

SailPoint Identity Security Cloud Integration Guide

SailPoint Identity Security Cloud is a cloud-based platform that provides comprehensive identity governance and administration, enabling organizations to manage access to applications, data, and systems securely. It leverages AI-driven insights to automate identity processes, ensure compliance, and protect sensitive resources across hybrid and multi-cloud environments.

Deployment Type

This integration supports **on-premises**, **private cloud**, and **vendor cloud** deployments through **port 403**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please confirm your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with SailPoint, collect the following details:

- URL
 - Default: `api.identitynow.com`
- API Version
 - SailPoint will introduce an annual release that includes both public and experimental APIs. Each yearly version will be named according to its release year. For instance, if the release occurs in 2026, the version will be designated as v2026.
- Client ID
- Client Secret

See instructions below to gather the required information.

Collect Org Name

1. In SailPoint Identity Security Cloud, select **Admin**.
2. Click **Dashboard**.
3. Click **Overview**.
4. View **Org Details**.
5. Copy the **Org Name**.

Collect Domain

While in SailPoint, copy the underlined value from the URL: `https://{tenantName}.identitynow.com/`.

Collect Client ID and Secret

1. In SailPoint, click the **dropdown** icon next to your username in the top right corner.
2. Select **Preferences**.
3. Select **Personal Access Tokens** from the left navigation menu.
4. Click **New Token**.
5. Add a **description** for the token (include where/for what this token is being used, i.e. GreyMatter Integration).
6. Enable the following scopes:

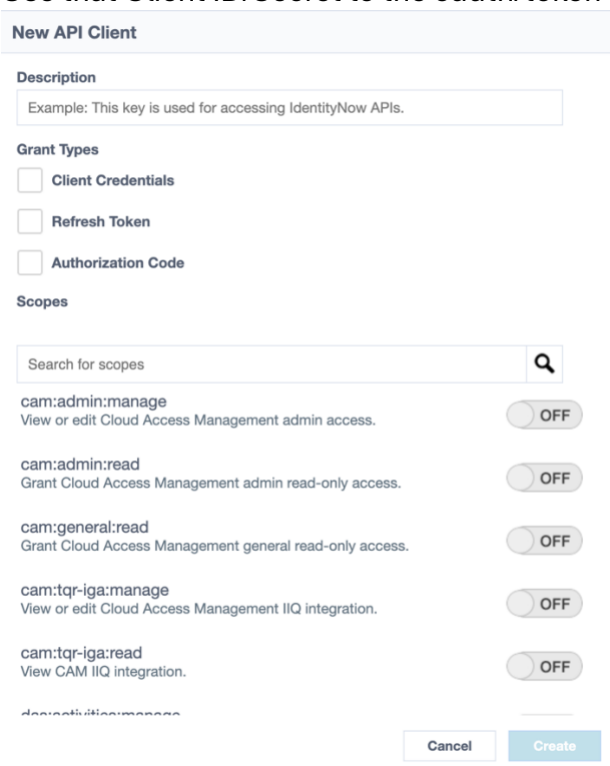
SailPoint Identity Security Cloud Integration Guide

- sp:search:read
 - idn:identity:read
 - idn:identity:manage
 - idn:role-unchecked:manage
 - idn:role-unchecked:read
 - idn:identity-account:read
 - idn:app-roles:read
 - idn:accounts:read
 - idn:accounts-state:manage
 - idn:account-provisioning:manage
7. Click **Create**.
 8. Click **Close** in the Update in Progress popup.
 9. Copy the **Secret** and **Client ID**. This is the only time you can see the Secret.

[See SailPoint Identity Services documentation.](#)

Generate Client Credentials for Set Password Play

1. Log in to Identity Security Cloud Tenant.
2. Navigate to Admin Tab > Global > Security settings > API Management.
3. Click +New.
4. Select 'Client Credentials' as grant type.
5. Select scopes: idn:password-info:read, idn:password-change:read, idn:password-change:manage.
6. Use that Client ID/Secret to the oauth/token api.



New API Client

Description

Grant Types

Client Credentials

Refresh Token

Authorization Code

Scopes

cam:admin:manage View or edit Cloud Access Management admin access.	<input type="checkbox"/>	OFF
cam:admin:read Grant Cloud Access Management admin read-only access.	<input type="checkbox"/>	OFF
cam:general:read Grant Cloud Access Management general read-only access.	<input type="checkbox"/>	OFF
cam:tqr-iga:manage View or edit Cloud Access Management IIQ integration.	<input type="checkbox"/>	OFF
cam:tqr-iga:read View CAM IIQ integration.	<input type="checkbox"/>	OFF

SailPoint Identity Security Cloud Integration Guide

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Investigate / Hunt	Multiple table queries	scope(sp:search:read)
Respond	Enrich User	scope(idn:identity:read) scope(idn:identity:manage) scope(idn:role-unchecked:manage) scope(idn:role-unchecked:read) scope(idn:identity-account:read) scope(idn:app-roles:read)
	Enable/Disable User	scope(idn:identity:read) scope(idn:identity:manage) scope(idn:accounts:read) scope(idn:accounts-state:manage) scope(idn:account-provisioning:manage) scope(idn:identity-account:read)
	Set Password	scope(idn:password-info:read) scope(idn:password-change:manage) scope(idn:password-change:read)

Respond

Playbook Name	Description	Required Input Variables
Enrich User	The results will return details on the account associated identities and specific roles assigned to the account.	user example: Cindy Little email example: Cindy.Little@sailpointdemo.com identity Id example: 000d79f081494c25b6af4c6af06e6b5a alias example: Cindy.Little Note: Identities can be searched by email, name, alias or id, whereas accounts can be searched by id or identityId.
Disable User	The result of the playbook will return transaction id along with a success message.	user example: Cindy Little email

SailPoint Identity Security Cloud Integration Guide

	<p>You can validate the success in the technology by navigating to the account and checking its status.</p>	<p>example: Cindy.Little@sailpointdemo.com</p> <p>Account Id example: 000d79f081494c25b6af4c6af06e6b5a</p> <p>alias example: Cindy.Little</p> <p>Note: Accounts can be searched by email, name, alias or id, but the most reliable method is account id.</p>
Enable User	<p>The result of the playbook will return transaction id along with a success message. You can validate the success in the technology by navigating to the account and checking its status.</p>	<p>user example: Cindy Little</p> <p>email example: Cindy.Little@sailpointdemo.com</p> <p>Account Id example: 000d79f081494c25b6af4c6af06e6b5a</p> <p>alias example: Cindy.Little</p> <p>Note: Accounts can be searched by email, name, alias or id, but the most reliable method is account id.</p>
Set Password	<p>The results return details on the password setting attempt.</p>	<p>User Example: "Cindy Little"</p> <p>Email Example:"Cindy.Little@sailpointdemo.com"</p> <p>identity Id Example: "000d79f081494c25b6af4c6af06e6b5a"</p> <p>Alias "Cindy.Little"</p> <p>Note: Identities can be searched by email, name, alias or id, whereas accounts can be searched by id or identityId</p>

Investigate/Hunt

Multiple Tables - Performs search queries on the following Elasticsearch indices:

- accessprofiles
- accountactivities
- entitlements
- events

SailPoint Identity Security Cloud Integration Guide

- identities
- roles
- *

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with SailPoint Identity Security Cloud, providing real-time insights into Identities, Roles, and Accounts from your organization's environment.

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.