

# Aqua Security Workload Protection Integration Guide

Aqua Security is the pioneer in securing containerized cloud native applications from development to production. Aqua's full lifecycle solution prevents attacks by enforcing pre-deployment hygiene and mitigates attacks in real time in production, reducing mean time to repair and overall business risk.

## Deployment Type

This integration supports **on-premises** and **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure whether your organization supports vendor cloud deployments, please ensure your organization's compatibility before continuing.

## Required Information and Setup

To integrate GreyMatter with Aqua Security Workload Protection, collect the following details:

- Console URL
  - U.S. Default: <https://cloud.aquasec.com>
  - Europe: <https://eu-1.cloud.aquasec.com>
  - Asia (Singapore): <https://asia-1.cloud.aquasec.com>
  - Asia Pacific (Sydney, Australia): <https://ap-2.cloud.aquasec.com>
- Authentication URL
  - U.S. Default: <https://api.cloudsploit.com>
  - Europe: <https://eu-1.api.cloudsploit.com>
  - Asia (Singapore): <https://asia-1.api.cloudsploit.com>
  - Asia Pacific (Sydney, Australia): <https://ap-2.api.cloudsploit.com>
- URL to Fetch Base API
  - U.S. Default: <https://prov.cloud.aquasec.com/v1/envs>
  - EMEA: <https://prov-eu-1.cloud.aquasec.com/v1/envs>
  - Asia (Singapore): <https://prov-asia-a.cloud.aquasec.com/v1/envs>
  - Asia Pacific (Sydney, Australia): <https://prov-ap-2.cloud.aquasec.com/v1/envs>
- API Key
- API Secret
- On-Premises Environment
  - Checkbox
  - Default: unchecked

**Note:** If you have a non-US based Aqua Security environment, the Console URL, API Authentication URL, and URL to Fetch Base API will differ from the default values.

If your chosen deployment is on-prem, update the Console URL, Authentication URL, and URL to Fetch Base API with the same URL, specify a username and a password in the API Key and API Secret fields (respectively), and enable the On-Premises Environment checkbox in the Connections Settings page.

# Aqua Security Workload Protection Integration Guide

See instructions below to gather the required information.

## Create a Permission Set

1. In Aqua, navigate to **Account Management**.
2. Click **User Management**.
3. Select **Permissions Sets**.
4. Click **Add Permissions Set**.
5. Enable the **Workload Protection** module.
6. Enable the following permissions:
  - Audit View
  - Images View
  - Incidents View
  - VMs View
  - Vulnerabilities View

## Create a Role

1. In Aqua, navigate to **Account Management**.
2. Click **User Management**.
3. Select **Roles**.
4. Click **Add Role**.
5. Assign the newly created permission set from the previous set.
6. Assign the global application scope or a custom scope (if desired).

## Generate the API Key and Secret

1. In Aqua, navigate to **Account Management**.
2. Click **Settings**.
3. Select **API Keys**.
4. Click **Generate Key**.
5. Specify the description.
6. Click **Create**.
7. Save the **API Key** and **Secret**.

## Enable API Permissions

1. On the API Keys page within the Account Management Settings page, click the vertical **More** icon on the same row as the newly generated API key.
2. Click **Edit**.
3. In the Global Permissions section, disable the **Enable global admin permission option**.
4. In the Granular Permissions section, enable the required permissions:
  - **tokens:readwrite**

# Aqua Security Workload Protection Integration Guide

- **roles:assign**

5. In the tokens:readwrite permission, click the **dropdown** menu.
6. Select the previously created role.
7. **Save.**

## Permissions and Functionality

### Permissions

[Aqua Security Permissions Documentation](#)

GreyMatter Capability	Action(s)	Required Permission
API Authentication	N/A	tokens:readwrite roles:assign
Investigate / Hunt	Perform Query	Workload Protection > Audit View
Detection at Source - Vendor Authored	Get Detection Records	Workload Protection > Incidents
Respond	Enrich Host	Workload Protection > VMs View
	Enrich Vulnerability	Workload Protection > Vulnerabilities Workload Protection > Images

### Respond

Playbook Name	Description	Required Input Variables
Enrich Host	Returns virtual machine information such as associated IPs, operating system, cloud provider.  In the Aqua Security Workload Protection console, navigate to “Inventory“ to view virtual machine information.	<b>Virtual Machine Name</b> Example: ip-10-0-5-173.us-west-2.compute.internal
Enrich Vulnerability	Returns image vulnerability information such as description, severity, and affected resources.  In the Aqua Security Workload Protection console, navigate to “Security Reports“ > “Vulnerabilities“ to view vulnerability information.	<b>CVE ID</b> Example: CVE-2021-40465

### Investigate/Hunt

**Audit Events:** Queries Aqua Security audit events, which is a log of security-related events.

The field schema is defined by the vendor. A misconfigured field mapping does not break the query, any field that does not exist is not applied to the filter.

### Detect

# Aqua Security Workload Protection Integration Guide

Aqua Security Workload Protection supports **Detection at Source (Vendor Authored)**.

In Aqua, incidents are classified as runtime security events with critical or high severity, triggered by the detection of Indicators of Compromise (IoCs) and Indicators of Attack (IoAs). They include:

- Violations of Runtime Policy controls
- Behavioral detection based on Aqua predefined signatures
- Real-time Malware detection

**Note Syncing** and **State Syncing** are *not* supported.

**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.