# Integrate with SailPoint

CA Privileged Access Manager populates SailPoint integration tables with CA Privileged Access Manager Users (with current Role and User Group assignments), Roles, and User Groups. CA Privileged Access Manager Roles and User Groups are imported by SailPoint to be defined as Entitlements. CA Privileged Access Manager Users are imported and made into IdentityIQ Users in SailPoint. Whenever changes occur within CA Privileged Access Manager, these tables are updated on a configurable interval.

- Setup
- CA Privileged Access Manager Configuration
- SailPoint Configuration
- Operations and Attributes
- Aggregation Tasks
- Workflow Example
- Activity Log

## Setup

SailPoint is activated with a CA Privileged Access Manager licensing option. Integration is accomplished using the SailPoint STI (Simple Table Integration).

### CA Privileged Access Manager Configuration

To configure SailPoint integration in CA Privileged Access Manager, follow these steps:

1. Go to **Configuration**, **3rd Party**, **SailPoint**.
2. Enter the **Database User**, and **Database Password**. The password is used in SailPoint configuration, which follows.
3. Set the **Update Interval**, in seconds. This value determines how often CA Privileged Access Manager checks for incoming SailPoint requests, exports relevant data to SailPoint.
4. For **SailPoint Whitelist**, enter at least one SailPoint server address. These addresses are the only connections to allow for SailPoint integration. Valid entries are IP address, hostname, and FQDN values.
5. Select **Save** to save your settings.
6. Select **Install** to set up the SailPoint integration Tables. The installation is only done once. This button is enabled if SailPoint is licensed, and disabled again once the installation is complete.
7. Select **Download** to acquire a zip file of the CA Privileged Access Manager SailPoint application. Use this file during the configuration of the SailPoint side of the integration.

Unzip this file and save CAPamConfiguration.xml in a location accessible by your SailPoint application.

8. The **Import** button is optional. You can manually direct CA Privileged Access Manager to read the provisioning queue, which is automatically done according to the Update Interval setting.
9. The **Export** button is optional. You can manually direct CA Privileged Access Manager to populate the SailPoint tables, which is automatically done according to the Update Interval setting.

# SailPoint Configuration

To configure the integration in SailPoint, follow these steps:

1. In SailPoint IdentityIQ, click the configuration gear icon and select **Global Settings**.
   The Global Settings page appears.
2. Select the **Import from File** option in the lower right.
3. Select **Choose File** under **Import Objects**. Select CAPamConfiguration.xml, which you downloaded during the CA Privileged Access Manager configuration.
4. Select **Import.**
5. Under **Applications**, **Application Definitions**, click on the **CAPam** application.
   The **Edit Application CAPam** page appears.
6. Select the Configuration tab.
7. Under **Settings**, enter the correct **Connection Password**, which was not provided in the configuration XML file. This is the password that you entered in step 2 of CA Privileged Access Manager Configuration.
8. Scroll down to **Object Type: usergroup**. Under **Settings**, enter the correct **Connection Password**.
9. Scroll down to **Object Type: role**. Under **Settings**, enter the correct **Connection Password**.
10. Scroll down to **Object Type: group**. Under **Settings**, enter the correct **Connection Password**.
11. Scroll to the bottom of the page and select **Test Connection**.
    "Test successful" appears. If not, edit the passwords.
12. Select **Save** to save your changes.

For your specific SailPoint IdentityIQ configuration, you can change the default provisioning policies that are provided by CA Privileged Access Manager. Inspect these settings to determine if you must change them.

1. Under **Configuration**, select **Provisioning Policies**.
2. Under **Object Type: account**, for the **Create** Type, select **User**.
   The **Attributes** for User appear.

3. Select an Attribute, such as **lastName**. See Operations and Attributes for a list of the supported operations and attributes.
   The **Edit Options** appear on the right.
4. Select **Value Settings**. The value for **lastName** can be a static Value, be Dependent, be determined by a Script, or be determined by a Rule.
5. If you want to save you changes, select **Save**.
6. On the **Edit Application CAPam**, **Password Policy** page, configure a default password policy that follows the default password policy set for CA Privileged Access Manager users.

# Operations and Attributes

The following operations and attributes are supported for SailPoint integration. The listed attributes must be associated with a rule or value in a Provisioning Policy in the SailPoint **CAPam** application for attributes to sync. The **CAPam** application is configured with some default values, but clients might need to adjust these settings.

## Create User

To create a user with the "local" authType, all the listed attributes are required. To create a user with the "cac" authType, none of the listed attributes are required.

- **firstName**: User first name
- **lastName**: User last name
- **email**: User email address
- **password**: User password
- **authType**: supported values are **local** or **cac** (for smartcard users)
- **IIQDisabled**: **true** if user is disabled, or **false** if user is enabled
- **Roles** and **User Groups** are assigned as **Entitlements**.

## Modify User

To modify a user, all attributes are optional.

- **firstName**: User first name
- **lastName**: User last name
- **email**: User email address
- **password**: User password
- **authType**: supported values are **local** or **cac** (for smartcard users)
- **IIQDisabled**: **true** if user is disabled, or **false** if user is enabled
- **Roles** and **User Groups** are assigned or removed as **Entitlements.**

## Delete User

- No attributes

# Aggregation Tasks

As part of the **CAPam** application setup in SailPoint, aggregation tasks are defined to SailPoint to collect the user and entitlement data from CA Privileged Access Manager. These tasks should be scheduled to execute regularly to keep this data in sync with CA Privileged Access Manager.

Follow these steps:

1. From the main SailPoint menu, select **Setup**, **Tasks**.
   Two Tasks are set up by the initial configuration:
   - **CAPam Account Aggregation** regularly reads the CA Privileged Access Manager User table to keep in sync with Users and their entitlements
   - **CAPam Group Aggregation** reads CA Privileged Access Manager User Roles and Groups and creates SailPoint Entitlements from them.
2. To schedule a task, right-click and select **Schedule** from the drop-down list to display the New Schedule dialog.
3. Select the **Scheduled Tasks** tab to edit schedules. You can select the **Run Now** box on the **Edit Schedule** tab to run the Task immediately.
4. To see a list of SailPoint entitlements, go to the main menu, **Applications**, **Entitlement Catalog**.

# Workflow Example

Once everything is configured in CA Privileged Access Manager and SailPoint IdentityIQ, the following example of the integration workflow is valid. This example shows a SailPoint making a provisioning request for a user.

1. Go to **Home**, and select **Manage User Access**.
   An IdentityIQ user list appears under the **Select Users** tab.
2. Select a User and click the **Manage Access** tab.
3. Select **Filters** on the right.
   The **Filter Access** panel appears.
4. From the **Entitlement Application** drop-down list, select **CAPam**, and **Apply**.
   The Roles and User Groups that are imported from CA Privileged Access Manager appear as Entitlements.
5. Select a User Group or Role as an Entitlement. Click the **Review** tab at the top of the page.
6. If the listed **Add Access** Entitlements are correct, select **Submit** at the bottom of the page.
   The Home page appears with a Success message at the top of the page.
7. SailPoint send this data to CA Privileged Access Manager as a provisioning request.

8. In CA Privileged Access Manager, go to **Users, Manage Users**, and find the new (or updated) User.
   The User should have the matching information, including Roles and Groups, as applicable.
9. The User should be able to log in to CA Privileged Access Manager with the appropriate entitlements.
10. An Aggregation Task runs in SailPoint, reading the information in the CA Privileged Access Manager integration tables,
    This Task closes the loop on the operation.

# Activity Log

The **Activity Log** displays information about every action pertaining to the SailPoint integration. Create, delete, and update actions, their source, time, and results are listed. To view the Activity Log, follow these steps:

1. Go to **Configuration**, **3rd Party**, **SailPoint**.
2. Select the **Activity Log** tab.
3. The log table is sortable by clicking column headings. You can filter data using the controls above the headings.
   The **Info** column provides error messages, if applicable.