Table of Contents

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

Overview .................................................................................................................... 5
  What’s New in QGS 1.1.1 Release ......................................................................... 5
  Features .................................................................................................................. 6
  Virtualization Server Requirements and Virtual Machine File Formats ................. 8

Qualys Gateway Service User Interface Module ..................................................... 10
  Qualys Gateway Service Module User Interface .................................................. 14
  Virtual Appliance Local Configuration .................................................................. 17
  Configuration Screens ............................................................................................ 17
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.

What’s New in QGS 1.1.1 Release

The following features and capabilities are new in this release:

• Qualys Gateway Service version 1.1 appliances will automatically upgrade to version 1.1.1 when available on check-in with the Qualys platform

• Support for TLS “step-up” for agents running on supported older operating systems that only support TLS 1.0 (Windows XP SP3, Windows Server 2003, Windows Server 2008)
  – This feature requires the QGS appliance to be configured using “Cache Mode”, the QGS certificated installed on all hosts, and the agent on the host configured to connect to the cache port on the QGS appliance
  – A new configuration “TLS Protocols” for each QGS appliances enables the appliance to accept older TLS 1.0 protocol from agent hosts and “step-up” the TLS connection to TLS 1.2 to the Qualys Platform

• The Appliances menu listing of QGS appliances has User Interface updates:
  – Adds new columns for “Proxy Port”, “Cache Port”, and “TLS Protocol Client” making it easy to see the configuration of each QGS appliance in the appliance listing
  – Adds new search tokens for the search query:
    • tlsProtocolClient – returns appliances with the minimum TLS protocol set values: “tls_1_0”, “tls_1_1”, “tls_1_2”, “tls_1_3”
    • proxyPort – returns appliances that match the proxy port number values: valid integer port number
    • cachePort – returns lists appliances values: valid integer port number
Overview

Features

- Combined the appliance status of CPU, RAM, and HDD into a single column for “Health” with different status labels/colors depending on threshold
  - Normal (green) – any metric less than 85% of max
  - Warning (orange) – any metric between 85-95% of max
  - Caution (red) – any metric over 95% of max
- Clicking on the appliance name (or selecting View Details from the Quick Action menu) shows the specific values for CPU, RAM, and HDD

- Fixed an issue where the Active Agents count in proxy mode was not displaying correctly on the main Appliance menu page
- Fixed an issue where older images on the virtual appliance were not removed on upgrade which caused the disk capacity to increase

Features

The following features and capabilities are available in QGS 1.0 release:

- 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 (an upcoming release will offer a caching option)
- SSL/TLS pass-through bypass (an upcoming release will offer a TLS step-up option)
- Can be deployed in High-Availability failover using external 3rd party load balancers (an upcoming release will offer integrated High-Availability without external dependencies)
- 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)

The following features and capabilities are available in QGS 1.1 release:

- Qualys Gateway Service version 1.0 appliances will automatically upgrade to version 1.1 when available on check-in with the Qualys platform
- Support for “Cache Mode”, where the QGS appliance caches Cloud Agent artifacts (manifests, installers, etc.) when first downloaded to serve to subsequent agents locally in the network
Cache Mode is implemented as a connection terminate-and-establish (instead of a transparent pass-through proxy) in order for the appliance to cache downloads and serve content from cache. Agent upload data is not cached or stored on the appliance.

Cache Mode requires the certificate of each appliance to be installed on each host with Cloud Agent.

The QGS UI provides the gateway appliance’s certificate (.pem) for download, plus an optional MSI installer to install on Windows hosts.

- Support for “Patch Cache Mode”, a configuration add-on to “Cache Mode”, where the QGS appliance caches patch files for Cloud Agents enabled with the Qualys Patch Management application.
- When QGS is configured in Patch Cache Mode, the QGS changes the Connection Security configuration to allow access from the agent to any Internet location as the Cloud Agent downloads patch files directly from the vendor websites.
- QGS configured in Patch Cache Mode requires a second virtual disk attached to the virtual appliance with sufficient free disk space.

- User-configurable proxy and cache ports
- Supports filtering by domain name on the upstream proxy server, if configured
- Create diagnostics file from the appliance’s local interface for analysis by Qualys Customer Support
- Bug fixes and improvements
Virtualization Server Requirements and Virtual Machine File Formats

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Supported Versions</th>
<th>File Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere / ESXi</td>
<td>5.5, 6.0, 6.5</td>
<td>VMDK, OVA, OVF</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>2012, 2012 R2, 2016</td>
<td>VHD</td>
</tr>
</tbody>
</table>

Virtual Machine Configuration

- 2 vCPUs
- 8 GB RAM minimum
- 8 GB Disk
  - For Patch Cache 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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Cloud Agent</th>
<th>Qualys Gateway Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2</td>
<td>qagpublic.qg2.apps.qualys.com (64.39.104.103:443)</td>
<td>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)</td>
</tr>
<tr>
<td>Platform</td>
<td>Cloud Agent</td>
<td>Qualys Gateway Service</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>EU 1</td>
<td>qagpublic.qg1.apps.qualys.eu (64.39.100.93:443)</td>
<td>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)</td>
</tr>
<tr>
<td>EU 2</td>
<td>qagpublic.qg2.apps.qualys.eu (154.59.121.74:443)</td>
<td>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)</td>
</tr>
<tr>
<td>IN 1</td>
<td>qagpublic.qg1.apps.qualys.in (103.216.98.40:443)</td>
<td>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)</td>
</tr>
<tr>
<td>CA 1</td>
<td>qagpublic.qg1.apps.qualys.ca (64.39.97.135:443)</td>
<td>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)</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 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.

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.

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 numbers of Cloud Agents deployed, this can save a significant amount of download bandwidth.

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 requests. 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.

5) To enable Patch Mode, toggle the On/Off slider to “On”

6) Click “Next” through the menu until “TLS Protocols”

7) 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
Qualys Gateway Service Module User Interface

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.

- **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

View List of Appliances and their Status
Download Image of the Virtual Appliance

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.
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.

DNS Servers:

- DNS: 8.8.8.8
- DNS: 1.1.1.1
- Search domain: corp.acme.com
Proxy Servers
Configure upstream Proxy Server, if using proxy chaining.
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.

Registration

Enter the Personalization Code generated in the QGS User Interface module.
Here’s an example of a redacted Personalization Code.

Registration in process

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

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

Appliance is registered successfully

Diagnostics

Qualys inc. USE: #1 to navigate ENTER to confirm

<table>
<thead>
<tr>
<th>Diagnostics</th>
<th>Docker containers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containers</td>
<td>Docker containers</td>
</tr>
<tr>
<td>Images</td>
<td>Docker images</td>
</tr>
<tr>
<td>Units</td>
<td>Services units</td>
</tr>
<tr>
<td>Logs</td>
<td>Logs</td>
</tr>
<tr>
<td>Stats</td>
<td>Container Stats</td>
</tr>
</tbody>
</table>

< OK >   < Back >
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.

Proxy
Executes a network connection test through a configured upstream proxy.

Stats
View utilization of the virtual appliance services.
Commands
Ping

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.