Password Safe

Blue Prism Integration

Integrate Blue Prism with Password Safe

Blue Prism is a global leader in intelligent enterprise automation, improving how employees work. Blue Prism helps organizations enhance operational efficiency by enabling users to automate tasks.

This guide covers how to use Password Safe as the central repository for just-in-time access to credentials in Blue Prism processes for automation.
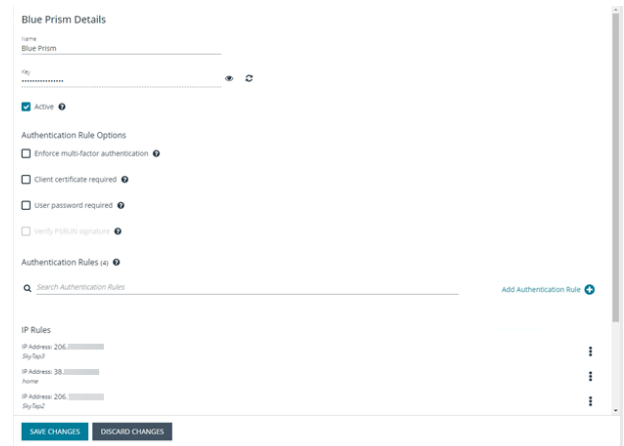
Password Safe provides a secure, flexible, and scalable credential provider for Blue Prism. With the additional support for Secrets Safe, organizations can provide Blue Prism users with the flexibility they need, while aligning with best practices when it comes to the protection and governance of privileged accounts.

> ℹ️ *For more information on obtaining the integration, please see [Blue Prism Digital Exchange](https://digitalexchange.blueprism.com/dx/entry/131112/solution/beyondtrust-password-safe---bring-your-own-credentials) at https://digitalexchange.blueprism.com/dx/entry/131112/solution/beyondtrust-password-safe---bring-your-own-credentials.*

# Create and Configure the Blue Prism Service Account

To configure a Blue Prism service account in Password Safe:

1. Create an API registration for Blue Prism.
2. Add IP rules to give the Blue Prism service account access to the Password Safe API interface.
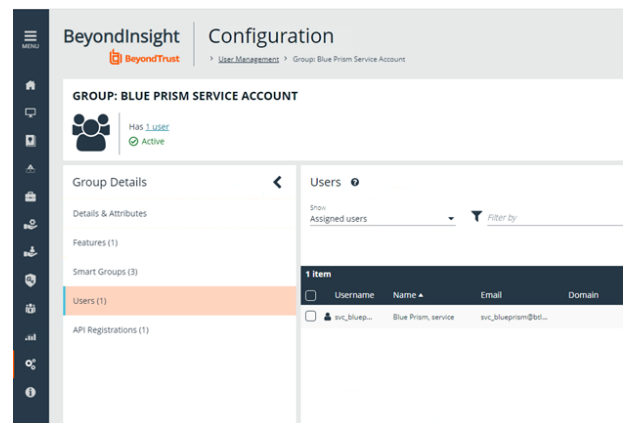
3. Under **Configuration** > **User Management**, create a group for the service account, and assign the API registration to the group.
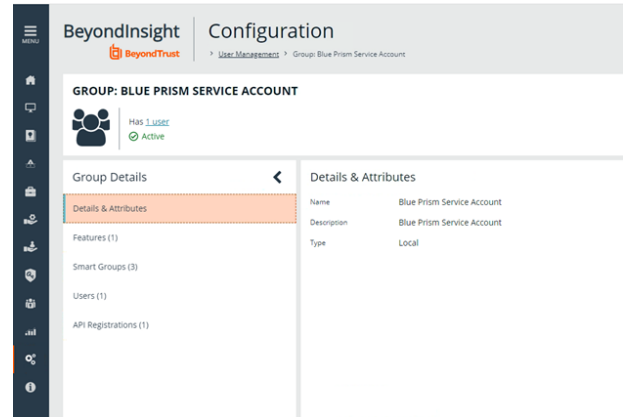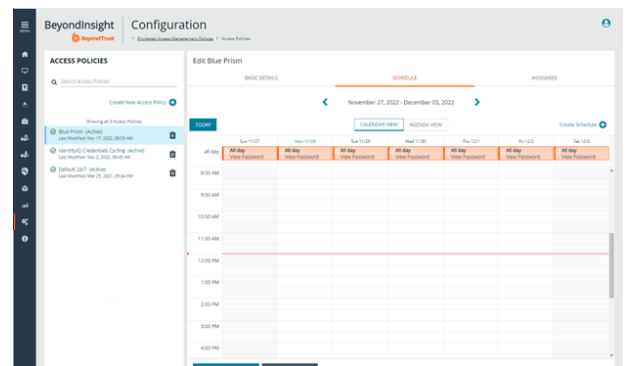

4. Create a user to add to the group. For example, *svc_blueprism*.

> 📌 **Note:** *Permissions are always assigned to a group in Password Safe.*

5. To create an access policy, go to **Configuration > Privileged Access Management Policies > Access Policies**.
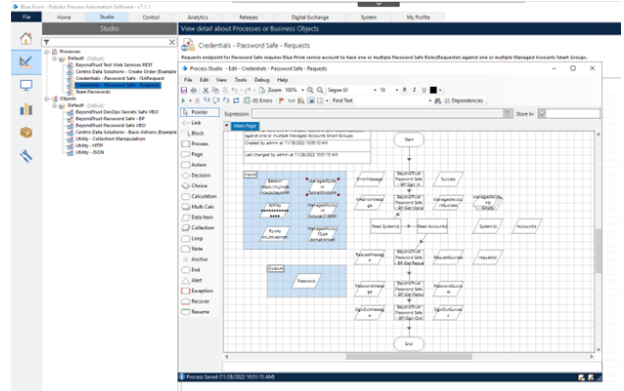
Password Safe User Requests

Configure the group with the **Requestor** role.

1. Add one or more managed account Smart Groups to the newly created group.
2. Add the Password Safe **Requestor** role and the access policy for Blue Prism.
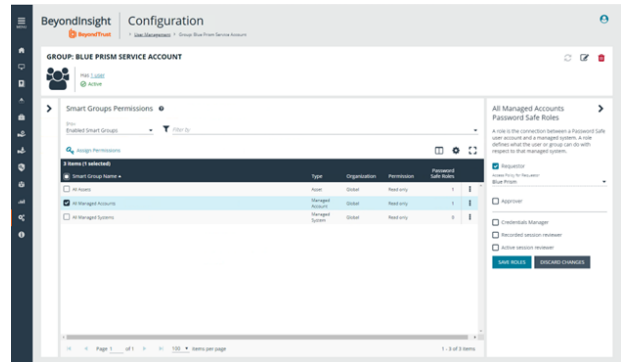
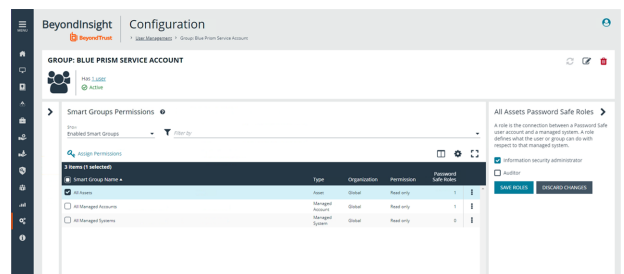3. Populate the Blue Prism inputs with the following:
   - Base URL
   - API key
   - Run As service account name
   - Managed System and Managed Account names, and Managed Account type.

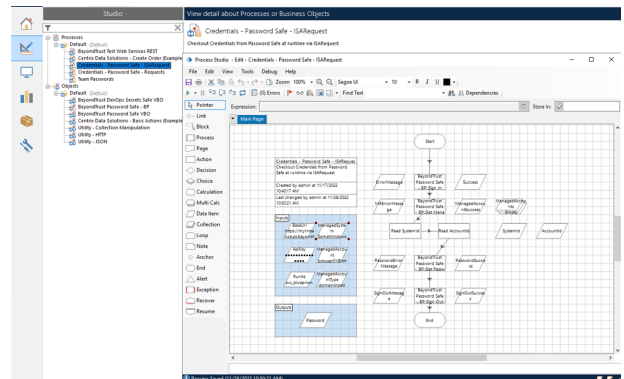# Password Safe ISA (Info Sec Admin) Requests

Configure the Blue Prism group with the Password Safe ISA role.

1. For the group, add the **Information security administrator** role for one or more assets Smart Groups.

2. In Blue Prism, populate the following:

- Base URL
- API key
- Run As service account name
- Managed System
- Managed Account name
- Managed Account type

Password Safe Secrets Safe Requests

Configure the Blue Prism group with the Secrets Safe (formerly, Team Passwords) role.

> **Note:** *When the Password Safe and Blue Prism integration was initially set up, the feature was called Team Passwords. The feature name has since changed to Secrets Safe. The screen captures in this guide show Team Passwords.*

1. For the group, add the feature called *Secrets Safe*, with **Read only** permission.
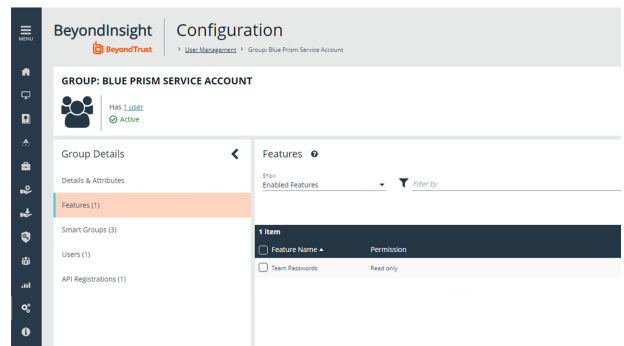
2. Using the process example (shown in the screen capture), provide inputs for the following:

- Base URL
- API key
- Run As service account name
- Folder name
- Credential name
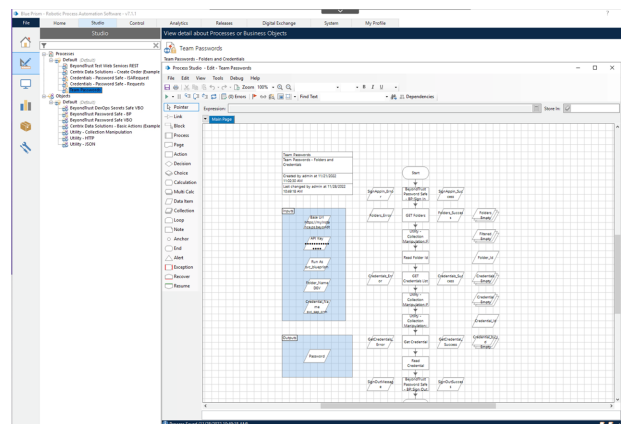
> ℹ️ *For more information about configuring Password Safe, please see:*
>
> - *Configure API Registration at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/configure-api-registration.htm*
> - *Configure Role Based Access at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/role-based-access/index.htm*
> - *Configure Password Safe Access Policies at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/configure-access-policies.htm*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

6

TC: 4/10/2024