BeyondTrust

BeyondInsight and Password Safe Third-Party Integration Guide

TC:4/10/2024

Table of Contents

BeyondInsight and Password Safe Third-Party Integration Guide

The BeyondInsight management console enables teams to centrally manage organization-wide IT security and compliance initiatives from a single, web-based console. It provides discovery, prioritization, and remediation of security risks by delivering what matters the most – context.

This document details the complementary technologies that BeyondInsight offers to an existing infrastructure. It highlights a critical step in the process for user and asset security events to be escalated into any third-party solution.

Configure Exabeam Event Forwarding

Create a connector to send all selected event data in Common Event Format (CEF) format to the Exabeam server.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Exabeam Event Forwarding** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Provide the required details for the Exabeam server:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter the **Host Name** and **Port**.
8. Expand **Event Filters**, and then select the events you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.

Note: *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

Configure FireEye TAP Cloud Collector

The FireEye® Threat Analytics Platform (TAP) generates events securely using the cloud connector. Create the FireEye connector to send BeyondInsight events to the FireEye TAP server.

Note: *You need a* ***FireEye Comm Broker Sender*** *installed and available to BeyondInsight.*

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **FireEye TAP Cloud Collector** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Provide the required details for your **FireEye Comm Broker Sender**:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter **Host Name** and **Port**.
8. Expand **Event Filters**, and then select the events that you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.

Note: *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

For more information, please see your FireEye documentation or contact the vendor to ensure the proper installation of the ***Comm Broker Sender****.*

Configure HP ArcSight Event Forwarding

HP ArcSight™ is a security management application that combines event correlation and security analytics to identify and prioritize threats. A dedicated ArcSight connector using CEF format is available in BeyondInsight.

> ***Note:*** *Use the connector over Syslog.*

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **HP ArcSight Event Forwarding** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Provide the required details for your ArcSight server:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter **Host Name** and **Port**.
8. Expand **Event Filters**, and then select the events that you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.

> ***Note:*** *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

Configure IBM QRadar Connector

IBM QRadar® is a security intelligence platform that provides a unified architecture for integrating security information and event management solutions. Create a QRadar connector to send selected event data in QRadar LEEF format.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **IBM QRadar** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Provide the required details for the IBM QRadar server:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter **Host Name** and **Port**.
8. Select the formatter from the dropdown list.
    - **LEEF Format V1** uses a static identifier per event type.
    - **LEEF Format V2** uses a unique event identifier generated per event type.
9. If you selected **LEEF Format V2** in the previous step, select the **Facility** from the dropdown list. This option is not available for **LEEF Format V1**.
10. Expand **Event Filters**, and then select the events that you want to forward.
11. Click **Test Connector** to send a test event message.
12. Click **Create Connector**.

> ***Note:*** *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

> ***Note:*** *Unique identifiers are preset, but can be customized if desired, using a setting in the BeyondInsight database table:*
>
> ***dbo.ConfigurationItem BeyondTrust.Configuration.ProductConfigurations.LeefFormatterConfig***

Password Safe QRadar Fields

Field	Value Type	Description
Category	String	System/Change
EventName	String	System / Functional / Managed / Change
LogID	Integer	PMMLogSystem/PMMLogChange table reference ID
LogTime	DateTime	Time of event

Field	Value Type	Description
Details	String	Miscellaneous additional information
UserName	String	Username associated with the event
RoleUsed	String	Role used
ObjectTypeID	Integer	Object Type reference ID
ObjectType	String	Object Type (e.g. Functional Account, System, Session)
ObjectID	Integer	Object reference ID
Operation	String	Operation (e.g.. Add, Update, Approve)
Failed	Boolean	True / False
Target	String	Describes the asset acted upon (e.g. Asset:testasset Account:testaccount)
UserID	Integer	User ID associated with the event
IPAddress	String	IP address of the system
ManagedAccountID	Integer	Managed Account reference ID
FunctionalAccountID	Integer	Functional Account reference ID
ManagedSystemID	Integer	Managed System reference ID
ChangeDt	DateTime	Time of password change

Field	Value Type	Description
ChangeReasonCd	String	Reason for password change: **A** = Password change by API **F** = Forced password reset **M** = Password reset on mismatch **N** = Manual password entry for new account **O** = Initial onboarding via smart rule **P** = Change by EPM agent **R** = Post release password reset **S** = Scheduled password change **T** = Ticket approval release password reset **U** = Manual password entry **V** = Approval release password reset **X** = Synced password with primary **Y** = Un-synced password from primary **Z** = Forced password sync with primary
Result	String	Password change result: (S)uccess or (F)ailed
Comment	String	Miscellaneous additional information
ReleaseID	Integer	Password release reference ID
RequestID	Integer	Request reference ID
WorkgroupID	Integer	Workgroup reference ID
Workgroup	String	Workgroup name
AccountName	String	Account name
NextChangeDate	DateTime	Next scheduled change date
ElevationCommand	String	Elevation command used, if any

Configure Local Event Log Forwarding

BeyondInsight can duplicate stored events within the **Windows Application Log**. This setting is available in the console on the **Connectors** page. It allows BeyondTrust Discovery Scanner events with user-defined filters to be duplicated in the log so that a log monitoring or scraper tool can perform monitoring for critical events.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Local Event Log Forwarder** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Expand **Event Filters**, and then select the events that you want to forward.
8. Click **Create Connector**.

Configure LogRhythm Event Forwarding

Create a LogRhythm® connector to forward BeyondInsight events to the LogRhythm server.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **LogRhythm Event Forwarding** from the **Connector Type** list.
5. Provide a connector name.
6. Leave **Active (yes)** enabled.
7. Provide the required details for the LogRhythm server:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter the **Host Name** and **Port**.
    - Select an optional syslog facility from the list.
8. Expand **Event Filters**, and then select the events you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.

Note: *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

Configure Trellix DXL Event Forwarding

The communication between BeyondInsight and the Trellix Data Exchange Layer (DXL) is managed by the BeyondTrust DXL Broker Service. This service is installed as an additional component to the main BeyondInsight installation and facilitates the brokering of events from BeyondInsight to the DXL fabric. Along with this service, the BeyondInsight instance must have a Trellix Agent and DXL Client installed to communicate with your Trellix DXL Broker instance. Within your Trellix ePO instance, you will need to ensure that the Trellix Agent and DXL Client installed on the BeyondInsight instance are configured for proper communication between BeyondInsight and ePO via the DXL fabric.

Installation and Configuration Overview

1. Install the Trellix Agent 5.5. on the BeyondInsight instance.
2. On the Trellix ePO instance:
    - Deploy the DXL Client to the BeyondInsight instance.
    - Configure the BeyondInsight event topics.
3. On the BeyondInsight instance:
    - Verify the Trellix Agent and DXL Client connectivity.
    - Install the BeyondInsight DXL Broker service.
    - Configure a Trellix Event Forwarding connector within the BeyondInsight management console.
    - Verify the installation and configuration.

Install the Trellix Agent

On the BeyondInsight instance, follow the steps below to install the Trellix Agent.

> ***Note:*** *If you cannot push the Trellix Agent from the ePO admin console due to firewall or other restrictions, you can install the agent manually by copying the installer to the BeyondInsight instance and then manually running the installer.*

1. Locate and run the Trellix Agent installer on the BeyondInsight instance. You must use the installer specific to your Trellix ePO instance. For example, it may be located at:

    C:\Program Files (x86)\Trellix\ePolicy Orchestrator\DB\Software\Current\EPOAGENT3000\Install\0409\FramePkg.exe

2. Copy the **FramePkg.exe** file to the BeyondInsight instance and run the installer.
3. Verify the installation by looking at the system tray for the Trellix icon.

Deploy the DXL Client to the BeyondInsight Instance

1. On the Trellix ePO instance, deploy the a DXL Client to the BeyondInsight instance using a **Client Task** from within the ePO administration console.
2. Create a **DXL Client Task**.
3. Select **Menu** > **Client Task Catalog**.

4. Under **Trellix Agent > Product Deployment**, click **New Task** and then select the following:
    - **Task Name:** Deploy DXL Client
    - **Target Platforms:** Check Windows
    - **Products and components:** Data Exchange Layer Client 4.0+, action=Install, ...
5. Click **Save**.
6. Deploy the DXL Client to the BeyondInsight instance.
7. Select **Menu > Systems > Locate**.
8. Find the BeyondInsight instance to view the server's detail page.
9. From the **Actions** list, select **Agent > Run Client Task Now**.
10. Locate the **Deploy DXL Client** task created above.
11. Select **Trellix Agent > Product Deployment > Deploy DXL Client**.
12. Click **Run Task Now**.

Configure the BeyondInsight Event Topics

On the Trellix ePO instance, create topic subscriptions for the BeyondInsight categories you wish to receive.

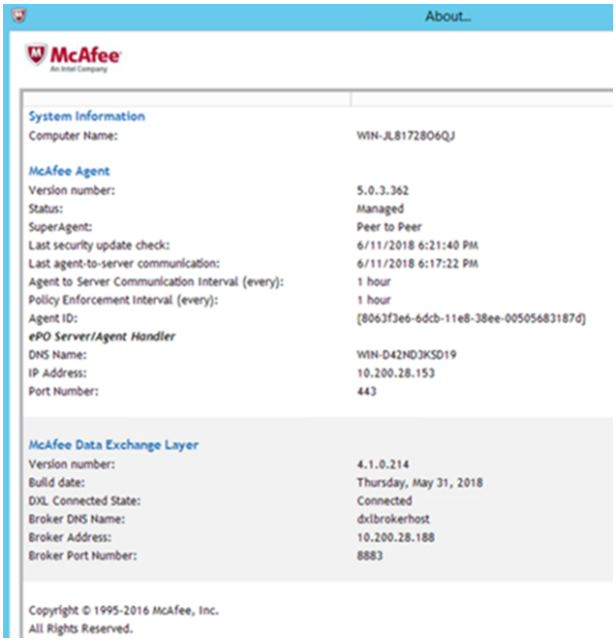
Open the ePO administration console, and then navigate to the **SIA DXL Task** and to the BeyondInsight topics of interest:

Appliance Health	/beyondtrust/event/beyondinsight/genapphlth
Clarity	/beyondtrust/event/beyondinsight/clarity_mlwr
File Integrity Monitoring	/beyondtrust/event/beyondinsight/fim
PBMac	/beyondtrust/event/beyondinsight/pbmac
PBPS	/beyondtrust/event/beyondinsight/pbps
PBW - Events	/beyondtrust/event/beyondinsight/pbw
PBW - Vulnerabilities	/beyondtrust/event/beyondinsight/pbw_vulnerability
Retina	/beyondtrust/event/beyondinsight/retina
Uncategorized Events	/beyondtrust/event/beyondinsight/uncategorized
Test Events	/beyondtrust/event/beyondinsight/test

Verify the Trellix Agent and DXL Client Connectivity

After the MacAfee Agent and DXL Clients are successfully installed, verify the connectivity on the BeyondInsight server by opening the system tray Trellix icon **About** section. It should list the Trellix Agent as running and connected and the DXL Client as running and connected.

> ***Note:*** *The DXL Client might not be in a connected state until BeyondInsight DXL Broker service is installed and running.*



Run the BeyondInsight DXL Broker Service Installer

1. Run the **BeyondInsightDXLMessageBroker.msi** installer from an elevated command prompt and go through the installation steps. Admin privileges are required to enable the MSMQ Windows feature.
2. An MSMQ Windows feature is enabled with a default DXL events (outbound) queue. This can be managed in the following location: **Computer > Manage > Services and Applications > Message Queue**.

> ***Note:*** *By default this queue is not accessible by the admin. In order to manage this queue, refer to the steps below.*

3. The installer deploys the BeyondInsight DXL Broker service, along with the service configuration, logs, and utilities to the following location: **C:\Program Files\BeyondInsight\DXL Broker Service**.
4. To view and manage the private queues, an admin user might need to do the following:
    - Take ownership of the queue through **Properties > Security > Advanced button > Owner**.
    - Change the owner to an admin user.
    - Add the admin user to **Users and Groups** for the queue and assign full control access.
    - Ensure that the Trellix system tray indicates that the DXL Client is connected.

Create the BeyondInsight DXL Event Forwarding Connector

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Trellix DXL Event Forwarding** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Expand **Event Filters**, and then select event types to forward.
8. Click **Test Connector** to send a test event message. Within ePO, verify that the **Test** topic has received the test event message.
9. Click **Create Connector**.

For more information, please see "Configure the BeyondInsight Event Topics" on page 13.

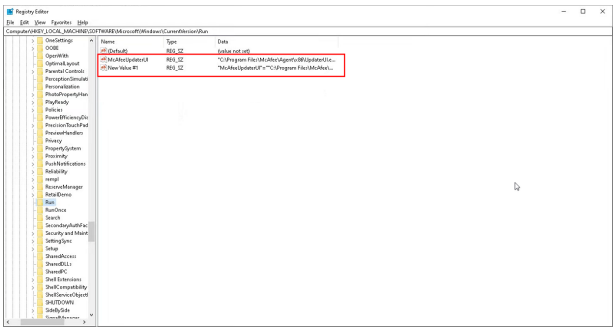
Troubleshoot Issues with Trellix DXL Connector

The Trellix Agent or DXL Client Not Showing as Connected

After installing the Trellix Agent and DXL Client, a machine reboot might be required to register the new software.

The Trellix Agent Icon Not Appearing in the System Tray

1. Open the Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run**.
3. Delete the **TrellixUpdaterUI** entry.
4. Create a new value named **TrellixUpdaterUI** with value of **C:\Program Files\Trellix\Agent\x86\UpdaterUI.exe /StartedFromRunKey**.
5. Restart the machine. The Trellix icon is displayed in the system tray.



The BeyondTrustDXLMessageBroker Installer Fails

To debug installer issues, you can execute the installer with the following command:

```
<path to your installer>\msiexec /i BeyondInsightDXLMessageBroker.msi /l*v MyLogFile.txt
```

A 1603 Error Code often indicates that the installer is not being executed with sufficient privileges to enable the MSMQ Windows feature.

The BeyondTrust DXL Message Broker Service Cannot be Restarted or Removed

If necessary, to forcibly remove a stuck service (and subsequently re-install the service), use the following command:

```
sc delete BeyondInsightDXLMessageBroker
```

Location of Log Files

- BeyondInsight Message Broker logs are located here by default:

  C:\Program Files\BeyondTrust\DXL Message Broker\Logs

- Trellix Agent and DXL Client logs are located here by default:

  C:\ProgramData\Trellix\Agent\logs

  C:\ProgramData\Trellix\Data_Exchange_Layer

Configure Trellix Syslog Event Forwarding

Trellix® Enterprise Security Manager (ESM) is the foundation of the Trellix® security information and event management solution (SIEM). You can create a connector to forward all data types to Trellix® Enterprise Security Manager.

You must configure your Trellix® SIEM Solution to receive Syslog data sources.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Trellix Syslog Event Forwarding** from the **Connector Type** list.
5. Click **Create Connector**.
6. Leave **Active (yes)** enabled.
7. Select an optional syslog facility from the list.
8. Provide the required details for the available output pipelines for the Trellix Syslog data source:
    - Select the protocol: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter **Host Name** and **Port**.
9. Select an output format: **NewLine Delimited**, **Tab Delimited**, or **Comma Delimited**.
10. Expand **Event Filters**, and then select the events you want to forward.
11. Click **Test Connector** to send a test event message.
12. Click **Create Connector**.

For more information, please see the Trellix documentation for configuring a Syslog data source to SIEM solution.

Configure Open Text NetIQ Sentinel Event Forwarding

Create a NetIQ connector to forward BeyondInsight events to the Open Text NetIQ® Sentinel™ server in the LEEF format.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **NetIQ Sentinel Event Forwarding** from the **Connector Type** list.
5. Provide a connector name.
6. Leave **Active (yes)** enabled.
7. Provide the required details for the Sentinel server:
    - Select the protocol from the **Available Output Pipelines** list: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter the **Host Name** and **Port**.
    - Select an optional syslog facility from the list.
8. Click **Test Connector** to send a test event message.
9. Click **Create Connector**.

Note: *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

SailPoint IdentityIQ Deployment Guide

Overview

The SailPoint IdentityIQ Deployment Guide outlines how to use a SailPoint IdentityIQ Privileged Access Management (PAM) application template. This quick start strategy leverages the PAM module for visibility and provides a provisioning policy form that replaces the default provisioning capabilities that come with the PAM module. The provisioning capabilities found within the PAM module are based on user entitlements, while Password Safe is exclusively based on Group Entitlements via Role Based Access Control (RBAC).

Container creation in Password Safe results in creating an account Smart Group , which includes conditions, actions, and resource consumption. Container creation is not applicable as a use case within the PAM module.

For Password Safe, privileged data items (discovered managed accounts) are displayed under containers (managed account Smart Groups). This use case does not apply to Password Safe, and is based on a different PAM Application design.

The application template, found in the Password Safe Resource Kit, helps complement the PAM module and allows provisioning without the need for complex customization.

When it comes to provisioning, a few strategies are available depending on the specific use case, or combination of account and group. In the table below, **Local** means created directly into Password Safe. The table below illustrates entitlement type used for provisioning vs account-group combinations.

	Group			
Account	Local	AD	Entra ID	LDAP
Local	PS			
AD	PS - Import	AD - Sync		
Entra ID	PS - Import		Entra ID - Sync	
LDAP	PS - Import			LDAP - Sync

PS – Import = Password Safe entitlements are provisioned via the Provisioning Policy – Form, within the application definition for Password Safe, by configuring attributes including nativeIdentifier (unique identifier associated to an individual account) and source, as described below in this document.

Sync = Password Safe group synchronization, via previously imported groups

Note: *Password Safe group synchronization is triggered*

- *by synchronization interval*
- *by manual synchronization*
- *at log in, where group memberships are re-evaluated or synchronized*

From an access perspective, group sync causes no delay versus provisioning and deprovisioning.

Create the SailPoint IdentityIQ Service Account in Password Safe

Creating a SailPoint IdentityIQ service account in BeyondInsight requires the following:

- Create a user group
- Enable features and Smart Groups for the user group

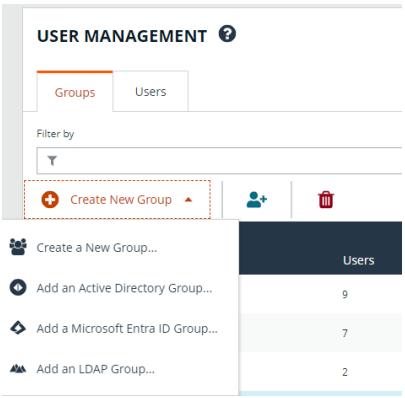
- Create a user account and add it to the user group
- Log in to BeyondInsight as the new service account user to generate OAuth credentials.

The below sections detail the steps to take to accomplish the above.

Create a New Group for the Service Account

To create a local group in BeyondInsight, follow the below steps:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **+ Create New Group**.



3. Select **Create a New Group.**
4. Enter a **Group Name** and **Description** for the group.
5. Click **Create Group**.
6. Follow the steps in the below sections to enable features and Smart Group for your newly created group.

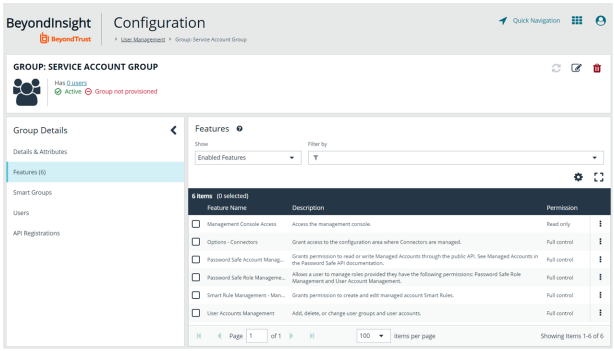
> ***Note:*** *In addition to creating groups locally, you can import Active Directory, Entra ID, and LDAP groups into BeyondInsight.*

Enable Features for the Group

To enable features for a group in BeyondInsight, assign permissions to the features as follows:

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, find the group and click on the corresponding ellipsis to right of the group.
3. Select **View Group Details** from the list.
4. Click **Features** located under **Group Details**.
5. Select **All Features** from the **Show** dropdown above the grid to display a list of features in the grid.

6. Select the **Management Console Access** feature and click **Assign Permissions > Assign Permissions Read Only** above the grid. This permission is required so the service account can log in to BeyondInsight and obtain the service accounts' unique OAuth credentials.
7. Select the following features and click **Assign Permissions > Assign Permissions Full Control** above the grid.

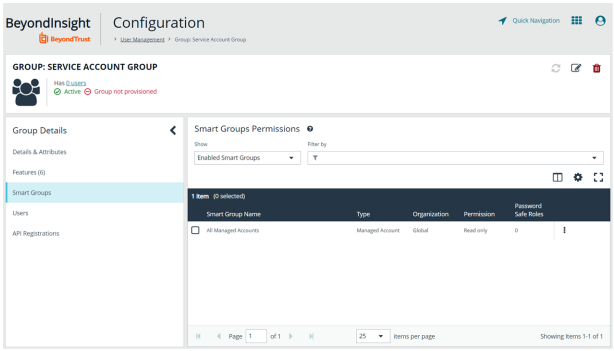


   - **Options - Connectors**: This feature is required to allow the creation of OAuth credentials by the member account. In production, this permission could be removed after connection is established, but is needed again to cycle **client_secret** and **refresh_token**.
   - **Password Safe Account Management**: This feature is required to read or write managed accounts through the public API.
   - **Password Safe Role Management**: This feature is required to allow visibility into account Smart Groups, which are assigned via user groups in BeyondInsight.
   - **Smart Rule Management - Managed Account:** This feature is required to manage Smart Rules for managed accounts.
   - **User Accounts Management**: This feature is required for the service account to manage user groups and user accounts.

Enable Smart Groups for the Group

To enable Smart Groups for a group in BeyondInsight, assign permissions to the Smart Groups as follows:

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, find the group and click on the corresponding ellipsis to right of the group.
3. Select **View Group Details** from the list.
4. Click **Smart Groups** located under **Group Details**.
5. Select **All Smart Groups** from the **Show** dropdown above the grid to display a list of Smart Groups in the grid.
6. Select the **All Managed Accounts** Smart Group and click **Assign Permissions > Assign Permissions Read Only** above the grid.



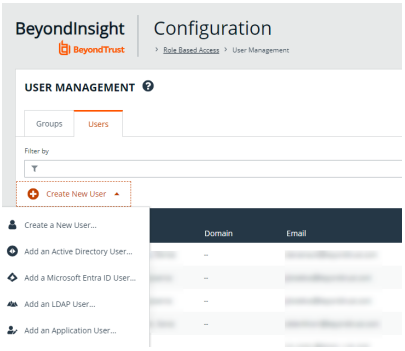
> ***Note:*** *Managed Account Smart Groups with a category of* ***Managed Accounts*** *are visible via the SCIM API. Managed Account Smart Groups with a category of* ***Platforms*** *are not visible. However, you can recreate the same Smart Group with a category of* ***Managed Accounts****.*

Create a New User and Assign to Group

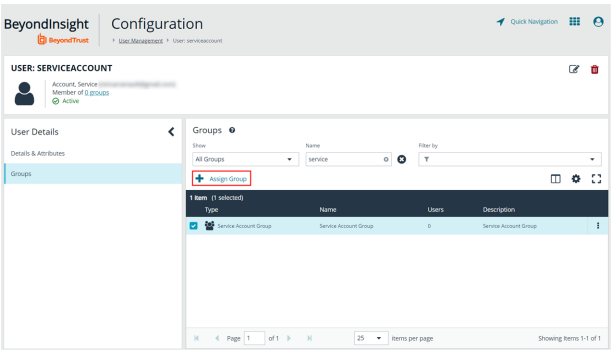
Once the group is created and assigned the appropriate features and Smart Groups permissions, you can create a new account in BeyondInsight for the service account and add it to the group.

> ***Note:*** *Permissions are assigned only to the group, not to the account.*

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Users** tab, click **Create New User**.
3. Select **Create a New User**.



4. Provide **Identification**, **Credentials**, **Contact Information**, **User Status**, and **Authentication Options** as needed.
5. Click **Create User**.
6. You are taken to the details page for the user account where **Groups** is automatically selected. Select **All Groups** from the **Show** dropdown above the **Groups** grid to list all available user groups.
7. Locate the group you created above for the service account, select it, and then click **Assign Group** above the grid.

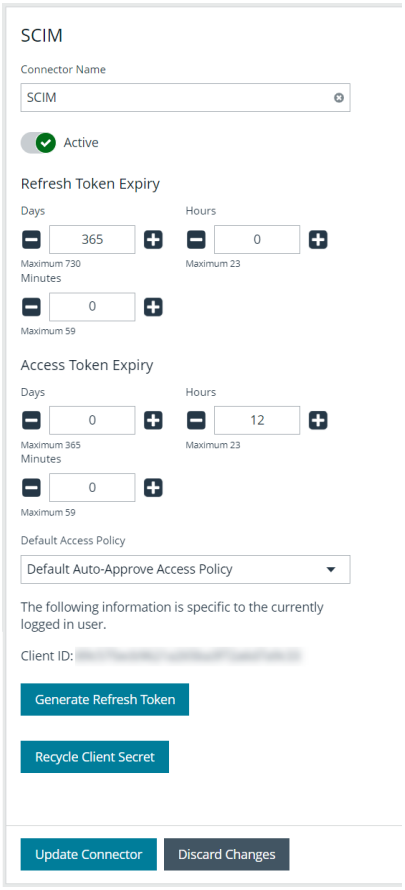


> ***Note:*** *In addition to creating user accounts locally, you can import AD, Entra ID, and LDAP accounts and add them to either local or imported groups.*

Generate OAuth Credentials

Once the user account is created and assigned to a group, you must log in as the new user to generate OAuth credentials.

1. Go to **Configuration > General > Connectors**.
2. Under **Connectors**, select the SCIM connector. Once selected, the SCIM connector information displays.



> ***Note:*** *Do not select the SailPoint connector. This was available in previous versions of BeyondInsight, but it is an older integration and is not based on SCIM.*

3. Each logged-in account in BeyondInsight has a unique client ID. The **Client ID** is located within the SCIM connector information. Highlight the ID, right-click, and save locally as **client_id** to a text file.
4. Click **Recycle Client Secret**.
5. Click **Recycle** on the **Recycle Secret Access Key** pop-up. This generates a unique access key.
6. Highlight the **Client Secret** access key, right-click, and save as **client_secret** to a text file.
7. Click **Generate Refresh Token** if you want to use this method of authentication. Use the account login password when prompted.

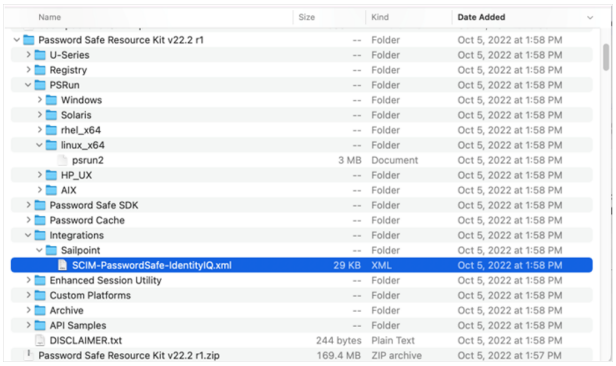
> ***Note:*** *The refresh token is used in the production environment. Client credentials (client ID and client secret) are used in a lab or test environment. Every Password Safe user with full control permissions to the **Options – Connectors** feature can obtain a **Client ID** and **Client Secret** via the connector.*

> ***Note:*** *Only one SCIM connector can be created by Password Safe per instance.*

Create the SailPoint IdentityIQ SCIM Application for Password Safe

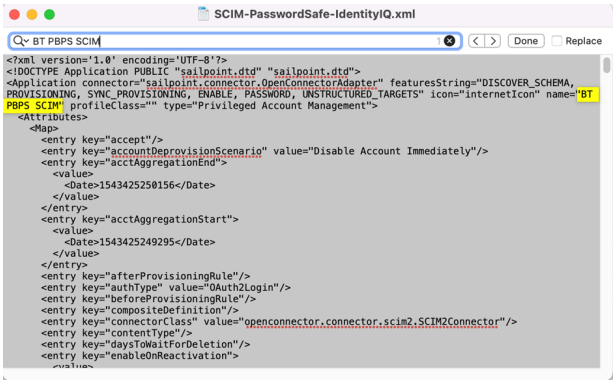
Access the Password Safe Resource Kit

The Password Safe Resource Kit is available with product downloads via the Customer Portal. A preconfigured application for Password Safe is available in the Resource Kit.



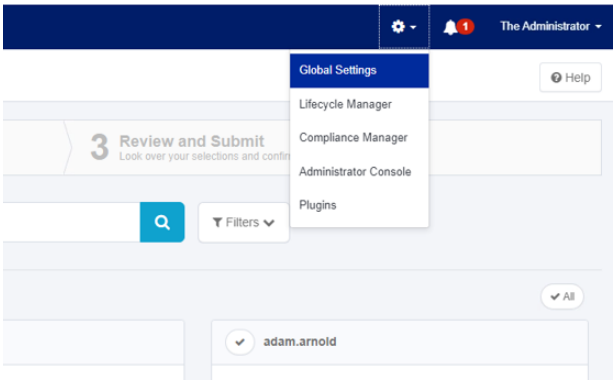
Before you import **SCIM-Password Safe-IdentityIQ.xml**, save a copy of the file and edit it using the text editor of your choice to change the application name. You can create one or more applications, each with a unique name.

Search for *BT PBPS SCIM* and replace the value with Password Safe or any desired value for the name.



Import the XML File

> ***Note:*** *To be able to import the* ***SCIM-PasswordSafe-IdentityIQ.xml*** *file, users must have administrator permissions.*

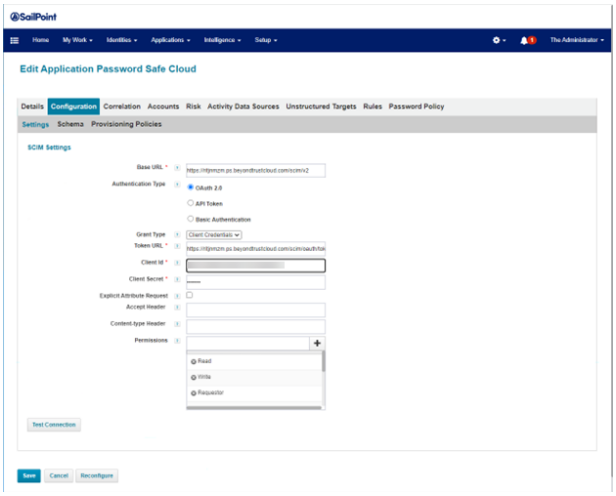


To import the XML file:

1. Log in to **SailPoint IdentityIQ**.
2. Click the gear icon at the top of the screen and select **Global Settings**.
3. On the **Global Settings** page, click **Import from File**.
4. On the **Import from File** page under **Import Objects**, click **Choose File** and navigate to the edited XML file.
5. Click **Import**.

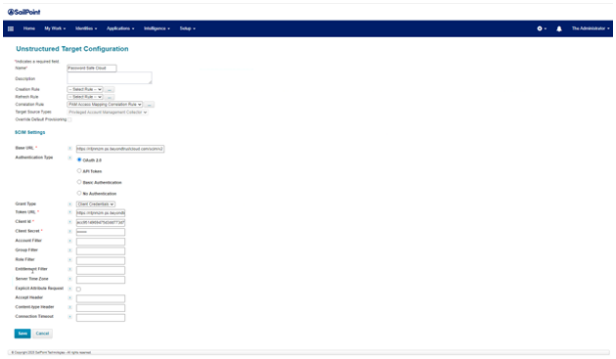
Application Definition

1. Under the **Application** menu item, select **Application Definition**. You are able to see and edit the new application.
2. Double-click the new application.
3. Click the **Configuration** tab. Then click **Settings**.
4. Under **Grant Type**, select **Client Credentials**.
5. Enter the **Base** and **Token URLs**.
6. Provide the **Client ID** and **Client Secret**, which you saved locally while in the **Generate oAuth Credentials** section of this guide.
7. Click **Test Connection**. If the test is successful, a *Connection Successful* message is displayed. If the test is not successful, an error message is displayed.



> ***Note:*** *Client credentials are recommended for testing. A refresh token is used in production where security requirements are higher.*

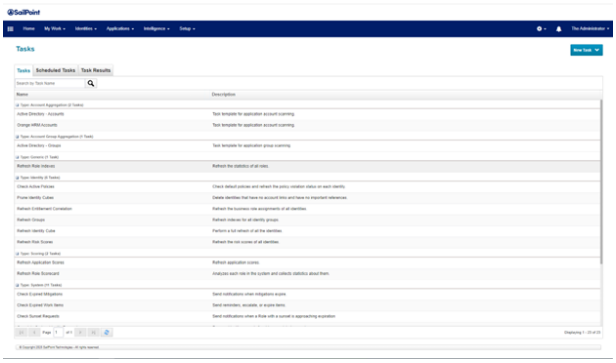
8. Click the **Correlation** tab.
9. Configure the **Account Correlation**, for example, by using an email address and username.
10. Click the **Unstructured Targets** tab.
11. Click the **Add New Unstructured Data Source** button.
12. On the pop-up dialog, click the **Create Target Source** button.
13. On the next screen, select **Privileged Account Management Collector** from the **Target Source Types** dropdown list.
14. Enter URLs and credentials.
15. Select **PAM Access Mapping Correlation Rule** from the **Correlation Rule** dropdown list.
16. Click **Save** on the **Unstructured Target Configuration** screen.
17. Click **Save** on the **Edit Application** screen.



Aggregate Accounts, Groups, and Entitlements from Password Safe

Before a user can start using SailPoint IdentityIQ, it must aggregate, or discover, Password Safe accounts, permissions, and groups.

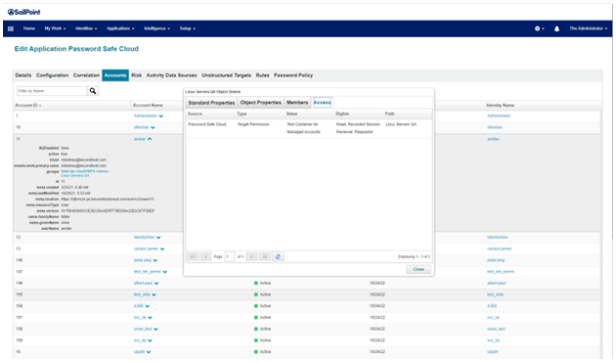
1. Under the **Setup** menu item, click the **Tasks** tab.
2. Under the **New Task** dropdown list select **Account Aggregation**.
3. Include a task name and update all remaining fields as required.
4. Click **Save**.
5. Repeat steps one through four, this time for **Account Group Aggregation**.
6. Repeat steps one through four, this time for **Target Aggregation**.
7. Once all three tasks have been created, right-click on the **Account** task and select **Execute in Background**. Repeat this step for **Group**, and then **Target**.



View Target Permissions and Entitlements

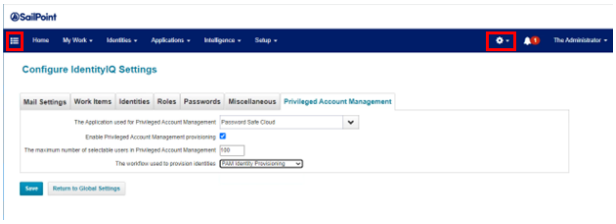
To view how permissions and accounts are represented in IdentityIQ after aggregation:

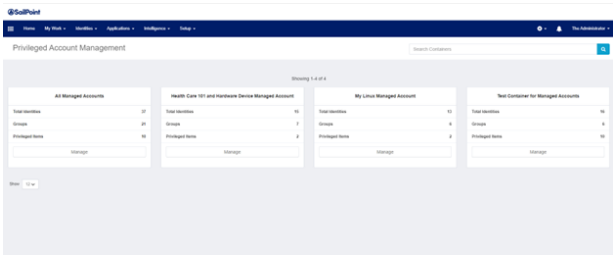
1. Return to the applications list by clicking the **Application** menu item, and then select **Application Definition**.
2. Double-click the application.
3. Click the **Accounts** tab.
4. Expand an account.
5. Click one of the groups listed, and then click the **Access** tab to view **Target Permissions**.
6. To view identity entitlements, click the **Identities** menu at the top of the page, and then select **Identity Warehouse**.
7. Double-click user name, and then click the **Entitlements** tab.



Configure the PAM Module to point to Password Safe

1. Click the gear icon in the upper right corner of **SailPoint IdentityIQ** and select **Global Settings**.
2. On the **Global Settings** page, click **IdentityIQ Configuration**.
3. Click the **Privileged Account Management** tab.
4. Select Password Safe from the first dropdown list.
5. Click **Save**.
6. Click the list icon in the upper left corner of **SailPoint IdentityIQ** to access the **Tasks** menu and expand **Manage Access.**
7. Select **Privileged Account Management** to view the PAM module for Password Safe.



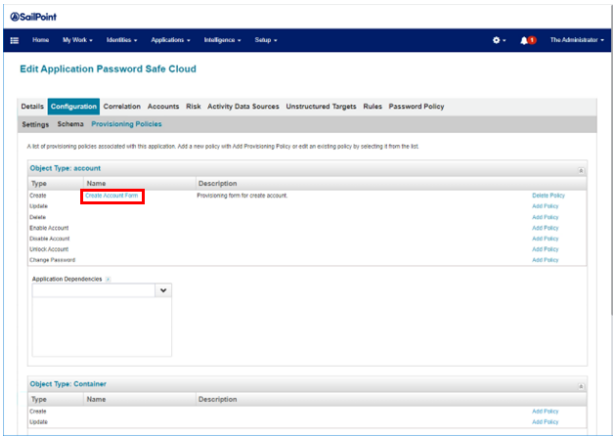


> ***Note:*** *The PAM module provides the* ***Add Identities*** *button, which is configured by default to provision entitlements to users. Password Safe allows for entitlements at the group level only, via its RBAC model. Some customers have reconfigured the PAM module to provision entitlements through Groups, but that is beyond the scope of this guide, and it is recommended that customers work with SailPoint Professional Services for such changes. However, the provisioning strategy described later in this guide provides provisioning support for both directory and non-directory or local users.*

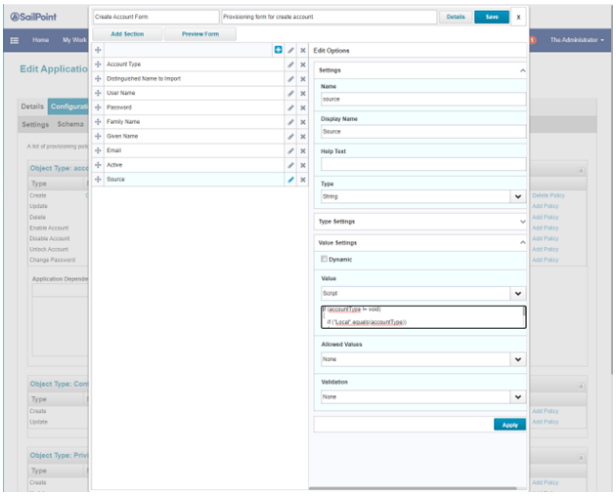
Provision Directory and Non-Directory Users

The application template for Password Safe comes with a preconfigured provisioning policy. To access the provisioning policy:

1. Under the **Applications** menu item, select **Application Definition**.
2. Double-click the application.
3. Click the **Configuration** tab.
4. Click **Create Account Form**.



> ***Note:*** *The "Source" attribute is required to recognize that an account exists in a source outside of Password Safe. Without knowing the source, provisioning fails to find and modify the account.*



5. On the next screen, create an attribute called *Source*:
   - Click the blue plus sign icon and select **Add Field**.
   - Under **Edit Options > Settings**, type *source* in the **Name** field.
   - Type *Source* in the **Display Name** field.
   - Under **Value Settings**, select *Script* from the **Value** dropdown list.
   - Under **Allowed Values**, select one or more values.
   - Enter a **Value Script**. In the below example, *Active Directory* is the name of the application in IdentityIQ:

> ***Example:***
>
> ```
> if (accountType != void)
> {
> ```

```
    if ("Local".equals(accountType))
    {
       return null;
    }
}
return "Active Directory";
```

Note: *Source must be null for local provisioning, otherwise this will instruct Password Safe to look for the user in the source/application.*

6. Next, create an attribute called *Active*.
    a. Click the blue plus sign icon and select **Add Field**.
    b. Under **Edit Options > Settings**, type *active* in **Name** field.
    c. Type *Active* in **Display Name** field.
    d. Under **Value Settings**, select *Value* from the **Value** dropdown list.
    e. Type *true* in the field under *Value*. If the value is not set to true, the account will be inactive in Password Safe.
7. Click the pencil icon to the right of the **Distinguished Name to Import** attribute. Add **Help Text** to explain that this is based on the import of a pre-existing account from Active Directory.

Note: *For an account with a source other than Password Safe, e.g.; in LDAP or AD, one Distinguished Name is presented. However, if the target user has multiple accounts in different directories, a list of accounts is provided. Each of these accounts should be provisioned.*

8. Click **Save** in the top right corner.

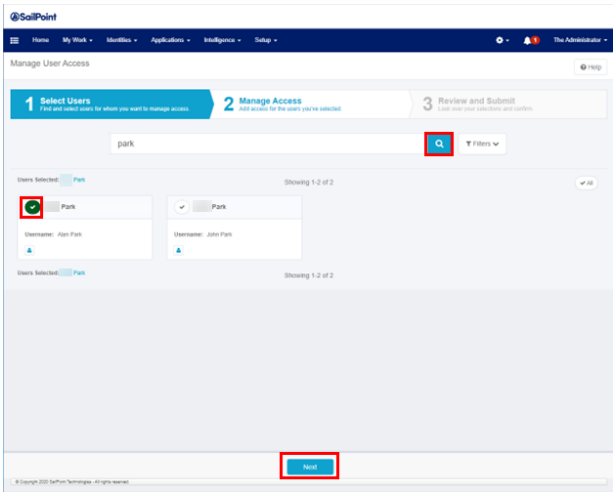
Note: *Password Safe cannot provision a new account to Active Directory. It can only import an existing account from Active Directory and add it to a Password Safe local group. Password Safe cannot modify accounts, groups, or group gemberships in Active Directory. Password Safe can import and synchronize groups and account members.*

Test the Integration

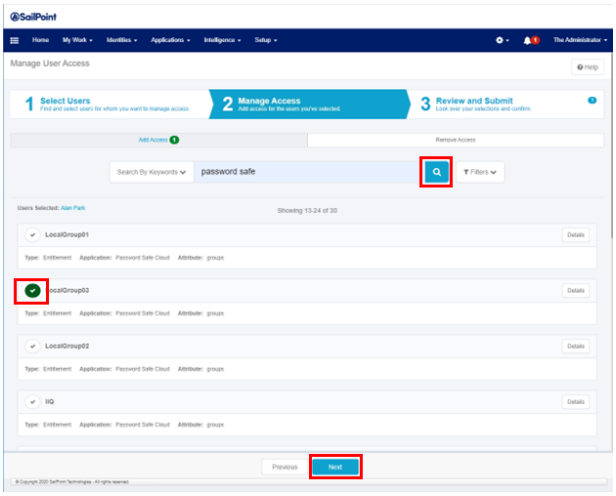
The most common scenario consists of a user with a directory account. For this scenario, use Password Safe as the application. To test this scenario:

1. On the **SailPoint IdentityIQ** homepage, click the menu icon in the upper left corner.
2. Select **Manage Access > Manage User Access**.

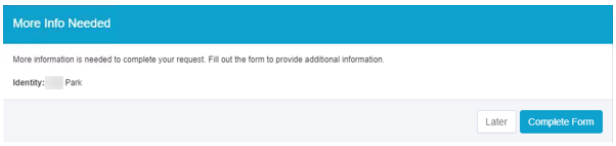
3. On the **Select User** screen, enter the username in the **Search** field and click the magnifying glass icon. One or more users are returned.
4. Click the check mark icon next to a user name to select that user.
5. Click **Next**.



6. On the **Manage Access** screen, type *Password Safe* in the **Search** field and click the magnifying glass icon. One or more groups are returned.
7. Click the check mark icon next to a local group to select that group.
8. Click **Next**.
9. On the **Review and Submit** screen, make sure everything is correct, and then click **Submit**.

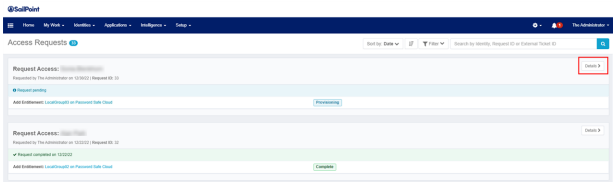


10. You may be asked for additional information. Click **Complete Form**.
11. On the next screen, under **Account Type**, click **Active Directory** to resolve the value (or values) via Directory Source.
12. Check the **Distinguished Name to Import** box.
13. Click **OK**.

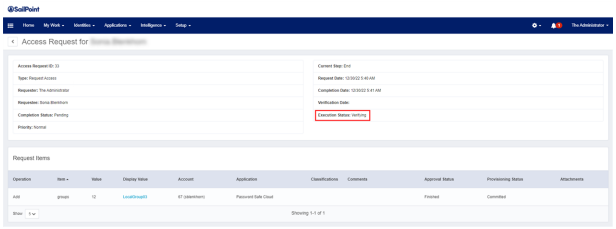


View Execution Status of User Access Request

1. On the **SailPoint IdentityIQ** homepage, click the menu icon in the upper left corner.
2. Select **Manage Access >Track My Requests**.



3. On the **Access Request** page, click **Details** to view the execution status of the request.
4. The access request is in *Verifying* status until aggregation is performed for Password Safe. Once aggregation is complete, the user account is imported from Active Directory into the Password Safe local group.

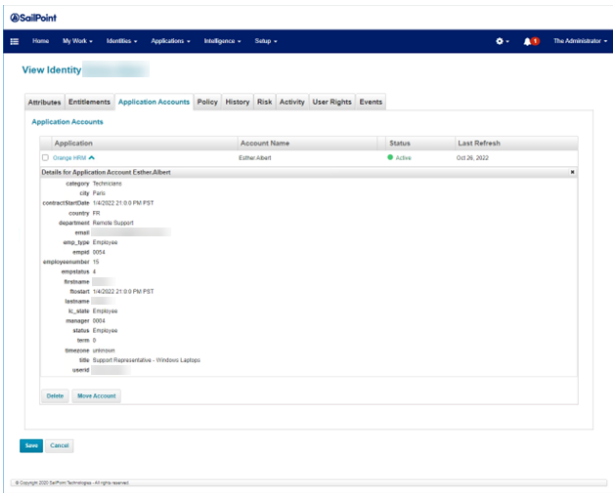


Provision a User Without a Directory Account

You might need to provision populations of users without a Directory Account. For example, this is required for vendor access.

To view application accounts assigned to a user:

1. On the **SailPoint IdentityIQ** homepage, click the **Identities** menu, and then select **Identity Warehouse**.
2. Select **Manage Access >Track My Requests**.
3. On the **Identity Warehouse** screen, enter the username in the **Search** field, and then click the magnifying glass icon. One or more users are returned.
4. Double-click the correct user name.
5. On the **View Identity** ***User.Name*** screen, click **Application Accounts**.

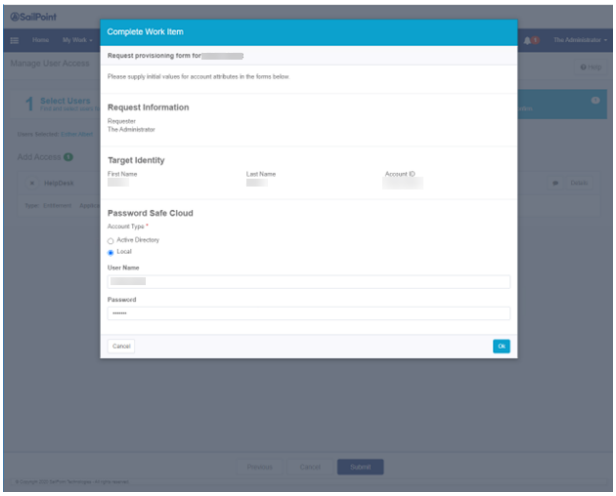


To provision a user without a directory account:

1. On the **SailPoint IdentityIQ** homepage, click the menu icon in the upper left corner.
2. Select **Manage Access > Manage User Access**.
3. On the **Select User** screen, enter the username in the **Search** field, and then click the magnifying glass icon. One or more users are returned.
4. Click the check mark icon next to a user name to select that user.
5. Click **Next**.
6. On the **Manage Access** screen, enter *Password Safe* in the **Search** field and click the magnifying glass icon. One or more groups are returned.
7. Click the check mark icon next to a local group to select that group.
8. Click **Next**.
9. On the **Review and Submit** screen, make sure everything is correct, and then click **Submit**.

10. Additional information is required. Click **Complete Form**.
11. On the next screen, under **Account Type**, select **Local**.
12. Provide a username and password.
13. Click **OK**.

> ***Note:*** *The **User Name** and **Password** values can be assigned dynamically in the **Provisioning Policy Create Form.***



The new local user account is now available in Password Safe. To view this account:

1. On the BeyondInsight homepage, select **Configuration > Role Based Access > User Management > Groups**.
2. Click the ellipsis to the right of the group that the new local user account was assigned to. Select **View Group details**.
3. Under **Group Details**, select **Users**. The new local user account is visible under **Assigned Users**.

Use SailPoint IdentityIQ Credential Cycling

Implementation Tutorial

Credential cycling is a feature that allows applications requiring credentials, such as username and password, to obtain that information directly from BeyondTrust Password Safe.

With credential cycling, credentials can be removed from application configurations and obtained at run time using an Application Programming Interface (API) call to Password Safe. Password Safe is then configured to rotate the credentials directly with the application target, helping to reduce the risk associated with stale credentials while eliminating the need for manual updates of credentials in a solution like SailPoint IdentityIQ.

Credentials used by SailPoint IdentityIQ are privileged credentials, since they allow access to private data. They also allow for provisioning and deprovisioning of permissions in critical systems and applications, such as Active Directory (AD).

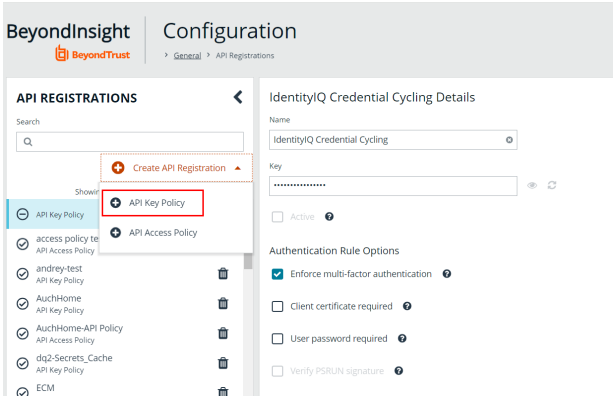
This tutorial outlines the steps required to configure credential cycling for a Java database connectivity (JDBC) application in SailPoint IdentityIQ.

> *For more information, please see the IdentityIQ Privileged Account Management documentation located in the SailPoint Community Portal at https://community.sailpoint.com/t5/IdentityIQ-Product-Guides/8-3-IdentityIQ-Privileged-Account-Management-Guide/ta-p/214154.*

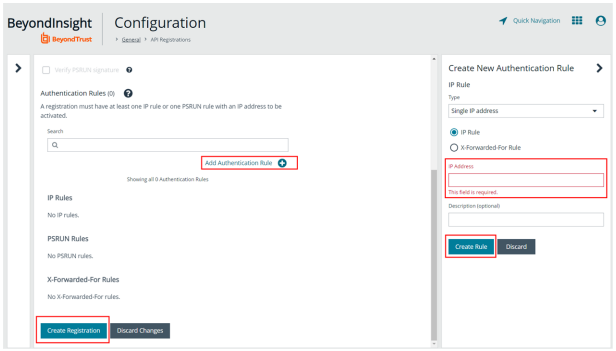
Create a Service Account for IdentityIQ Credential Cycling

Create an API Registration

1. Log in to the **BeyondInsight** console.
2. Go to **Configuration > General > API Registrations**.
3. Under **API Registrations**, click **Create API Registration**, and then select **API Key Policy**.
4. Name the new API registration *IdentityIQ Credential Cycling*.



5. Click **Add Authentication Rule**.
6. Add the IdentityIQ server IP address (located in IP Rule) to the **IP Address** field to allow the connection.
7. Click **Create Rule**.
8. Click **Create API Registration**.

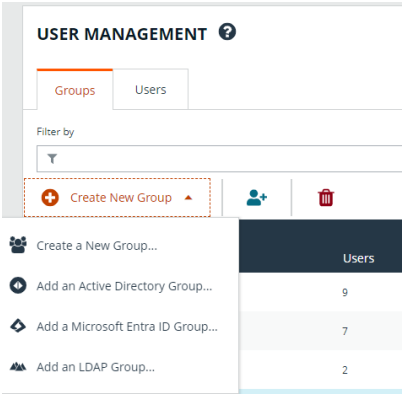


> ***Note:*** *For security options beyond API Key and IP Rule or Filter, it is possible to take advantage of the Password Cache. For more information, please see the Password Cache User Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cache/index.htm.*

Create a Local Group

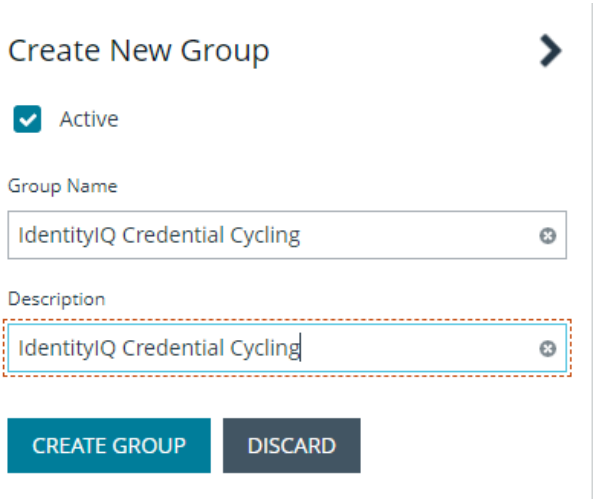
To create a local group in BeyondInsight, follow the below steps:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **+ Create New Group**.



3. Select **Create a New Group.**
4. On the next screen, provide a group name of *IdentityIQ Credential Cycling* and description.
5. Click **Create Group**.

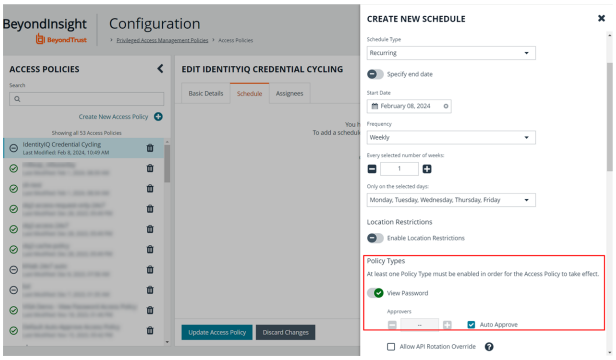
> ***Note:*** *In addition to creating groups locally, you can import Active Directory, Entra ID, and LDAP groups into BeyondInsight.*



Create an Account Access Policy

An access policy must be available for credential cycling. This is required to be able to grant the requestor the Password Safe role for the Smart Rule.

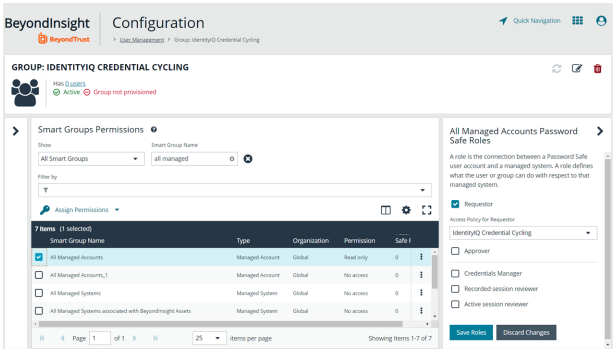
1. In **BeyondInsight**, go to **Configuration > Privileged Access Management Policies > Access Policies**.
2. Click **Create New Access Policy**.
3. Type *IdentityIQ Credential Cycling* in the **Access Policy Name** field and click **Create Access Policy**.
4. Click the **Schedule** tab, and then click **Create Schedule**.
5. Scroll down to **Policy Types** and enable **View Password**.
6. Check the **Auto Approve** box.
7. Scroll down to the bottom of the scheduling form and click **Create Schedule**.
8. Click **Make Available** on the prompt that displays.
9. Click **Update Access Policy**.



Assign an Account Smart Group

An account Smart Group must be assigned to the new local group that contains the application accounts required by IdentityIQ. To do this:

1. In **BeyondInsight**, go to **Configuration > Role Based Access > User Management > Groups**.
2. In the **Filter by** field, select **Name** from the dropdown list.
3. Type *IdentityIQ Credential Cycling* in the **Name** field.
4. Click the vertical ellipsis for the group and select **View Group Details**.
5. Under **Group Details**, select **Smart Groups**.
6. Locate the **All Managed Accounts** Smart Group in the **Smart Groups Permissions** grid and click the vertical ellipsis for it.
7. Select **Assign Permissions Read Only**.



8. Click the vertical ellipsis for the **All Managed Accounts** Smart Group again, and then select **Edit Password Safe Roles**.
9. Check the box next to **Requestor**.
10. Select **IdentityIQ Credential Cycling** from the **Access Policy for Requestor** dropdown.
11. Click **Save Roles**.

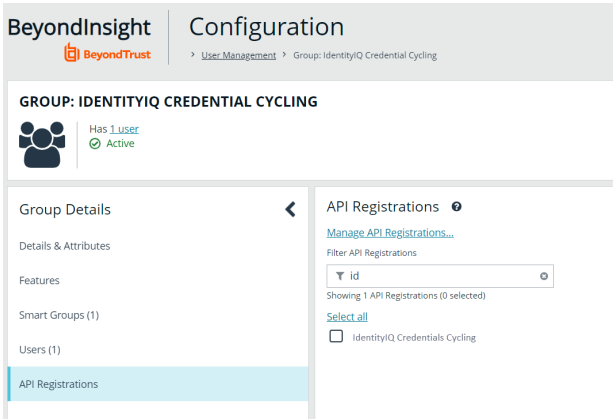
Add a User Account

A user account must be added to the group. IdentityIQ uses this account as the service account for credential cycling.

1. In **BeyondInsight**, go to **Configuration > Role Based Access > User Management > Groups**.
2. In the **Filter by** field, select **Name** from the dropdown list.
3. Type *IdentityIQ Credential Cycling* in the **Name** field.
4. Click the vertical ellipsis for the group and select **View Group Details**.
5. Under **Group Details**, select **Users**.
6. Above the **Users** grid, select **Users not Assigned** from the **Show** dropdown list.
7. Locate the user and select it.
8. Click **Assign User** above the grid. If you select **Assigned Users** from the **Show** dropdown list, the user is now listed.

Enable Credential Cycling API Registration for the Group

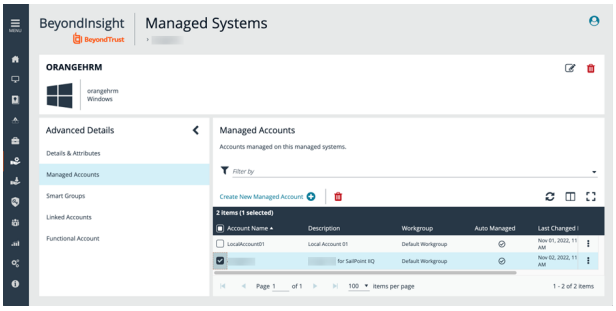
1. In **BeyondInsight**, go to **Configuration > Role Based Access > User Management > Groups**.
2. In the **Filter by** field, select **Name** from the dropdown list.
3. Type *IdentityIQ Credential Cycling* in the **Name** field.
4. Click the vertical ellipsis for the group and select **View Group Details**.
5. Under **Group Details**, select **API Registrations**.
6. Check the box next to the **IdentityIQ Credential Cycling** API registration created earlier in this tutorial to enable it.



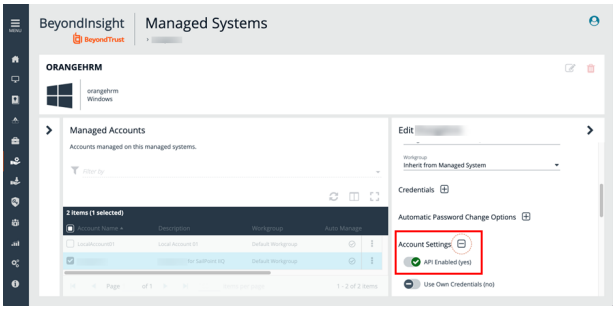
Identify Managed System and Managed Account

A managed system and a managed account must be identified in order for IdentityIQ to determine the password for that account. SailPoint Connector requires the correct username/password credentials to connect to the account.

1. In **BeyondInsight**, go to **Managed Systems**.
2. Check the box next to a managed system to select it, and then click the corresponding ellipsis to the right of the system. Select **Go to Advanced Details**.
3. Under **Advanced Details**, select **Managed Accounts**.
4. Check the box next to a managed account to select it.



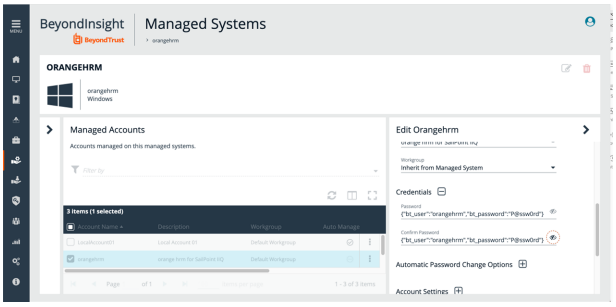
5. The managed account must have an API enabled. Click the corresponding ellipsis to the right of the group.
6. Under **Account Settings**, click the toggle button next to **API Enabled**.



Update Managed Account Password to JSON format

To allow IdentityIQ to retrieve credentials, the password for the managed account in Password Safe must use the JSON format.

1. In **BeyondInsight**, go to **Managed Systems**.
2. Check the box next to a managed system to select it, and then click the corresponding ellipsis to the right of the system. Select **Go to Advanced Details**.
3. Under **Advanced Details**, select **Managed Accounts**.
4. Check the box next to a managed account to select it, and then click the corresponding ellipsis to the right of the account. Select **Edit Account**.
5. Under **Credentials**, type the user (account name) and password for that account in the **Password** field using the following format:



Example:

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

6. Click **Update Account**.

Use IdentityIQ to Complete Credential Cycling Process

Customize the credentialConfigurationTemplate.xml File

In order to continue with the credential cycling process, the **credentialConfigurationTemplate.xml** file must be customized. It is recommended that you create a copy locally.

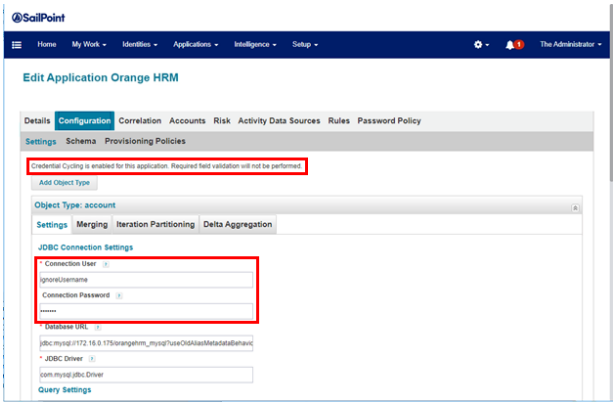
1. On your local drive, navigate to **Program Files > Apache Software Foundation > Tomcat 9.0 > webapps > identityiq > WEB-INF > config**.
2. Select the **credentialConfigurationTemplate.xml** file.
3. Right-click on the file and save a copy to edit it.
4. Open the copied file in a text editor of your choice. Change the following:
    - **url**, **runas**, and **apikey** to match your environment.
    - Replace **managedAccountName** and **managedSystemName** with the correct values.
    - Specify the name of the application that uses credential cycling.
    - Identify application attributes.

Populate User and Password with Credential Cycling

In IdentityIQ, you must populate the connection user and connection password in the application using credential cycling.

To view connection user and connection password:

1. Log in to SailPoint IdentityIQ.
2. Under **Applications**, select **Application Definition**.
3. Click the desired application.
4. Click **Configuration > Settings** to view **Connection User** and **Connection Password**.



> ***Note:*** *If the application is enabled for credential cycling, and note is displayed on the screen.*

Application attributes differ from the label used on the **Application Configuration** page. In order to identify the application attributes, use the */debug* interface.

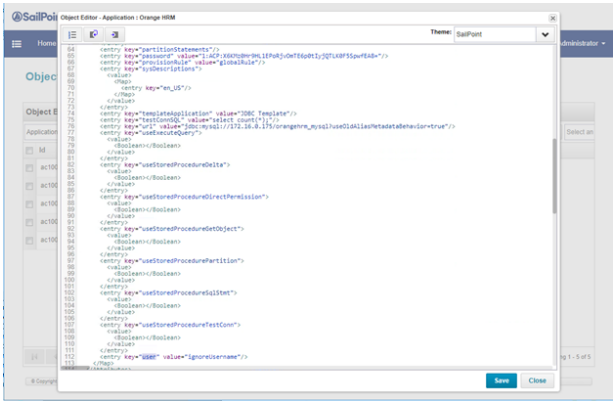
1. Go to https://identityiq_server:8443/identityiq/debug.
2. Select **Application**.
3. Click the desired application to open the **Object Editor**.
4. Locate **key=”password”** and **key=”user”** and identify the values. These 2 values are required for application attributes.
5. Manually update the following values in the template file for the desired application:
    - <CredentialAssociation applicationName="*Application Name*"

      attributeName="user"

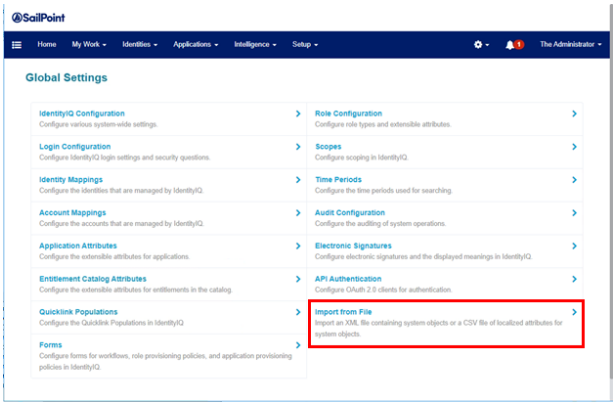
      credentialAttributeName="bt_user">
    - <CredentialAssociation applicationName="*Application Name*"

      attributeName="password"

      credentialAttributeName="bt_password"/>

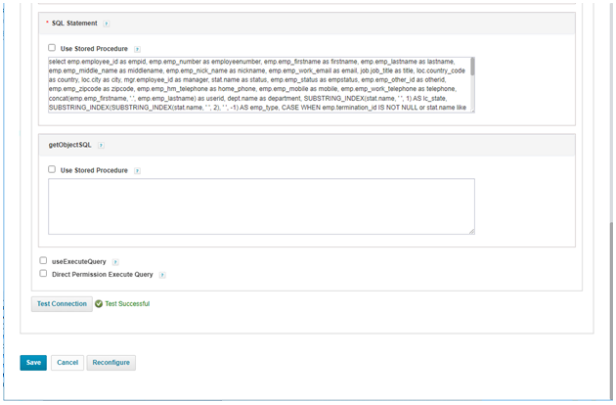


6. Click **Save**.
7. Import the template file to IdentityIQ. This applies the template to the application:
    - Click the gear icon on the upper right side of the screen.
    - Select **Global Settings**.
    - Select **Import From File**.
    - Click **Choose File** and navigate to the template file.
    - Click **Import**.



At this point, you should be able to test the application successfully, preview the application via schema, and aggregate. Once an application is configured for credential cycling, credentials in **Settings** are ignored. To test the application:

1. Log in to SailPoint IdentityIQ.
2. Under **Applications**, select **Application Definition**.
3. Click the desired application.
4. Click **Configuration > Settings**.
5. At the bottom of the page, click **Test Connection**. If successful, a *Test Successful* message is displayed.



Configure SCIM Connector for Sailpoint IndentityIQ

The SCIM connector adds a SCIM API to Password Safe to allow third-party applications to view and modify users, groups, and Smart Rule permissions.

> *For more information, please see the following:*
> - *SCIM implementations at http://www.simplecloud.info/*
> - *The PAM extension at https://datatracker.ietf.org/doc/html/draft-grizzle-scim-pam-ext-00*

SailPoint IdentityIQ Integration

IdentityIQ currently supports:

- Reading users, groups, Smart Rules, and Smart Rule permissions into their system
- Creating users, and adding and removing users to and from groups

Although this is what the IdentityIQ supports, the SCIM connector follows the SCIM and PAM extension standard, so it is possible to assign permissions to groups. IdentityIQ supports assigning permissions to users only, which isn't compatible with Password Safe.

Configure SailPoint IdentityIQ

To help configure the SCIM API in IndentityIQ, an application XML prebuilt with local and AD user provisioning is available on the BeyondTrust customer portal.

> *For more information, please see the SailPoint IdentityIQ Deployment Guide Tutorial at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/integrations/third-party/identity-iq.htm.*

Account Schema

To configure the IdentityIQ SCIM application manually to be compatible with Password Safe, there are some default schema settings you need to modify, as follows:

- Under **name**, remove **middleName**, **honorificPrefix**, and **honorificSuffix**.
- Remove **nickName**, **profileUrl**, **title**, **userType**, **preferredLanguage**, **locale**, and **timezone**.

For the provisioning form, if you intend to create Active Directory users only, the native identifier must be populated with the **distinguished name**. All other fields are populated with what is in Active Directory. The following script populates IdentityIQ fields with allowed values for **distinguished name**:

```
import java.util.*;
import sailpoint.object.*;
import sailpoint.api.*;

List adLinks = new ArrayList();
if (identity != null) {
  Application targetApplication = context.getObjectByName(Application.class, "Active Directory");
```

```
  // "Active Directory" here is the name of the AD application you want to use
  IdentityService identityService = new IdentityService(context);
  List links = identityService.getLinks(identity, targetApplication);
  if (links != null) {
    for (Link link : links) {
      adLinks.add((String)link.getAttribute("distinguishedName"));
    }
  }
}
return adLinks;
```

Create the SCIM Connector

The below steps detail how to create and update a SCIM connector in BeyondInsight.

> ***Note:*** *Only one SCIM connector can be created by Password Safe per instance. If your Password Safe instance already has a SCIM connector configured, then you must log in to BeyondInsight with the service account credentials you created for the integration and generate OAuth credentials as detailed in* ***step #9*** *below.*

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **SCIM** from the **Connector Type** dropdown.
5. Click **Create Connector**.

6. Set the **Refresh Token Expiry**.

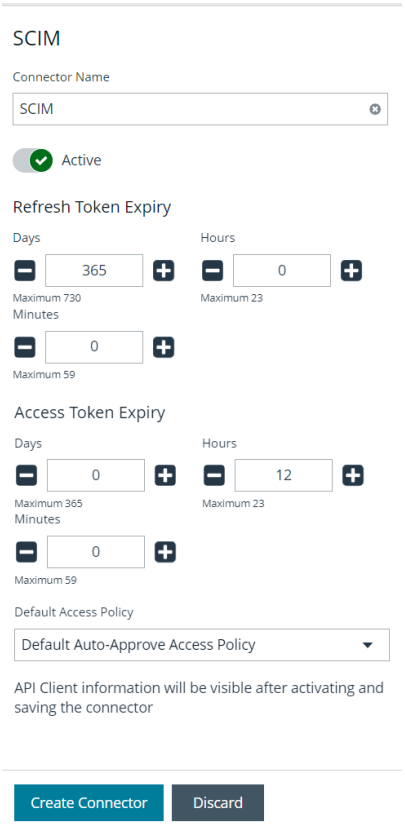
> ***Tip:*** *This is intended to be long-lived.*

7. Set the **Access Token Expiry**.

> ***Tip:*** *This is intended to be short-lived.*

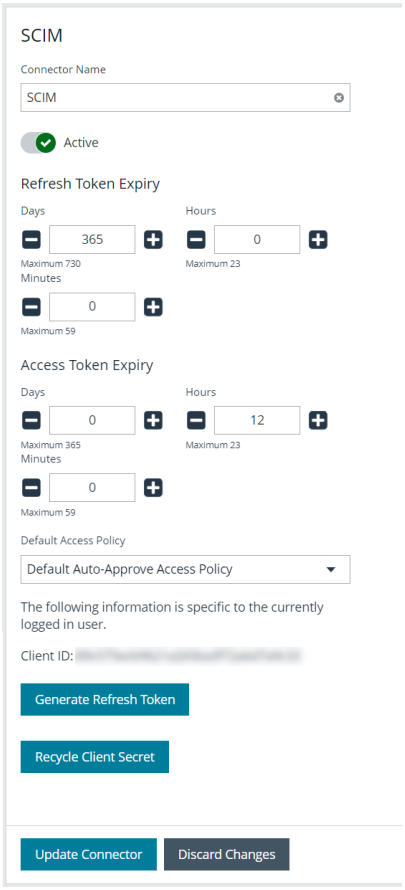
> ***Note:*** *Refresh and access tokens are an OAuth 2.0 concept.*

8. Select a **Default Access Policy**, and then click **Create Connector**.



> ***Note:*** *If the **Requestor** role is assigned to a group via the SCIM API, this access policy is assigned. The API does not support assigning different access policies. The container permissions you can provision include **Read**, **Write**, and Password Safe roles, such as **Requester** and **Approver**.*

9. Now that the connector has been created, the API is available to access, and you see the **Client ID** specific to the user currently logged into BeyondInsight when viewing the SCIM connector from the **Connectors** page. You can also generate a refresh token and recycle the client secret as follows:
    - To generate a refresh token:
        - Click **Generate Refresh Token**.
        - Enter your **Password** and **Client Secret**.
        - Click **Generate Refresh Token**.
    - To create a new client secret key:
        - Click **Recycle Client Secret**.
        - Click **Recycle** on the **Recycle Secret Access Key** pop-up. This generates a unique access key and invalidates the previous key.
    - Click **Update Connector** after generating the refresh token or recycling the client secret.



> ***Note:*** *Every Password Safe user with full control permissions assigned to the* ***Options – Connectors*** *feature can obtain a* ***Client ID*** *and* ***Client Secret*** *via the connector. Using client credentials (client ID and client secret) is recommended for lab or testing environments. For a production environment, using refresh tokens is a more secure option.*

10. To obtain a refresh and access token using the API, you can use client credentials or password authentication. Send a POST request with a body in one of these formats:

> ***Note:*** *The* ***Client ID*** *and* ***Client Secret*** *are part of your credentials for requesting refresh and access tokens. The authentication endpoint is* ***[host]/scim/oauth/token****.*

Client Credentials:

```
grant_type=client_credentials&client_id=[Client ID]&client_secret=[Client Secret]
```

Password:

```
grant_type=password&username=[Username]&password=[Password]
```

If you already have a refresh token, you can get a new access token with a POST request in this format:

```
grant_type=refresh_token&refresh_token=[Refresh Token]
```

Note: *The base URL for non-authentication requests is* ***[host]/scim/v2****.*

How to Configure SailPoint IdentityNow Integration

Overview

IdentityNow is a Software as a Service (SaaS) identity governance solution from SailPoint. This guide covers the steps required to configure OAuth Service Account in either Password Safe or Password Safe Cloud for SailPoint IdentityNow.

For more information, please see IdentityNow for BeyondTrust Password Safe at https://community.sailpoint.com/t5/Connector-Directory/IdentityNow-for-BeyondTrust-Password-Safe/ta-p/211776.

***Note:** Steps for the service account creation also applies to SailPoint IdentityIQ, but the focus of this guide is IdentityNow.*

Step-by-Step Installation and Configuration

Creating an IdentityNow service account in BeyondInsight requires the following:

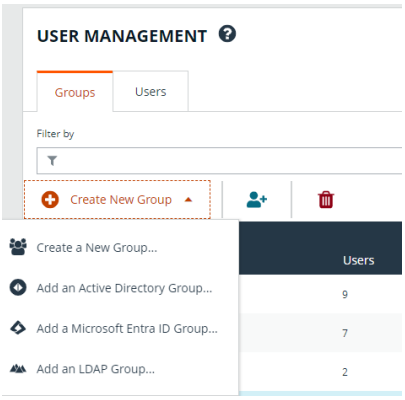
- Create a user group
- Enable features and Smart Groups for the user group
- Create a user account and add it to the user group
- Log in to BeyondInsight as the new service account user to generate OAuth credentials.

The below sections detail the steps to take to accomplish the above.

Create a New Group for the Service Account

To create a local group in BeyondInsight, follow the below steps:

1. Navigate to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, click **+ Create New Group**.



3. Select **Create a New Group.**
4. Enter a **Group Name** and **Description** for the group.

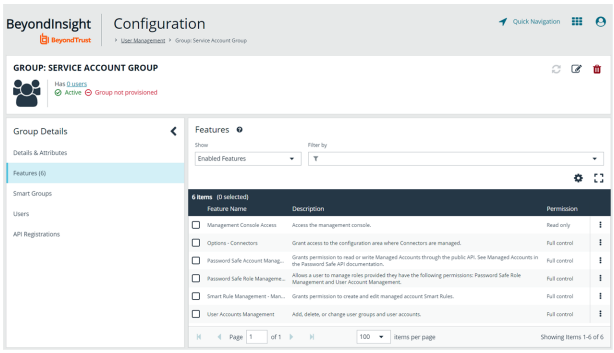
5. Click **Create Group**.
6. Follow the steps in the below sections to enable features and Smart Group for your newly created group.

> ***Note:*** *In addition to creating groups locally, you can import Active Directory, Entra ID, and LDAP groups into BeyondInsight.*

Enable Features for the Group

To enable features for a group in BeyondInsight, assign permissions to the features as follows:

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, find the group and click on the corresponding ellipsis to right of the group.
3. Select **View Group Details** from the list.
4. Click **Features** located under **Group Details**.
5. Select **All Features** from the **Show** dropdown above the grid to display a list of features in the grid.
6. Select the **Management Console Access** feature and click **Assign Permissions > Assign Permissions Read Only** above the grid. This permission is required so the service account can log in to BeyondInsight and obtain the service accounts' unique OAuth credentials.
7. Select the following features and click **Assign Permissions > Assign Permissions Full Control** above the grid.



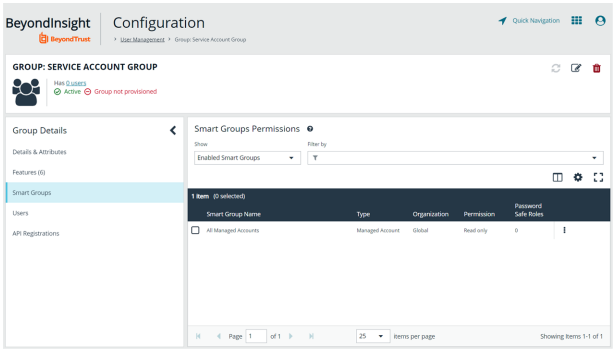
   - **Options - Connectors**: This feature is required to allow the creation of OAuth credentials by the member account. In production, this permission could be removed after connection is established, but is needed again to cycle **client_secret** and **refresh_token**.
   - **Password Safe Account Management**: This feature is required to read or write managed accounts through the public API.
   - **Password Safe Role Management**: This feature is required to allow visibility into account Smart Groups, which are assigned via user groups in BeyondInsight.
   - **Smart Rule Management - Managed Account:** This feature is required to manage Smart Rules for managed accounts.
   - **User Accounts Management**: This feature is required for the service account to manage user groups and user accounts.

Enable Smart Groups for the Group

To enable Smart Groups for a group in BeyondInsight, assign permissions to the Smart Groups as follows:

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Groups** tab, find the group and click on the corresponding ellipsis to right of the group.
3. Select **View Group Details** from the list.
4. Click **Smart Groups** located under **Group Details**.
5. Select **All Smart Groups** from the **Show** dropdown above the grid to display a list of Smart Groups in the grid.

6. Select the **All Managed Accounts** Smart Group and click **Assign Permissions > Assign Permissions Read Only** above the grid.



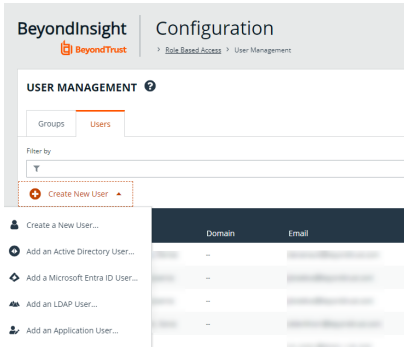
> ***Note:*** *Managed Account Smart Groups with a category of* ***Managed Accounts*** *are visible via the SCIM API. Managed Account Smart Groups with a category of* ***Platforms*** *are not visible. However, you can recreate the same Smart Group with a category of* ***Managed Accounts****.*

Create a New User and Assign to Group

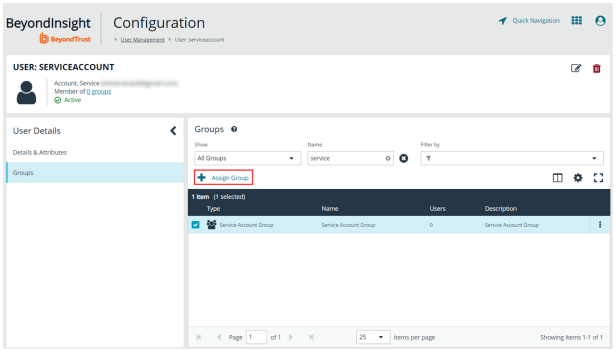
Once the group is created and assigned the appropriate features and Smart Groups permissions, you can create a new account in BeyondInsight for the service account and add it to the group.

> ***Note:*** *Permissions are assigned only to the group, not to the account.*

1. Go to **Configuration > Role Based Access > User Management**.
2. From the **Users** tab, click **Create New User**.
3. Select **Create a New User**.



4. Provide **Identification**, **Credentials**, **Contact Information**, **User Status**, and **Authentication Options** as needed.
5. Click **Create User**.
6. You are taken to the details page for the user account where **Groups** is automatically selected. Select **All Groups** from the **Show** dropdown above the **Groups** grid to list all available user groups.
7. Locate the group you created above for the service account, select it, and then click **Assign Group** above the grid.



> ***Note:*** *In addition to creating user accounts locally, you can import AD, Entra ID, and LDAP accounts and add them to either local or imported groups.*

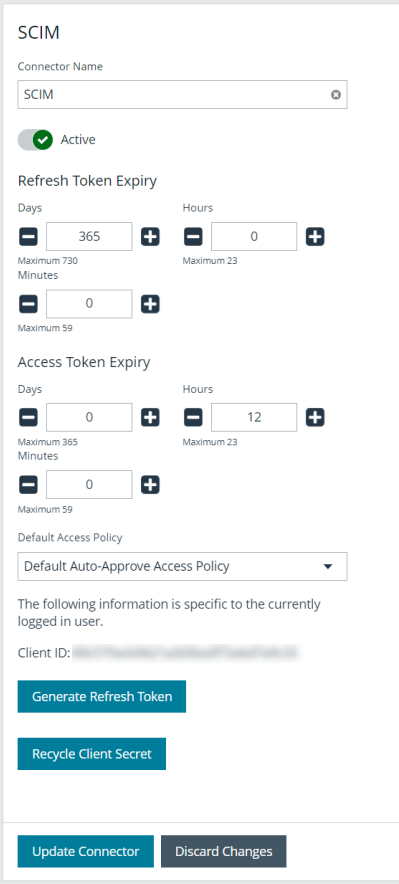
Generate OAuth Credentials

Once the user account is created and assigned to a group, you must log in as the new user to generate OAuth credentials.

1. Go to **Configuration > General > Connectors**.
2. Under **Connectors**, select the SCIM connector. Once selected, the SCIM connector information displays.

> ***Note:*** *Do not select the SailPoint connector. This was available in previous versions of BeyondInsight, but it is an older integration and is not based on SCIM.*

3. Each logged-in account in BeyondInsight has a unique client ID. The **Client ID** is located within the SCIM connector information. Highlight the ID, right-click, and save locally as **client_id** to a text file.
4. Click **Recycle Client Secret**.
5. Click **Recycle** on the **Recycle Secret Access Key** pop-up. This generates a unique access key.
6. Highlight the **Client Secret** access key, right-click, and save as **client_secret** to a text file.
7. Click **Generate Refresh Token** if you want to use this method of authentication. Use the account login password when prompted.



> ***Note:*** *The refresh token is used in the production environment. Client credentials (client ID and client secret) are used in a lab or test environment. Every Password Safe user with full control permissions to the **Options – Connectors** feature can obtain a **Client ID** and **Client Secret** via the connector.*

> ***Note:*** *Only one SCIM connector can be created by Password Safe per instance.*

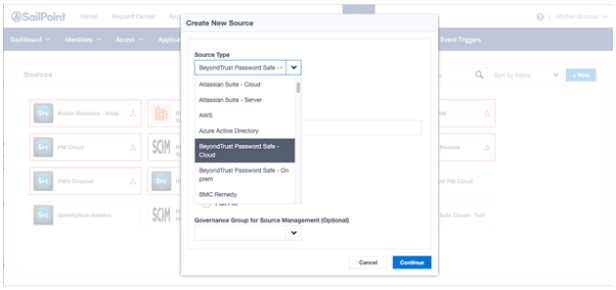
Configure the BeyondTrust Source Type in IdentityNow

BeyondTrust provides an Access Data Source supported by default with IdentityNow. Once IdentityNow has visibility into a data source, it can manage information at the source location.

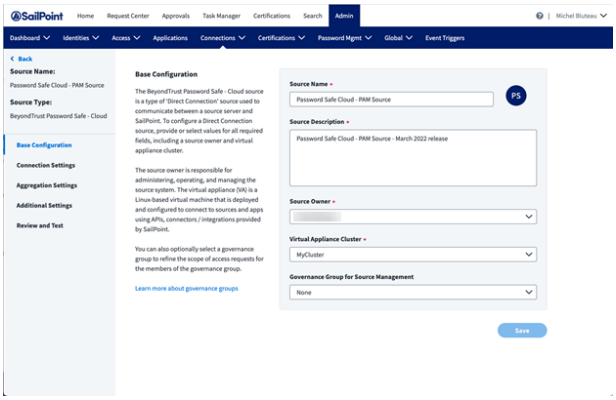
> ***Note:*** *Users must have the appropriate credentials to log in to IdentityNow.*

Configure a Source Type for BeyondTrust

1. In the **IdentityNow** console, go to **Admin > Connections > Sources**.
2. Click the **New** button in the top right corner.
3. Under **Source Type** select **BeyondTrust Password Safe - Cloud**.
4. Include a **Source Name**, **Description**, **Source Owner**, and **Connection Type**.
5. Click **Continue**.

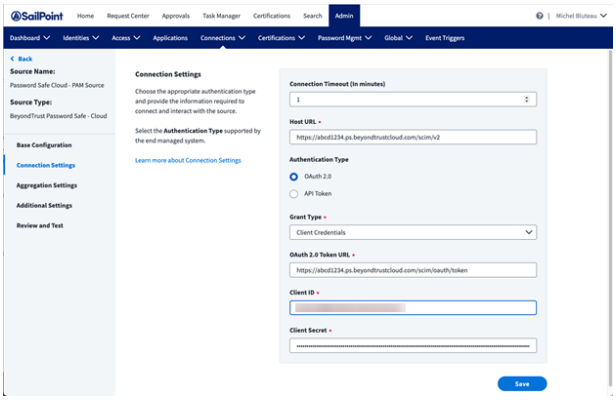


6. On the next screen, under **Base Configuration**, select a **Virtual Appliance Cluster**.
7. Click **Save**.

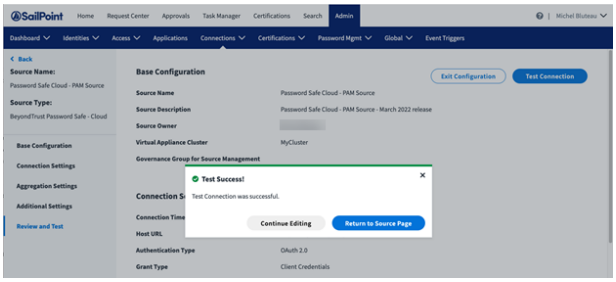


Update Connection Settings

1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. On the next screen, click the **Edit Configuration** button in the top right corner.
3. On the next screen, select **Connection Settings** on the left hand side.
4. For a production environment, select the **API Token** option. For a test environment, select the **OAuth 2.0** option.
5. Fill out the rest of the form as required with information saved earlier in the "Generate OAuth Credentials" on page 47 section.
6. Click **Save**.

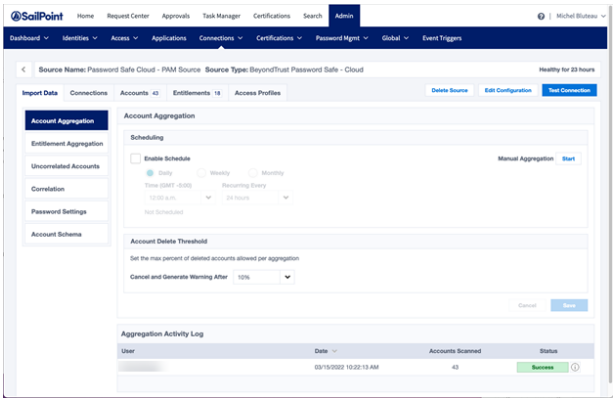


7. Once connection settings have been saved, test the connection:
   a. Select **Review and Test** on the right hand side of the screen.
   b. Click **Test Connection** on the upper left hand side of the screen.



Aggregate Accounts and Entitlements

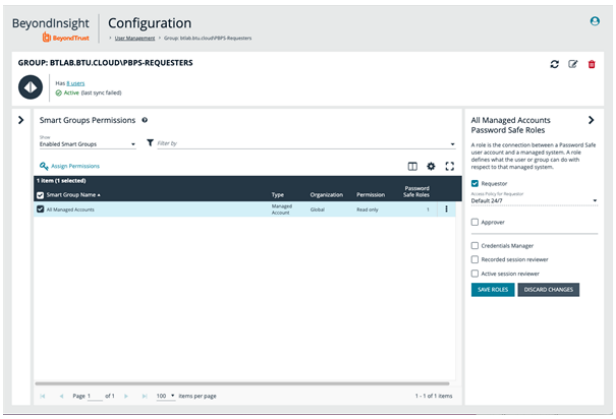
1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. On the next screen, select the **Import Data** tab.
3. Select **Account Aggregation** and enter the necessary information.
4. Click **Save**.
5. Select **Entitlement Aggregation** and enter the necessary information.
6. Click **Save**.



Smart Group Permissions

Within Password Safe, permissions are granted via groups. A Smart Group is a filtered list of managed accounts. All managed accounts are granted the read only permission.

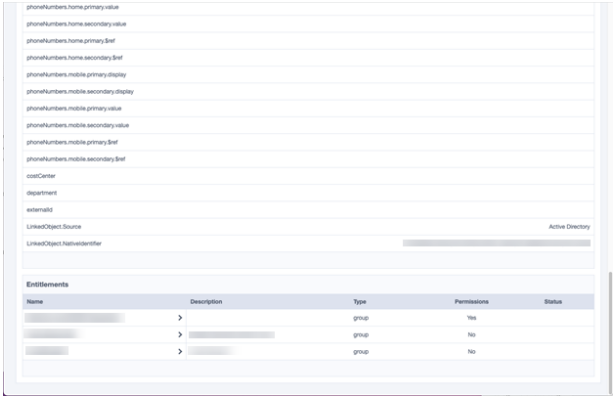
1. In the **Password Safe** console, go to **Configuration > Role Based Access > User Management > Groups**. Select the group and then click on the corresponding ellipsis to right of the group.
2. Select **View Group Details**.
3. Select **Smart Groups** under **Group Details**.
4. Select a managed account and then **Assign Permissions**.
5. Assign permissions as read only.
6. Select the managed account again and then click on the corresponding ellipsis to right of the account.
7. Select **Edit Password Safe Roles**.
8. Assign role as **Requestor**.
9. Select **Access Policy for Requestor** from the drop down.
10. Click **Save Roles**.



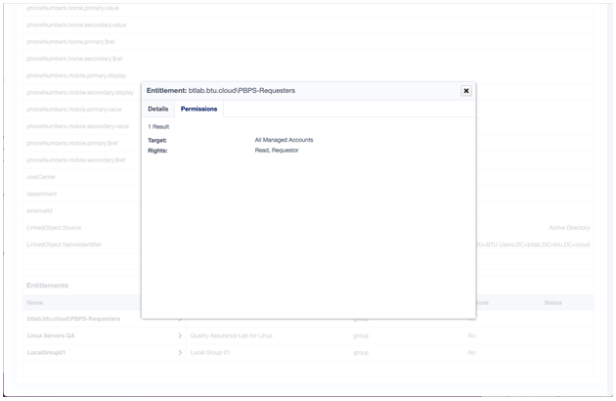
View User Entitlements

To view user entitlements and Password Safe groups assigned to the user:

1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. Select **Accounts**.
3. Select the user.
4. Select **Accounts**.
5. Select the **Source Name**.
6. Scroll to the bottom of the screen to view entitlements.



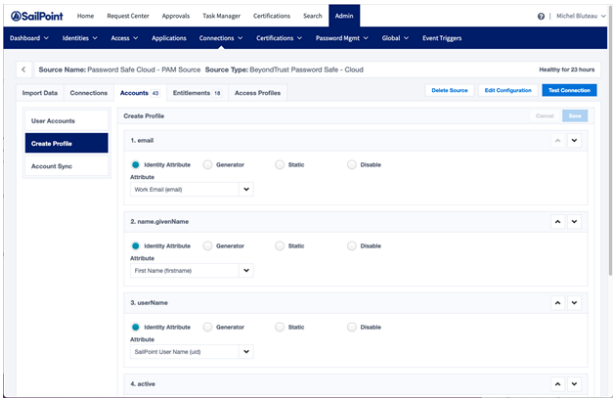
7. To view **Entitlement Details and Permissions**, expand the appropriate user group.
8. Select either the **Details** tab or **Permissions** tab to view information. Here you can find the target (**Smart Group/Rule All Managed Accounts**), **Smart Group Permissions** (Read or Write), and the **Password Safe Role** (Requestor).



Create Profile

BeyondTrust source types come with a preconfigured Create Profile.

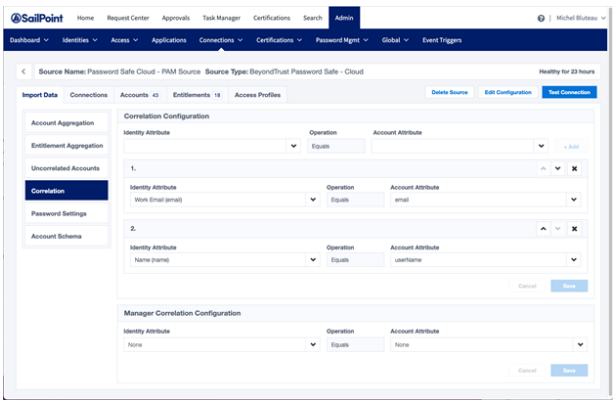
1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. Select **Accounts**.
3. Select **Create Profile**.



Correlation

BeyondTrust source types come with a preconfigured Correlation.

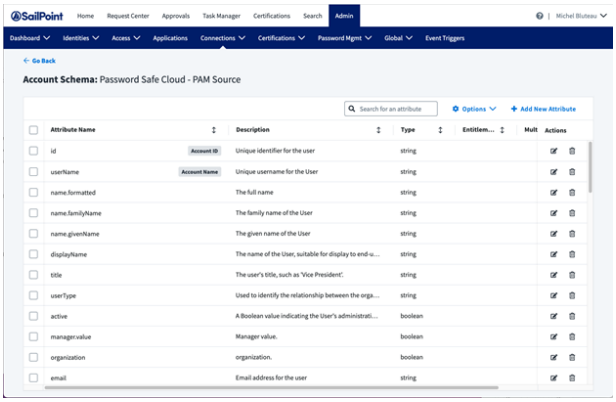
1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. Select **Import Data**.
3. Select **Correlation**.



Schema

BeyondTrust source types come with a preconfigured Schema.

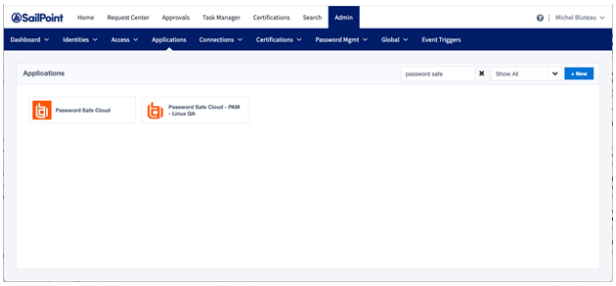
1. In the **IdentityNow** console, go to **Admin > Connections > Sources**. Select the test source.
2. Select **Import Data**.
3. Select **Correlation**.

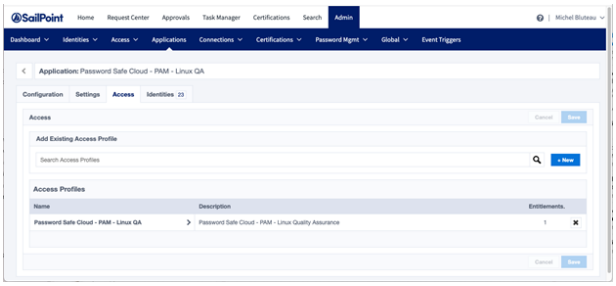


Once the BeyondTrust source is in place, you have access to IdentityNow business processes including Access Request, Access Certification, automated provisioning for Joiner, Mover, Leaver, Search and Analytics, and more.

It is possible to create Access Profiles that consume Password Safe Groups and then assign the Access Profiles to Roles or Applications.

> *For more information on assigning Access Profiles to Roles or Applications, please visit SaaS Product Documentation / IdentityNow at https://documentation.sailpoint.com.*





Configure SNMP Trap and Syslog Event Forwarding

BeyondInsight, Discovery Scanner, Password Safe, and Endpoint Privilege Management products can forward the following:

- SNMP traps using versions 1, 2, or 3
- Events through a syslog daemon

With this forwarding function, it is feasible to integrate critical event information directly into a NMS, SIM, NAC, or other log consolidation, or event management systems.

A standard SNMP MIB, EEYE-REM_EVENT-MIB.MIB, is available for decoding traps at the destination and is located at **C:\Program Files (x86)\BeyondTrust\BeyondInsight**. On a U-Series Appliance with Server 2016, the path is slightly different: either **C:\Program Files (x86)\eEye Digital Security\Retina CS**, or **C:\Program Files (x86)\Security Scanner\Help\Snmp**.

Note: *This MIB is valid for BeyondInsight and Discovery Scanner.*

You can configure SNMP and syslog event forwarding settings from the **Connectors** page. Both protocols work for all data aggregated by BeyondInsight and Discovery Scanner.

Enable SNMP Event Forwarding

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **SNMP Event Forwarder**.
5. Leave **Active (yes)** enabled.
6. Select an **Output Format** and provide the name of the **SNMP Community**.
7. Provide the IP address and port for the SNMP Trap receiver.
8. Select the events that you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.

Enable Syslog Event Forwarding

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Syslog Event Forwarder** under Connector Type.
5. Click **Create Connector** to open Syslog Event Forwarder pane.
6. Leave **Active (yes)** enabled.
7. Provide the required details for the syslog server:
    - Select the Available Output Pipeline:**TCP**, **TCP-SSL**, or **UDP**.
    - Enter **Host Name** and **Port**.

8. Select an output format: **NewLine Delimited**, **Tab Delimited**, or **Comma Delimited**.
9. Select an optional syslog **Facility** from the list.
10. Select **Format Specification**.
11. Select the events that you want to forward.
12. Click **Test Connector** to determine if event is successful.
13. Click **Create Connector**.

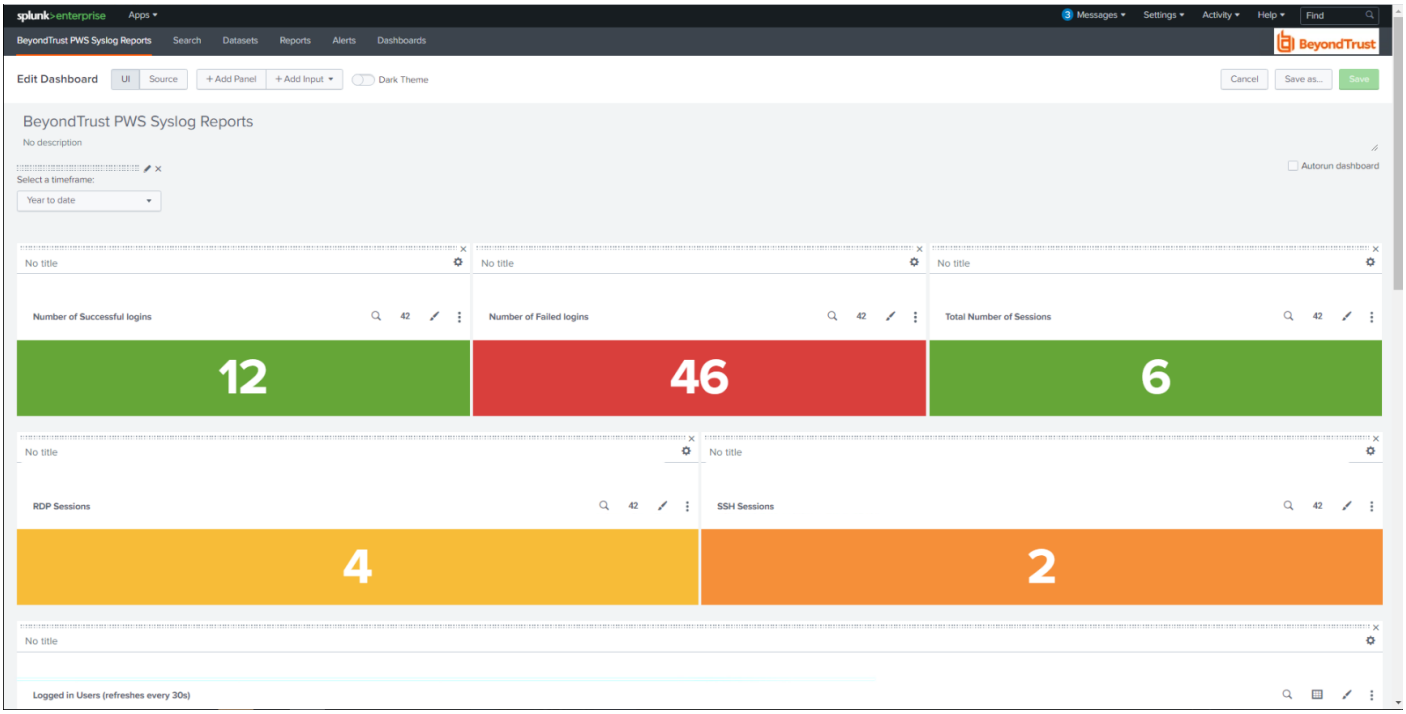
Note: *If an event is received from Password Safe Cloud, a* ***Resource Zone*** *can now be associated with any connector that sends data using syslog. If selected, Password Safe Cloud proxies the syslog data through the Resource Brokers associated with that* ***Resource Zone****.*

Splunk App for Password Safe and Password Safe Cloud

The Splunk App for BeyondTrust Password Safe allows customers to visualize and interpret the large number of events forwarded to Splunk by BeyondTrust. The app consists of a sample of relevant reports in various formats, grouped within a single Dashboard.

Using the Dashboard, customers can more rapidly benefit from the integration between Password Safe and Splunk by leveraging working reports that can be used as is or as templates for custom reports.

The BeyondTrust Password Safe Dashboard:



Prerequisites

Configure Password Safe to forward events to Splunk.

Configure the Splunk Event Forwarder Connector

As a prerequisite, you must configure an HTTP EC data source in Splunk and note the API key for the configuration settings in the following procedure.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Splunk Event Forwarder** from the **Connector Type** list.
5. Click the toggle to enable the **Active (yes)** option. Check **Enable Event Forwarding**.

6. Enter the following details for the Splunk server:
    - **Host Name:** (Required) The host name or IP address for your Splunk server.
    - **Port:** (Required) The port used to communicate with your Splunk instance. The default is **8088**.
    - **API Key:** (Required) The Splunk API Key from your Splunk instance.
    - **Index:** The name of the data repository on the Splunk server.
    - **Source Type:** Data structure identifier for an event. The value is assigned to the event data collected.
    - **Source:** Source value to assign to the event data. For example, set this key to the name of the application you are gathering events from.
    - **Host:** The hostname of the client from which the data is forwarded.
7. Expand **Event Filters**, and then select the events that you want to forward.
8. Click **Test Connector** to send a test event message.
9. Click **Create Connector**.

Validate Events

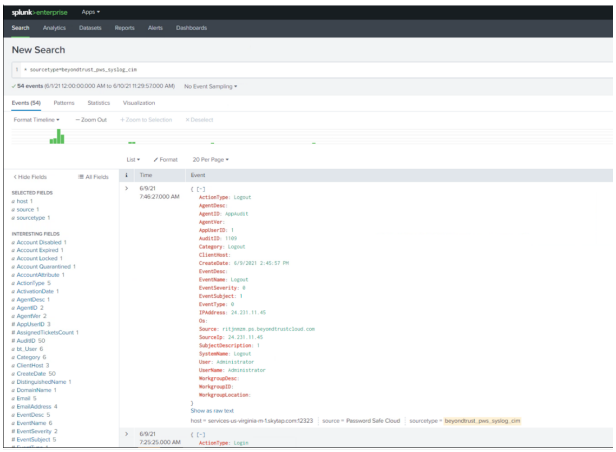
Validate events from Password Safe and/or Password Safe Cloud are received via Data Inputs by Splunk. Adjustments might be required to align with expected values from Reports for **source**, **sourcetype**, and **index**.

Each report in the Dashboard filters data like this:

(source=password_safe OR sourcetype=beyondtrust) index=idx_beyondtrust

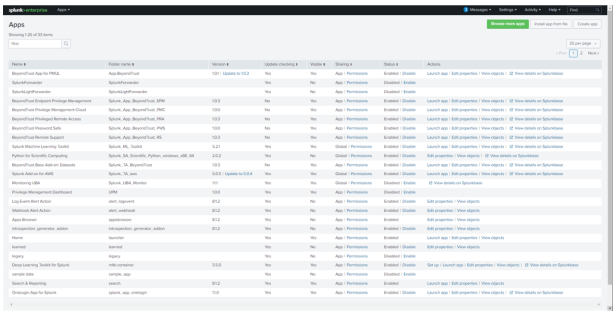
You can create a reserved Data Input for Password Safe in Splunk and assign desired values for the above attributes.

1. Confirm all prerequisites are in place by searching for Password Safe events.

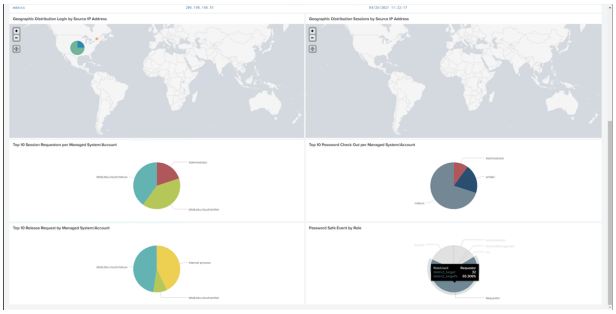


2. Import the app either from Splunkbase or file. Notifications will be received when updates beyond version 1.0 are available.

3. Click **Apps > Manage Apps** to browse Splunkbase and search for the Password Safe App.



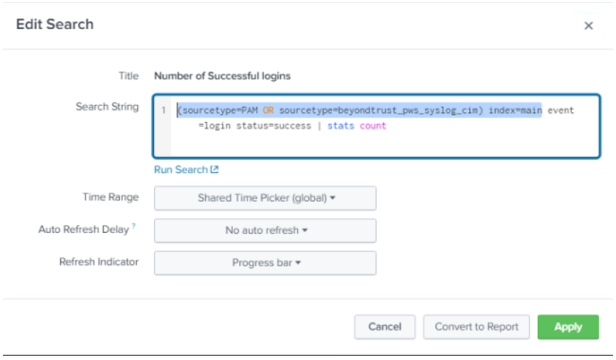
4. Access the Password Safe App Dashboard.



Troubleshooting

If reports don't show any data, there might be a mismatch with **source** or **sourcetype**, and **index**. If Data Inputs or the event forwarder (Password Safe) cannot be configured for the values expected by the reports and associated queries, an alternative is to edit each report query to resolve mismatches. Each report query can also be tested with Splunk Search App.

The screen capture shows an example of a modified query for a report.



Configure Universal Event Forwarder

Create a universal connector to forward events to configured listeners using an XML or JSON format.

1. In BeyondInsight, go to **Configuration > General > Connectors**.
2. From the **Connectors** pane, click **Create New Connector**.
3. Enter a name for the connector.
4. Select **Universal Event Forwarder** from the list.
5. Leave **Active (yes)** enabled.
6. Provide the required details for the server:
    - Select the protocol: **TCP**, **TCP-SSL**, or **UDP**.
    - Enter the **Host Name** and **Port**.
7. Select an output format:
    - **XML**: Displays the events in XML format.
    - **JSON**: Displays the events in JSON format. If this format is selected, enable the **Use Syslog**option to add the syslog header format to the JSON output file. If you use the syslog format, you must select a facility from the list.
8. Expand **Event Filters**, and then select the events that you want to forward.
9. Click **Test Connector** to send a test event message.
10. Click **Create Connector**.