Cisco ISE Integration Guide

Cisco ISE is a comprehensive network access control system that provides centralized authentication, authorization, and accounting (AAA) for users and devices connecting to the network.

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 Cisco ISE, collect the following details:

- URL
  - Example: https://10.220.23.216/ers/config
- Username
- Password

Note: Important: If you have a distributed environment, our internal teams will need to access the mnt node that has access to your anc entities. If you have a distributed environment, work with a member of ReliaQuest's CSM or Implementation's teams to make sure all the correct credentials are provided.

See instructions below to gather the required information.

Create a Policy to Connect to GreyMatter

1. In Cisco ISE, select **Operations**.
2. Click **Policy List** at the top of the page.
3. Create a new policy with the name **RQ_Block**.
4. Select **Quarantine** in the action dropdown.
5. Click **Save**.

Enable ERS

1. Within Cisco ISE Primary Administration Node (PAN), navigate to **Administration**.
2. Click **System**.
3. Click **Settings**.
4. Select **ERS Settings** from the left navigation menu.
5. Select **Enable ERS for Read/Write** to activate the External RESTful Services API.
6. Click **Save**.

Create an ERS Admin User

1. Within Cisco ISE Primary Administration Node (PAN), navigate to **Administration**.

2. Click **System**.
3. Click **Admin Access**.
4. Select **Administrators**.
5. Open the **Admin Users** tab.
6. Click **Add**.
7. Enter the user's details and assign them to the **ERS-Admin** group.

Learn more from Cisco documentation.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Respond	Enrich Policy	ERS-Admin
	Isolate Host	ERS-Admin
	Unisolate Host	ERS-Admin

Respond

Playbook Name	Description	Required Input Variables
Enrich Policy	Details of policy associated with it with action (e.g block, allow) will be shown	**Policy name** • Block • Unblock • RQ_Block
Isolate Host by Mac	Isolation of host and by applying to a policy	**Hostname** • MacAddress
Unisolate Host by Mac	Unisolation of host and by clearing the policy	**Hostname** • MacAddress

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.