Qualys Integration Guide

RELIAQUEST

By combining Qualys' industry-leading vulnerability management capabilities with GreyMatter's advanced security analytics and automation platform, organizations can gain a holistic view of their security posture and quickly identify and respond to potential threats. With this direct source, security teams can provide a more proactive and effective defense against cyberattacks.

Deployment Type

This integration supports **on-premises**, **private cloud**, and **vendor cloud** deployments through **port 443**. If your organization uses on-premises deployments, make sure the IP addresses listed below are added to a tunnel between you and ReliaQuest.

Cloud deployments do not require any action to be taken on your end.

Important note regarding on prem connections:
You must allow the ReliaQuest IPs to establish connectivity with your Qualys server over **port 443.** A member of ReliaQuest's CSM/Implementations Teams will reach out and request the server IP. They will provide this IP to RQ NetOps, who will add it to the tunnel between you and ReliaQuest.

Source IP Allowlist

See IP Allowlist based on your organization's location.

Required Information and Setup

Collect these credentials for the GreyMatter Connection Settings page.

- URL
  - Default: https://qualysguard.qg2.apps.qualys.com/
- Username (for API account)
- Password (for API account)

To establish connectivity and use the Respond playbooks associated with this integration, you must also create an API account configured to the Qualys Unit Manager role.
To complete these actions, follow the steps below:

Create a new API account

1. Navigate to **Users** > **Users** > **New dropdown** > **User**.
2. In the **General Information** tab, add the email address, first name, last name, title, and phone number.
3. In the **Locale** tab, set the language to English. Then select the date format and time zone to your preference.
4. In the **User Role** tab, mark the **Allow Access to API** checkbox.
5. Check the **Allow access to GUI** box (for first-time setup required – can be removed after the password is reset).
6. Select the **Manager** role.

7. If tag-based user scoping is enabled, assign the user-appropriate host tags.
8. Assign the **All** scope in the Asset Group tab.
9. Click **Save**.
10. Log into the newly created user using GUI to reset the password and activate the account.

Important: The Security tab does not require any action because GM does not support MFA.

See Qualys documentation.

The following must also be created:

- Scan template named **RQ_Template**
- Option profile named **RQ_OP_Scan**
- Scanner Appliance named **RQ-Qualys-Scanner**

Collect Qualys API URL

The API URL depends on the location of your Qualys Platform. Here's how to find yours:

1. Identify your platform.
2. Within your Qualys account, click **Help**.
3. Select **About**.
4. Copy the **API server URL** under Security Operations Center (SOC).

Keep the required details for input on the GreyMatter Connections Settings page.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Respond	Enrich Host	Qualys Unit Manager role
	Enrich IP	Qualys Unit Manager role
	Initiate IP Scan	Qualys Unit Manager role
	Scan Results	Qualys Unit Manager role

Respond

PLAYBOOK NAME	DESCRIPTION	REQUIRED INPUT VARIABLE(S)
Enrich Host	Retrieves host information associated with hostname and its Vulnerabilities	**Hostname** Example: Computer123
Enrich IP	Retrieves host information associated with hostname.	**Hostname** Example: Computer123
Initiate IP Scan	Launches Scan on Vulnerability Management.	**Hostname**

		Example: Computer123
Scan Results	View Scan Results on Vulnerability Management.	**IP** Example: 10.219.201.10

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.