Privileged Account Management

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint Technologies,” (design and word mark), “SailPoint,” (design and word mark), "Identity IQ,” “IdentityNow,” “SecurityIQ,” “Identity AI,” “Identity Cube,” and “SailPoint Predictive Identity” are registered trademarks of SailPoint Technologies, Inc. “Identity is Everything,” “The Power of Identity,” and “Identity University” are trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind regarding these materials or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

About Privileged Account Management

Privileged Account Management (PAM) refers to managing access to privileged or high-level accounts such as domain administrator accounts, root accounts, or superuser accounts, as well as to critical or sensitive accounts and systems. These privileges are often associated with IT accounts, such as root access to a Unix system or the ability to add or delete email accounts on a Microsoft Exchange application. They can also apply to access to sensitive accounts such as a company's social media, or sensitive assets such as a financial database or list of credit card numbers or security certificates.

By controlling access to privileged accounts, PAM solutions provide a way to protect organizations from accidental or deliberate misuse of privileged access. There are numerous PAM solution providers in the market, such as Thycotic, Leiberman, CyberArk, and BeyondTrust. The details of how access to privileged accounts is managed can vary by solution provider, and might mean different things to different companies. Things like automatic rotation of credentials, time-boxing user access, making passwords invisible to end users, and tracking and auditing actions can all be parts of a PAM solution.

Think of PAM solutions as a library, but instead of books, the library holds privileged accounts. To check a book out of the library you need a library card, but for PAM, you need some kind of credential or authorization to access what is in the library, or vault. ("Vault" is a common term for the logical container of assets protected by PAM.) However, unlike a library card, which gives you access to every book in a library, with PAM your credential might only give you access to a limited set of specific PAM vaults, and not every vault that is managed by the PAM solution.

PAM Terminology

Although specific terms for common PAM concepts vary from vendor to vendor, in general these are the terms you will encounter when working with PAM solutions:

- **Vault or safe:** a logical container or folder that contains privileged accounts and passwords. A safe or vault is a container in which you store privileged access, for example, a container for all your company's Windows administrator accounts, or a container for all Unix root accounts. In IdentityIQ, these are called containers.

- **Privileged Item:** a piece of privileged data that is managed by the PAM solution, such an account, credential, file, or key. The types and names of privileged data vary by PAM vendor.

Additional Resources

Privileged Access Management Best Practices

Privileged Access Management Use Cases

Privileged Account Management in IdentityIQ

> 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. It gives you a complete and centralized view of your PAM containers, including which individuals and groups have access to each container, and what privileged items each container holds. It also automates governance controls, enabling you to securely manage access to PAM containers.

IdentityIQ is not a PAM solution per se and does not provide the same features a PAM solution does; rather, the IdentityIQ PAM module integrates with market-leading PAM solution providers (such as Thycotic, Leiberman, CyberArk, and BeyondTrust) to provide governance features that the PAM solutions themselves do not offer. While the native PAM solution determines *what is in* a container, and IdentityIQ PAM module governs *who has access* to a container, and *what permissions* they have in it

The SailPoint IdentityIQ Privileged Account Management Module gives you:

Complete visibility and governance over privileged accounts

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

Simplified and centralized administration

With the 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 multiple 3rd-party PAM solutions at once

The IdentityIQ Privileged Account Management Module enables you to deploy multiple instances and integrate with multiple PAM vendors at the same time. The IdentityIQ Privileged Account Management Module provides an open, standards–based integration framework (SCIM) that supports any third-party solution.

Activating the Privileged Account Management Module

To activate the PAM module:

1. Log on to IdentityIQ as an administrator.

2. Click **gear > Global Settings** and select **Import from File**.

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 PAM features are now active inside of the IdentityIQ product.

Components Installed with the PAM Module

The installed PAM components include:

Business Processes

PAM Approval Subprocess

Approval subprocess for PAM requests. This generates approvals based on the approvalScheme, audits the approval decisions, and returns the approved status.

PAM Identity Provisioning

The business process that handles provisioning of identities for PAM.

PAM Identity Provisioning Notify

This subprocess handles notification from the PAM provisioning workflows.

PAM Initialize

This subprocess initializes the various objects necessary when executing the PAM workflow. This creates the ProvisioningProject and IdentityRequest.

PAM Request Finalize

This subprocess handles the final step from the PAM business processes.

Email Templates

PAM Approval

Notifies approvers when they need to approve a request changes a user's permissions on a PAM container.

PAM Manager Notification

Notifies managers when an employee's access to PAM containers is modified.

PAM Requester Notification

Notifies requesters when their requests for PAM access modification are completed.

PAM User Notification

Notifies users when they are given access or removed to a PAM container.

User Capabilities

PAM Administrator

Gives users full access to all PAM module functionality; this capability is assigned by default to members of the **PAMAdministrator** Dynamic Scope/Quicklink Population, and can also be assigned directly to individual users.

PAM Viewer

Gives read-only access to PAM features and information.

Dynamic Scope

PAMAdministrator

Lets associated users see and use the Quicklink that grants access to PAM functionality.

Quicklink

Privileged Account Management

The Quicklink menu item available by default to members of the PAMAdministrator Dynamic Scope. This Quicklink appears in the main menu under **Manage Access > Privileged Account Managment**. In the Debug pages, this Quicklink object is named `View PAM Container List`.

Audit Event

Approve PAM Request / Reject PAM Request

You can select these in the **gear menu > Global Settings > Audit Configuration** page if you want to audit PAM-related events.

Rules

PAM Group Refresh

This rule make external groups non-requestable. You might want to make external groups non-requestable if, for example, your organization's process is for group membership to be requestable through an external application such as Active Directory, which is a common use case

Map Demodata PAM Application Names

A sample rule included in the `examplerules.xml` file in the `[installdir]\WEB-INF\config` directory. PAM solutions have the concept of "external" users and groups: accounts and groups that are defined in an external system such as Active Directory, and are used within the PAM system to control access. When these objects are aggregated from the PAM system, they include a *source* attribute for the name of the external system from which they came (the name used by the PAM system). When stored as Links and ManagedAttributes, these names need to match the Application name. This rule maps the name as known on the external system to a name that can be used locally.

Application Types

Privileged Account Management application (connector) type

Aggregates users, groups, and containers into IdentityIQ.

Privileged Account Management collector type

Reads in permissions users have on containers, and can write permissions back to the target system.

Configuring the Privileged Account Management Module

Configuring the PAM module in IdentityIQ involves several steps:

- Configuring applications to connect to your PAM vendor to aggregate data about PAM accounts and groups. The PAM application should include a collector to aggregate data about PAM vaults and permissions. See Configuring a PAM Application.
- Setting global options for PAM, that determine things like how PAM containers can be modified within IdentityIQ, and which business process to use for provisioning PAM identities. See PAM Global Configuration Settings
- Configuring the tasks that will aggregate and index PAM data, and refresh identities. See Privileged Account Management Tasks: Aggregation, Indexing, and Refresh

Configuring a PAM Application

The PAM module includes a PAM-specific application (connector) type: Privileged Account Management. To use the PAM feature, configure a PAM application to connect to each of your PAM vendor systems.

Applications should be configured to include both a **connector** and **a target collector**.

- The **connector** aggregates users, groups, and containers into IdentityIQ.
- The **target collector** reads in permissions users have on containers, and can write permissions back to the target system.

> Important: The PAM connector type is based on IdentityIQ's SCIM 2.0 connector, with special schemas, object types, and policies. The SCIM 2.0 Connector documentation, which is available in the SailPoint documentation portal, gives detailed information about all the configuration parameters in this application definition. The information below provides some essential and PAM-specific information about configuring PAM applications.

To configure a PAM application:

1. Click **Applications > Application Definition > Add New Application**.
2. Enter a **Name** and **Owner** for the PAM application.
3. For **Application Type** choose **Privileged Account Management**
4. On the **Configuration** tab, click **Settings** to enter connection information. Note the following:

- The Base URL is the URL to the PAM vendor's SCIM server.
- The PAM connector type supports several methods for authentication. These are discussed in detail in Configuring Authentication for the PAM Application
- **Note**: For Thycotic implementations, it is not recommended that you select the Explicit Attribute Request setting, as this may cause issues when aggregating.

5. Also on the **Settings** tab, add **Permissions**; these are the container permissions that will display for the PAM container in the PAM UI. The permissions you enter here should correspond to the permissions used by the vendor's PAM application, and will vary depending on vendor. To add a permission, type the permission name in the **Permissions** field and click the plus icon to add it.

6. On the **Provisioning Policies** tab, edit the out-of-the-box policies for creating accounts and creating containers as needed. These policies determine which fields are presented to users when adding accounts or containers, and can also determine how container information is displayed in the Entitlement Catalog.

7. Set up an **Unstructured Target Collector** for the application. This will aggregate permissions users and groups have on containers.

   a. Click the **Unstructured Targets** tab.

   b. Click **Add New Unstructured Data Source**.

   c. An **Add or Create** dialog appears. Click **Create TargetSource**.

   d. Enter a **Name** (required) and **Description** (optional).

   e. Choose or create a **Correlation Rule** for correlating the data. You can use the **PAM Access Mapping Correlation Rule** which is provided out of the box, or create your own rule.

   f. For **Target Source Type**, choose **Privileged Account Management Collector**.

   g. A new set of **SCIM Settings** fields is displayed. For the Base URL, enter the URL to the PAM vendor's SCIM server. For details on authentication settings, see Configuring Authentication for the PAM Application. For other fields, refer to the SCIM 2.0 Connector documentation.

   h. **Save** the data source.

8. *Optional*: On the **Rules** tab, choose rules for managing your PAM application:

- You can create a **Customization Rule** on the application to map external application names to internal IdentityIQ application names, and / or external users to IdentityIQ identities.
- You can use the **PAM Group Refresh** rule (included with the PAM module) to make external groups non-requestable. You might want to make external groups non-requestable if, for example, your organization's process is for group membership to be requestable through an external application such as Active Directory; this is a common use case.

9. **Save** the Application definition.

Configuring Authentication for the PAM Application

The PAM application supports three types of authentication:

- OAuth2.0
- API Token
- Basic Authentication

> Important: Details of how to obtain the necessary credentials will vary by solution provider, so you should **consult your PAM solution provider's documentation** for details.

OAuth2.0

OAuth 2.0 is an industry-standard protocol for authorization. It provides a variety of authorization flows for web applications, desktop applications, mobile phones, and devices.

The PAM application supports several grant types for OAuth 2.0:

- Refresh Token
- Client Credentials
- JWT
- Password

Refresh Token

This grant type is used by clients in order to exchange a refresh token for a new access token when the existing access token has expired. This allows the PAM application to get a new session when the current session expires, without having to re-authenticate as frequently. This grant type is commonly used together with Authorization Code to prevent a user from having to log in several times per day.

> Note: Before any OAuth 2.0 token requests can be initiated, a Client ID and secret are necessary. Details of how to obtain the necessary credentials will vary by solution provider, so you should consult your PAM solution provider's documentation for details.

For more information see OAuth 2.0 Refresh Token.

To configure Refresh Token authentication:

1. Enter the **OAuth 2.0 Token URL** for generating access token. This URL is on the PAM solution provider side. Refer to your PAM solution provider system administrator or documentation for information about this URL.
2. Enter the **Client ID** for OAuth 2.0 authentication. This is obtained from your PAM solution provider.
3. Enter the **Client Secret** for OAuth 2.0 authentication. This is obtained from your PAM solution provider.
4. Enter the **Refresh Token** used to generate an access token. This is obtained from your PAM solution provider.

Client Credentials

The Client Credentials grant is used when applications request an access token to access their own resources, not on behalf of a user.

> Note: Before any OAuth 2.0 token requests can be initiated, a Client ID and secret are necessary. Details of how to obtain the necessary credentials will vary by solution provider, so you should consult your PAM solution provider's documentation for details.

For more information see OAuth 2.0 Client Credentials Grant.

To configure Client Credentials authentication:

1. Enter the **OAuth 2.0 Token URL** for generating access token. This URL is on the PAM solution provider side. Refer to your PAM solution provider system administrator or documentation for information about this URL.
2. Enter the **Client ID** for OAuth 2.0 authentication. This is obtained from your PAM solution provider.
3. Enter the **Client Secret** for OAuth 2.0 authentication. This is obtained from your PAM solution provider.

JWT

A JWT (JSON Web Token) securely authenticates the connection to an external application to perform operations as required. A JWT contains encoded JSON objects, and is signed using a signing algorithm to ensure that the claims cannot be altered after the token is issued. These tokens have a specific structure consisting of a header, payload, and signature.

JWTs can be used as OAuth 2.0 Bearer Tokens to encode all relevant parts of an access token into the access token itself instead of having to store them in a database.

You can use the **Additional Payload** field for systems where authentication may require additional parameters along with mandatory fields.

For example, if the PAM system expects the `client_id` and `client_secret` in the payload, then it must be provided in the **Additional Payload** field. The **Additional Payload** field accepts additional body parameters in JSON format.

For more information, see JWT Profile for OAuth 2.0 Access Tokens.

To configure JWT authentication:

1. Enter the **OAuth 2.0 Token URL** for generating access token. This URL is on the PAM solution provider side. Refer to your PAM solution provider system administrator or documentation for information about this URL.
2. In the **JWT Header** field, you can add additional headers in JSON format if required. The header consists of the type of the token (JWT) and the signing algorithm being used. For example:

```
{
     "typ" : "JWT",
     "alg" : "RS256"
}
```

3. Enter the **JWT Issuer** for authorization. The Issuer is the party that issued the JWT. For example: `https://issuer.example.com/`
4. Enter the **JWT Subject** for authorization. The Subject is the user for which the access token is being requested. For example: `145234573`
5. Enter the **JWT Audience**. This is the recipient for which the JWT is intended, and is takes the form of an array of case-sensitive strings, each containing a StringOrURI value.
6. You can add **Additional Payload** details as needed. See above for details about Additional Payload values.
7. Enter the **Private Key** and the corresponding **Private Key Password** to be used to sign the JWT.

Password

The Password grant type is a way to exchange a user's credentials for an access token. Although this type is supported, it is considered less secure than other grant types.

You can use the **Additional Payload** field for systems where authentication may require additional parameters along with mandatory fields.

For example, if the PAM system expects the `client_id` and `client_secret` in the payload, then it must be provided in the **Additional Payload** field. The **Additional Payload** field accepts additional body parameters in JSON format.

For more information see OAuth 2.0 Password Grant.

To configure Password authentication:

1. Enter the **OAuth 2.0 Token URL** for generating access token. This URL is on the PAM solution provider side. Refer to your PAM solution provider system administrator or documentation for information about this URL.
2. Enter the **OAuth 2.0 Username** and the corresponding **Password**.
3. You can add **Additional Payload** details as needed. See above for details about Additional Payload values.

API Token

API tokens allow a user to bypass two-step verification and SSO, in order to authenticate and retrieve data, and requires only an API Token. The token is self-contained and contains all the information it needs for authentication. The token type must be included with the value. For example:

```
Bearer <AUTH TOKEN>
```

For more information see OAuth Access Tokens.

Basic Authentication

Basic Authentication is a simple method for authenticating, requiring only a **Username** and **Password**.

For Basic Authentication, it is a best practice to set up an identity within IdentityIQ specifically for performing this authentication.

PAM Global Configuration Settings

Part of configuring the PAM module is configuring global settings for the module. Global settings include things like how PAM containers can be modified within IdentityIQ, and which business process to use for provisioning PAM identities

To configure PAM's global settings, click the **gear icon > Global Settings > IdentityIQ Configuration** and select the **Privileged Account Management** tab.

Define the following:

Enable adding and removing identities in PAM containers

Allow PAM users to manually add or remove identities on the container details page.

Enable adding and removing privileged items in PAM containers

Allow PAM users to manually add or remove privileged items on the container details page.

Enable owners to modify PAM containers

Allow owners of PAM containers to change or edit their containers.

Enable the creation of PAM containers

Allow PAM users to manually add PAM containers on the Privileged Account Management page.

The maximum number of selectable users in Privileged Account Management

The maximum number of identities you can take action on at one time in the PAM module.

The workflow used to provision identities

The workflow, or business process, that defines the provisioning process for the PAM Module. Business processes are defined and maintained on the Business Process Editor page. See the **Business Processes** documentation for more information.

A rule to filter privileged items that can be added to containers

You can use a rule to add business logic to limit which privileged items can be added to PAM containers. Rules must be of rule type `PrivilegedItemSelector` to be included in the dropdown list. You can also click the **[...]** icon to open the rule editor to create or edit a rule.

Allowing View-Only Access to PAM Containers

To give users view-only access to PAM containers and their data, you can grant the **PAM Viewer** capability to those users.

For details on how to grant capabilities to users, see the **Identity Management** documentation.

Privileged Account Management Tasks: Aggregation, Indexing, and Refresh

Once your PAM applications have been configured to connect to your PAM vendors, and your PAM global settings have been configured, you can aggregate data from your PAM vendor systems. Data is aggregated using tasks. In addition to data aggregation tasks, tasks for indexing effective access and for updating identities should be configured for PAM.

The following tasks are required for the PAM feature, and should be run in this sequence:

- **Account Aggregation** – this task aggregates **PAM accounts** from your PAM vendor. Other than setting the PAM application as the application to scan, there are no other specific options you need to select specifically for PAM; you can choose Account Aggregation Options that suit your business needs.
- **Account Group Aggregation** – this task aggregates **group information** from your PAM vendor. Other than setting the PAM application as the application to scan, there are no other specific options you need to select specifically for PAM; you can choose Account Group Aggregation Options that suit your business needs.
- **Target Aggregation** – this task aggregates **data about PAM vaults and the rights that users** have to those vaults. Configure the task to select your PAM Target Source (that is, the Unstructured Target Collector you configured when setting up your PAM application) as the target source to aggregate.
- **Effective Access Indexing** – this task refreshes the effective access privileges on the PAM containers; that is, container access that is granted by virtue of membership in a group. Check the **Index Entitlement Targets** and **Index unstructured targets** options when running this task for PAM.
- **Identity Refresh** – this task refreshes identities with relevant PAM group and permissions data. For PAM, run this task with the **Refresh Identity Entitlements for all links** selected.

Refer to the IdentityIQ **Tasks** documentation for detailed information on defining tasks.

Adding a PAM Quicklink Card to the Home Page

The Privileged Account Quicklink is added to your Quicklink menu during the installation process, under the **Manage Access** sub-menu.

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.

For more information about Quicklinks and Quicklink cards, see the IdentityIQ **Getting Started** documentation.

Managing Privileged Accounts

To open the Privileged Account Management page, use the Quicklink menu and select **Manage Access > Privileged Account Management**. A Quicklink card can also be enabled on the IdentityIQ home page for quicker access. See Adding a PAM Quicklink Card to the Home Page for details on how to enable this card.

The Privileged Account Management page shows all the PAM containers in your installation. The containers display the following information:

- **Container Name** – the display name aggregated from the privileged account management application
- **Application** – the name of the privileged account management application associated with this container
- **Total Identities** – the total number of identities associated with the container either directly or through a group
- **Privileged Items** – the number of privileged items to which this container grants access, these are usually privileged accounts
- **Groups** – the number of groups associated with the container
- **Owner** – the owner of this privileged account management container. An owner can be an individual or a workgroup. See PAM Container Owners for details about PAM container ownership.

The **Add Container** button lets you manually add containers. See Adding New PAM Containers Manually.

Finding PAM Containers

Use the **Filter** and **Search** options at the top of the page to find specific containers.

Viewing PAM Container Details

You can click **View Details** to see and edit details about identities and items in the container. The ability to view or make changes to this information is controlled using SailPoint rights and capabilities and through the configuration settings. Users with a PAM Administrator capability can edit containers and their contents; users with a PAM Viewer capability can only view containers and their contents. See Container Details.

> 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 and are included in certain Certifications, requests are tracked through the lifecycle manager process, and provisioning transactions are listed in the Administrator Console.

Container Details

Click **View Details** on a container to view and edit its contents.

The page contains three tabs:

Identities

All identities with access to the privileged items, either directly or effectively – Container Details: Identities

Groups

All groups with access to the privileged items – Container Details: Groups

Privileged Items

All the items to which this container provides access – Container Details: Privileged Items

PAM Container Owners

The PAM feature lets you designate owners for your PAM containers. This option allows you to separate the responsibility for the PAM container's *contents* from responsibility for the PAM *application* itself.

In other words, the PAM application owner is the identity or workgroup responsible for the connection to the PAM source; the PAM container owner is responsible for approving changes to the identities or items in a PAM container.

PAM Container Owners and Viewing/Editing Privileges

The PAM feature uses two user rights to control who can view or edit a PAM container. If you plan to use container owners to designate who will manage your containers, be sure that your owners have the correct user rights:

- **PAM Administrator** – the user can view and edit all PAM containers.
- **PAM Viewer** – the user can view all PAM containers, and can edit any container the user is an owner of.

Note that if you designate an identity or workgroup as a PAM container owner, but do not also add the PAM Administrator or PAM Viewer capability to that identity or workgroup, the container owner will not be able to directly manage the container(s) they own.

For details about how approvals are handled for changes to PAM containers, see Approvals for Changes to PAM Containers.

Container Details: Identities

Use this tab to view, add, or remove identities in this container.

The add and remove features are only available if this option was enabled during your PAM configuration. See PAM Global Configuration Settings for more information on these configuration options and Adding and Removing Identities in a PAM Container for details on adding and removing identities.

The **Direct Access** tab shows identities granted direct access to this container (view, add, remove)

The **Effective Access** tab shows identities granted access to this container through group membership (view only)

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 one has been assigned.

Details

View details, permissions granted and the account and application from which they were granted, or **Remove** the identity from the container. For more details, see Adding and Removing Identities in a PAM Container

Container Details: Groups

Use this tab to view detailed information about groups.

Display Name

The display name of the group as aggregated from the PAM 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

Use this tab to view, add, or remove privileged items to which this container grants access. Privileged items are things like accounts, credentials, files, and keys.

The add and remove features are only visible if enabled during your PAM configuration. See PAM Global Configuration Settings for more information on these configuration options, and Adding and Removing Privileged Items in a PAM Container for details on adding and removing items.

Adding New PAM Containers Manually

PAM containers are typically created through aggregation from the PAM vendor application. In addition, system administrators, and other users with the **PAM Administrator** capability, can manually add PAM containers in IdentityIQ.

Some global and application-level settings for PAM determine whether this option is available and how it works:

- The option to add containers must be enabled globally. To enable this option, navigate to the **gear menu > Global Settings > IdentityIQ Configuration > Privileged Account Management** tab, and select **Enable the creation of PAM containers**. See PAM Global Configuration Settings.
- A provisioning policy for creating containers must be defined in the application definition for the PAM application that will be associated with the new container. This policy determines which specific fields need to be defined for a new container when it is added. See Configuring a PAM Application.

To add a PAM container:

1. In the Quicklink menu, click **Manage Access > Privileged Account Management**.
2. Click **Add Container**.
3. Choose the **PAM application** for this container from the dropdown. Note that the drop-down only lists applications of type Privileged Account Management. When you choose the application, additional **Create Container Policy** fields appear for the container, based on the provisioning policy that is set for the application.
4. Enter a **Display Name**, **Description**, and **Owner** for the container.
5. **Create Container Policy** fields; any fields required by the provisioning policy for creating containers will appear and should be completed. This information is used to provision the container in the PAM system, and can also determine how container information is displayed in the Entitlement Catalog. The provisioning policy for creating containers is defined in the application definition. See Configuring a PAM Application.
6. Click **Submit**.

By default, the creation of a new PAM container must be approved by the owner of the PAM application associated with the container. An approval item is created for the application owner and can be accessed through the **Approvals** tile on the approver's home page.

> Note: PAM container creation is handled by a workflow task. To monitor status of this task, use the **gear icon > Administrator Console > Provisioning** tab. You can view the results of this task in either the Administrator Console **Tasks** tab, or in the **Setup > Tasks > Task Results** tab.

Adding and Removing Identities in a PAM Container

System administrators, and other users with the **PAM Administrator** capability, can manually add or remove identities in a PAM container.

Some global settings for PAM determine whether this option is available and how it works. See PAM Global Configuration Settings for more information on these configuration options.

- The option to add or remove identities in a PAM containers must be enabled globally. To enable this option, navigate to the **gear menu > Global Settings > IdentityIQ Configuration > Privileged Account Management** tab, and select the **Enable adding and removing identities in PAM containers** option.
- The approval path for additions or deletions of identities in a PAM container is determined by the business process selected **for The workflow used to provision identities**.

To add or remove identities in a PAM container:

1. In the Quicklink menu, click **Manage Access > Privileged Account Management**.
2. Click **View Details** for the container whose items you want to modify.
3. Click **Add Identities**. Note that you can only add or remove an identity from the Direct Access list; the Effective Access list is view-only.
4. Choose the identities to add. Note that you can only select identities that have an account on the PAM application associated with this container.

   > Note: You can use the **Manage Access** feature in Lifecycle Manager to request that an account be added for a user on the PAM application, if one does not exist. See the **Lifecycle Manager** documentation for more information.

5. Click **Next.**
6. Select permissions for these users on this container. You may be prompted to select an account, if the user has more than one account on the application.
7. Click **Submit** to begin the approval/provisioning process.

8. To remove identities, click the **Remove** button beside the identity, and confirm the deletion. You select multiple identities and click **Bulk Remove** to remove multiple identities at once.

   > Note: Any approvals that are required by the business process for identity provisioning in PAM must be completed, as part of the addition or removal process.

For details about approval paths and notifications for changes to PAM containers, see Approvals for Changes to PAM Containers and Notifications About Changes to PAM Containers.

Adding and Removing Privileged Items in a PAM Container

Although you cannot create new privileged items directly in IdentityIQ, any privileged items that have been aggregated from your PAM vendor(s) can be manually added to PAM containers.

The option to add privileged items to containers must be enabled globally. To enable this option, navigate to the **gear menu > Global Settings > IdentityIQ Configuration > Privileged Account Management** tab, and select the **Enable adding and removing privileged items in PAM containers** option. With this option enabled, users can also remove privileged items from containers. See PAM Global Configuration Settings.

To add or remove items in a PAM container:

1. In the Quicklink menu, click **Manage Access > Privileged Account Management**.
2. Click **View Details** for the container whose items you want to modify.
3. Click the **Privileged Items** tab.
4. Click **Add Privileged** Items.
5. Select the items to add from the dropdown. You can select more than one item before you submit the change, but items are selected one at a time.

   > Note: Be sure to select *all* the items you want to add before submitting the request, because once the request has been submitted, the resulting business process must be completed before you can add more items to this container.

6. Click **Submit**.
7. To remove an item from the container, click the **Remove** button beside the item, and confirm the deletion. You can select multiple items and remove them in bulk using **Bulk Remove**.

By default, changes to items in a PAM container must be approved by the owner of the PAM container. If there is no owner set for the container, approvals go to the owner of the PAM application associated with the container. Approvals are accessed through the **Approvals** tile on the approver's home page.

Once the addition or removal of items has been approved, these new associations between the items and the container are provisioned to the PAM application, according to the provisioning policies that are defined in the application definition for the application. See Configuring a PAM Application.

> Note: The addition of items to a PAM container is handled by a workflow task. To monitor status of this task, use the **gear icon > Administrator Console > Provisioning** tab. You can view the results of this task in either the Administrator Console **Tasks** tab, or in the **Setup > Tasks > Task Results** tab.

For details about approval paths and notifications for changes to PAM containers, see Approvals for Changes to PAM Containers and Notifications About Changes to PAM Containers.

Approvals for Changes to PAM Containers

Changes to PAM containers follow an approval path that is defined by a business process. The approval process varies, depending on what is being changed in the PAM container: *identities*, or *items*.

Approvals for Changes to Identities in a PAM Container

The business process for managing PAM container approvals is set in **gear > Global Settings > IdentityIQ Configuration** on the **Privileged Account Management** tab. By default, IdentityIQ uses the out-of-the-box **PAM Identity Provisioning** business process for these approvals.

The PAM Identity Provisioning business process routes approvals for changes to identities in a PAM container to the identity's manager. This behavior can be changed by modifying the `approvalScheme` variable in the business process.

The business process can specify a single value for the approver, or can specify several values in a comma-separated list. If multiple values are provided, the order in which they are listed in the comma-separated list determines the order in which they are processed.

Approver options include:

- Manager – the identity's manager gets the approval item
- None – approvals are disabled
- Identity – the identities/workgroups in the variable `approvingIdentities` get the approval item.

- Owner – the owner of the container gets the approval item. If the container has no owner, then the application owner gets the approval item.

Electronic Signatures

The PAM Identity Provisioning business process supports the use of electronic signatures for approvals. Use these process variables in the business process to specify electronic signature objects, as needed:

- `managerElectronicSignature`
- `identityElectronicSignature`
- `ownerElectronicSignature`

Approvals for Changes to Items in a PAM Container

Approvals for changes to the items in a PAM container are managed by the **Entitlement Update** business process. If an owner is defined for a PAM Container, by default approvals for changes to the items in a container will go to the container's owner. If no owner is defined for a container, approvals will go to the owner of the application associated with the container.

Container owners can be aggregated from the PAM application and can also be manually added to a container through the Entitlement Catalog.

For more information about the Entitlement Catalog, see the *IdentityIQ Application Management Guide*.

For more information about configuring the PAM application, see Configuring a PAM Application. For more information on aggregating PAM data, see Privileged Account Management Tasks: Aggregation, Indexing, and Refresh.

Fallback Approvers for Changes to a PAM Container

You can also set a **fallback approver** for both the PAM Identity Provisioning business process and the Entitlement Update business process. A fallback approver is an identity or workgroup that will handle approvals in cases where the designated approver can not be resolved. For example, if the business process specifies "manager" as the approver, but an identity does not have an assigned manager, a fallback approver (if one has been set) will handle approvals for that identity.

Notifications About Changes to PAM Containers

The approval business process that governs changes to PAM containers can call another business process to define how notifications about changes and approvals are handled.

By default, IdentityIQ uses the out-of-the-box **PAM Identity Provisioning Notify** business process to handle notifications. This notification business process is called by the approval business process; there is no UI option (apart from the business process UI itself) for choosing a business process for handling notifications.

The business process that handles notifications about changes to PAM containers includes a string that specifies who should be notified when a change request has been completed.

The value of this string can be null, or it can be a comma-separated list of one or more of the following options:

- None or null – disable notifications, meaning no notifications are sent
- User – the Identity that is being updated will be notified
- Manager – the manager of the Identity that is being updated will be notified
- Requester – the person that has requested the update will be notified
- Owner – the owner of the container will be notified

PAM Notification Templates

The PAM module provides several out-of-the-box notification templates to use for PAM notifications. The **PAM Identity Provisioning Notify** business process specifies which of these notification templates to use for which type of user (manager, requester, etc.). The templates can be viewed and edited in the Debug pages by choosing **EmailTemplate** in the object browser. To more easily locate the PAM notification templates, filter the template list using the term "PAM."

Using Rapid Setup Joiner and Leaver Processes for PAM Users

You can use Rapid Setup to manage joiner and leaver processes for PAM applications, in the same manner as for any other application. If you want to use Rapid Setup with your PAM applications, you can configure Rapid Setup to run additional functions that are specific to PAM, such as deleting containers via a rule.

A set of sample Rapid Setup rules is included with Rapid Setup. Sample Rapid Setup rules are in the `rsexamplerules.xml` file, which is located in your IdentityIQ installation directory under `<identityiq_home>\WEB-INF\config\rapidsetup`.

For information on how to import files into IdentityIQ, see the **System Configuration** documentation.

The sample rules include examples of rule logic for performing PAM-specific actions, such as deleting containers. Once imported, the rule must be modified to reference the correct PAM applications and associated PAM containers. Then the rule can be selected as part of your Rapid Setup global configuration. See PAM Global Configuration Settings.

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

This section gives an overview of the process for configuring credential cycling. More detailed information about template configuration is provided in Solution-Specific Configuration Details.

> Note: To enable credential cycling, BeyondTrust PowerBroker Password Safe application passwords must be configured in the JSON format:
> `{"bt_user":"MyUserName","bt_password":"MyPasswordValue"}`

Prerequisites for Credential Cycling

- Install and configure the PAM Module. See Activating the Privileged Account Management Module.

- Define a PAM application in IdentityIQ. See Configuring a PAM Application.

Edit and Import the Configuration Template

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

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

The file is fully commented to provide guidance as you insert your configuration settings.

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

The basic steps you will follow for using the configuration template are:

- Edit your copy of the template to add information about which of your applications will use credential cycling
- Import the edited template file into IdentityIQ using **Gear icon > Global Configuration > Import File**
- Importing the file creates a new configuration object in IdentityIQ: **Credential Configuration**

Modifying Your Credential Cycling Configuration

If you need to update your credential cycling configuration, you can modify and reimport the credential configuration template, or you can edit the **Credential Configuration** object directly in the Debug pages. Choose Configuration in the Debug page's *Select an object* list box, to find **Credential Configuration** in the list of objects.

Solution-Specific Configuration Details

See these sections for solution-specific guidance on the configuration template:

- BeyondTrust Credential Cycling Configuration
- CyberArk Credential Cycling Configuration
- Direct Mapping Credential Cycling Configuration

BeyondTrust Credential Cycling Configuration

This section provides details on configuring credential cycling for use with BeyondTrust.

Note that to enable credential cycling with the BeyondTrust PowerBroker Password Safe application, passwords must be configured in the JSON format. For example:

```
{"bt_user":"MyUserName","bt_password":"MyPasswordValue"}
```

In the **Credential Source** section, you configure:

- The URL to your BeyondTrust source
- The "run as" user for authenticating to your source
- An API key for authentication
- Your BeyondTrust Managed System and Managed Account names. In the Credential Source section, you set values for your overall BeyondTrust implementation.

> Note: If specific applications will use different or unique Managed Systems or Managed Accounts, you can set values for those that are specific to particular applications in the Credential Association section. Values set in the Credential Source section are

> overridden by values of the same name in the Attributes map of each Credential Association.

In the **Credential Association** section, you configure:

- The name(s) of your IdentityIQ applications that will use credential cycling
- The attributes for your application's username and password, and the corresponding BeyondTrust username and password that provides the secure credential to the application at runtime.
- Any application-specific overrides to the overall BeyondTrust Managed System or Managed Account names

```
<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/publ-
ic/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="bt_user">
                  <!-- *** 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_man-
aged_account_name"/>
                    </Map>
                  </Attributes>
                </CredentialAssociation>
                <CredentialAssociation applicationName="application_name"
                                       attributeName="application_password_attribute"
                                       credentialAttributeName="bt_password"/>
              </CredentialSource>
```

CyberArk Credential Cycling Configuration

This section provides details on configuring credential cycling for use with CyberArk.

Prerequisites for CyberArk Credential Cycling

These prerequisites are specific to CyberArk, and are in addition to the general prerequisites for credential cycling outlined in Credential Cycling Configuration.

- Install CyberArk's **Credential Provider API** on the server hosting your IdentityIQ instance. The Credential Provider API enables passwords that are stored in CyberArk Digital Vaults to be retrieved by IdentityIQ.

  If you are using multiple hosts, install the Credential Provider API on all of your **task hosts**. If you are using **UI hosts** for actions such as test connections, previewing account information, running targeted aggregations, managing accounts, processing access requests, or business processes configured to run in the foreground, the Credential Provider API must be installed on those hosts as well.

  Note that the Credential Provider API is **not** the same as CyberArk's **Central** Credential Provider.

  For version 8.4 of IdentityIQ, use version 9.8 of all CyberArk components.

- **JavaPasswordSDK.jar**: IdentityIQ distributes a version of the JavaPasswordSDK.jar for the CyberArk integration. This jar contains several classes that allow IdentityIQ to communicate with the CyberArk's Credential Provider.

  CyberArk customers should confirm the appropriate version of the library for their version of CyberArk, and obtain it from the vendor if necessary.

- Obtain **application IDs**, corresponding **safe** names, and **folder** names from your CyberArk administrator.

Application Hash Value Authentication for CyberArk

IdentityIQ uses the "Application Hash Value" method of authenticating to the CyberArk API; other methods of authentication will not work.

Verify connectivity to the CyberArk Digital Vault using the command line `clipasswordsdk` before attempting to construct the attributes of the Credential Cycling Configuration object.

How to generate a hash to add to the application if the SCIM server is not installed on the IdentityIQ server

> Note: For more information, refer to CyberArk's Credential Provider documentation and ASCP Implementation Guide.

First, ensure that you have extracted the **pam-credential.jar** file from the **identityiq.war** file.

If you have deployed IdentityIQ using the "exploded" form of the war file, you don't need to take any extra steps to extract the **pam-credential.jar** file; however, if you are not using this deployment strategy, you will have to extract the **pam-credential.jar** from the **identityiq.war** file, perform the steps below, then repackage the **pam-credential.jar** back into the **identityiq.war** file.

1. Run the CyberArk utility **JavaAIMGetAppInfo** (under `\CyberArk\ApplicationPasswordProvider\Utils`):

   (Unix) `java -jar javaaimgetappinfo.jar GetHash -AppExecutablesPattern=/{path to identityiq directory}/WEB-INF/lib/pam-credential.jar`

   (Windows) `java -jar JavaAIMGetAppInfo.jar GetHash /AppExecutablesPattern=C:\{path to identityiq directory}\WEB-INF\lib\pam-credential.jar`

2. Copy the generated hash to the vault:

   a. Log in to the CyberArk Web Application.

   b. Navigate to Applications > SailpointIIQ > Authentication > Add Hash and paste the generated hash.

3. Restart the CyberArk Privileged Session Managers service to make the configuration change to take place immediately. Alternatively you can wait approximately 3 minutes to allow the CyberArk Privileged Session Manager to read the new configuration.

Working with the CyberArk Configuration Template

IdentityIQ provides a template to use as a guide for creating your CyberArk configuration. The template defines:

- Which of your applications in IdentityIQ will use credential cycling.
- The CyberArk source values to use for credentials.
- How these source values map to your IdentityIQ application fields for authentication.

In the **Credential Source** section, you configure:

- The name of your CyberArk **safe**. This information comes from CyberArk.
- The **folder** where your secure credentials are stored. This information comes from CyberArk. Use "root" here if you do not use folders.
- An **appId**, which is a unique identifier, used for authorization, which the CyberArk Credential Provider creates when it is installed on a host. This information comes from CyberArk.

> Note: These values can also be added in the Credential Association section, and settings in the Credential Association section will override values in the Credential Source section. Configuring applications in the Credential Association section is useful if you need to define multiple applications in the configuration file. See the CyberArk Configuration Template - Configured Example section below for an example of this type of structure.

In the **Credential Association** section, you configure

- The name(s) of your IdentityIQ **applications** that will use credential cycling.
- The attributes for your application's **username**, and the corresponding CyberArk username that provides the secure username credential to the application at runtime.
- The attributes for your application's **password**, and the corresponding CyberArk password that provides the secure password to use for the application at runtime.
- A CyberArk **object**, which is the name identifier for the password or certificate data object in the CyberArk container.
- Any application-specific overrides to the overall CyberArk settings.

CyberArk Configuration Template - Defaults

> Note: The template provided with IdentityIQ includes individual sections for CyberArk, BeyondTrust, and a solution-neutral mapping option. Remove the sections that you will not use before importing the template.

```
?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE sailpoint PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<sailpoint>
  <Configuration name="CredentialConfiguration">
    <Attributes>
      <Map>
        <entry key="sources">
          <value>
            <List>
<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>
           </List>
          </value>
        </entry>
      </Map>
    </Attributes>
  </Configuration>
    </sailpoint>

```

CyberArk Configuration Template - Configured Example

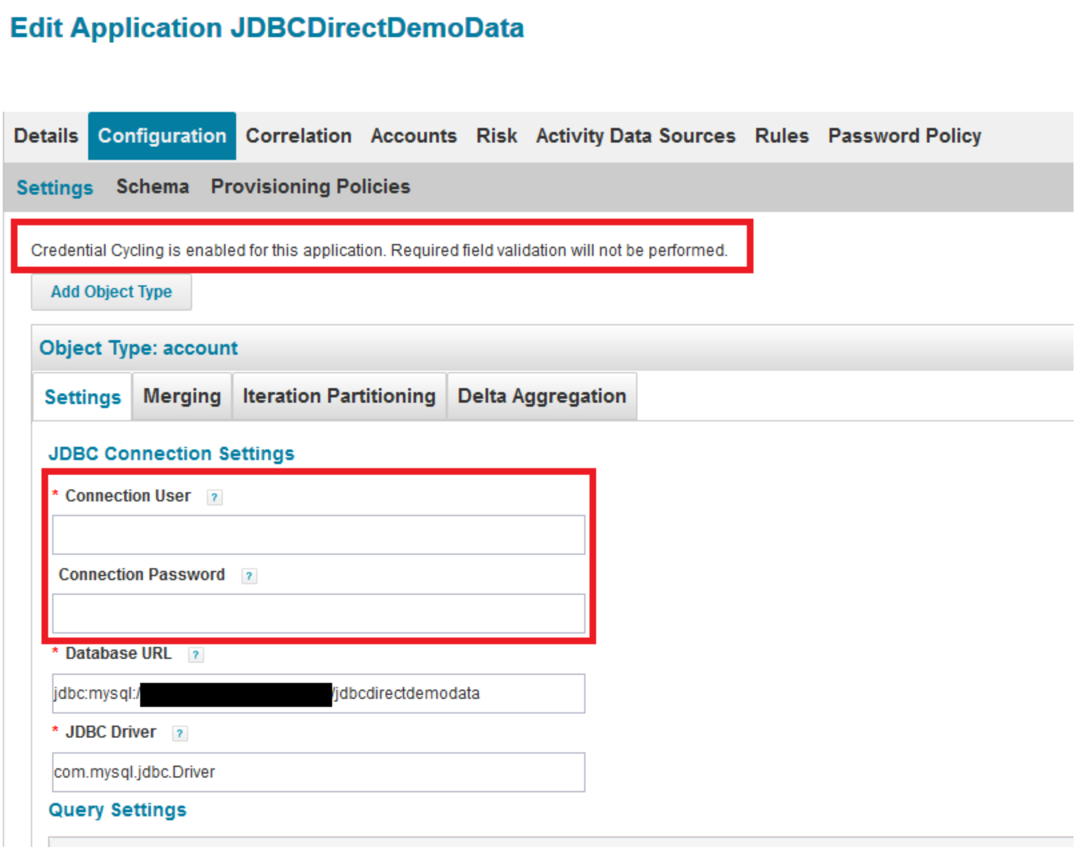
Note that this example includes only the CyberArk-specific elements in the template. See the example above or the configuration template supplied with IdentityIQ for additional elements required in the template.

In this example, application details are specified in the `CredentialAssociation` element. The values are defined as follows:

- **JDBCDirectDemoData** is the application in IdentityIQ that will use credential cycling.
- **SailPointIdentityIQ** is the unique application identifier in CyberArk for this IdentityIQ instance.
- **Demodata** is the specific safe within CyberArk which contains credentials for the JDBCDirectDemoData system.
- **Database-MySQL-JDBCDirDemoData** represents the collection of attributes in CyberArk which store password and user name information for the JDBCDirectDemoData application.
- The **user** `attributeName` key is the attribute in the JDBCDirectDemoData application in IdentityIQ that holds the username for connecting to the JDBCDirectDemoData system. The **PassProps.Username** `credentialAttributeName` key is the corresponding attribute in CyberArk which holds the username credential, which will be passed to the IdentityIQ **user** attribute.
- The **password** `attributeName` key is the attribute in the JDBCDirectDemoData application in IdentityIQ that contains the password for connecting to the JDBCDirectDemoData system. The **Password** `credentialAttributeName` key is the corresponding attribute in CyberArk which holds the password credential, which will be passed to the IdentityIQ **password** attribute.

```
<CredentialSource credentialClass="sailpoint.pam.credential.CyberArkCredentialManager"
name="cyberark">
              <CredentialAssociation applicationName="JDBCDirectDemoData" attrib-
uteName="password" credentialAttributeName="Password">
                <Attributes>
                  <Map>
                    <entry key="appId" value="SailpointIdentityIQ"/>
                    <entry key="folder" value="root"/>
                    <entry key="object" value="Database-MySQL-JDBCDirDemoData"/>
                    <entry key="safe" value="Demodata"/>
                  </Map>
                </Attributes>
              </CredentialAssociation>
              <CredentialAssociation applicationName="JDBCDirectDemoData" attributeName="user" credentialAttributeName="PassProps.Username">
                <Attributes>
                  <Map>
                    <entry key="appId" value="SailpointIdentityIQ"/>
                    <entry key="folder" value="root"/>
                    <entry key="object" value="Database-MySQL-JDBCDirDemoData"/>
                    <entry key="safe" value="Demodata"/>
                  </Map>
                </Attributes>
              </CredentialAssociation>
    </CredentialSource>
```

Here is how credential cycling, as configured using the template above, will appear in IdentityIQ in the **JDBCDirectDemoData** application. The message indicates that the **Connection User** and **Connection Password**, which are marked with asterisks indicating that they are required, do not need to be supplied here because they will be provided through credential cycling.



Edit Application JDBCDirectDemoData

Credential Cycling is enabled for this application. Required field validation will not be performed.

Object Type: account

JDBC Connection Settings

* Connection User ?

Connection Password ?

* Database URL ?

jdbc:mysql:/[redacted]/jdbcdirectdemodata

* JDBC Driver ?

com.mysql.jdbc.Driver

Query Settings

Configuring Multiple Applications in the CyberArk Configuration Template

A single configuration template is used to configure all applications that will use CyberArk credential cycling.

To configure multiple applications in the template, use Credential Associations elements to define each of them. See the CyberArk Configuration Template - Configured Example section above for an example.

Special Considerations for Active Directory

A special syntax is used to replace Active Directory Application attributes when using credential cycling. The feature uses SailPoint's MapUtil API. Here is an example:

```
<CredentialSource credentialClass="sailpoint.pam.credential.CyberArkCredentialManager"
name="cyberark">
 <Attributes>
  <Map>
   <entry key="appId" value="CyberArk"/>
   <entry key="folder" value="root"/>
   <entry key="object" value="ActiveDirectory"/>
   <entry key="safe" value="MicrosoftSafe"/>
  </Map>
 </Attributes>
   <CredentialAssociation applicationName="ActiveDirectory" attributeName="domainSettings
```

```
[domainNetBiosName=DOMAINNAME].password" credentialAttributeName="password"/>
</CredentialSource>

```

Additional Resources

Video: IdentityIQ CyberArk Integration Demo

Direct Mapping Credential Cycling Configuration

Use this section of the template for solution-neutral direct attribute mapping. Be sure to remove the CyberArk and BeyondTrust sections of the template.

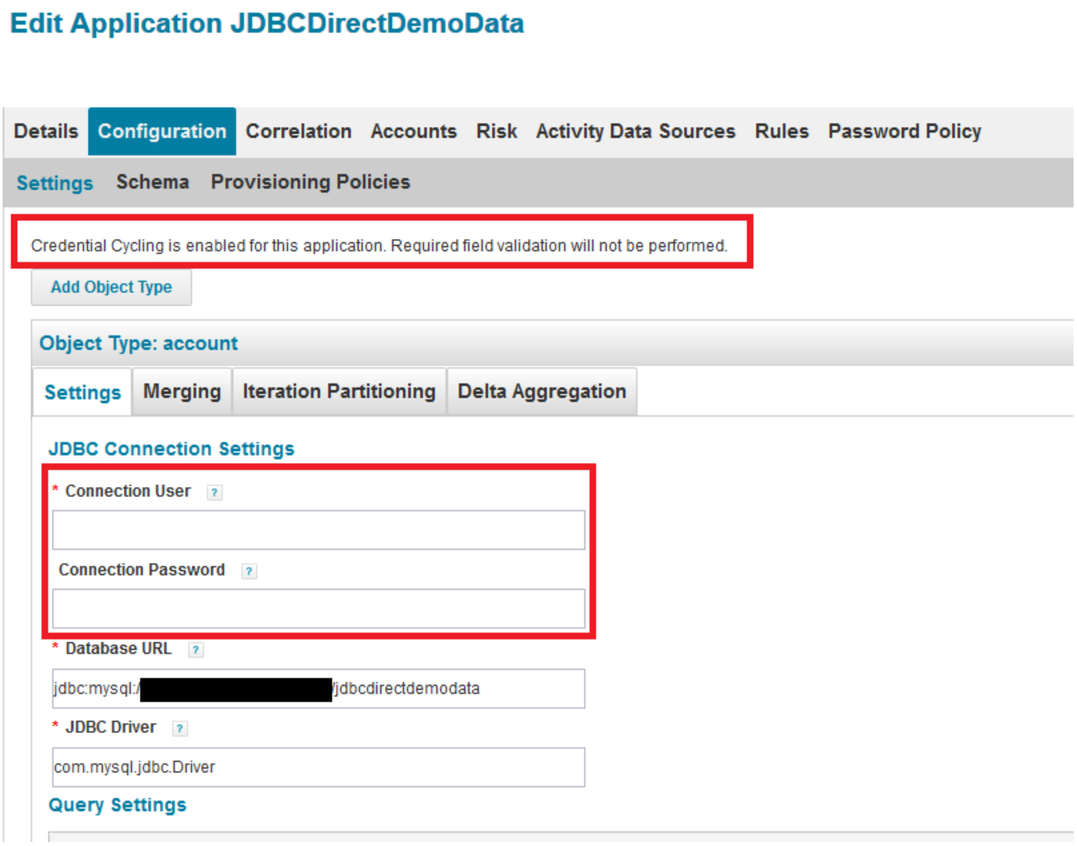
In the **Credential Source** section, you configure your actual credential values, since you are not connecting to a third-party PAM source. It is a good practice to use encrypted passwords in this section.

The **Credential Associations** settings connect the values in the Credential Source section to your applications as shown in the template XML below.

```
<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 (in this example, **Connection User** and **Connection Password**) 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.



Credential Cycling is enabled for this application. Required field validation will not be performed.

* Connection User

Connection Password

* Database URL

jdbc:mysql:/[redacted]/jdbcdirectdemodata

* JDBC Driver

com.mysql.jdbc.Driver