

Qualys Gateway Service

User Guide
Version 1.8

February 10, 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 **8**
Qualys Gateway Service Module User Interface 13
Virtual Appliance Local Configuration 16
Configuration Screens 16

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	VMDK, OVA, OVF
Microsoft Hyper-V	2012, 2012 R2, 2016	VHD

Virtual Machine Configuration

- 2 vCPUs
- 8 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

Network Configuration

QGS requires connectivity to four (4) URLs/IPs 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/IPs.

- One URL/IP is for Cloud Agents to connect through QGS to the Qualys Platform
- Three URLs/IPs are for QGS to connect to Qualys Platform for management functions
- One URL/IP is for operating system updates as this appliance is based on Flatcar Linux

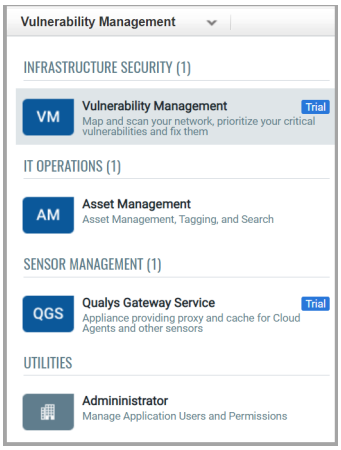
Platform	Cloud Agent	Qualys Gateway Service
US 1	qagpublic.qg1.apps.qualys.com (64.39.104.93:443)	camspublic.qg1.apps.qualys.com (64.39.96.183:443) camspm.qg1.apps.qualys.com (64.39.96.181:443) camsrepo.qg1.apps.qualys.com (64.39.96.182:443) update.release.flatcar-linux.net
US 2	qagpublic.qg2.apps.qualys.com (64.39.104.103:443)	camspublic.qg2.apps.qualys.com (64.39.96.179:443) camspm.qg2.apps.qualys.com (64.39.96.177:443) camsrepo.qg2.apps.qualys.com (64.39.96.178:443) update.release.flatcar-linux.net
US 3	qagpublic.qg3.apps.qualys.com (64.39.104.113:443)	camspublic.qg3.apps.qualys.com (64.39.96.175:443) camspm.qg3.apps.qualys.com (64.39.96.173:443) camsrepo.qg3.apps.qualys.com (64.39.96.174:443) update.release.flatcar-linux.net
US 4	qagpublic.qg4.apps.qualys.com (139.87.107.253:443)	camspublic.qg4.apps.qualys.com (139.87.106.68:443) camspm.qg4.apps.qualys.com (139.87.105.91:443) camsrepo.qg4.apps.qualys.com (139.87.104.252:443) update.release.flatcar-linux.net
EU 1	qagpublic.qg1.apps.qualys.eu (64.39.100.93:443)	camspublic.qg1.apps.qualys.eu (64.39.100.50:443) camspm.qg1.apps.qualys.eu (64.39.100.51:443) camsrepo.qg1.apps.qualys.eu (64.39.100.52:443) update.release.flatcar-linux.net
EU 2	qagpublic.qg2.apps.qualys.eu (154.59.121.74:443)	camspublic.qg2.apps.qualys.eu (154.59.121.88:443) camspm.qg2.apps.qualys.eu (154.59.121.86:443) camsrepo.qg2.apps.qualys.eu (154.59.121.87:443) update.release.flatcar-linux.net
IN 1	qagpublic.qg1.apps.qualys.in (103.216.98.40:443)	camspublic.qg1.apps.qualys.in (103.216.98.50:443) camspm.qg1.apps.qualys.in (103.216.98.51:443) camsrepo.qg1.apps.qualys.in (103.216.98.52:443) update.release.flatcar-linux.net
CA 1	qagpublic.qg1.apps.qualys.ca (64.39.97.135:443)	camspublic.qg1.apps.qualys.ca (64.39.97.143:443) camspm.qg1.apps.qualys.ca (64.39.97.144:443) camsrepo.qg1.apps.qualys.ca (64.39.97.145:443) update.release.flatcar-linux.net

Platform	Cloud Agent	Qualys Gateway Service
AE 1	qagpublic.qg1.apps.qualys.ae (193.123.67.247:443)	camspublic.qg1.apps.qualys.ae (193.123.67.119:443) camspm.qg1.apps.qualys.ae (193.123.66.50:443) camsrepo.qg1.apps.qualys.ae (193.123.70.220:443) update.release.flatcar-linux.net
UK1	qagpublic.qg1.apps.qualys.co.uk (151.104.33.9:443)	camspublic.qg1.apps.qualys.co.uk (151.104.32.191:443) camspm.qg1.apps.qualys.co.uk (151.104.34.156:443) camsrepo.qg1.apps.qualys.co.uk (151.104.32.108:443) update.release.flatcar-linux.net
AU 1	qagpublic.qg1.apps.qualys.com.au (152.67.106.2:443)	camspublic.qg1.apps.qualys.com.au (168.138.104.94:443) camspm.qg1.apps.qualys.com.au (168.138.109.86:443) camsrepo.qg1.apps.qualys.com.au (168.138.104.114:443) update.release.flatcar-linux.net

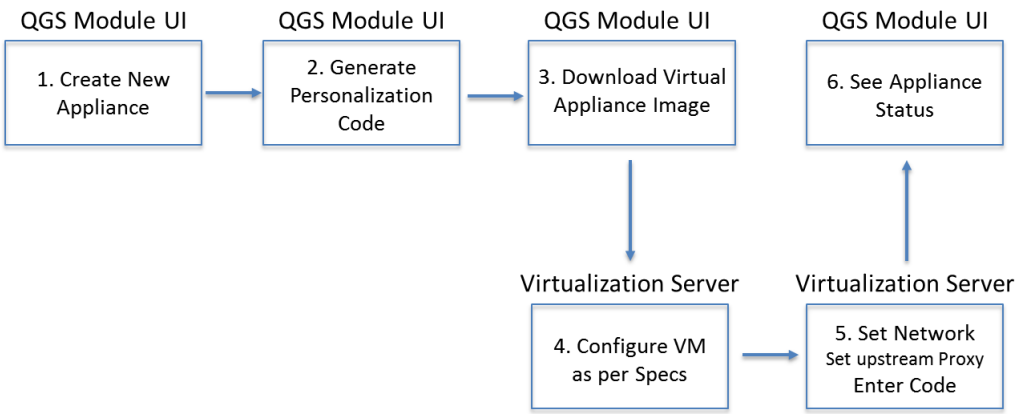
Qualys Gateway Service User Interface Module

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 caching for Qualys Patch Management requires a second virtual hard drive to be added to the virtual appliance before Patch Cache Mode can be enabled as a feature. 100-250GB is recommended.

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

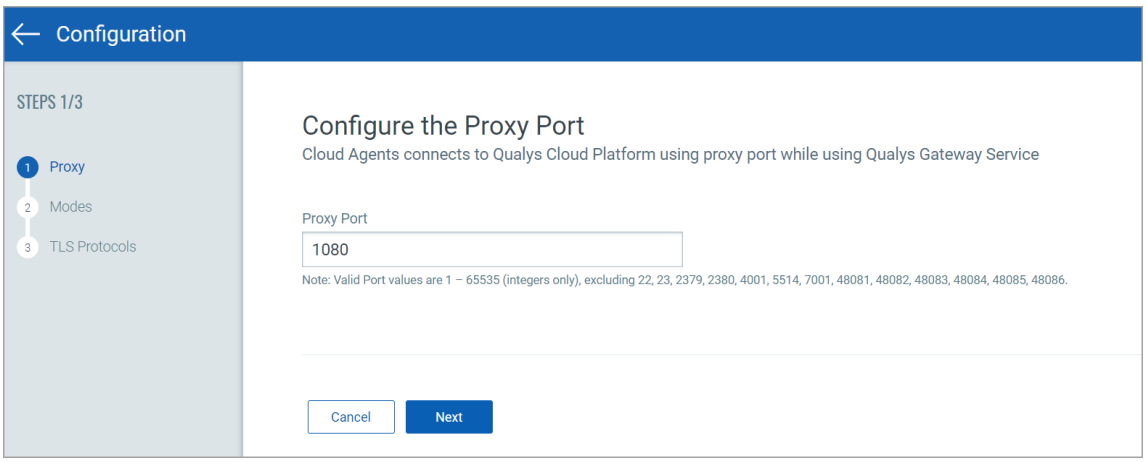
After successful appliance deployment and registration, you can change the proxy port from default 1080 to any allowable port number.

Note: In the proxy mode, the QGS appliance can work as a transparent proxy, and traffic can be routed to any domain. Also, there is no caching of the requested artifact within the appliance.

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.

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 will 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 the 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.

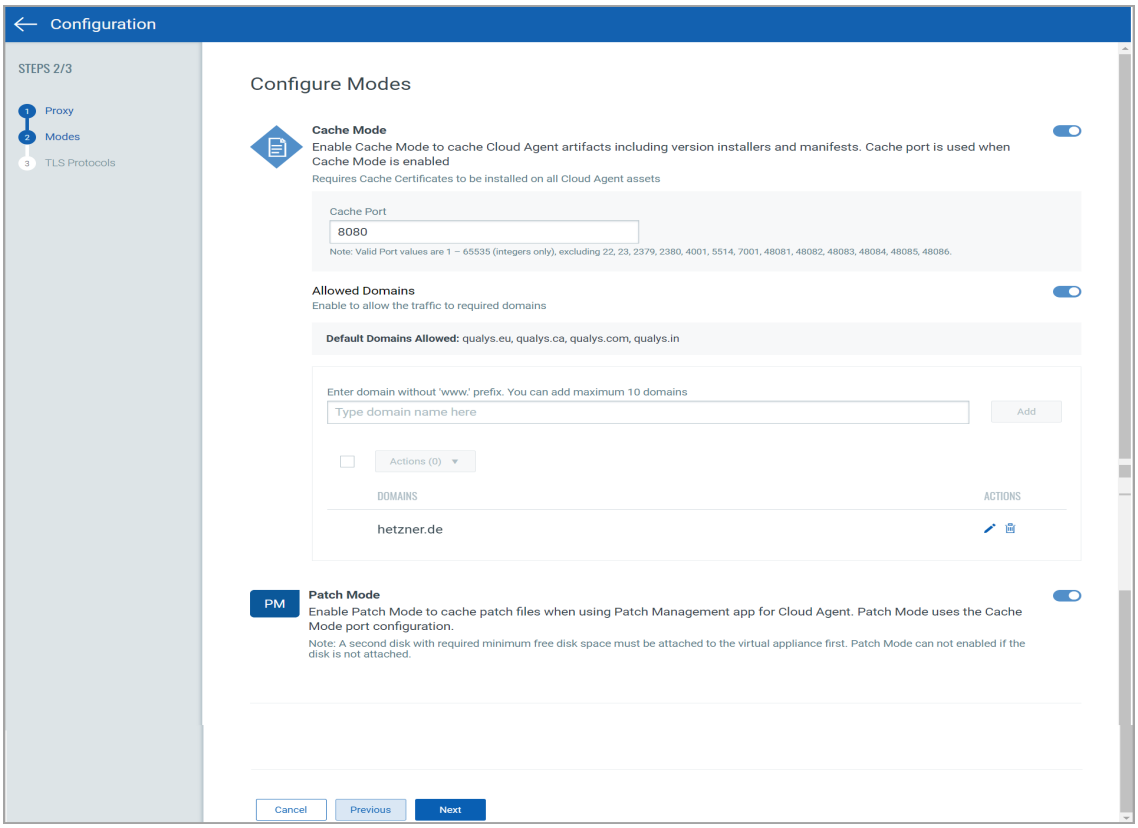
Note: Valid Port values are 1 – 65535 (integers only), excluding 22, 23, 2379, 2380, 4001, 5514, 7001, 48081, 48082, 48083, 48084, 48085, 48086.

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

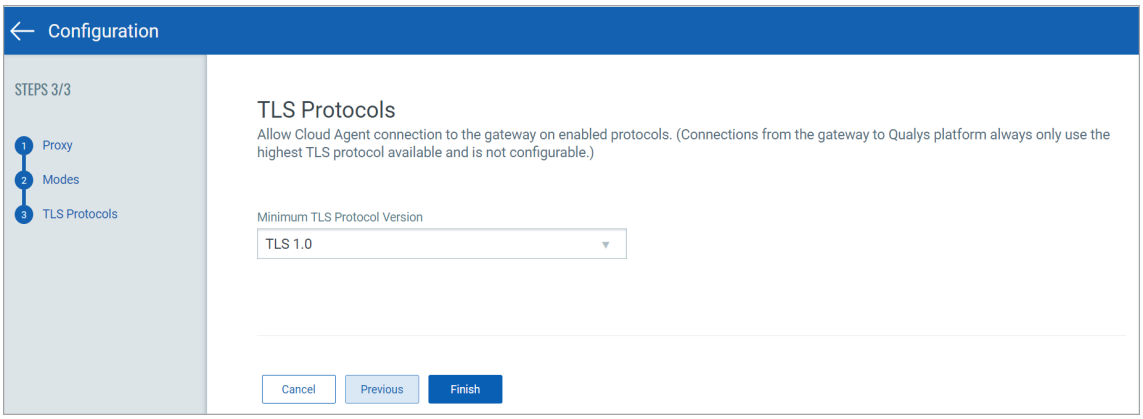


6) To enable Patch Mode, toggle the On/Off slider to **On**

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



Note: To enable this mode, a second virtual disk drive of at least 10 GB (100-250 GB recommended) must 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.

Cloud Agent Windows 3.1 supports multiple proxy servers (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.

Cloud Agent Linux, AIX, and Mac add this feature in the upcoming version 2.5 release.

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

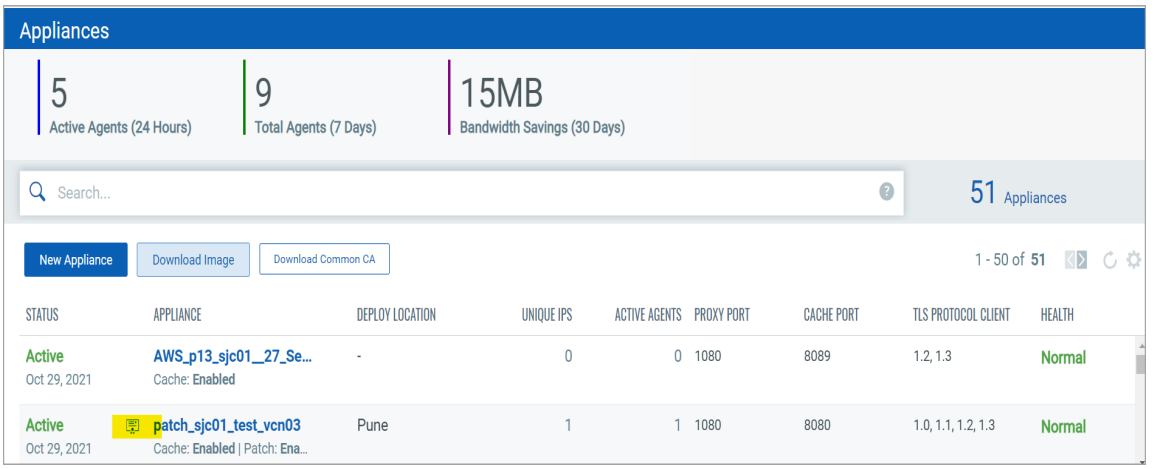
- Use any supported software distribution tool to deploy the certificate PEM to the host certificate store

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.

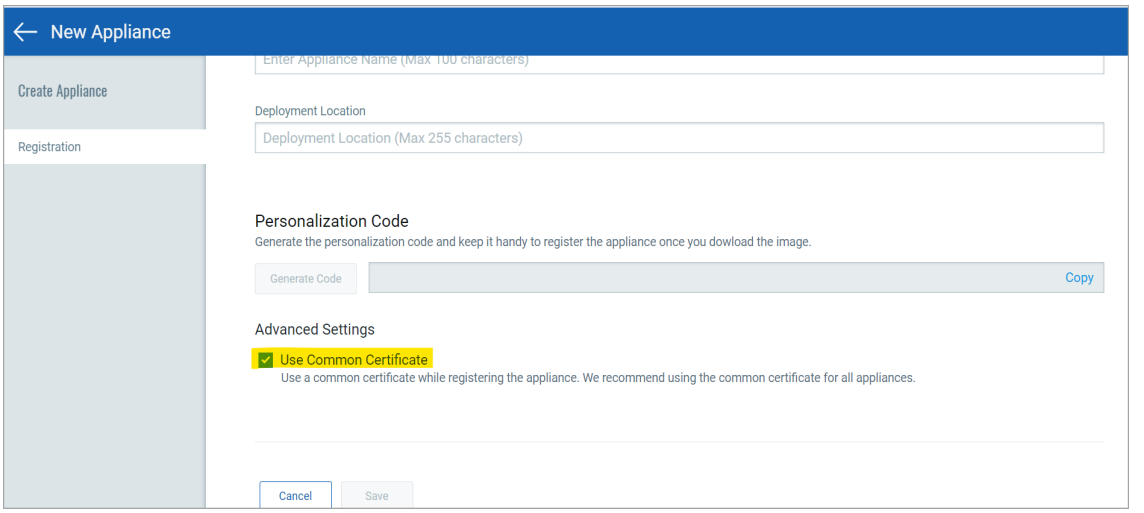
- Status: This column shows the current status of your appliance. Appliances with common CA certificate enabled will be shown an icon (Highlighted) on the appliance list page.

- Unique IPs: This column shows the count of unique IPs which were communicated through QGS appliance from last 60 minutes.

- Active Agents: This column shows the number of active agents communicated via QGS from last 24 hours when QGS and Cloud Agent are configured to be used in **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

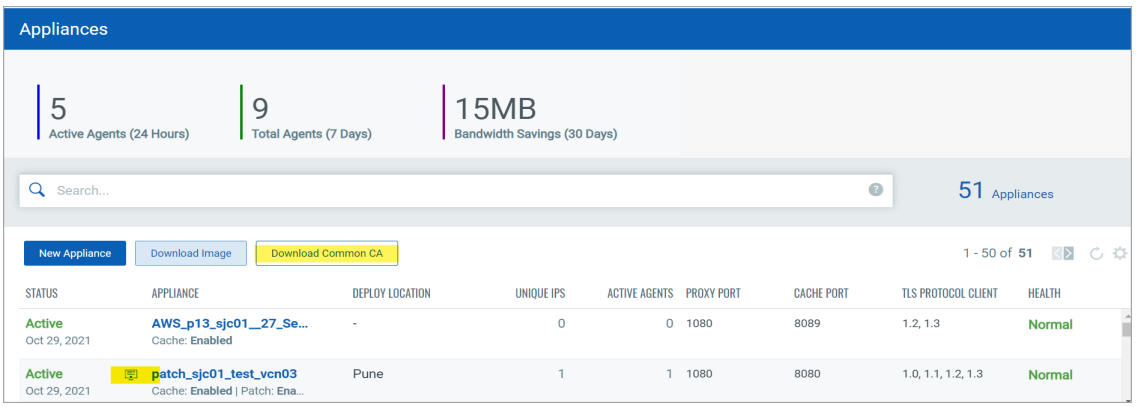


The appliance can be created with a Common CA certificate enabled. It can help you to deploy a single certificate across all the cloud agents meant for the particular appliance.

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.

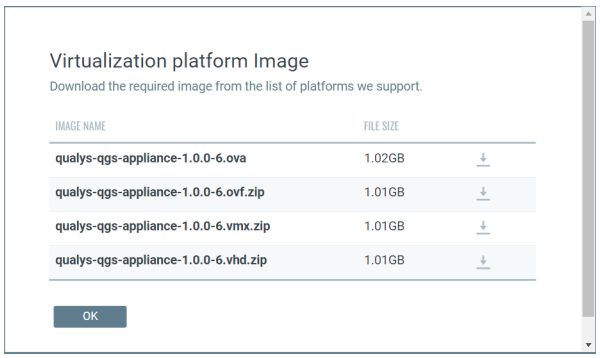
View List of Appliances and their Status



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.

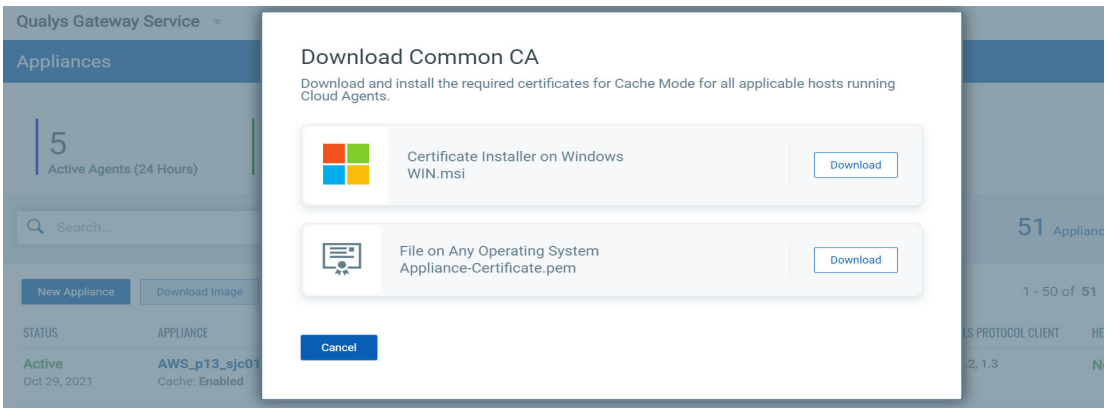
Download Image of the Virtual Appliance



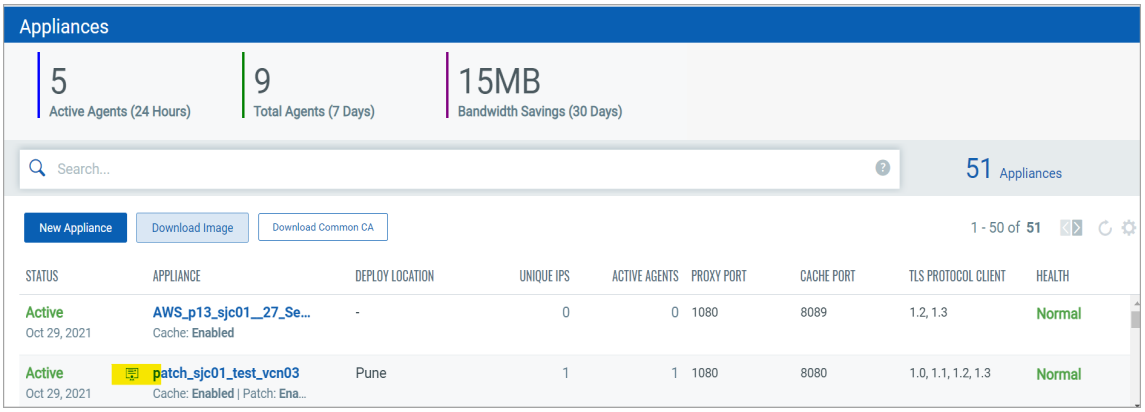
Download Common CA

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

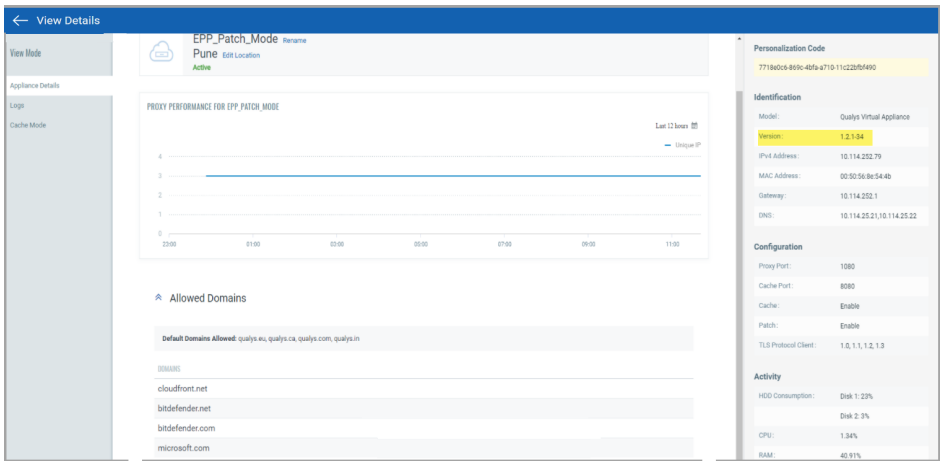
Note: To download the common CA Certificate, you must create or register a new appliance with the common CA certificate option enabled. It is not possible to download the common CA Certificate if you are using the existing appliances.



After Successful Setup and Registration, the Appliance has Active Status



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.

Note: The “version” displayed in the right-hand pane of the QGSUI Appliance Details page is the QGS Manifest version, which is similar across all Pods. (Highlighted in the above screenshot).

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

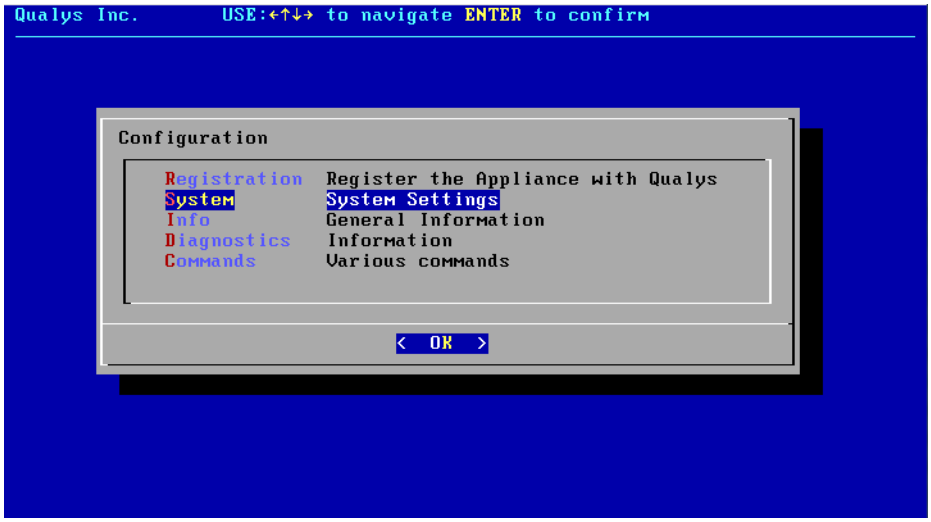
Next we'll document the screens used to configure & manage the Qualys Gateway Service.

QGS virtual appliance starting up

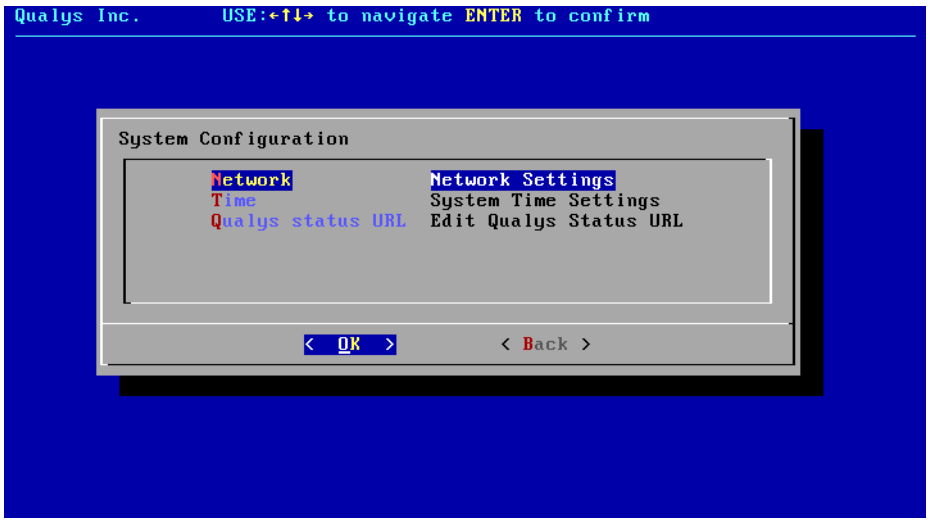


Main Configuration Menu

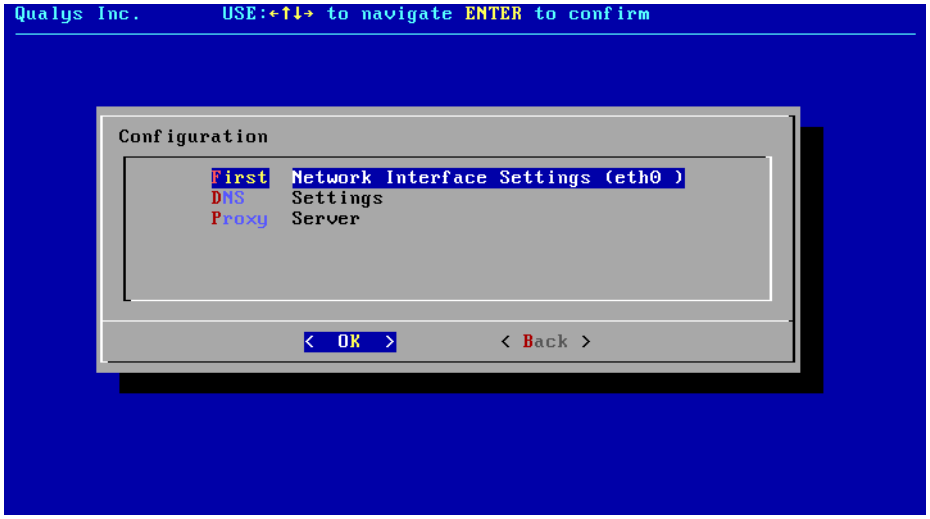
Under System menu, configure Network Settings



Network Configuration



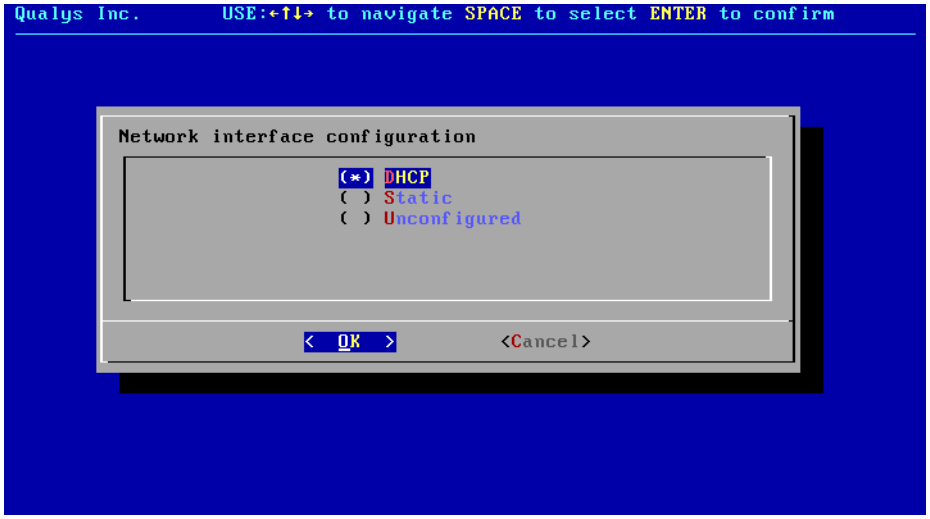
First ethernet interface



DHCP

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

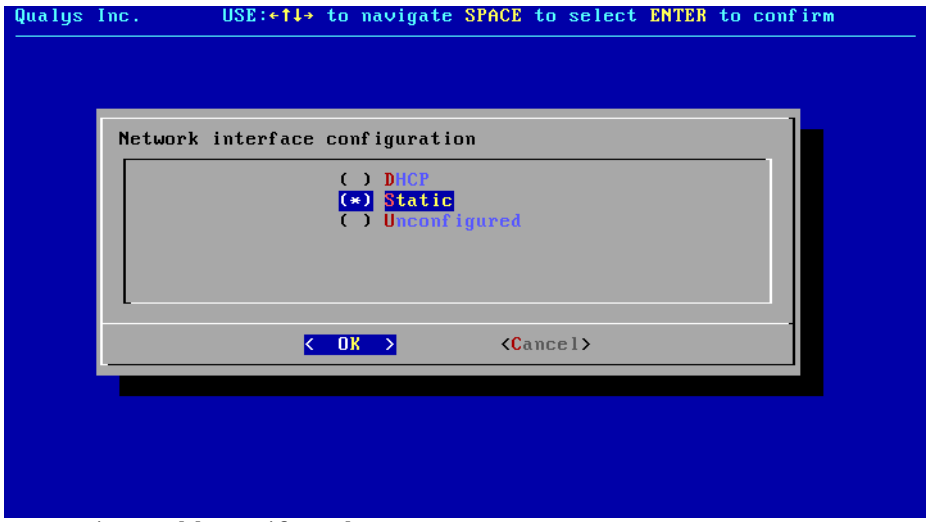
This is the IP of the QGS proxy that Cloud Agents will connect running on port 1080.



Static

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

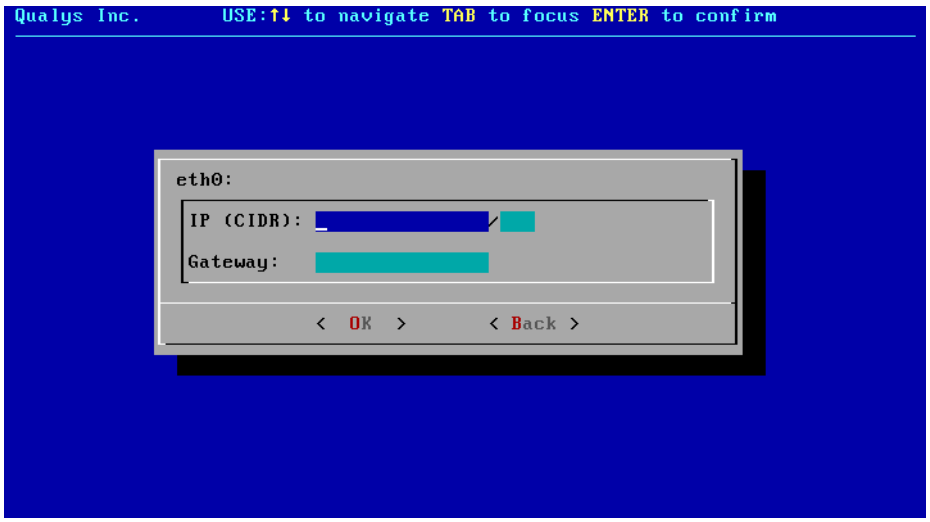
Cloud Agents connect to the Static IP Address on port 1080.



Set static IP address, if used.

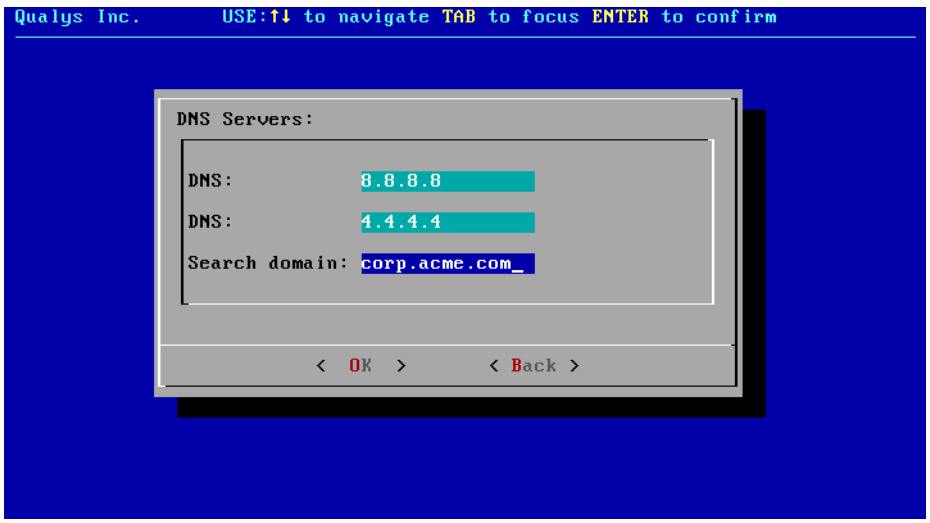
IP address uses a 32-bit netmask, e.g. “/24” for 255.255.255.0

Specify the Default Gateway IP address.



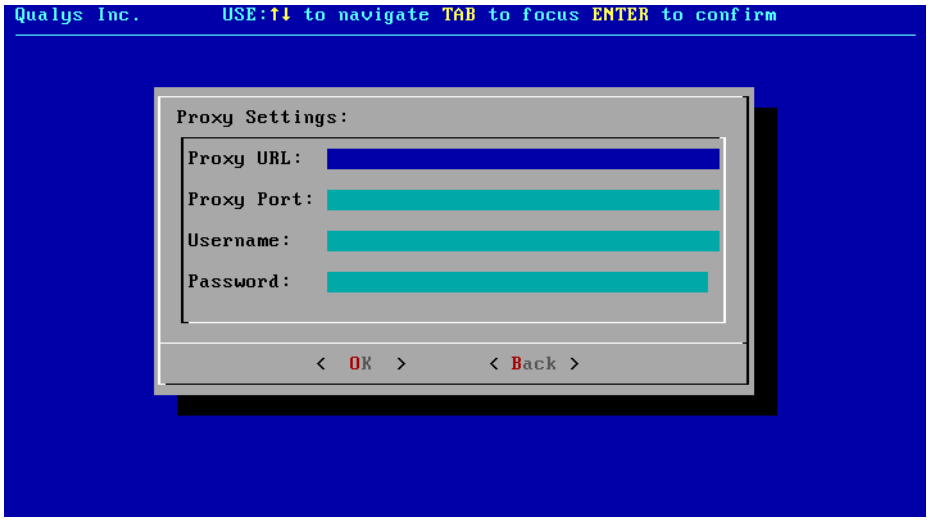
DNS Servers

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

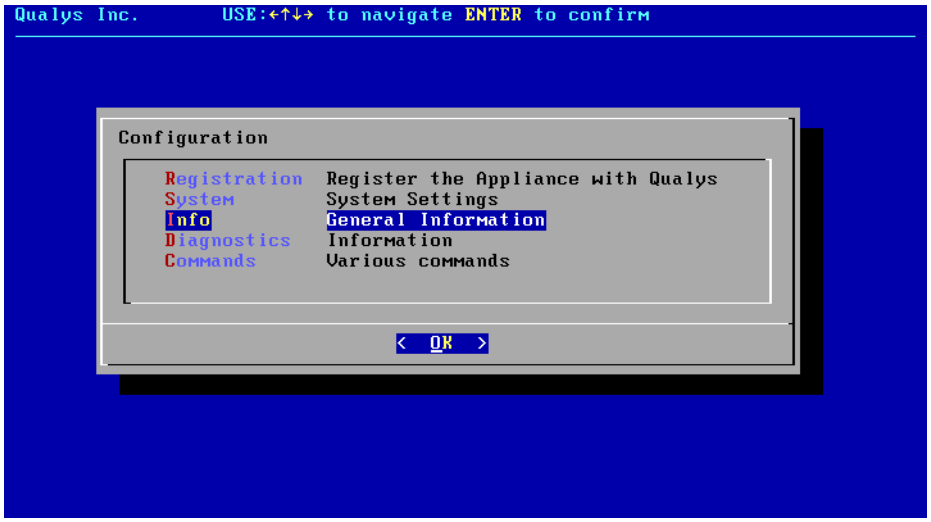


Proxy Servers

Configure upstream Proxy Server, if using proxy chaining.



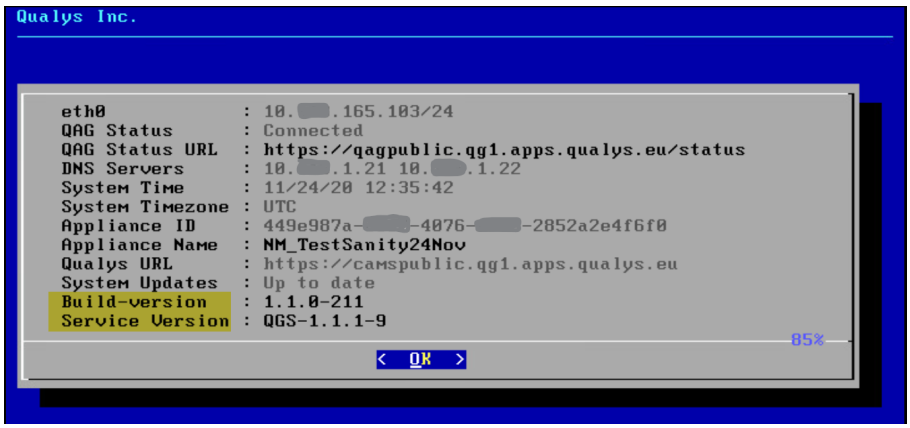
Info



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.

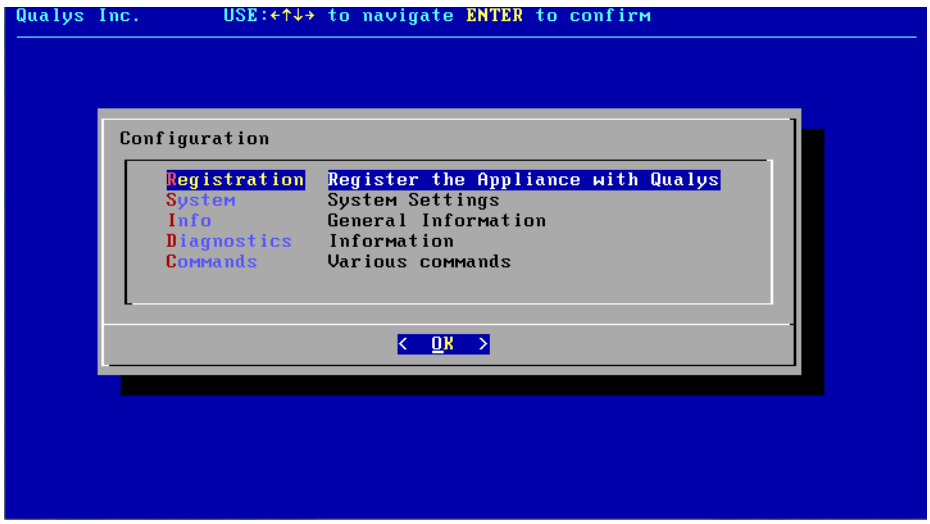


Note: On the above image, we have highlighted the build version and service version.

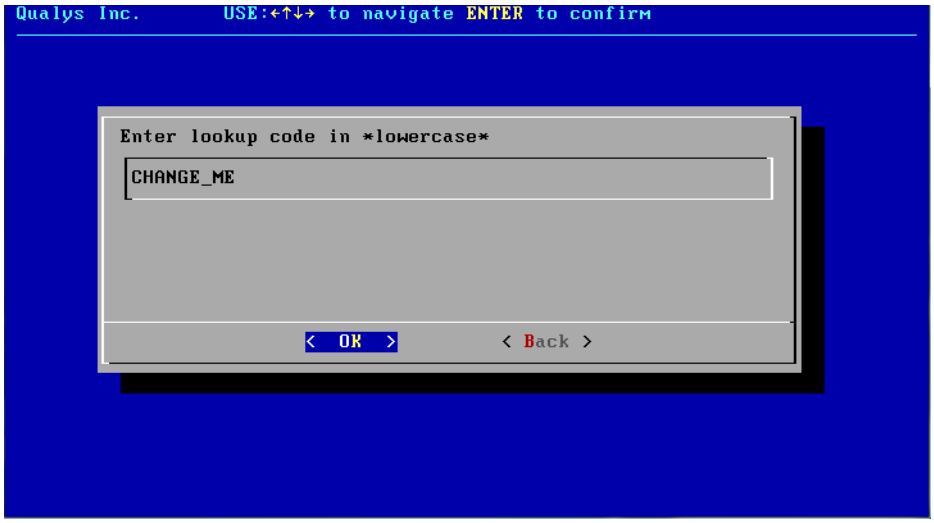
Build Version: This is the appliance build version which is available as "Virtualization Platform Image" on QGSUI.

Service Version: This is the QGS manifest version which is available as a Version on the Appliance detail page on QGSUI.

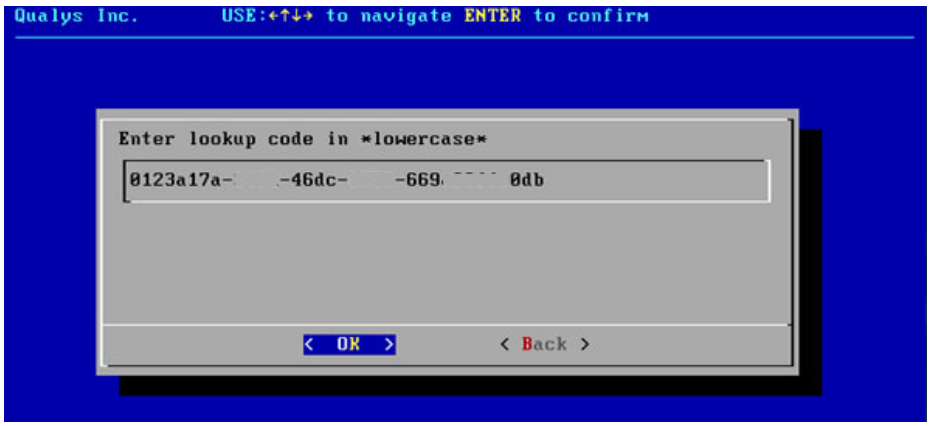
Registration



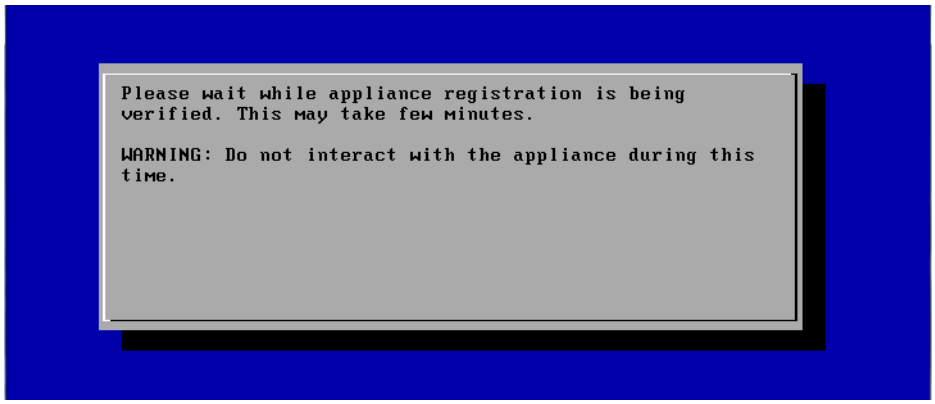
Enter the Personalization Code generated in the QGS User Interface module.



Here's an example of a redacted Personalization Code.



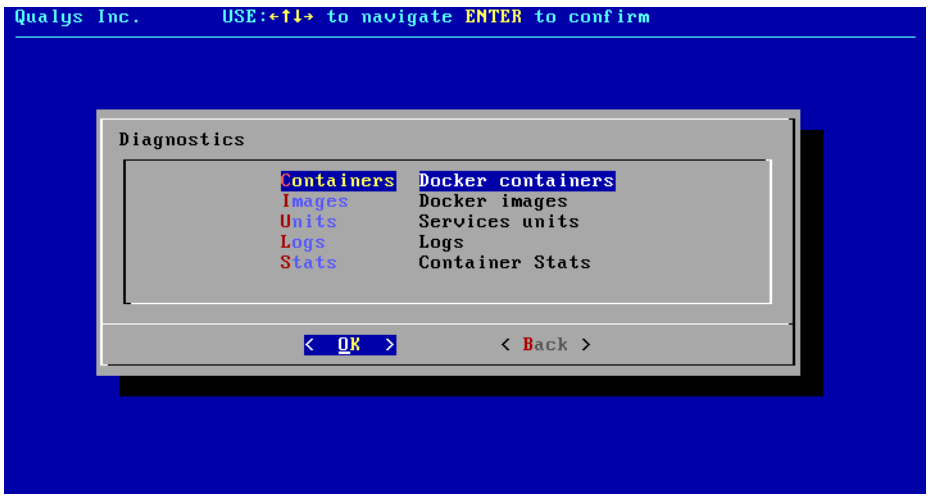
Registration in process



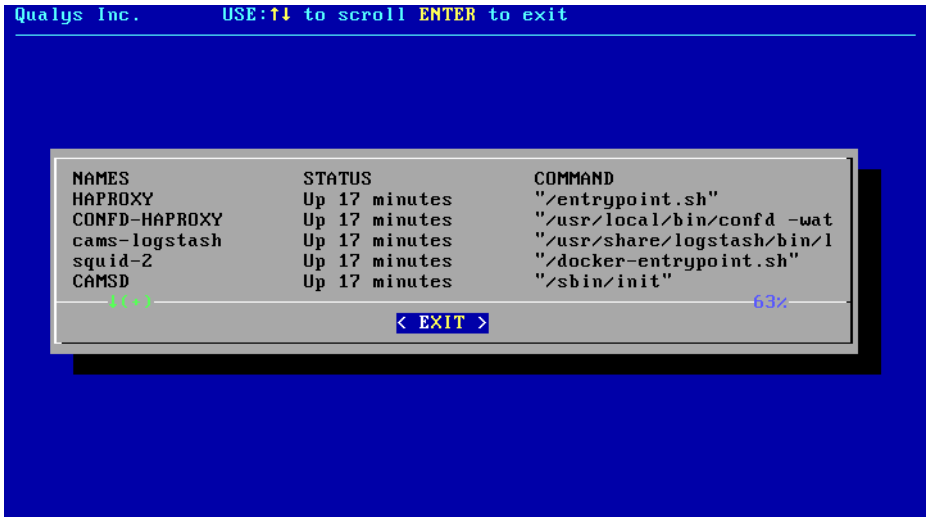
Successful Registration



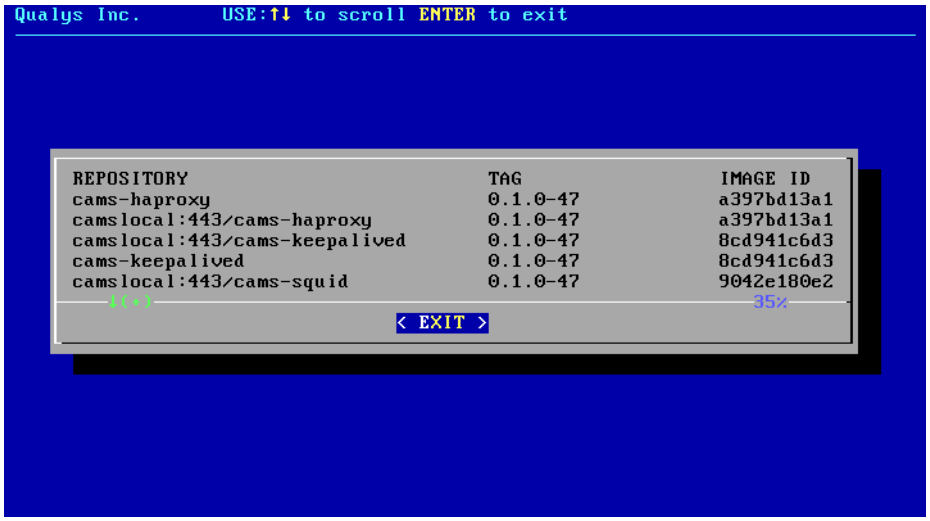
Diagnostics



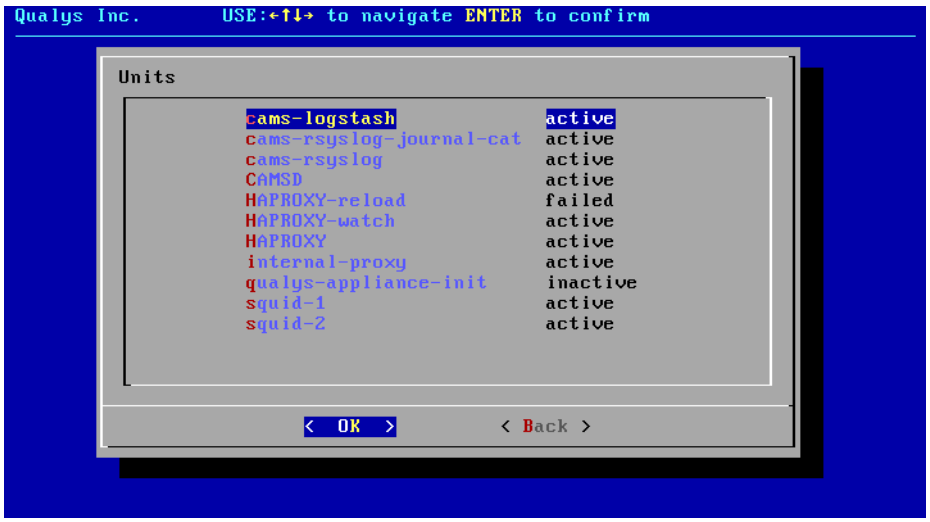
Containers



Images



Units

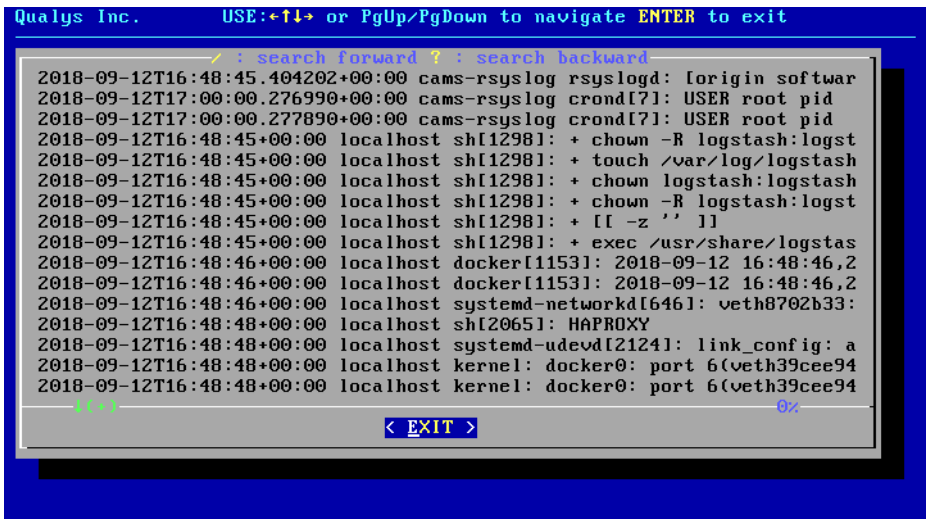


Logs

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.



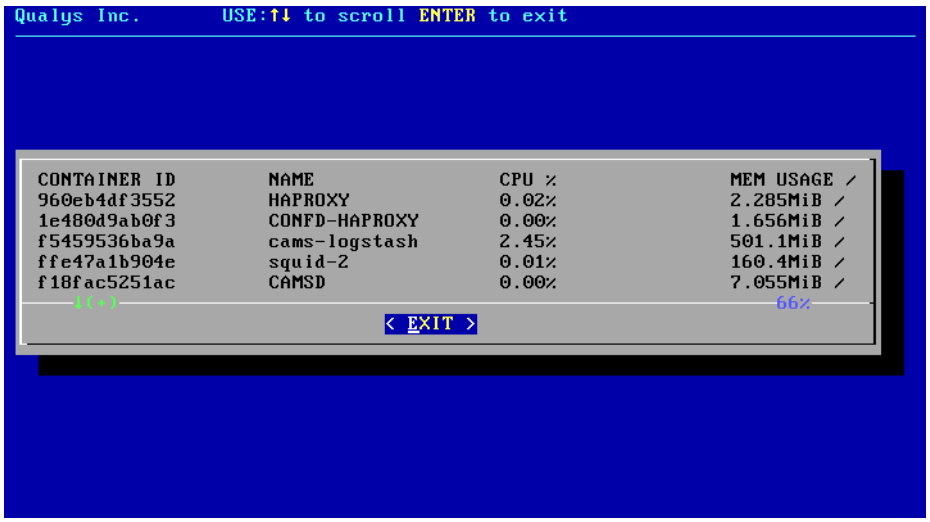
Don't worry to delete or archive logs! The QGS appliance will automatically clean up its logs and disk space as it reaches capacity.

Proxy

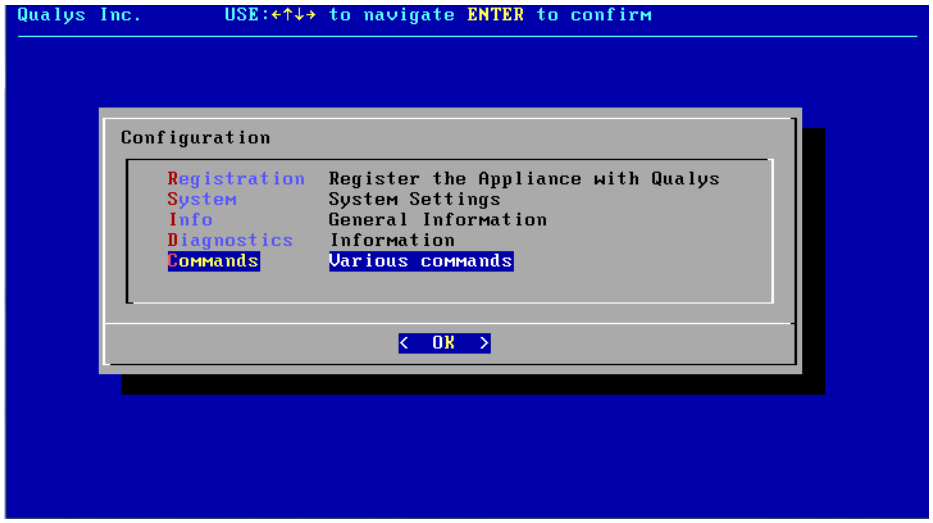
Executes a network connection test through a configured upstream proxy.

Stats

View utilization of the virtual appliance services.

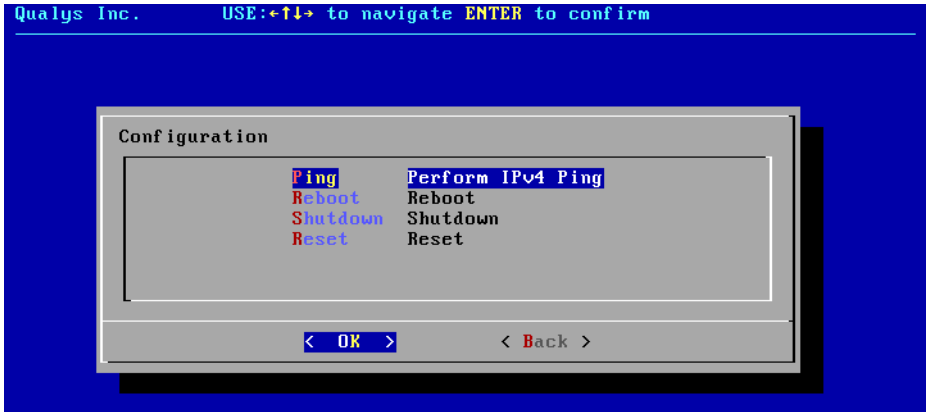


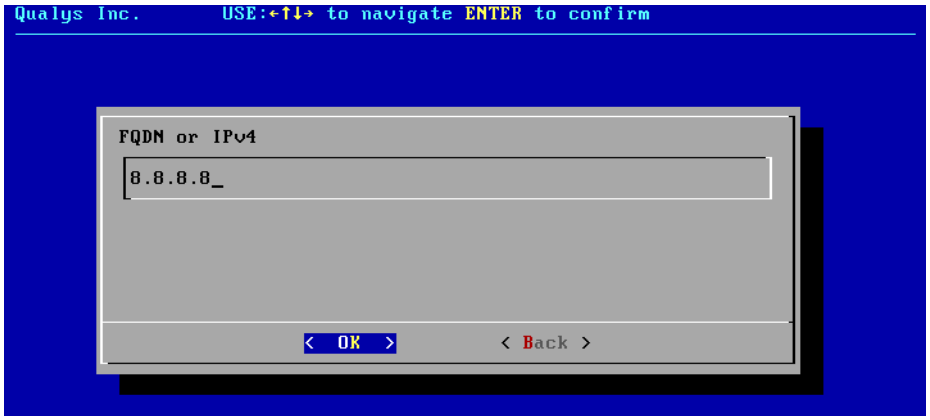
Commands



Ping

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

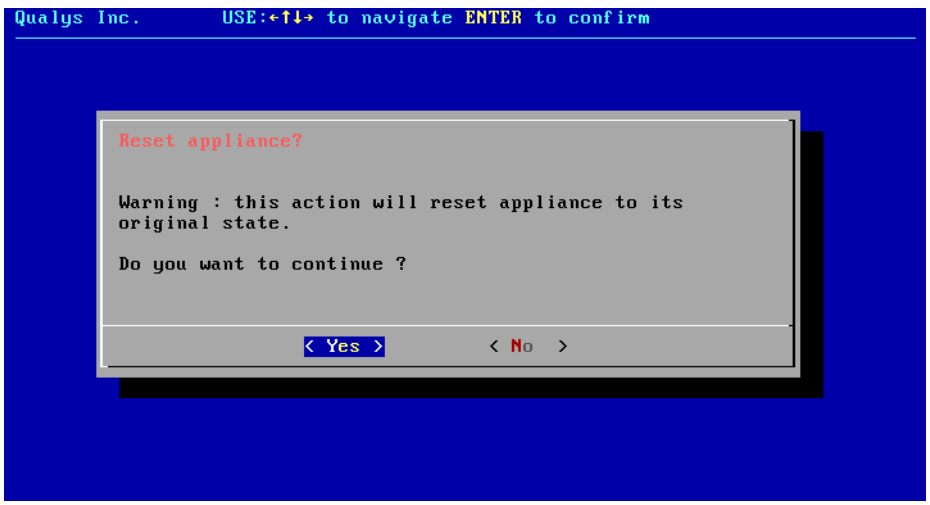




Reset appliance

Reset appliance to its original unconfigured state.

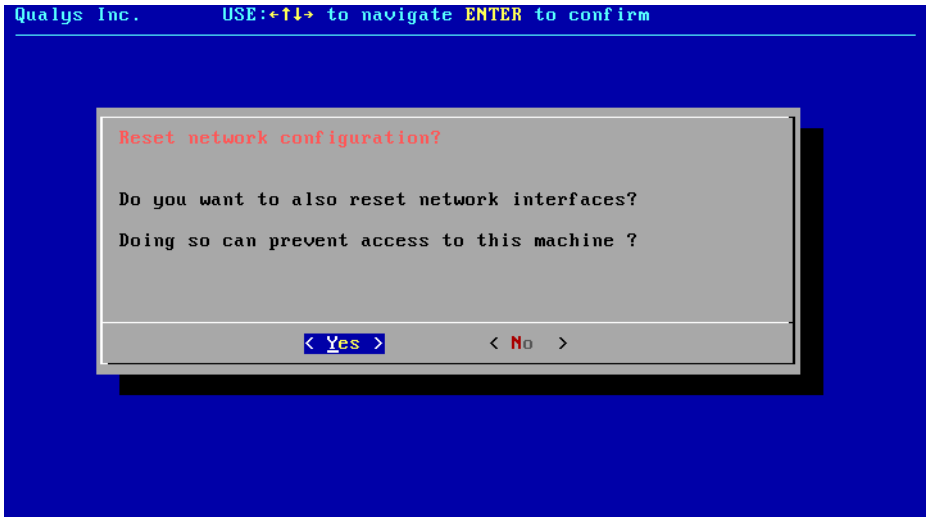
Warning: All configurations and log files will be deleted.



Reset network interface

Reset network interface of virtual appliance.

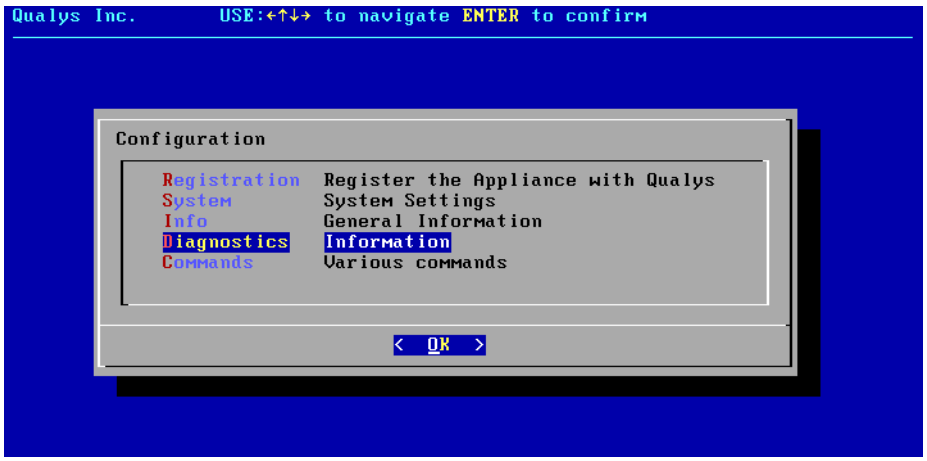
Note: This only resets the network configuration of the appliance.



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.