SailPoint IdentityIQ

Version 8.0

Privileged Account Management Module Guide

Table of Contents

Privileged Account Management Overview 1

Complete visibility and governance over privileged accounts 1

Simplify and centralize administration 1

Integration with 3rd party PAM solutions 1

Privileged Account Management Page 1

Container Details Page 2

Container Details Identity Tab 2

Container Details Group Tab 3

Container Details Privileged Items Tab 3

Privileged Account Management Add or Remove an Identity 3

Privileged Account Management Quicklink 4

Privileged Account Management Tasks 4

Privileged Account Management Application Configuration 4

Application Configuration - Direct 4

Application Configuration - Plugin 5

Create a Privileged Account Management Database 5

Define a JDBC Application 5

Privileged Account Management SCIM Bridge Plugin 6

Privileged Account Management Setup Tab 6

Privileged Account Management Activation and Deployment 7

Privileged Account Management Credential Cycling 8

Credential Cycling Configuration 9

Working with the Credential Configuration Template 9

Template General Guidelines 9

Credential Cycling in an Application 13

Privileged Account Management Overview

Note: You must have the SailPoint Lifecycle Manager installed to use the Privileged Account Management Module effectively.

The SailPoint IdentityIQ Privileged Account Management (PAM) Module extends identity governance processes and controls to highly privileged access, enabling you to centrally manage access to privileged and non-privileged accounts.

The SailPoint IdentityIQ Privileged Account Management Module enables you to:

- Establish complete visibility and governance across all privileged accounts
- Automate governance controls, providing a complete view of an identity's access and its associated privileged accounts, eliminating over-entitled users
- Speed the delivery of provisioning and deprovisioning privileged access based on lifecycle event changes
- Rapidly deploy and integrate with your PAM vendor of choice, through a SCIM-based integration model

Complete visibility and governance over privileged accounts

By extending identity governance to privileged accounts, enterprises get 360-degree view over all access, especially high-risk identities with privileged access.

Simplify and centralize administration

Using the IdentityIQ Privileged Account Management Module, IdentityIQ can serve as a central platform to govern access to both privileged and non-privileged accounts according to established policies. This prevents overprovisioning and limits the risk of providing access to highly privileged accounts to unauthorized users. It also speeds the delivery of privileged access based on user role or lifecycle event changes.

Integration with 3rd party PAM solutions

The IdentityIQ Privileged Account Management Module enables you to deploy and integrate with the PAM vendor of choice. The IdentityIQ Privileged Account Management Module provides an open, standards–based integration framework (SCIM) that supports any third-party solution.

Privileged Account Management Page

You must be a system administrator or have the PAM Administrator user capability to access the Privileged Account Management page.

Note: The identities and entitlements contained in your privileged account management system are available throughout the IdentityIQ product. For example, the identities are incorporated in the Identity Warehouse, the entitlements display in the Entitlement Catalog, they are included in certain Certifications, requests are tracked through the process, and provisioning transactions are listed on the Administrator Console.

Navigate to the Privileged Account Management page from the Quicklink menu anywhere in the product or on your Home page by clicking the Privileged Account Management Quicklink card. In the Quicklink menu, select **Manage Access -> Privileged Account Management**.

Note: See the SailPoint IdentityIQ *User Guide* or the online help for information on using and setting up the Quicklink menu and Quicklink cards.

Note: The Privileged Account Management Quicklink is turned on as part of the Privileged Account Management activation process. You, or your administrator, must manually setup a Quicklink card.

Use the Privileged Account Management page to view every container within your privileged account installation. The containers display the following:

- Container Name — the display name aggregated from your privileged account management application
- Total Identities — the total number of identities associated with the container either directly or through a group
- Groups — the number of groups associated with the container
- Privileged Items — the number of privileged items to which this container grants access, these are usually privileged accounts

Click **Manage** to view and manage a container’s content.

Container Details Page

Use the container detail page to view the content of a container.

The page contains three tabs:

- Identities — all identities with access to the privileged items, either directly or effectively - “Container Details Identity Tab” on page 2
- Groups — all groups with access to the privileged items - “Container Details Group Tab” on page 3
- Privileged Items — all the items to which this container provides access - “Container Details Privileged Items Tab” on page 3

Container Details Identity Tab

Use this tab to add or remove identities and to view detailed information. You can display:

- Direct Access — identities granted direct access to this container (view, add, remove)
- Effective Access — identities granted access to this container through group membership (view only)

Table 1—Container Detail Page Identity Tab Descriptions

Column	Description
Direct Access	
Display Name	The display name of the identity as aggregated from the privileged account management application
Status	Current status of the identity as determined through aggregation
Manager	The listed manager of this identity, if available
Details	View details, permissions granted and the account and application from which they were granted, or **Remove** the identity from the container - "Privileged Account Management Add or Remove an Identity" on page 3
Effective Access	
Display Name	The display name of the identity as aggregated from the privileged account management application

Table 1—Container Detail Page Identity Tab Descriptions

Column	Description
Status	Current status of the identity as determined through aggregation
Manager	The listed manager of this identity, if available
Details	View details, the permissions granted and the groups from which they were granted

Container Details Group Tab

Use this tab to view detailed information.

Table 2—Container Detail Page Group Tab Descriptions

Column	Description
Display Name	The display name of the group as aggregated from the privileged account management application
Description	A description of this group, if one is available
Details	View details, the identities contained within the group, the permission granted the group by this container, and all of the permissions granted this group and the containers through which they are granted

Container Details Privileged Items Tab

Use this tab to view the name and type for the privileged items to which this container grants access.

Privileged Account Management Add or Remove an Identity

Note: **You can only add or remove an identity from the Direct Access list, the Effective Access list is view only.**

Note: **The Add and Remove processes follows the workflow as defined when the Privilege Account Management Module was deployed.**

Note: **You can track your requests through IdentityIQ. See the SailPoint IdentityIQ *User Guide* or online help for information on how to track your requests.**

Add Identities:

Note: **You can only add identities that have an existing account on your privileged account management application. You can request an account be added using SailPoint's Lifecycle Manager's Mange Access features if one does not exist.**

1. Click **Add Identities**
2. Select an identity, either by entering a name or selecting using the drop-down arrow
3. Click **Next** to view the Add Container Permissions dialog
4. Select the permissions to grant
5. You might be prompted to select an account, if the user has more than one account on the application
6. Click **Submit** to begin the approval/provisioning process

Remove:

Click **Remove** and confirm your decision to begin the removal process. Use **Bulk Remove** to remove multiple identities at once.

Privileged Account Management Quicklink

The Privileged Account Quicklink is added to your Quicklink panel during the installation process. You can manually add a Quicklink card to your Home page as well.

1. Go to your Home page
2. Click **Edit**
3. Click **Add Card**
4. Select **Privileged Account Management** and **Save**
5. **Save** again on the Home Edit page to load the card

Refer to the online help for more information on Quicklinks and Quicklink cards.

Privileged Account Management Tasks

You need to configure new tasks to aggregate and update information in IdentityIQ.

The following tasks are required:

- Account Aggregation
- Account Group Aggregation
- Target Aggregation
- Effective Access Indexing
- Identity Refresh — with the **Refresh Identity Entitlements for all links** selected

Refer to the SailPoint IdentityIQ *Administration Guide* for detailed information on defining tasks in IdentityIQ.

Privileged Account Management Application Configuration

There are two possible application configuration scenarios available for the Privileged Account Management Module. The first is a direct connection, for PAM vendors using SailPoint’s SCIM API, and the second involves using the PAM Plugin, for those who do not.

Application Configuration - Direct

If you use the SailPoint SCIM API, define a Privileged Account Management application type to communicate information to IdentityIQ. This application is very similar to the SCIM Application type. Refer to the SCIM application connector documentation available on Compass for detailed information.

On the newly created application, go to the Unstructured Target Configuration tab and create a Privileged Account Management unstructured target collector using the **Privileged Account Management Collector** Type.

Application Configuration - Plugin

PAM vendors not using the SailPoint SCIM API need to create a database to hold their privileged information, for example accounts, account groups, and containers, a JDBC application type, used by the PAM plugin to interact with the database, and install the PAM Plugin.

Create a Privileged Account Management Database

Create a database that contains the privileged account information to be shared with IdentityIQ, for example accounts, account groups, and containers (safes). This database needs to be synced periodically, through an agent, and be able to connect with the PAM Plugin through a JDBC application type.

Define a JDBC Application

Note: This application will only be used by the PAM Plugin to interact with the privileged account information in the created database. This application will not be aggregated into IdentityIQ

Define a JDBC application type on the Application Definition page. This application contains the information needed to enable the PAM Plugin to interact with the privileged account database.

Configuration Tab:

Define the JDBC Connection Settings, for example the Database URL and JDBC Driver.

Define SQL Statements and getObjectSQL for each object in the PAM database.

The following objects are required:

- account
- group
- Container
- ContainterPermission
- PrivilegedData (optional)
- PrivilegedDataPermission (optional)

For example:

SQL Statement

```
SELECT u.id, u.userName, u.formattedName, u.familyName as lastname, u.givenName as
firstname, u.middleName, u.honorificPrefix, u.honorificSuffix,

       u.displayName, u.nickname as nickName, u.profileURL as profileUrl, u.title,
u.usertype as userType, u.preferredLanguage, u.locale, u.timezone,

       !u.active as IIQDisabled, u.email, u.source, u.source_native_identifier as
sourceNativeIdentifier, g.id as groups, g.displayName as groupNames

  FROM users u

        left outer join user_group_assignments uga on uga.user_id = u.id

        left outer join groups g on g.id = uga.group_id

ORDER BY u.id
```

getObjectSQL

```
SELECT u.id, u.userName, u.formattedName, u.familyName as lastname, u.givenName as
firstname, u.middleName, u.honorificPrefix, u.honorificSuffix,
       u.displayName, u.nickname as nickName, u.profileURL as profileUrl, u.title,
u.usertype as userType, u.preferredLanguage, u.locale, u.timezone,

       !u.active as IIQDisabled, u.email, u.source, u.source_native_identifier as
sourceNativeIdentifier, g.id as groups, g.displayName as groupNames

  FROM users u

        left outer join user_group_assignments uga on uga.user_id = u.id

        left outer join groups g on g.id = uga.group_id

WHERE u.id = '$(identity)'
```

Rule Tab:

If you are enabling provisioning in the Privileged Account Management Module you must select a Provisioning Rule Type and specify a Provisioning Rule. You can import a rule into IdentityIQ or create one using the Rule Editor.

Refer to the JDBC application connector documentation available on Compass for detailed information.

Privileged Account Management SCIM Bridge Plugin

SailPoint provides a SCIM privileged account management bridge that provides a PAM REST API that the PAM collector and connector can use if a PAM vendor does not support the API. This has a pluggable PAMEngine interface that enables using an engine plugin to communicate with the vendor through some other means (JDBC, a vendor-specific API).

Note: Partitioning will not be supported by the engine.

This PAM Plugin is available on the Plugins page of Compass. Login using your Compass password or contact your support manager.

Install the PAM Plugin by dragging and dropping it onto the Installed Plugins page. To access this page, click on the gear icon and select **Plugins**.

Configure the plugin:

- SCIM PAM Engine Plugin Name — optional and not necessary with the JDBC Engine Plugin
- SCIM PAM Engine Class Name— The fully-qualified class name of the SCIM PAM Engine, for example sailpoint.pam.scimBridge.engine.JdbcPamEngine
- JDBC Application Name — The name of the JDBC application that is configured to communicate with the PAM database (only used with JDBC PAM Engine or a vendor-specific API)

This application will be configured with the JDBC URL, username, password, rules, schemas, etc... It will not be aggregated from directly (for example - it should not be included in any account or group aggregation tasks), but will be used by the engine to communicate.

Privileged Account Management Setup Tab

Use the Privileged Account Management tab on the Configure Identity Settings page to set up your deployment of the Privileged Account Management module. Click the gear icon and select Global Settings -> IdentityIQ Configuration to display the Privileged Account Management tab.

Define the following:

- The Application used for Privileged Account Management — the application used to aggregate information from the privileged account management database into IdentityIQ. This application must be specified whether you are connecting directly or using the plugin. This is the Privileged Account Management Application described in “Application Configuration - Direct” on page 4.
- Enable Privileged Account Management provisioning — turn provisioning on or off.
- The maximum number of selectable users in Privileged Account Management — the maximum number of identities you can take action on at one time.
- The workflow used to provision identities — the workflow, or business process, that defines the provisioning process for the Privileged Account Management Module. Business processes are defined and maintained on the Business Process Editor page. See the SailPoint IdentityIQ *Administration Guide* for details on the Business Process Editor.

Privileged Account Management Activation and Deployment

Use the following information to activate the Privileged Account Management Module.

1. Log on to your instance of IdentityIQ as an administrator.
2. Click on Global Settings under the gear icon and select the Import from File Page.
3. Click **Browse** and browse to the following directory:
   identityiq_`*home*\WEB-INF\config`
   where identityiq_home is the directory in which you extracted the identityiq`.war` file during the IdentityIQ installation procedure.
4. Select the `init-pam.xml` file and click **Import**.
5. When the import is complete, click **Done**.

The Privileged Account Management features are now active inside of the IdentityIQ product.

These features include:

- Configure IdentityIQ Configuration
    - Privileged Account Management tab
- Application
    - Privileged Account Management application type
    - Privileged Account Management collector type
- Business Processes (workflows)
    - PAM Approval Subprocess
    - PAM Identity Provisioning
    - PAM Identity Provisioning Notify
    - PAM Initialize
    - PAM Request Finalize
- User Capabilities
    - PAM Administrator
- Quicklink Panel — available anywhere in the product
    - Privileged Account Management quicklink
- Dynamic Scope
    - PAMAdministrator
- Email Templates
    - PAM Approval
    - PAM Manager Notification
    - PAM Requester Notification
    - PAM User Notification
- Rules
    - PAM Access Mapping Correlation Rule
    - PAM Group Refresh
- Audit Events
    - Approve PAM Request/ Reject PAM Request

Privileged Account Management Credential Cycling

Credential cycling enables applications that require credentials, such as username and password, to obtain that information directly from a PAM vendor, such as a CyberArk or Beyond Trust vault. Credential cycling enables credentials to be authenticated directly from the PAM source at runtime.

An administrator defines which applications will use credential cycling, which PAM solution provides those credentials, and how each of the applications will contact the PAM repository to retrieve the credentials. This is done using a configuration file that is imported into IdentityIQ as an object.

Credential Cycling Configuration

A more detailed look at the template and the configuration options is provided in a later section.

Prerequisites:

- Install and configure the PAM Module (with link)
- Define an application in IdentityIQ

A template file is provided in your IdentityIQ installation for use as a model for setting up your own configuration. The template file is:

`\WEB-INF\config\credentialConfigurationTemplate.xml`

Edit this file to set your own PAM solution and values. The template includes models for BeyondTrust and CyberArk, as well as a solution-neutral mapping option.

- Include information about which of your applications will use credential cycling.
- Import the edited XML file into IdentityIQ using **Gear icon > Global Configuration > Import File**
- Importing the file creates a new object in IdentityIQ: Credential Configuration

If you need to update your credential cycling configuration, modify and re-import the credential configuration XML. You can also edit the Credential Configuration object directly in the Debug pages.

Working with the Credential Configuration Template

The `credentialConfigurationTemplate.xml` is located in the `WEB-INF\config` directory of your IdentityIQ installation.

The template file includes sections for BeyondTrust, CyberArk, and a solution-neutral mapping option. If you are using a PAM solution other than BeyondTrust or CyberArk, you can use those sections of the template as a model for configuring another PAM solution.The file is fully commented to provide guidance as you insert your configuration settings.

Template General Guidelines

When working with templates, the best practice is to make a copy of this template to hold your specific configuration values, rather than modifying the original template file.

The template includes individual sections for BeyondTrust, CyberArk, and a solution-neutral mapping option. Remove the sections that you will not use before importing the template. For example, if you want to implement just a CyberArk solution, remove the template sections for BeyondTrust and the mapping option.

BeyondTrust

Here are some key points to observe when you work with the BeyondTrust portion of the template:

```
<CredentialSource credentialClass="sailpoint.pam.credential.BeyondTrustCredentialManager"
name="beyondTrust ">

        <!-- The attributes in this map are used mainly to communicate with BeyondTrust.

          Any values here can be overridden by values of the same name in the attributes

          map of each credential association.  Required attributes must either be configured

          here or in every credential source.  Attributes:
```

```
  Required:  url
  Required:  runas
  Required:  apikey
  Required:  managedSystemName
  Required:  managedAccountName
  Optional:  durationMinutes
  Optional:  credentialCacheMinutes
  Optional:  checkInReason
  Optional:  checkOutReason
  -->
<Attributes>
 <Map>
  <entry key="url">
   <value><String>https://your.beyondtrust.server/BeyondTrust/api/public/v3/</String></value>
  </entry>
  <entry key="runas">
   <value><String>runas_user</String></value>
  </entry>
  <entry key="apikey">
   <value><String>your_beyondtrust_api_key_goes_here</String></value>
  </entry>
  <entry key="managedAccountName" value="beyond_trust_managed_account_name"/>
  <entry key="managedSystemName" value="beyond_trust_managed_system_name"/>
 </Map>
</Attributes>
<!-- ***Application Configuration -->
<CredentialAssociation applicationName="application_name"
            attributeName="application_username_attribute"
            credentialAttributeName="BeyondTrust_username_attribute">
 <!-- *** Attribute values go here.  These attributes can be used to override values from
    *** above, or can be left out if not needed -->
 <Attributes>
  <Map>
```

```
           <entry key="managedAccountName" value="special_beyond_trust_managed_account_name"/>
          </Map>
         </Attributes>
        </CredentialAssociation>
        <CredentialAssociation applicationName="application_name"
                    attributeName="application_password_attribute"
                    credentialAttributeName="BeyondTrust_password_attribute"/>
       </CredentialSource>
```

CyberArk

Here are some key points to observe when you work with the CyberArk portion of the template:

```
<CredentialSource credentialClass="sailpoint.pam.credential.CyberArkCredentialManager" name="cyberark">
        <!-- The attributes in this map are used mainly to communicate with CyberArk.
           Any values here can be overriden by values of the same name in the attributes
           map of each credential association.  Required attributes must either be configured
           here or in every credential source.  Attributes:
          Required:  safe
          Required:  folder
          Required:  appId
          Required:  object
         -->
        <Attributes>
         <Map>
          <entry key="safe" value="cyber_ark_safe_name"/>
          <entry key="folder" value="cyber_ark_folder_name"/>
          <entry key="appId" value="cyber_ark_app_ID"/>
         </Map>
        </Attributes>

        <!-- *** Application Configuration -->
        <CredentialAssociation applicationName="application_name"
                    attributeName="application_username_attribute"
                    credentialAttributeName="CyberArk_username_attribute">
         <!-- *** Attribute values go here.  These attributes can be used to override values from
```

```
     *** above, or can be left out if not needed -->
  <Attributes>
   <Map>
    <entry key="object" value="object_value"/>
   </Map>
  </Attributes>
 </CredentialAssociation>
</CredentialSource>
```

Credential Mapping

Here are some key points to observe when you work with the mapping portion of the template:

```
<CredentialSource credentialClass="sailpoint.pam.credential.MapCredentialManager"
name="mapCredManager">
        <!-- The attributes in this map are the values that will be returned by the map credential manager.
           It's probably a good idea to encrypt these so they are not stored in plain text if the values
           are sensitive -->
        <Attributes>
         <Map>
          <entry key="credentialValues">
           <value>
            <Map>
             <entry key="map_username_attribute" value="john_doe_username"/>
             <entry key="map_password_attribute" value="super_secret_password"/>
            </Map>
           </value>
          </entry>
         </Map>
        </Attributes>
        <!-- *** Application Configuration -->
        <CredentialAssociation applicationName="application_name"
                    attributeName="application_username_attribute"
                    credentialAttributeName="map_username_attribute"/>
        <CredentialAssociation applicationName="application_name"
                    attributeName="application_password_attribute"
                    credentialAttributeName="map_password_attribute"/>
```

```
	</CredentialSource>
```

Credential Cycling in an Application

When credential cycling is configured for an application, the Application Definition page displays a message for the users. Although the relevant credential fields are still marked as requiring values, these fields are not validated when credential cycling is enabled, and so can be left blank, or can include dummy values.