RELIAQUEST®

FedRAMP Splunk Integration Guide

By combining the advanced analytical capabilities of Splunk with the unified security features of GreyMatter, this connection provides unparalleled control over your organization's security posture.

This guide includes connection instructions for those who operate under the Federal Risk and Authorization Management Program (FedRAMP).

Deployment Type

This integration supports **on-premises, private cloud**, and **vendor cloud** deployments through **port 8089**.

If you are using on-premises deployments, you must allow the IP addresses listed below. Work with your CSM or Implementations Specialist to establish a network tunnel between your environment and GreyMatter.

Connectivity from GreyMatter to Splunk is established using the GreyMatter VPN Agent. The GreyMatter VPN Agent is installed on a host in your environment and must have connectivity to Splunk over Port 8089. Please refer to the GreyMatter VPN Agent Connectivity Documentation and reach out to your Customer Success Manager (CSM) or Implementation Specialist for more details.

If you are using cloud deployments, you do not need to add the IP address listed below to your allowlist.

Add the ReliaQuest IP Addresses

1. Within Splunk, click **Settings**.
2. Select **Server Settings**.
3. Navigate to **IP Allowlist**.
4. Click **Search Head API Access.**
5. Enter the ReliaQuest IP Addresses.

Required Information and Setup

To integrate GreyMatter with Splunk, collect and save the following details:

- URL
  - **On prem**: https://<splunk-host>:8089
  - **Cloud**: <https://<deployment-name>.splunkcloud.com:8089
- API Token
- Username Password

Learn more about FedRAMP compliance with Splunk.

See instructions below to gather the required information.

Health Configuration

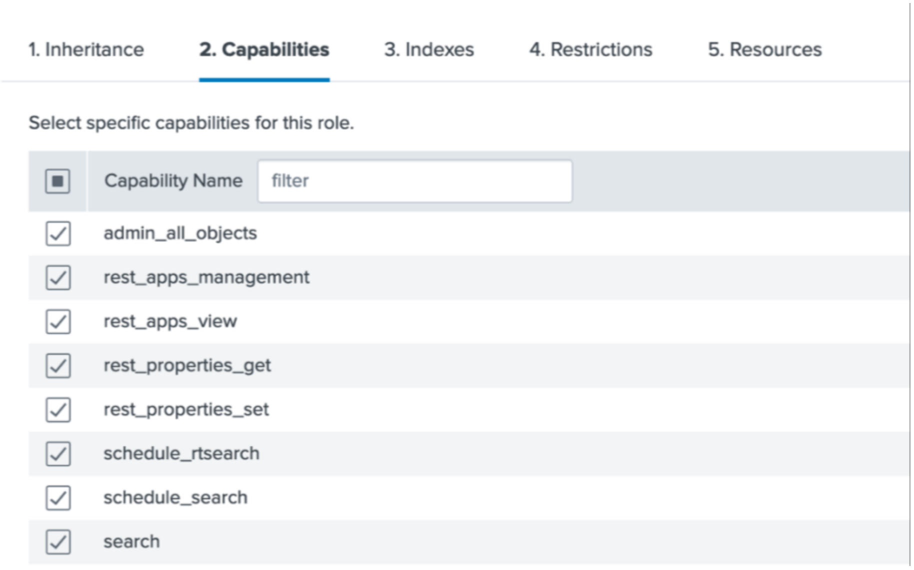
Follow the steps in the Health Configuration guide to ensure you are alerted if GreyMatter experiences an issue with your Splunk connection.

Create a new role within Splunk

1. To create a new role, select **Roles** from the **Settings** menu.
2. Click the **New Role** button.
3. Fill in the Role Name field (i.e. GreyMatter_svc). Copy and store the name somewhere safe; you'll need to send it to your CSM later. Disregard the **Inheritance** section.
4. Click the **Capabilities** tab and mark the checkboxes next to the following capabilities:
   - Rest_apps_management
   - Rest_apps_view
   - Rest_properties_set
   - Rest_properties_get
   - Schedule_rtsearch
   - Schedule_search
   - Search
   - Admin_all_objects (required for Intel Updates and to create the kvstore object).

   If you are using Splunk v. 10, replace Admin_all_objects with
     - Edit_saved_search
     - Edit_saved_search_owner
     - List_saved_search

   Important: If you plan to use Enterprise Security, you will need the ess_analyst role added as well.

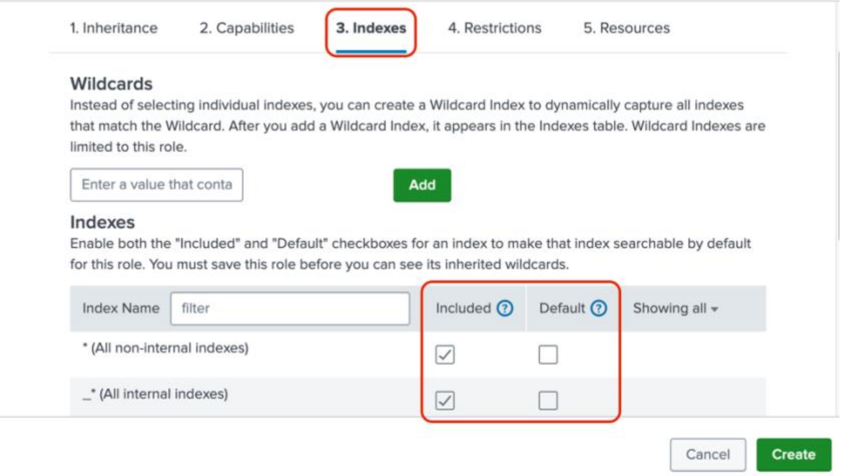


Select specific capabilities for this role.

■	Capability Name
☑	admin_all_objects
☑	rest_apps_management
☑	rest_apps_view
☑	rest_properties_get
☑	rest_properties_set
☑	schedule_rtsearch
☑	schedule_search
☑	search

5. Click the **Indexes** tab and only mark the **Included** checkbox for the following permissions:
   - (All non-internal indexes)
   - (All internal indexes)
6. Mark the **Default** checkbox next to the Main permission.

7. Click the **Create** button.



Wildcards

Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes that match the Wildcard. After you add a Wildcard Index, it appears in the Indexes table. Wildcard Indexes are limited to this role.

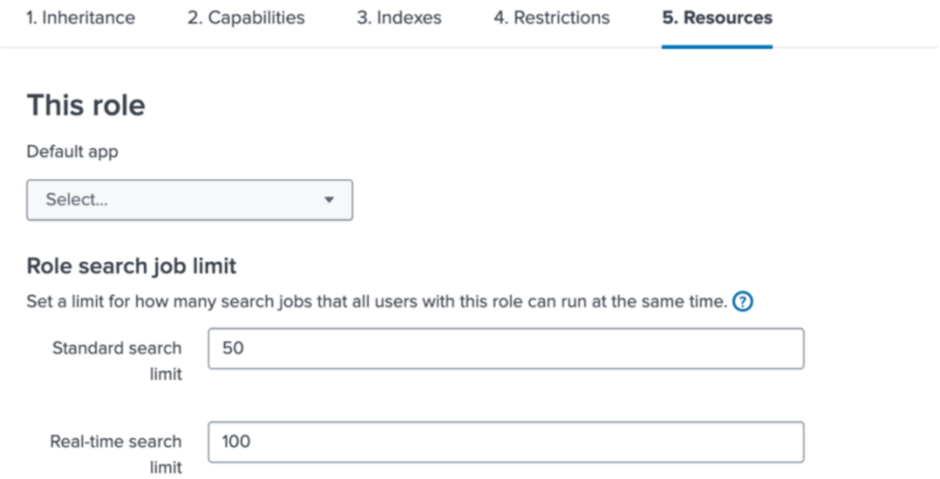
Enter a value that conta

Indexes

Enable both the "Included" and "Default" checkboxes for an index to make that index searchable by default for this role. You must save this role before you can see its inherited wildcards.

Index Name (filter)	Included	Default
* (All non-internal indexes)	☑	□
_* (All internal indexes)	☑	□

8. Click the **Resources** tab, then adjust the settings as they are listed below:
   - User Search Job Limit - Standard Search Limit
     - This is the number of simultaneous searches the Splunk service account is able to run.
     - 10 is recommended, 12 is max for larger environments. Minimum of 7 depending on the amount of content for the customer.
     - 0 is infinite.
   - Disk Space Limit
     - 'Standard Search Limit' should be adjusted to 2048MB
9. Once you've finished making these changes, click the **Save** button.



This role

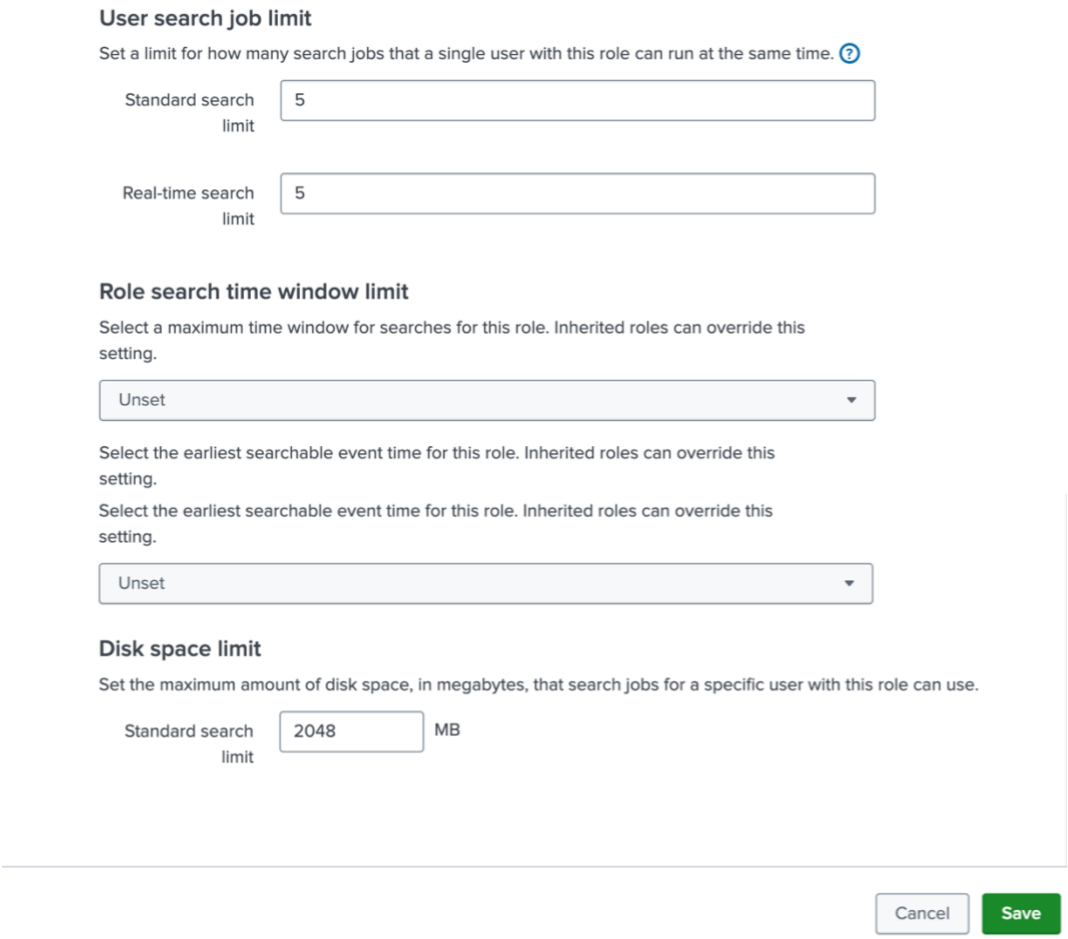
Default app: Select... ▾

Role search job limit

Set a limit for how many search jobs that all users with this role can run at the same time.

Standard search limit: 50

Real-time search limit: 100



User search job limit

Set a limit for how many search jobs that a single user with this role can run at the same time.

Standard search limit: 5

Real-time search limit: 5

Role search time window limit

Select a maximum time window for searches for this role. Inherited roles can override this setting.

Unset

Select the earliest searchable event time for this role. Inherited roles can override this setting.

Select the earliest searchable event time for this role. Inherited roles can override this setting.

Unset

Disk space limit

Set the maximum amount of disk space, in megabytes, that search jobs for a specific user with this role can use.

Standard search limit: 2048 MB

Create a new user within Splunk

Important: You must have Splunk administrator privileges to create a service account. If your SIEM is Splunk Cloud, reach out to Splunk Support and they will create the service account for you.

1. To create a new role, select **Users** from the **Settings** menu in Splunk.
2. Click **New User**.
3. Add an Account Name (Recommended: greymatter_svc).
4. Set **Password**.
5. Set the **Role** created above.
6. Enable **no need to require password change**.
7. Click **Save User**.

Important: If you are a multi-tenant customer, create a new user for each business unit. Dependent upon your architecture, a business unit may have multiple indices. Make sure the service account's permissions are configured to pull from all of the applicable indices.

Obtain Token

1. In Splunk, select **Tokens** from the **Settings** menu.

2. Click **Tokens**.
3. Select **New Token**.
4. Click **Assign User** and add the previously created user (greymatter_svc).
5. Set the **Audience** (Recommended: GreyMatter API Access).
6. Click **Save Token**.

Learn more about creating authorization tokens in Splunk documentation.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Investigate / Hunt	Perform Query Get Fields Get Sources	Rest_apps_management Rest_apps_view Rest_properties_set Rest_properties_get Schedule_rtsearch Schedule_search Search
Asset Inventory	Asset Inventory	Rest_apps_management Rest_apps_view Rest_properties_set Rest_properties_get Schedule_rtsearch Schedule_search Search
Detect	Get Detection Records Update Detections Perform GM Detect Query	Rest_apps_management Rest_apps_view Rest_properties_set Rest_properties_get Schedule_rtsearch Schedule_search Search
	Detection Push	Edit_log_alert_event
Intel Push	Intel Push	Admin_all_objects Rest_apps_management Rest_apps_view Rest_properties_set Rest_properties_get Schedule_rtsearch Schedule_search Search

Investigate/Hunt

GreyMatter Investigate queries all indexes by default.

Asset Inventory

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

Detect

Splunk supports **Alert Ingestion and Detection at Storage (ReliaQuest-Authored).**

Intel Push

Intel indicators of compromise (IOCs) feed to Splunk through Intel Push.

IOC Types: All list types are supported. Template files are used for detection logic.

By default, the IOC never expires.

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.