

CATO SASE Integration Guide

CATO SASE (Secure Access Service Edge) is a cloud-native solution that integrates networking and security functions like SD-WAN, SSE, and ZTNA into a unified platform. By setting up CATO SASE as a direct source for GreyMatter, security operations teams can query and respond to threats in their cloud environments using GreyMatter's capabilities.

Deployment Type

This integration supports **vendor cloud** deployments through **port 443**.

If you already know that your environment supports this deployment, 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 CATO SASE, collect the following details:

- GraphQL URL
 - Default: <https://api.catonetworks.com/api/v1/graphql2>
- API Key
- Account ID
- Section Name (optional)

See instructions below to gather the required information.

Create API Key

1. In the navigation menu, click **Resources**.
2. Select **API Keys**.
3. Click **New** to open the Create API Key panel.
4. Enter a **Key Name**.
5. Select the API Permission for this key.
6. Select an expiration date. (Optional – Recommended for API Keys with Edit permissions.)
7. In Allow access from IPs, select **Specific IP List** (Optional). Leave as **Any IP address** as the default if you do not want to enter the IP addresses.
8. Define the IP Addresses allowed to use this API Key (Optional, see [ReliaQuest IP Allowlist](#)).
9. Click **Apply**.
10. Copy the API Key generated and save it to a secure location. Once you close the pop-up, you can't access the API Key value.
11. Click **OK** to close the pop-up.

Find Account ID

There are two ways you can find your account ID.

URL:

CATO SASE Integration Guide

Log into Cato Management and view the numerical string immediately following the #!/ characters in your browser's address bar. This string is your account ID.

Account Info Page:

In Cato Management, open the Account menu and select **Account Info** to view your account ID.

Create New Section

If you would like to separate the ReliaQuest Block + Intel Lists, create a new section and add the name in the GreyMatter integration settings.

1. Navigate to the **Security** tab in CATO.
2. Select **Internet Firewall** in the left navigation menu under Security Configuration.
3. Click the **New** button.
4. Select **New Section**.
5. Name the section appropriately (i.e. ReliaQuest GreyMatter Block Section).
6. Select the desired position of the section.
7. Click **Save**.
8. Copy and paste the section name for GreyMatter Integration Settings.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Intel Push	INTEL_PUSH	Edit
Respond	BLOCK_IP	Edit
	BLOCK_DOMAIN	Edit
	BLOCK_PORT	Edit
	UNBLOCK_IP	Edit
	UNBLOCK_DOMAIN	Edit
	UNBLOCK_PORT	Edit

Respond

Playbook Name	Description	Required Input Variables
Block IP	Port added to the ReliaQuest Block IP Firewall Rule. * This is only for outbound traffic.	IP Address
Unlock IP	IP removed from the ReliaQuest Block IP Firewall Rule. * This is only for outbound traffic.	IP Address
Block Domain	Port added to the ReliaQuest Block Port Firewall Rule. *	Domain

CATO SASE Integration Guide

	This is only for outbound traffic.	
Unblock Domain	Domain removed from the ReliaQuest Block Domain Firewall Rule. * This is only for outbound traffic.	Domain
Block Port	Port added to the ReliaQuest Block Port Firewall Rule. * This is only for outbound traffic.	TCP Port Number
Unblock Port	Port removed from the ReliaQuest Block Port Firewall Rule. * This is only for outbound traffic.	TCP Port Number

* In CATO SASE, identify the ReliaQuest-specific IOCs by navigating to Security > Firewalls > Internet Firewalls. All ReliaQuest-related firewall rules are prepended by “ReliaQuest GreyMatter” and follow the general naming convention of “ReliaQuest GreyMatter {Action Name} {Firewall type} Rule.”

Intel Push

Intel Push creates a new internet firewall rule for each IOC type. These IOCs are blocked at the firewall level (layer 7).

In CATO SASE, identify the ReliaQuest-specific IOCs by navigation to Security > Firewalls > Internet Firewalls. Add ReliaQuest-related firewall rules are prepended by “ReliaQuest GreyMatter.”

IOC Types: IP, Domain, Emergency, IOC Lists

By default, the IOC never expires. An expiry period can be set if needed.

[Learn more about GreyMatter Intel Push.](#)

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.