- 1.flatcar.pool.ntp.org
- 2.flatcar.pool.ntp.org
- 3.flatcar.pool.ntp.org



**NTP Servers:**

NTP:

NTP:

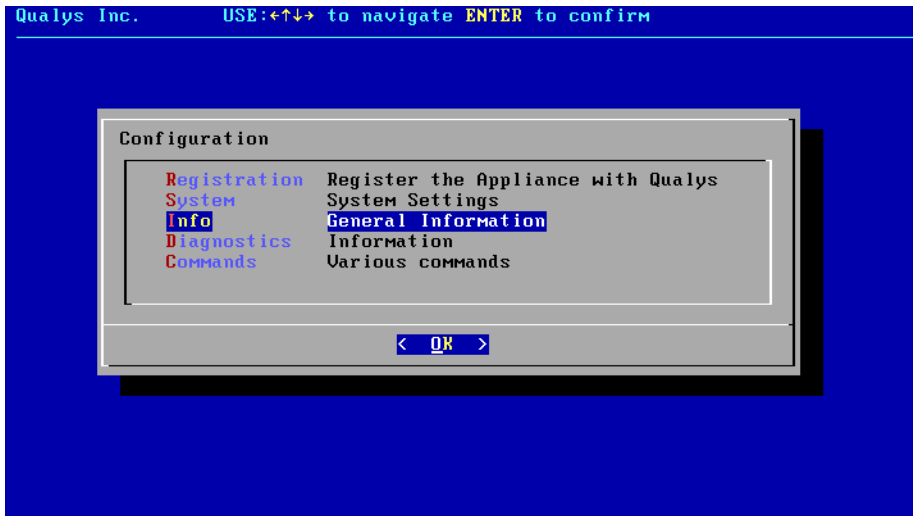
NTP:

< **OK** >      < **Back** >

- If NTP servers are specified, the QGS appliance will contact the specified NTP servers only.

- If you remove the NTP server, the appliance will start communicating to flatcar default NTP servers again.

## Info

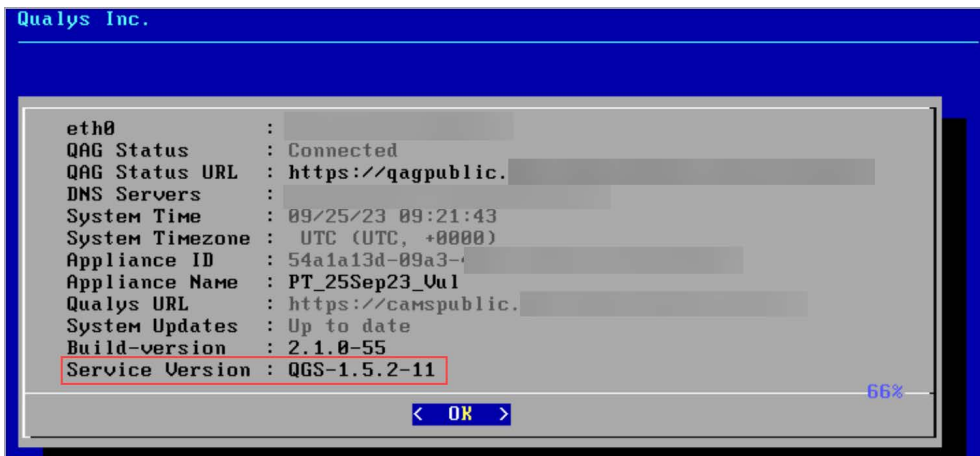


### QAG Status: Connected

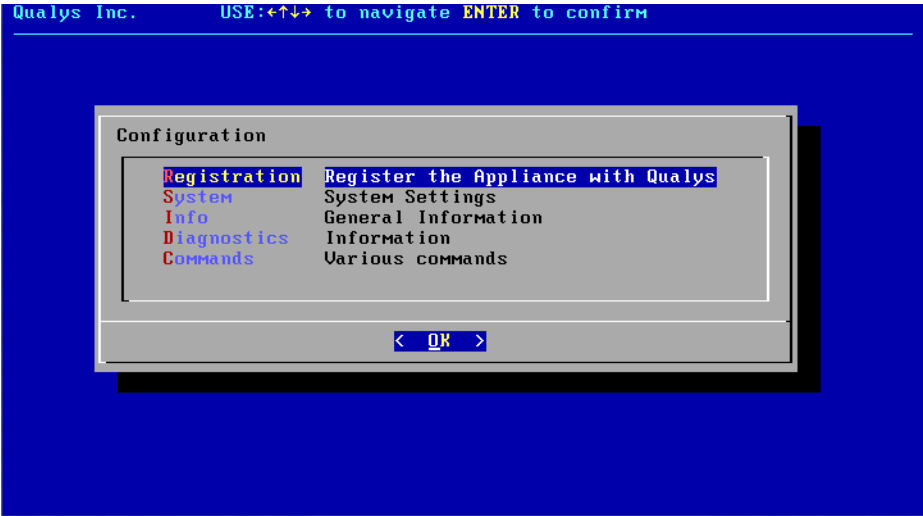
QAG Status: Connected shows that QGS can connect to the Qualys POD.

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.

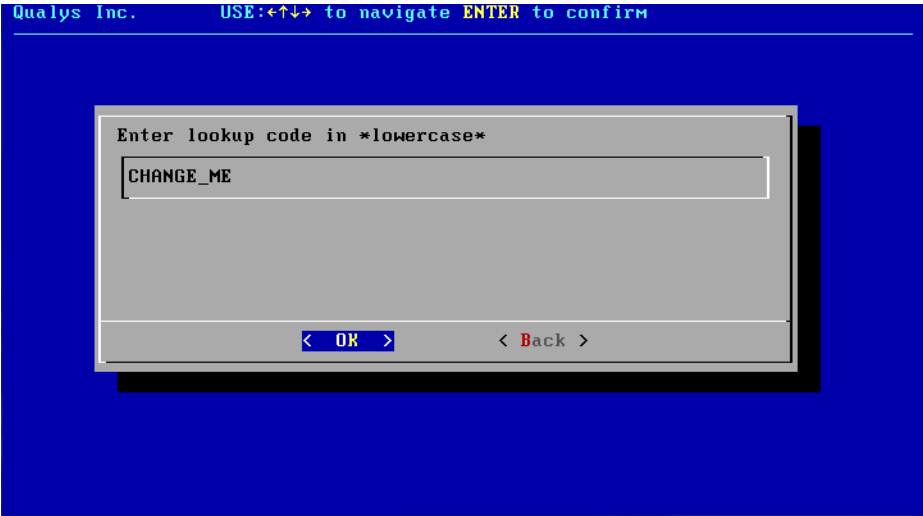


# Registration

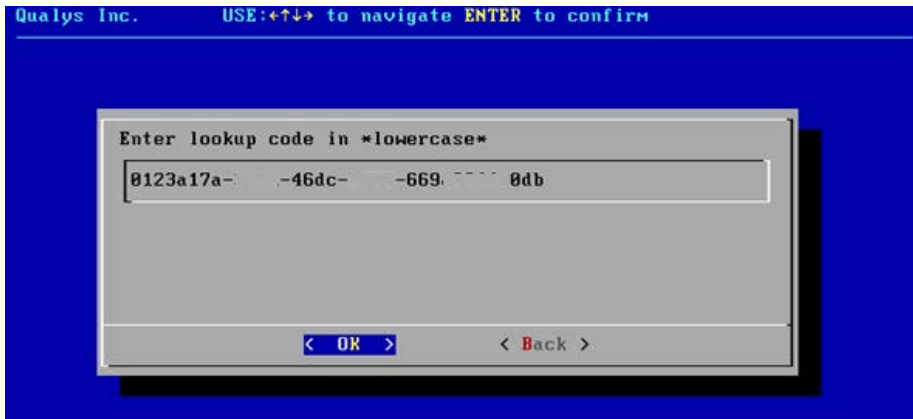


## Personalization Code

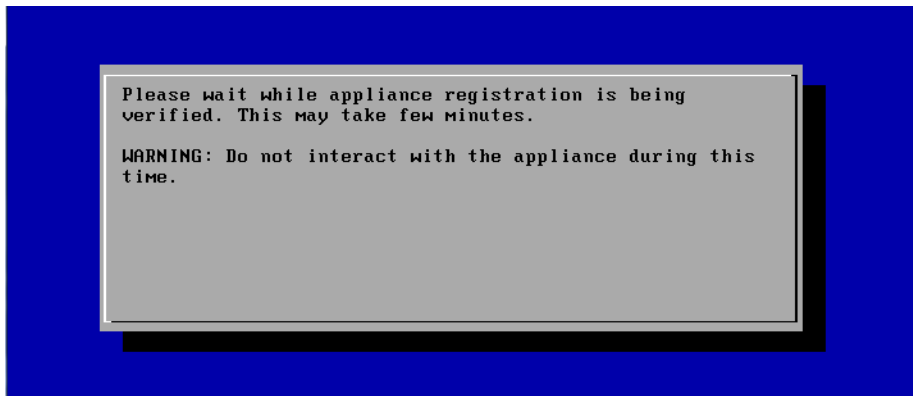
Enter the Personalization Code generated in the QGS User Interface module.



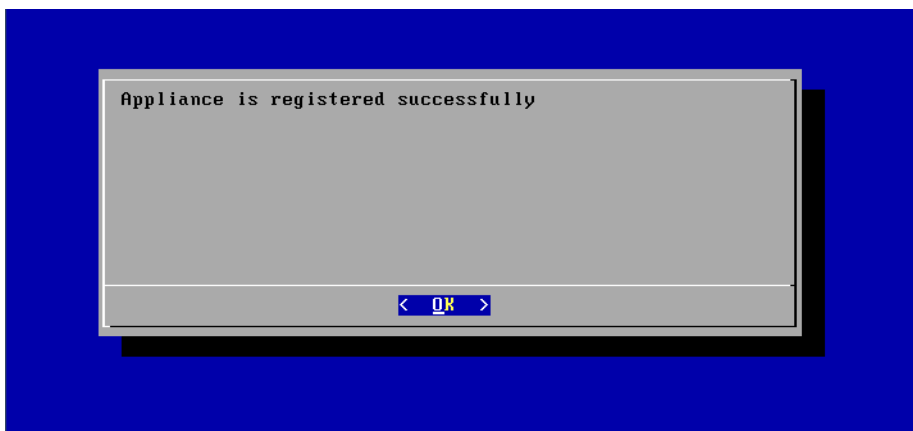
Here's an example of a redacted Personalization Code.



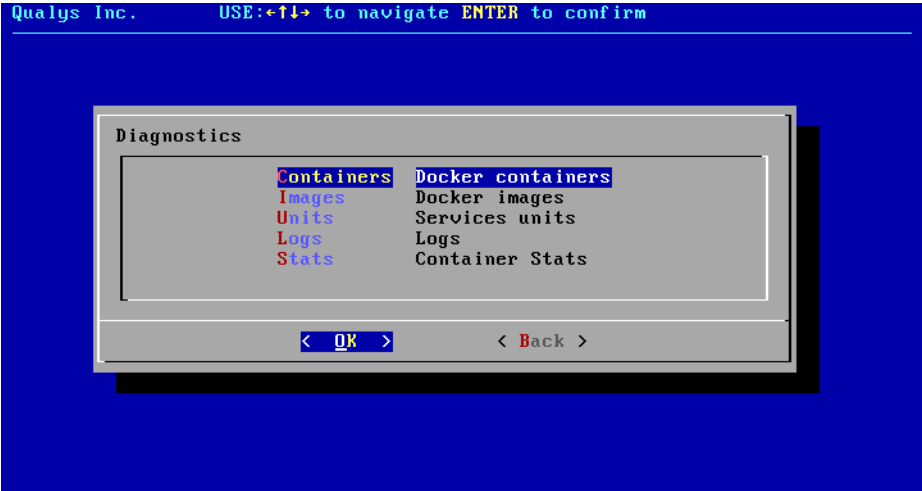
### Registration-in-progress



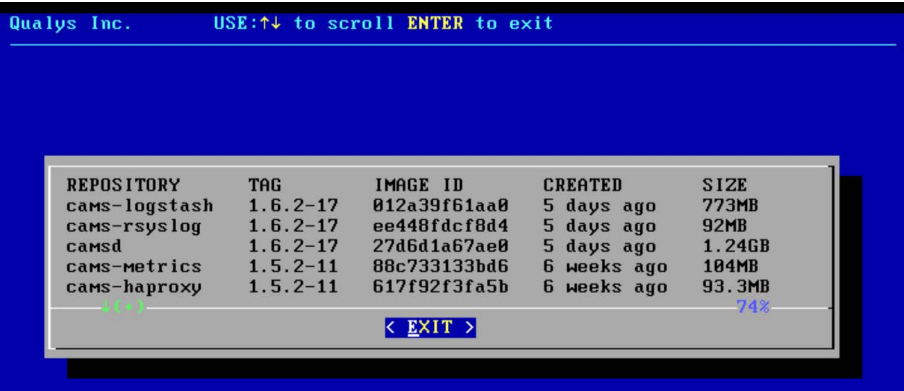
### Successful Registration



# Diagnostics



# Containers



The version can change according to the CAMS/QGS releases and will be conveyed to you with the help of release notes.

You need to wait at least **Two** hrs to enable the cache/patch on the QGSUI until all the latest containers/images are available on the appliance.



Images

You can see **Seven** images and **Eight** containers under **Diagnostics > Images** and **Diagnostics**.

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

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
cams-logstash	1.6.2-17	012a39f61aa0	5 days ago	773MB
cams-rsyslog	1.6.2-17	ee448fdcf8d4	5 days ago	92MB
camsd	1.6.2-17	27d6d1a67ae0	5 days ago	1.24GB
cams-metrics	1.5.2-11	88c733133bd6	6 weeks ago	104MB
cams-haproxy	1.5.2-11	617f92f3fa5b	6 weeks ago	93.3MB

74%

< EXIT >

Units

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

Units	
cams-logstash	active
cams-rsyslog-journal-cat	active
cams-rsyslog	active
CAMSD	active
HAPROXY-reload	failed
HAPROXY-watch	active
HAPROXY	active
internal-proxy	active
qualys-appliance-init	inactive
squid-1	active
squid-2	active

< OK >      < Back >

## 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.

```
Qualys Inc.      USE:↑↓ or PgUp/PgDown to navigate ENTER to exit

  / : search forward ? : search backward
2018-09-12T16:48:45.404202+00:00 cams-rsyslog rsyslogd: [origin softwar
2018-09-12T17:00:00.276990+00:00 cams-rsyslog crond[71]: USER root pid
2018-09-12T17:00:00.277890+00:00 cams-rsyslog crond[71]: USER root pid
2018-09-12T16:48:45+00:00 localhost sh[1298]: + chown -R logstash:logst
2018-09-12T16:48:45+00:00 localhost sh[1298]: + touch /var/log/logstash
2018-09-12T16:48:45+00:00 localhost sh[1298]: + chown logstash:logstash
2018-09-12T16:48:45+00:00 localhost sh[1298]: + chown -R logstash:logst
2018-09-12T16:48:45+00:00 localhost sh[1298]: + [[ -z '' ]]
2018-09-12T16:48:45+00:00 localhost sh[1298]: + exec /usr/share/logstas
2018-09-12T16:48:46+00:00 localhost docker[11531]: 2018-09-12 16:48:46,2
2018-09-12T16:48:46+00:00 localhost docker[11531]: 2018-09-12 16:48:46,2
2018-09-12T16:48:46+00:00 localhost systemd-networkd[646]: veth8702b33:
2018-09-12T16:48:48+00:00 localhost sh[20651]: HAProxy
2018-09-12T16:48:48+00:00 localhost systemd-udevd[21241]: link_config: a
2018-09-12T16:48:48+00:00 localhost kernel: docker0: port 6(veth39cee94
2018-09-12T16:48:48+00:00 localhost kernel: docker0: port 6(veth39cee94

  11/11 8%
```

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

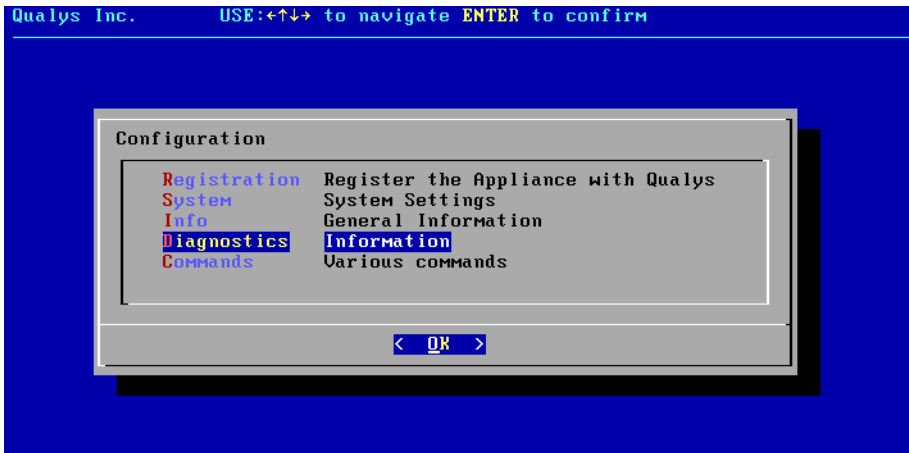
CONTAINER ID      NAME                CPU %      MEM USAGE /
960eb4df3552      HAProxy             0.02%      2.285MiB /
1e480d9ab0f3      CONFD-HAProxy       0.00%      1.656MiB /
f5459536ba9a      cams-logstash       2.45%      501.1MiB /
ffe47a1b904e      squid-2             0.01%      160.4MiB /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

  11/11 56%
```

## Diagnostics Mode

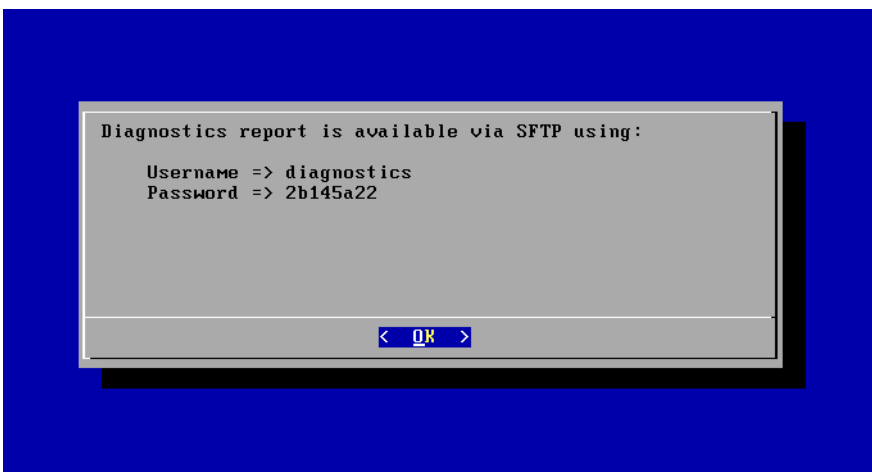
The QGS Appliance supports a Diagnostic mode to help accelerate Qualys Customer Support troubleshooting and problem resolution, primarily for initial network setup and registration issues. The Diagnostic mode is a user-initiated command that creates an encrypted report archive for the customer to collect 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.

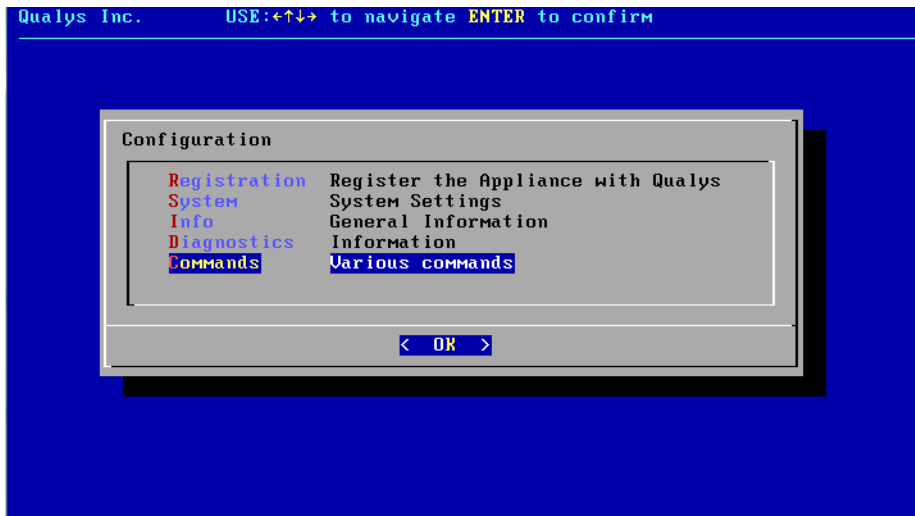
### Generate Upstream PCAP File

Follow these steps to create a packet capture file for the network communications between the QGS and the next hop, upstream.'

1. Navigate to text UI and hit the **Generate TCP dump**. You need to wait for 5 minute.
2. Generate the diagnostics logs as the dump file is captured in diagnostics reports.
3. Any PCAP file previously generated will be overwritten in the process.

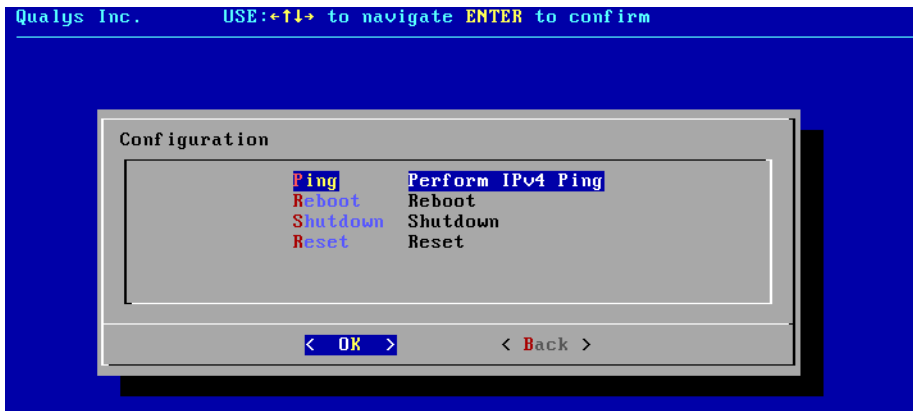
### Commands

You can run commands to restart/reboot the appliance or fetch its ping.

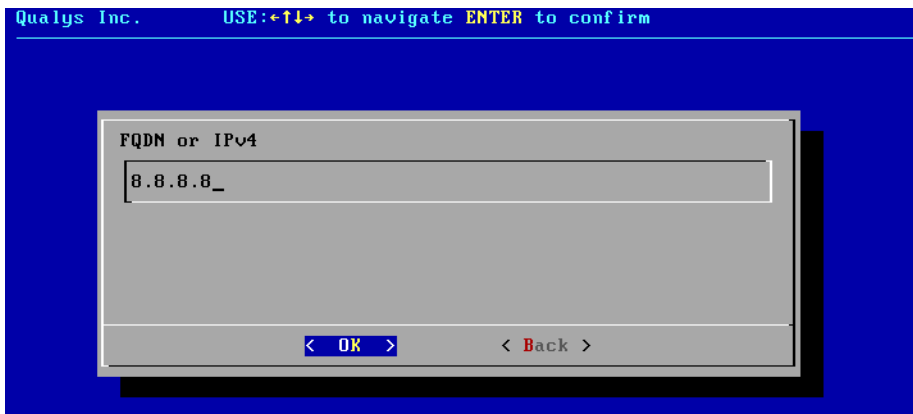


## Ping

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



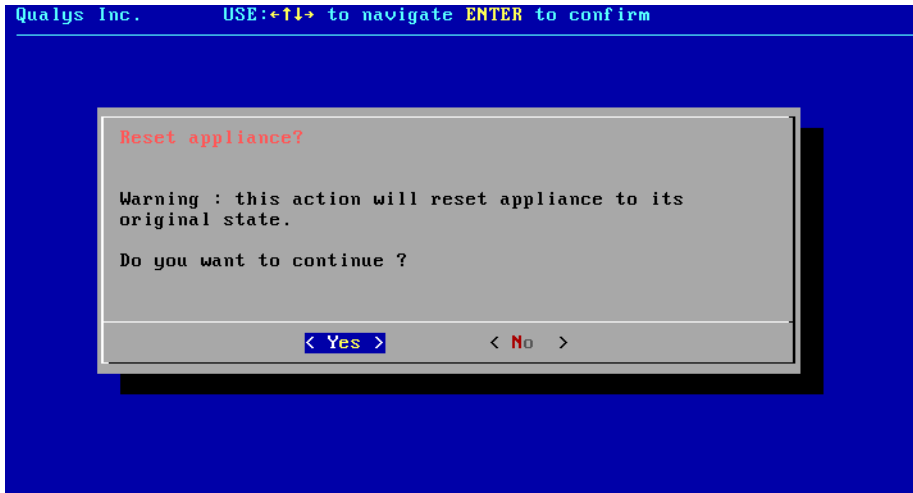
ICMP message types 0 and 8 are required to perform the connectivity checks using ping. When using ping, ensure ICMP 0,8 are enabled for IPs/URLs mentioned in the Network Configuration section.



## Reset appliance

Reset appliance to its original unconfigured state.

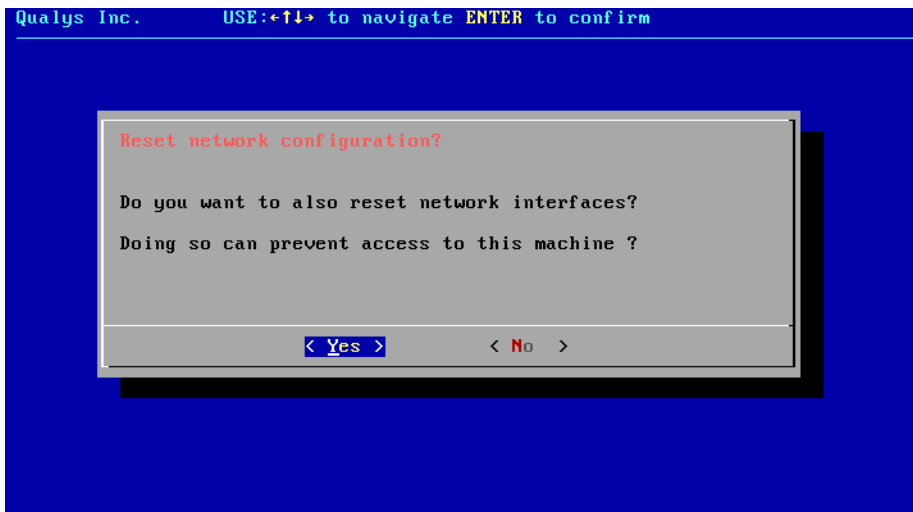
**Warning:** All configurations and log files will be deleted.



## Reset network interface

Reset network interface of virtual appliance.

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

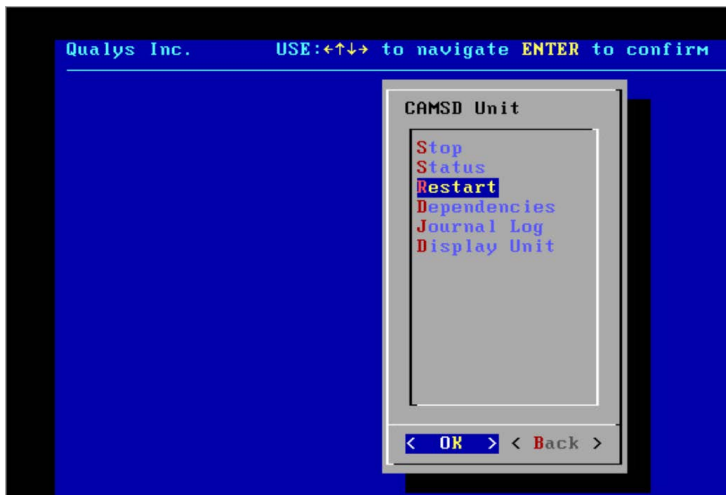


## Appendix - Things to Remember

- 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.
- The appliance logs are not immediately available directly on the root location if the diagnostics logs are generated repeatedly on the same appliance. Instead, it can be found in the "/var/diagnostics" location.

## Frequently Asked Questions

### - How do I know whether the appliance is upgraded to the latest services or not?

Go to the appliance's Text User Interface (TUI), click the **Info** tab and click **OK** to see the details.

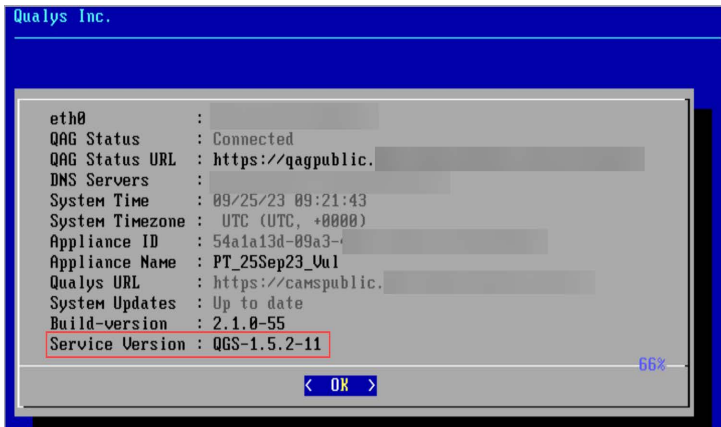
- When the minimum requirement for the primary disk and RAM are not fulfilled, the following message is shown on the appliance TUI under the Info tab.



- A Minimum 16GB of RAM is recommended for CAMS/QGS appliances. A total of 3000 concurrent cloud agent requests are supported by a QGS appliance. In case of more than 3000 agents communicating simultaneously, customers should deploy a new appliance instead of increasing RAM on the existing appliance.

### - How do I know whether the appliance is upgraded to the latest version or not?

Go to the appliance's Text User Interface (TUI), click the **Info** tab and click **OK** to see the appliance is upgraded to the latest version or not.

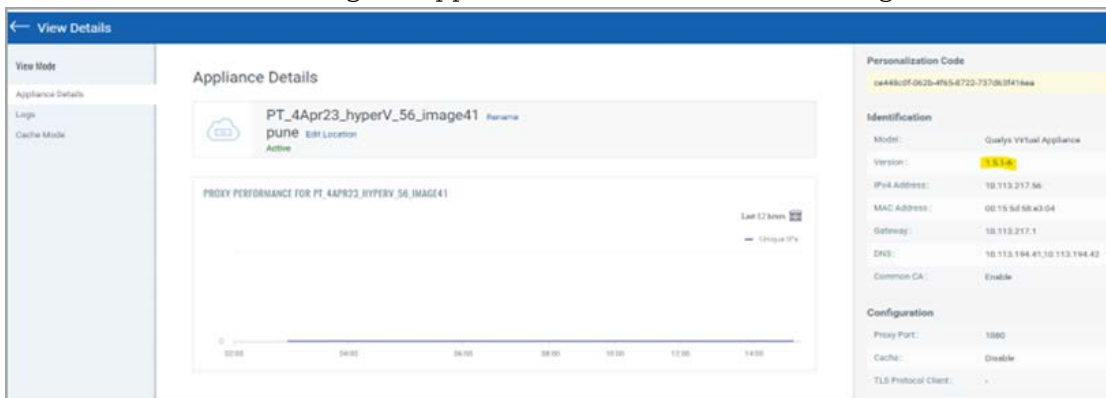


You can verify that all the latest images are present on the appliances by navigating to **TextUI > Diagnostics > Images**. Refer to the following screenshot.



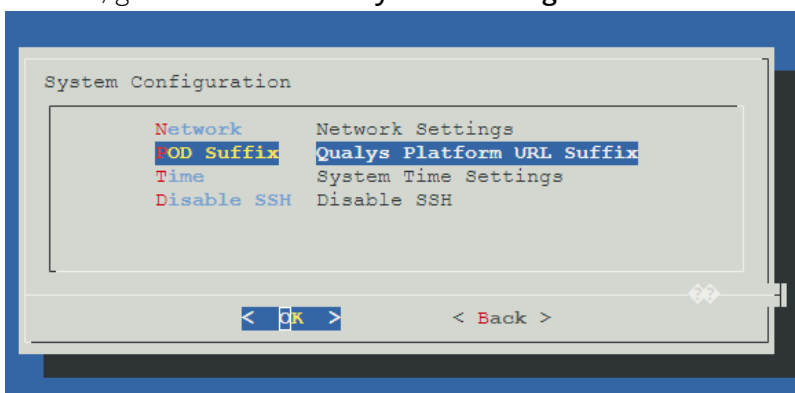


Also, you can verify the appliance with the latest image version by navigating to the QGS UI > **APPLIANCES** > clicking the Appliance. As shown in the following screenshot.



### - How to add POD suffix details for the image version 2.1.0 and above using TextUI

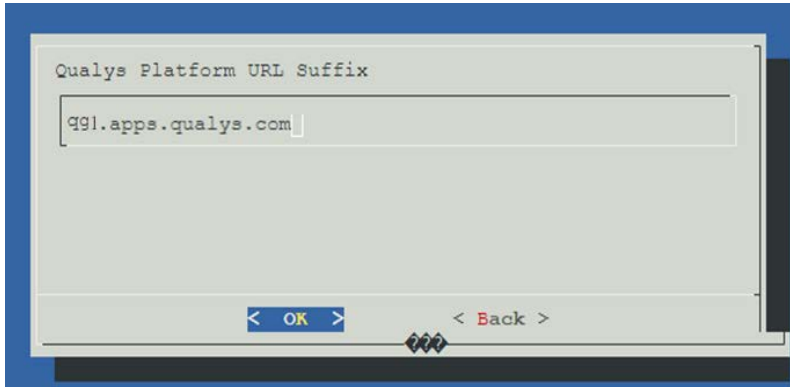
You can add a POD suffix details for the image version **2.1.0 and above** for all supported formats; go to the **TextUI** > **System Settings** > **POD Suffix**.



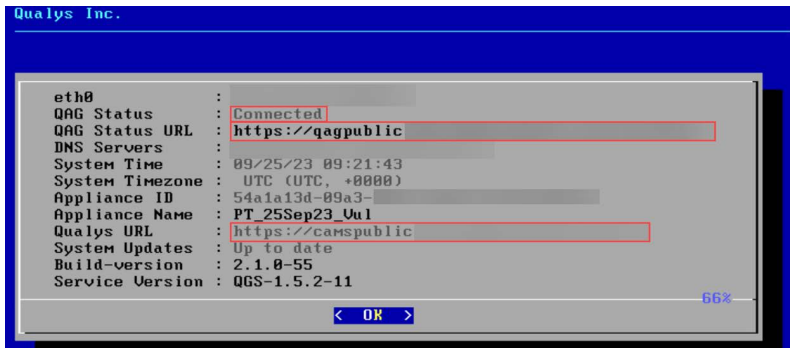
The POD Suffix option will be grayed out after the successful upgradation of the existing appliances deployed with image version 1.1.0.

To know the POD suffixes for corresponding PODs, refer to the [POD Suffixes](#) table.

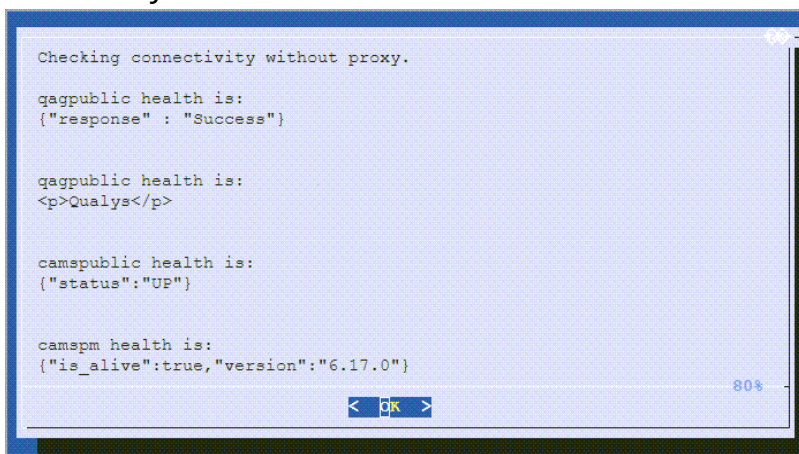
**Note:** We recommend entering the correct POD suffix because the cloud metadata services will always overwrite an incorrectly entered POD suffix.



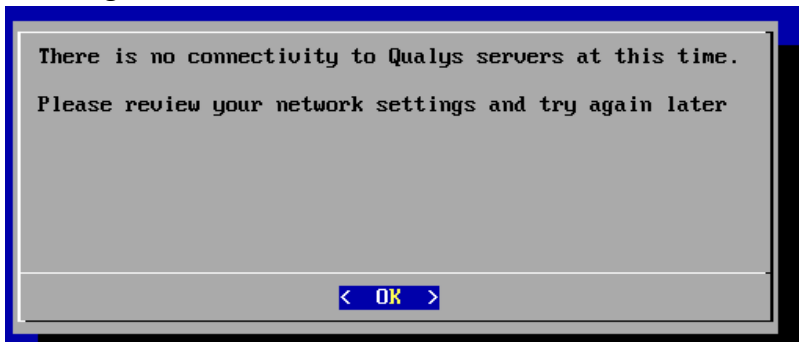
Go to the **Information** tab to check the connected status and pod suffix with qagpublic and camspublic. As highlighted in the following screenshot.



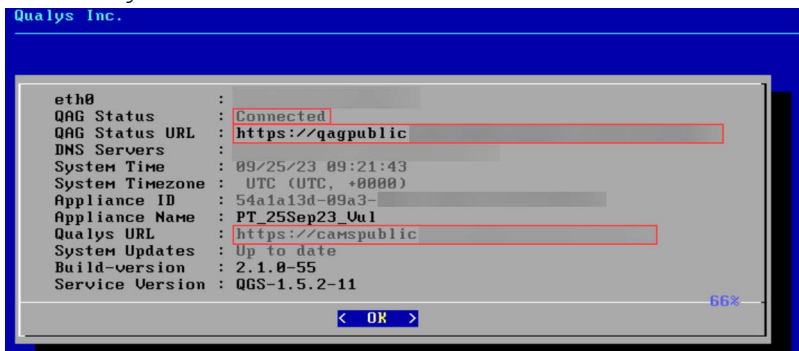
To check the connectivity with the backend services; go to the **TextUI > Diagnostics > Connectivity**.



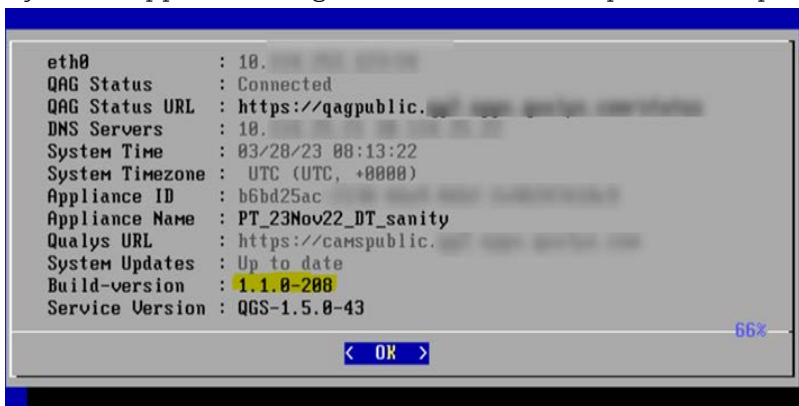
If any of the services from CAMSPM, CAMSREPO, camspublic, and qagpublic is not connected to the appliance, you cannot register the appliance. You will observe the following error shown on the screenshot.



If you use appliance image version 2.1.0 and above, you must provide a POD Suffix as the mandatory field.



If you use appliance image version 1.1.0 -X, the pod suffix option will not be available.



## POD Suffixes

To identify the Platform URL Suffix for your subscription, refer to the *Platform URL Suffix* section of the [Qualys Platform Identification](#).