Qualys Gateway Service
User Guide
Version 3.2.2

August 10, 2023
# Table of Contents

**About this Guide** .................................................................................................................. 4
About Qualys .......................................................................................................................... 4
Qualys Support ....................................................................................................................... 4

**Overview** ............................................................................................................................ 5
Virtualization Server Requirements and Virtual Machine File Formats ......................... 6

**Qualys Gateway Service User Interface Module** ................................................................. 9
Qualys Gateway Service Module User Interface .............................................................. 15
Virtual Appliance Local Configuration ............................................................................... 18
Configuration Screens ......................................................................................................... 19

**Appendix - Things to Remember** ..................................................................................... 34
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 Machine Configuration

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

Note: The QGS installable may occupy lesser space than the minimum space requirements. However, we recommend that the VM must meet the minimal requirements of 30 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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Cloud Agent</th>
<th>Qualys Gateway Service</th>
<th>Platform URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>camspublic.qg1.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg1.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg1.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td>US 2</td>
<td>qagpublic.qg2.apps.qualys.com</td>
<td>qagpublic.qg2.apps.qualys.com</td>
<td>qg2.apps.qualys.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspublic.qg2.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg2.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg2.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspublic.qg3.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg3.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg3.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspublic.qg4.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg4.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg4.apps.qualys.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td>EU 1</td>
<td>qagpublic.qg1.apps.qualys.eu</td>
<td>qagpublic.qg1.apps.qualys.eu</td>
<td>qg1.apps.qualys.eu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspublic.qg1.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg1.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg1.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td>EU 2</td>
<td>qagpublic.qg2.apps.qualys.eu</td>
<td>qagpublic.qg2.apps.qualys.eu</td>
<td>qg2.apps.qualys.eu</td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspublic.qg2.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camspm.qg2.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>camsrepo.qg2.apps.qualys.eu</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>update.release.flatcar-linux.net</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Cloud Agent</td>
<td>Qualys Gateway Service</td>
<td>Platform URL</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>IN 1</td>
<td>qagpublic.qg1.apps.qualys.in</td>
<td>qagpublic.qg1.apps.qualys.in&lt;br&gt;camspublic.qg1.apps.qualys.in&lt;br&gt;camspm.qg1.apps.qualys.in&lt;br&gt;camsrepo.qg1.apps.qualys.in&lt;br&gt;update.release.flatcar-linux.net</td>
<td>qg1.apps.qualys.in</td>
</tr>
<tr>
<td>CA 1</td>
<td>qagpublic.qg1.apps.qualys.ca</td>
<td>qagpublic.qg1.apps.qualys.ca&lt;br&gt;camspublic.qg1.apps.qualys.ca&lt;br&gt;camspm.qg1.apps.qualys.ca&lt;br&gt;camsrepo.qg1.apps.qualys.ca&lt;br&gt;update.release.flatcar-linux.net</td>
<td>qg1.apps.qualys.ca</td>
</tr>
<tr>
<td>AE 1</td>
<td>qagpublic.qg1.apps.qualys.ae</td>
<td>qagpublic.qg1.apps.qualys.ae&lt;br&gt;camspublic.qg1.apps.qualys.ae&lt;br&gt;camspm.qg1.apps.qualys.ae&lt;br&gt;camsrepo.qg1.apps.qualys.ae&lt;br&gt;update.release.flatcar-linux.net</td>
<td>qg1.apps.qualys.ae</td>
</tr>
<tr>
<td>UK1</td>
<td>qagpublic.qg1.apps.qualys.co.uk</td>
<td>qagpublic.qg1.apps.qualys.co.uk&lt;br&gt;camspublic.qg1.apps.qualys.co.uk&lt;br&gt;camspm.qg1.apps.qualys.co.uk&lt;br&gt;camsrepo.qg1.apps.qualys.co.uk&lt;br&gt;update.release.flatcar-linux.net</td>
<td>qg1.apps.qualys.co.uk</td>
</tr>
</tbody>
</table>
Qualys Gateway Service User Interface Module

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

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

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

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

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

**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.

**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.

Cache Mode and Patch Mode Configuration

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

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

<table>
<thead>
<tr>
<th>File Type</th>
<th>Interval</th>
<th>Number of Agents</th>
<th>Bandwidth without Caching</th>
<th>Bandwidth with Caching</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Manifest</td>
<td>Daily</td>
<td>1,000</td>
<td>2 GB</td>
<td>2 MB</td>
</tr>
<tr>
<td>VM Manifest</td>
<td>Daily</td>
<td>5,000</td>
<td>10 GB</td>
<td>2 MB</td>
</tr>
<tr>
<td>VM Manifest</td>
<td>Daily</td>
<td>10,000</td>
<td>20 GB</td>
<td>2 MB</td>
</tr>
<tr>
<td>VM Manifest</td>
<td>Daily</td>
<td>25,000</td>
<td>50 GB</td>
<td>2 MB</td>
</tr>
</tbody>
</table>

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.
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

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

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 2000 concurrent cloud agent requests are supported by a QGS appliance. In case of more than 2000 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
The Activity Summary widgets provide aggregate activity information for all QGS appliances in the subscription. Active Agents and Total Agents count the number unique agent IPs connecting through all appliances. Bandwidth Savings is calculated in cache mode.

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

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

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

In **Proxy** mode, you’ll see only unique IPs count on QGSUI, while in **Cache** mode you’ll see count of active agent and unique IPs on QGSUI.
Create New Appliance / Generate Personalization Code / Use Common Certificate

![Qualys Gateway Service User Interface Module](image)

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**

<table>
<thead>
<tr>
<th>Appliances</th>
<th>5 Active Agents (24 Hours)</th>
<th>9 Total Agents (7 Days)</th>
<th>15MB Bandwidth Savings (30 Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>51 Appliances</strong></td>
<td>Search...</td>
<td>Download image</td>
<td>Download Common CA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STATUS</th>
<th>APPLIANCES</th>
<th>DEPLOY LOCATION</th>
<th>UNIQUE IPS</th>
<th>ACTIVE AGENTS</th>
<th>PRIORITY PORT</th>
<th>CACHE PORT</th>
<th>TLS PROTOCOL CLIENT</th>
<th>HEALTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>AWS_p13_sp01_27_Seq...</td>
<td>Cache: Enabled</td>
<td>0</td>
<td>0</td>
<td>8080</td>
<td>8099</td>
<td>1.2.1.3</td>
<td>Normal</td>
</tr>
<tr>
<td>Active</td>
<td>patch_sp01_test_vcn03</td>
<td>Pune</td>
<td>1</td>
<td>1</td>
<td>1080</td>
<td>8000</td>
<td>1.0, 1.1, 1.2, 1.3</td>
<td>Normal</td>
</tr>
</tbody>
</table>

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

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

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

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

After Successful Setup and Registration, the Appliance has Active Status
View Details, Stats, and Logs of an Active Appliance

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

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

Virtual Appliance Local Configuration

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

Local Configuration Menu Structure
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.

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
- 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

[Image of Qualys Gateway Service User Interface Module Configuration Screens]
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
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

**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.

![Diagnostics report is available via SFTP using:]

- **Username** => diagnostics
- **Password** => 2b1d5a22

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

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

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

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

1. Connect to the appliance Text user interface.
2. Go to the Diagnostics and select Units.
3. Go to the CAMSD unit and click Restart.
4. Wait at least 45 minutes to 1 hour for the appliance to become active on the UI.
- 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.
- **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.

![Requirements mismatch](image)

- A Minimum 16GB of RAM is recommended for CAMS/QGS appliances. A total of 2000 concurrent cloud agent requests are supported by a QGS appliance. In case of more than 2000 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.

![Latest version](image)

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 2.1.0-48 using TextUI

You can add a POD suffix details only for the image version 2.1.0-48 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**.

**Note:** we recommend using the User Data option only when the instance is launched using the scripts during the instance creation. For more details on user data, instance creation, and script launching, refer to the [Qualys Gateway Service Deployment Guide](#).
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*.

**How to generate/create the network dump file in the appliance?**

The following are the steps you need to perform to create a TCP dump:

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.

**Note:** When you regenerate the TCP dump, the older TCP dump file gets replaced with the new TCP dump file.