iboss CASB Integration Guide

iBoss is a cloud-native cybersecurity platform specializing in Zero Trust Secure Access Service Edge (SASE) solutions, offering secure, fast, and scalable access to applications, data, and resources from anywhere. It replaces traditional VPNs, firewalls, and proxy appliances with a unified platform that protects against threats, prevents data loss, and ensures compliance for modern, distributed workforces.

Deployment Type

This integration supports **on-premises**, **private cloud**, 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, please check your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with iboss CASB, collect the following details:

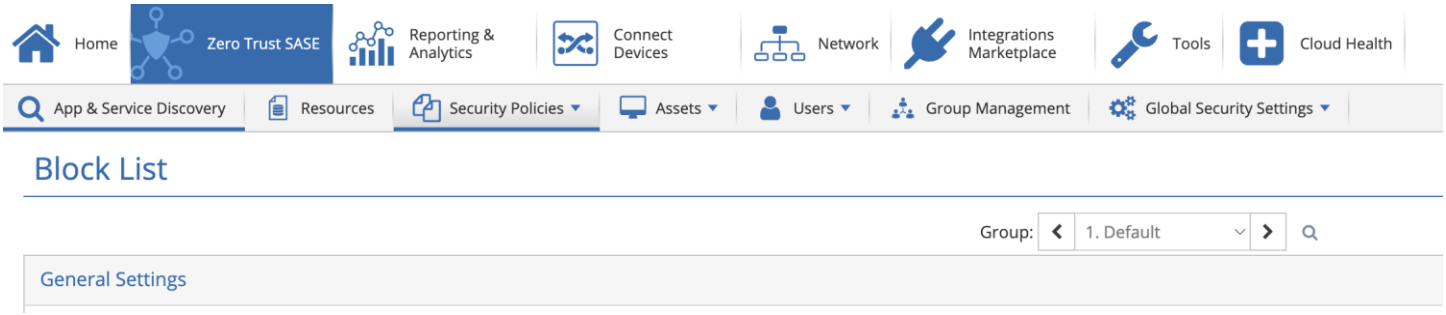
- URL
  - Default: https://api.ibosscloud.com
- Username
- Password
- Allow List ID
  - Default 1
- Block List ID
  - Default: 1

See instructions below to gather the required information.

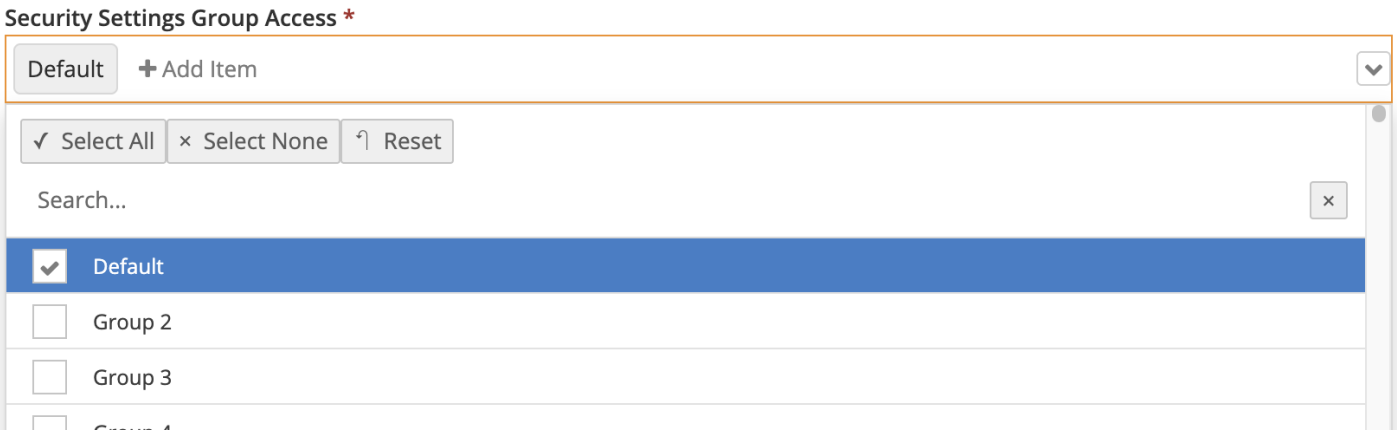
Gather Allow and Block List IDs

If you would like Allow and Block activities executed on a group besides the default (1), make sure the correct group is set in the iboss console.

In the CASB page, open the Allow List and choose the correct group from the dropdown. Do the same for the Block List.



The Group can be selected when RBAC permissions are set up for the API credentials to limit which groups can be updated when Blocking/Allowing URLs:



Create an Access Group with the Required Permissions

The API access requires administrative privileges for the iboss Zero Trust SSE account. To add them:

1. On the Home page of the iboss console, click **Administrators**.
2. Select **System Administrator Management** from the dropdown.
3. Select the **Role-Based Access Control tab**.
4. Click **Add Custom RBAC Group**.
5. On the Gateway Permissions tab, add the Administrator Type as **Delegated**.
6. Check the box for **Block List** and **Allow List** in the Permissions dropdown.
7. Add the associated **Management Group**.
8. Select **Default** in the Security Settings Group Access dropdown.
9. Toggle on the following permissions:
    - Can Access Malware Reports & Logs
    - Can Access DLP Reports & Logs
    - Can Access Asset Database
    - Can Access Incidents

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Investigate / Hunt		

Respond

Playbook Name	Description	Required Input Variables
Allow URL	Add URL to allowlist. The results include confirmation or error reasons.	URL Example: domain.com

	Validate the Allow list in the iboss console under the Security Policies menu.	
Unallow URL	Removes URL from allowlist. The results include confirmation or error reasons. Validate the Allow list in the iboss console under the Security Policies menu.	URL Example: domain.com
Block URL	Add URL to block list. The results include confirmation or error reasons. Validate the Block list in the iboss console under the Security Policies menu.	URL Example: domain.com
Unblock URL	Removes URL to block list. The results include confirmation or error reasons. Validate the Block list in the iboss console under the Security Policies menu.	URL Example: domain.com
Enrich Device	Returns asset-specific details:	Device ID or Device Type Example: EC207056-7CF0-E305-D1EB-B67BA272A858

Investigate/Hunt

GreyMatter returns activity events logged in iboss. Filtering of logs includes:

- date range
  - startTimeMillies
  - endTimeMillies
- action
- email
- category
- destinationIP
- sourceIP
- urlFilter
- userName

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with iboss CASB, providing real-time insights into what assets you own, their status, and potential risks.

Detect

iboss CASB supports **Detection at Source**, which retrieves detection incidents.

Note Syncing and **State Syncing** are supported for **Vendor-Authored detections**.

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.