

Upwind CNAPP Integration Guide

Upwind's next-generation cloud security platform combines cloud security posture management with runtime context and real-time threat detection, providing comprehensive visibility across identities, vulnerabilities, and active threats in cloud environments. A GreyMatter integration enhances security operations by leveraging Upwind's identity management insights, and real-time threat detections to strengthen GreyMatter's detection and enrichment capabilities with cloud-native security context.

Deployment Type

This integration supports **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, please check your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Upwind, collect the following details:

- BaseURL
 - US: <https://api.upwind.io>
 - EU: <https://api.eu.upwind.io>
 - ME: <https://api.me.upwind.io>
- Organization ID
- Token URL
 - Default: <https://auth.upwind.io/oauth/token>
- Client ID
- Client Secret
- Test Connection Offset (Days)
 - Default: 1
 - Used to do a successful test connection and ensure we retrieve detection events.

See instructions below to gather the required information.

Retrieve Client ID and Secret

1. In the Upwind console, click the **Settings** button in the bottom left corner.
2. Open the **Credentials** tab.
3. Click **Generate Credential**.
4. Select **API** in the 'I want to use these credentials for section.'
5. Enter a meaningful name in the **Name** field (example: api-reliaquest-greymatter-upwind-integration).
6. Click **Generate**.
7. Copy the **Client ID** and **Client Secret** to a safe place for collection later.
IMPORTANT: This is the only time you can collect this specific Client ID and Secret. If not collected, generate new credentials.
8. Click **Save**.

Upwind CNAPP Integration Guide

Functionality

Note: No necessary permissions are listed in Upwind documentation.

Respond

Playbook Name	Description	Required Input Variables
Enrich Vulnerability	List of findings where the CVE vulnerability has been seen.	CVE

Detect

Upwind CNAPP supports **Detection at Source** (vendor-authored).

Note Syncing *is not* supported.

State Syncing *is* supported.

* The list detections endpoint does not return detailed information about the detection. A subsequent request is made to another endpoint to retrieve the verbose detection details.

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.