BeyondTrust Technical Integration Guide for SailPoint

SCIM Connector

Overview

The SCIM connector adds a SCIM API to BeyondInsight to allow third party applications to view and modify our users, groups, and smart rule permissions.
This implements http://www.simplecloud.info/ for Password Safe.
It also implements the PAM extension viewable here: https://tools.ietf.org/html/draft-grizzle-scim-pam-ext-00

SailPoint IdentityIQ Integration

IdentityIQ currently supports:
Reading users/groups/smart rules/smart rule permissions into their system
Creating users and adding/removing users to and from groups
Although this is what the IdentityIQ supports, the SCIM connector follows the SCIM and PAM extension spec, so it is possible to assign permissions to groups. IdentityIQ only supports assigning permissions to users at the moment.
To help make configuring the SCIM API in IdentityIQ simple, an application XML pre-build with local and AD user provisioning is available on the BT customer portal.

To configure the IdentityIQ SCIM application manually, there are some configuration differences from the default schema to modify, as follows.
Account Schema:

- Under name, remove middleName, honorificPrefix, and honorificSuffix
- Remove nickName, profileUrl, title, userType, preferredLanguage, locale, timezone
- Remove all email fields and replace with a single "email" field

For the provisioning form, if you intend to create Active Directory users only, the native identifier needs to be populated with the distinguished name. All other fields will be populated with what's in Active Directory. The following is a script to populate IdentityIQ fields 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

1. Log in to BeyondInsight management console and click Configuration.
2. Under General, click Connectors.
3. Click +, and then select SCIM Connector.
4. Provide a name and description for the connector.
5. Set the Access token expiry. This is intended to be short-lived.

6. Set the Refresh token expiry. This is intended to be long-lived. Refresh and Access tokens are an OAuth 2.0 concept.
7. Select Default access policy. If a requestor role is assigned to a group via the SCIM API, this access policy will be assigned. The API does not support assigning different access policies.

Once you enable and save the connector, the API will be available to access. On the Connector page you will see credential information specific to your user account:

- Client ID
- A button to recycle your client secret
- A button to generate a refresh token (you must provide your client secret and login password)

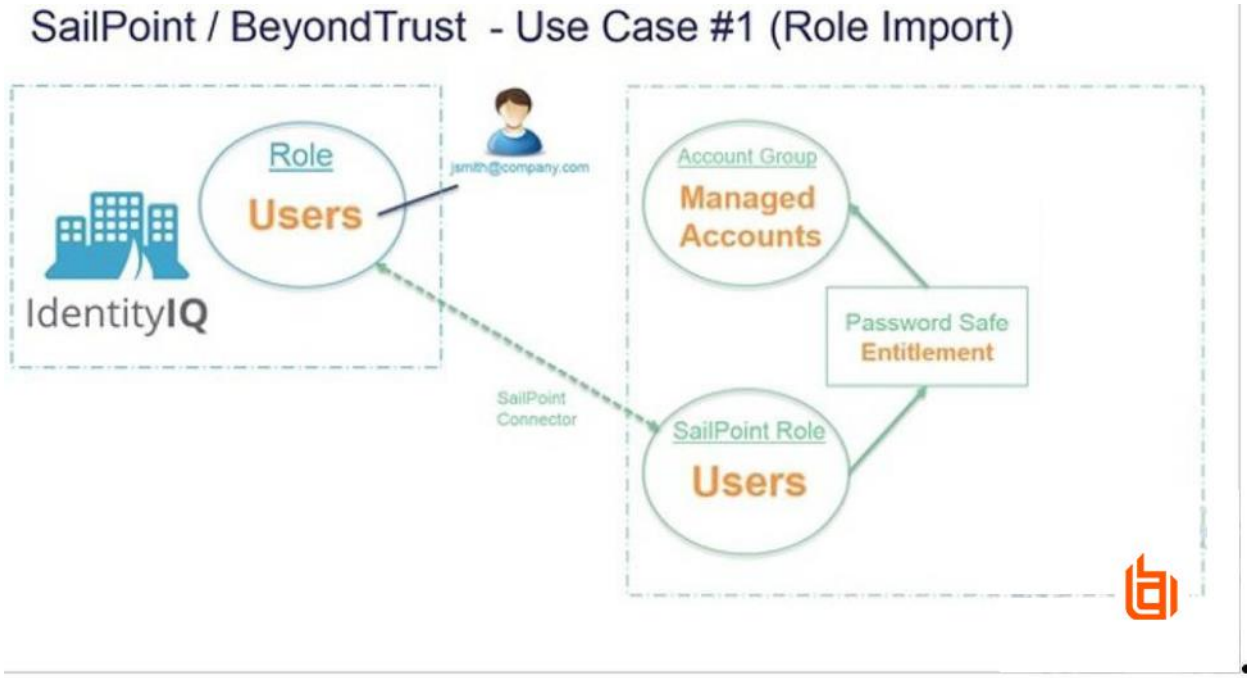
The client ID and secret are part of your credentials for requesting refresh and access tokens. The authentication endpoint is [host]/scim/oauth/token/.
To request a refresh token you would send a POST request with a body in this format:
grant_type=password&client_id=[ClientID]&client_secret=
[ClientSecret]&username=[username]&password=[password]

SailPoint

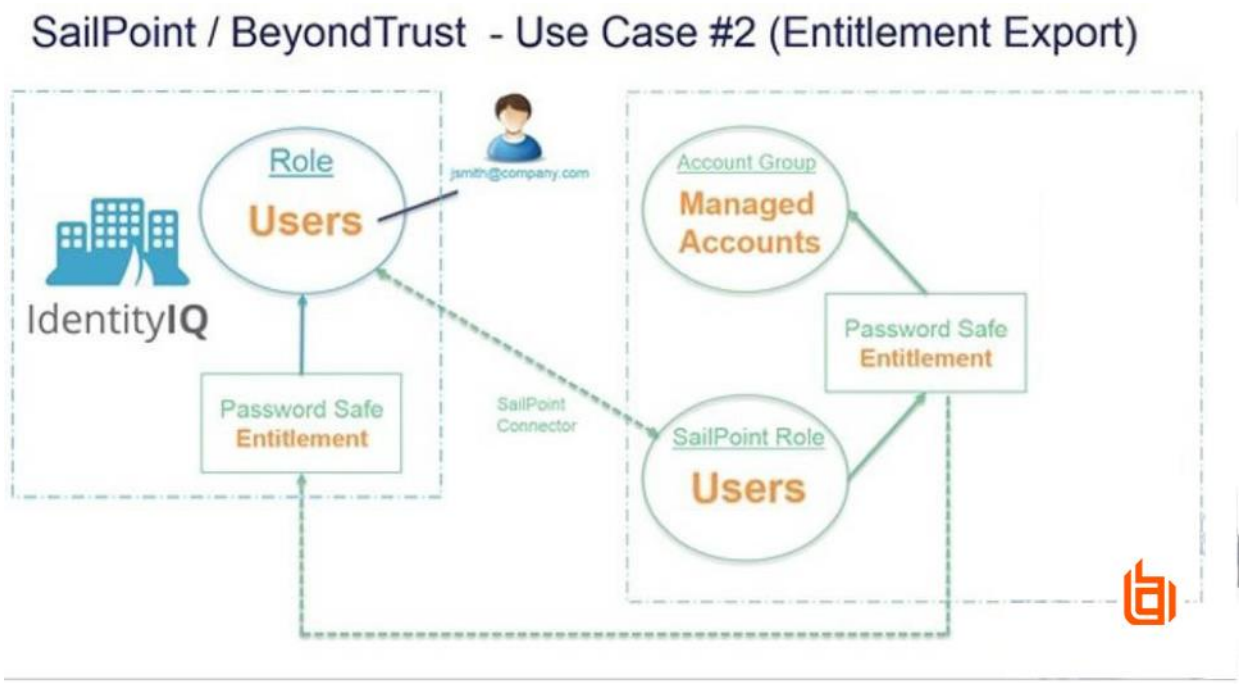
IdentityIQ is an identity and access management solution from SailPoint.
User accounts and roles created in IdentityIQ can be imported and managed in BeyondInsight.

Overview

The following illustrations show the use cases for SailPoint and BeyondInsight.
The first use case imports SailPoint user groups (based on SailPoint roles) in to BeyondInsight.



The second use case, sends and synchronizes permissions in BeyondInsight to IdentityIQ.

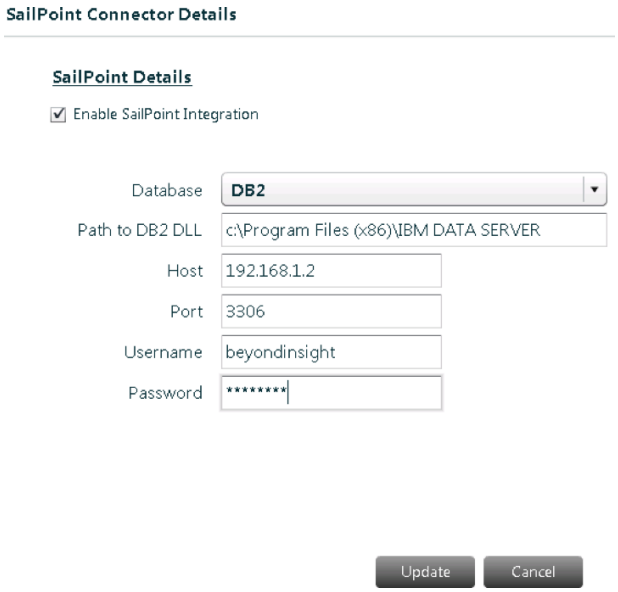


Create the Connector

1. Log on to BeyondInsight management console and click **Configuration**.
2. Under General, click **Connectors**.
3. Click +, and then select **SailPoint Integration**.
4. Select the **Enable SailPoint Integration** check box, and then provide the following information:
   - **Host** - The IP address or host name of the SailPoint instance.
   - **Port** - The port to use to connect to the SailPoint MySQL instance.
   - **Database** - Select a database type from the list: MySQL, Oracle, DB2, Microsoft SQL Server.

Note: If you are using DB2, you must install a driver package on the BeyondInsight server. The name of the package: ibm_data_server_driver_package_win64_v11.1. You can download the package from the following web site:
http://www-01.ibm.com/support/docview.wss?uid=swg21385217. Set the path in the Path to DB2 DLL box as shown in the screen capture.

   - **Username / Password** - The database credential. The user needs Read/Write access to the STI database and Read access to the IdentityIQ database.



5. Click **Update**.

After you create the connector, you can proceed with additional configuration.

Create a SailPoint User Group

1. Log on to BeyondInsightmanagement console and click **Configuration**.
2. Under Role Based Access, click **Users & Groups**.
3. Under User Groups, click +, and then select **SailPoint Group**.

4. Select a SailPoint role from the list that you want toimport.

5. Assign permissions for this group.
6. Click **Create**.

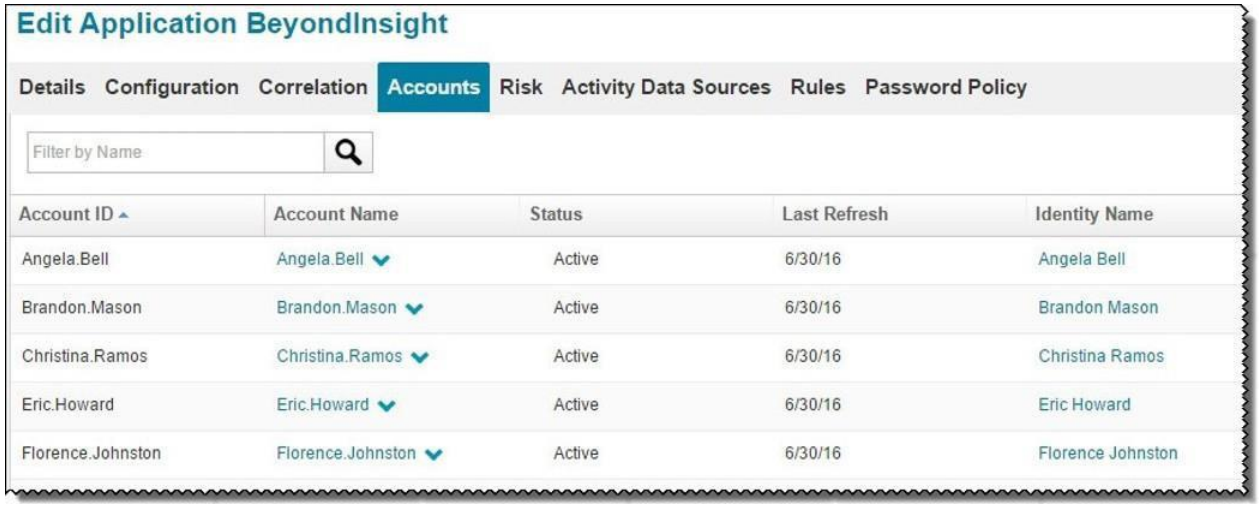
The user accounts will be imported from SailPoint. You can then log on as these users in BeyondInsight and Password Safe using their Active Directory credentials.

Viewing Permissions in IdentityIQ

Periodically the permissions and users will be synchronized with SailPoint.
You can view BeyondInsight and Password Safe permissions in SailPoint by performing the following:

1. Log on to IdentityIQ.
2. You can view the permissions in one of two places. The first is on the BeyondInsight application:
3. Select the **Define** tab, and then select **Applications**.
4. Select BeyondInsight from the list.
5. Click **Accounts**.

You will see all the users associated with BeyondInsight. Click on a user to view BeyondInsightattributes.



The second way to view this data is by finding the user you are interested in:

1. Select the **Define** tab, and then select **Identities**.
2. Enter the user name in the filter criteria box and sear
3. Click the user name to view details.
4. Select the Application Accounts tab.
5. Look for the BeyondInsight application and click the arrow next to it. You will see the BeyondInsight specific attributes for this user.
6. Now that you can access the user specific data, clicking on any of the roles the user is associated with under
7. BeyondInsight's attributes will open a pop-up displaying more information.
8.
9. Navigating to the Object properties tab will display its permissions query which will display all
10. of BeyondInsight's PAM permission data.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralized management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.

BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com