Axonius Integration Guide

By using Axonius as a direct source for GreyMatter, asset data from existing data sources can be aggregated, normalized, correlated to uncover security issues and automate remediation actions to reduce your attack surface and simplify workflows.

Those operating under the Federal Risk and Authorization Management Program (FedRAMP) require different instructions for configuration with GreyMatter. See the FedRAMP-specific configuration guide for more details.

Deployment Type

GreyMatter supports **private cloud** deployments of Axonius through **port 443**.

If you already know your deployment method, continue to the next step. If you do not know what your Axonius deployment method is, contact your internal Network or IT Infrastructure team to confirm.

Required Information and Setup

To integrate GreyMatter with Axonius, collect the following details:

- URL
- API key
- API secret

See instructions below to gather the required information.

Enable API Access for the User Role

To get an **API key** and **API secret**, you must first configure the required role user in Axonius

See the Instructions in Axonius documentation.

1. Open the **Manage Roles** page.
2. Click **Settings** in the top right corner of the page.
3. Click **Manage Roles**.
4. Select the **Viewer** role.
5. Make sure the **API access** box in the API Access category is checked.
6. Click **Save**.

Click the number in the Users column next to the Role name to see a list of users assigned to this role.

Assign the role to a user account

1. Open **User Management** in the Settings**.**
2. Search for and select the user.
3. Edit the user profile and assign the desired role (Viewer) from the available roles list.
4. **Save** changes.

Create the API key and API secret

1. Log in to Axonius with a user account whose role has the **API access enabled** permission.
2. At the bottom of the **Navigation** toolbar, click on the account avatar.
3. Click **User Settings.**
4. Select the **API Key** tab. Copy the existing API key and secret. To reset them, click Reset Key.

Permissions and Functionality

Permissions

See more about Axonius permissions.

GreyMatter Capability	Action(s)	Required Permission
Respond	Enrich User	Device Assets
	Enrich Device	User Assets
Asset Inventory	Fetch Identities	Identities
	Fetch Softwares	Software Assets
	Fetch Assets	Device Assets

Respond

Playbook Name	Description	Required Input Variables
Enrich Device	Retrieves a list of systems associated with the device name.	**Device name** Example: Computer123 * The Hostname, HostID, IP Address or Mac Address can be passed as an input in the legacy playbook.
Enrich User	Return list of all system users or a single system user.	**Username** Username example: jsmith.john@test.com

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with Axonius, providing real-time insights into what assets you own, their status, and potential risks. GreyMatter executes the following actions to retrieve information:

- Fetch Assets: Retrieves device and asset data.
- Fetch Identities: Pulls identity records for user visibility and correlation.
- Fetch Softwares: Collects software inventory data across managed assets.