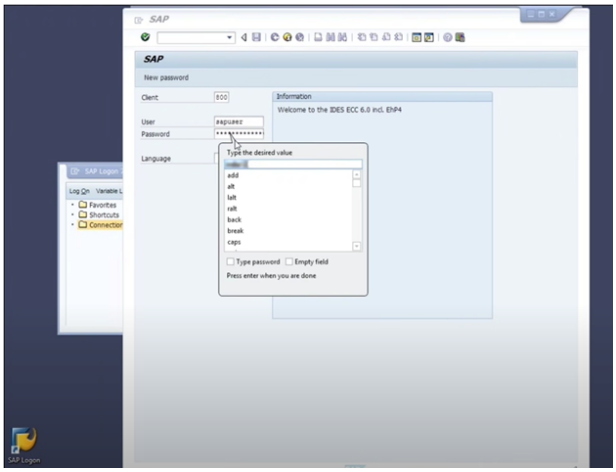
Integrate UiPath Orchestrator with Password Safe

UiPath Orchestrator is a robotic process automation tool used for large-scale end-to-end automation. It allows organizations to automate and orchestrate various processes that would normally require a human worker. Robotic Process Automation, or RPA, allows organizations to free human workers from repetitive tasks like data entry so they can focus on less repetitive and more productive activities.

UiPath provides software robots to automate tasks, for example, data entry via SAP GUI.

Automating data entry in a solution like SAP begins with authentication. UiPath automation supports BeyondTrust Password Safe, Password Safe Cloud, and Secrets Safe (formerly known as Team Passwords). Support for Password Safe managed accounts allows UiPath software robots to check out fresh credentials that are managed by Password Safe for operations (e.g. root account for Linux OS). Support for Secrets Safe allows UiPath users to create and delegate access to pools of credentials that are separate from operational accounts. Secrets Safe allows the grouping of credentials under both local and directory (Active Directory, LDAP) groups, leveraged as secrets. Access to credentials can be granted to individual team members.



The dual support of operational and team-managed credentials allows maximum flexibility from an automation perspective, removing delays and allowing collaborative sharing of credentials while maintaining corporate oversight. Secrets Safe helps improve the user experience for UiPath users.

BeyondTrust privileged access management solutions deliver the visibility and control you need to reduce risk, achieve least privilege, and gain operational efficiency.

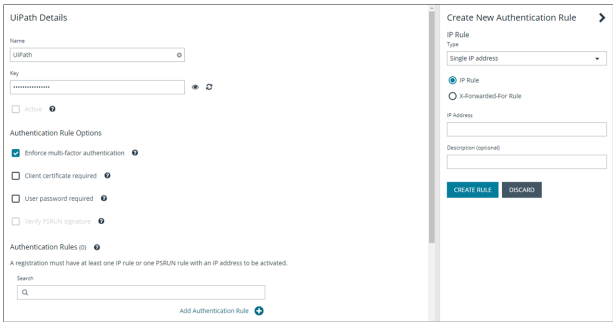
Note: *Orchestrator is available as a cloud service or a standalone product. The standalone product requires an additional integration step, noted below.*

For more information, please see the Orchestrator User Guide at https://docs.uipath.com/orchestrator/. Select the appropriate version to match your delivery of Orchestrator: Automation Cloud, Automation Suite, or Standalone.

Configure UiPath Orchestrator Service Account in Password Safe

Create an API Registration

1. In the **BeyondInsight Console**, go to **Configuration > General > API Registrations**.
2. Click the **Create New API Registration** button.
3. Type *UiPath* in the **API Registration Name** field.
4. Click the **Create API Registration** button.
5. Add an IP Rule to allow Orchestrator to call the Web Service API (REST) for Password Safe.
    a. In the **UiPath Details** pane, under **Authentication Rules**, click the **Add Authentication Rule** button.
    b. Under **IP Rule**, select **Single IP Address** as the **Type**.
    c. Provide the IP Address of your UiPath server or instance.
    d. Click **Create Rule**.



Create a New Group with API Access

Once the API Registration is created, you must assign it to a group. To create a new group:

1. In the **BeyondInsight Console**, go to **Configuration > Role Based Access > User Management > Groups > Create New Group > Create a New Group**.
2. Add a **Group Name** and **Description**, and then click **Create Group**. The **Group Details** page is displayed.
3. Under **Group Details**, select **API Registrations**. Click the check box next to the UiPath API Registration created above to assign it to the group.

You must turn on API access for a Password Safe managed account to be accessible to the API methods.

1. Select **Managed Accounts**.
2. Click the vertical ellipsis button for a managed account, and then select **Edit Account**.
3. Expand **Account Settings**, and then click the toggle to set the **API Enabled** option to **yes**.
4. Click **Update Account**.

Create a New User

Create a new user to add to the group. Delegation is by group only, and not directly with users.

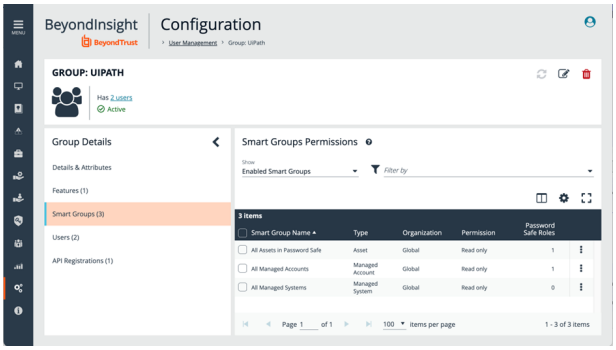
1. In the **BeyondInsight Console**, go to **Configuration > Role Based Access > User Management > Users > Create New User > Create a New User.**
2. On the pop-out screen, provide **Identification**, **Credentials**, **Contact Information**, **User Status**, and **Authentication Options** as needed.
3. Click **Create User**.

4. Return to the **Group Details** page to add the new user to the group:
    a. Go to **Configuration > Role Based Access > User Management > Groups**.
    b. Find the group, and then right click on the ellipsis to the right of that group. Select **View Group Details**.
    c. Under **Group Details**, select **Users**.
    d. Under the **Show** dropdown list, select **Users Not Assigned**. Filter by the name of the user just created, then click the check box to the left of the username.
    e. Click the **Assign User** button to assign the user to the group.

Assign Smart Rules to the Group

Several Smart Groups with Read Only permissions must be added to the newly created group:

1. Go to **Configuration > Role Based Access > User Management > Groups.** Find the group and click on the corresponding ellipsis to the right of the group.
2. Select **View Group Details** from the list.
3. On the next screen, select **Smart Groups** located under **Group Details**.
4. Under **Smart Group Permissions**, a list of **All Smart Groups** is displayed. Check the box next to the following Smart Groups to assign them:
    a. All Assets in Password Safe
    b. All Managed Accounts
    c. All Managed Systems



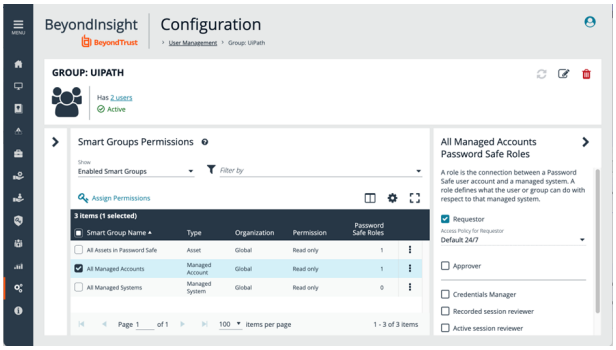
5. Once the Smart Groups are selected, click the **Assign Permissions** button, and then select **Assign Permissions Read Only**.

> ***Note:*** *All Assets in Password Safe, All Managed Accounts, and All Managed Systems, should be replaced with more granular Smart Groups to provide access to a subset of the Accounts and Systems that are accessed by UIPath.*

Add Requestor Role and Access Policy

The All Managed Accounts Smart Group must include a requestor role and an access policy:

1. Right click on the ellipsis to the right of the All Managed Accounts Smart Group. Select **Edit Password Safe Roles**.
2. Click the **Requestor** check box.
3. Select an **Access Policy for Requestor** from the dropdown list.
4. Click **Save Roles**.



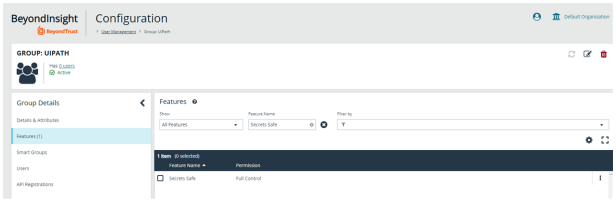
Add Information Security Administrator Role for Assets

1. Right click on the ellipsis to the right of the All Assets in Password Safe Smart Group. Select **Edit Password Safe Roles**.
2. Click on the **Information Security Administrator** check box.
3. Click **Save Roles**.

Add Secrets Safe (Team Passwords) Feature

To add the Secrets Safe feature to your new group:

1. Navigate to your group. Right click on the ellipsis to the right of the group and select **View Group Details**.
2. Under **Group Details**, click on **Features**.
3. Under the **Show** dropdown list, select **All Features**.
4. Filter by **Feature Name**.
5. Type *Secrets Safe* in the **Feature Name** text box.



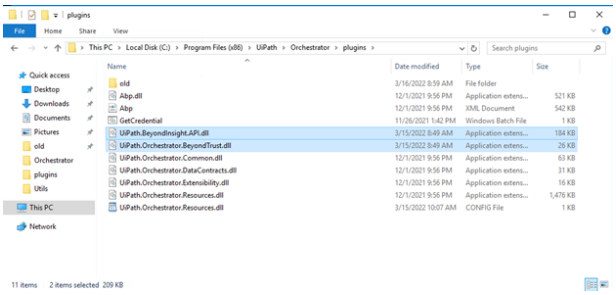
6. Click the check box next to Secrets Safe, and then click the **Assign Permissions** button. Select **Assign Permissions Full Control**.

> ***Note:*** *If including the Secrets Safe feature, you will need to assign ownership or permissions to all Secrets Safe (Team Passwords) credentials available in UiPath.*

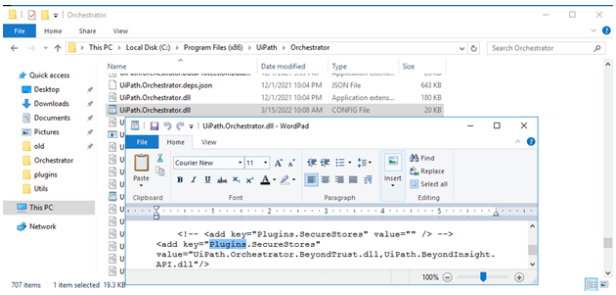
Install and Configure the Integration Plugin with UiPath Orchestrator

> ***Note:*** *This section applies to Orchestrator Standalone only. For more information on installing the plugin, please see BeyondTrust integration at https://docs.uipath.com/orchestrator/standalone/2023.10/user-guide/integrating-credential-stores#beyondtrust-integration.*

Obtain the BeyondTrust plugin zip file (UiPath.SecureStore.BeyondTrust.1.3.0.zip). Copy the two dll files into the plugins subdirectory.



Add the plugins section to the UiPath.Orchestrator.dll.config file found in the Orchestrator directory with the following:



Example:

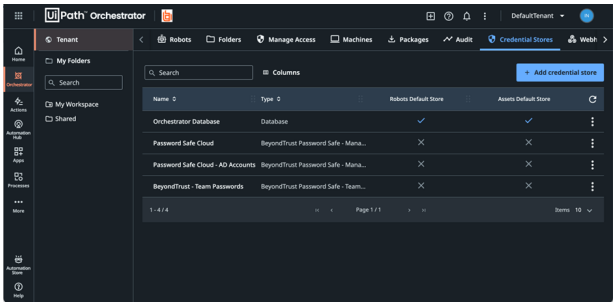
```
<addkey="Plugins.SecureStores"value="UiPath.Orchestrator.BeyondTrust.dll,UiPath.BeyondInsight.API.dll"/>
```

Restart Orchestrator to put the change into effect.

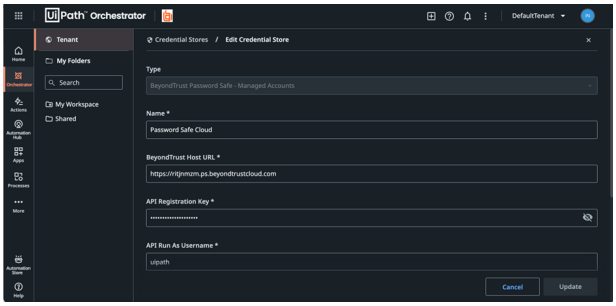
Integrate Password Safe with UiPath

The images below demonstrate how to use the integration from UiPath UI via examples. These images show where to find the integration and how to use it.

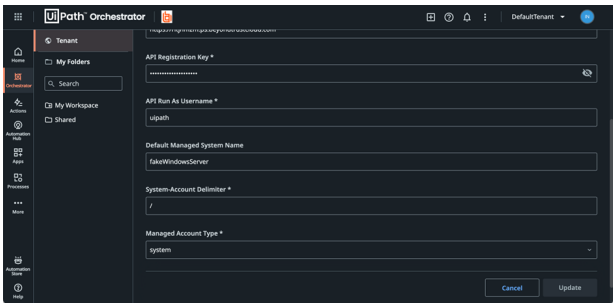
This image shows examples of credential stores created with the integration.



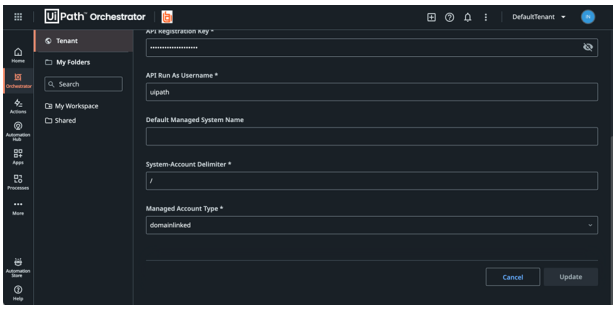
This image displays Password Safe local accounts.



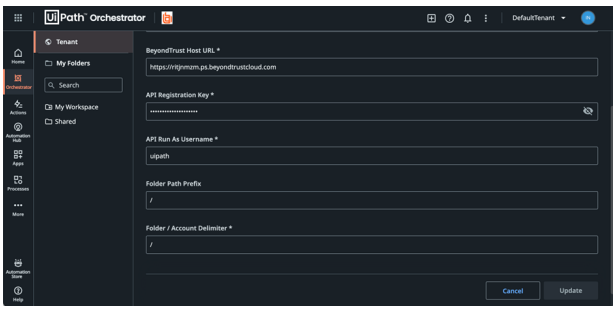
For local account support, select *system* from the **Managed Account Type** dropdown list.



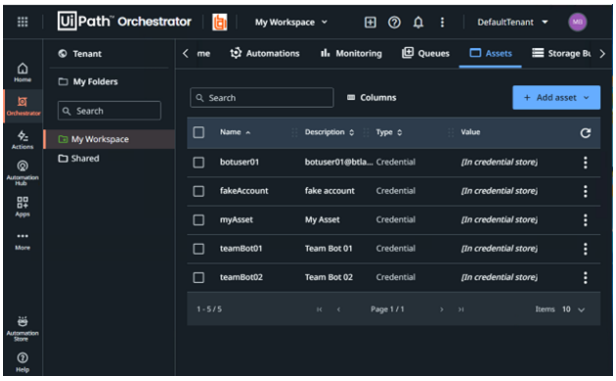
This example uses domainlinked accounts instead of local Managed Accounts. A domainlinked account exists under a directory Managed System, but the account must be linked under an asset (e.g. Windows Server) to be available for UiPath to checkout.



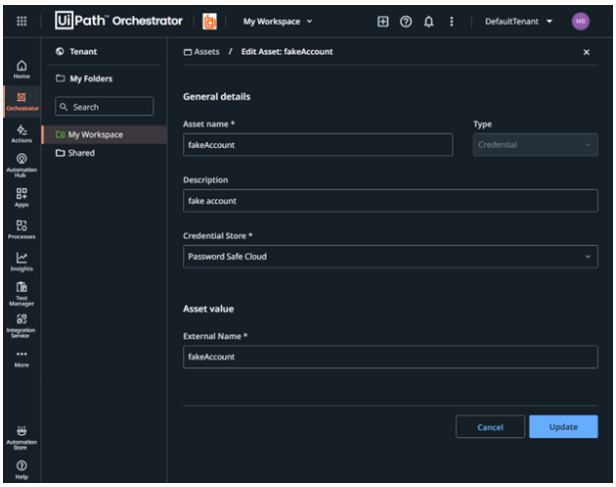
This image displays Secrets Safe (Team Passwords) support.



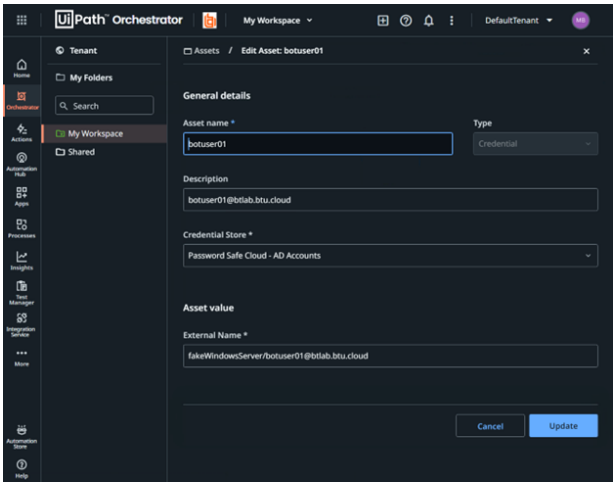
You can create assets in UiPath to act as pointers to credentials managed by Password Safe.



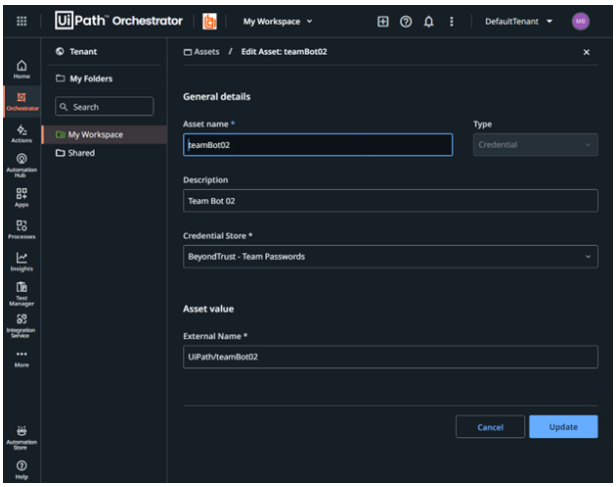
This image shows an asset example for a local account.



This image shows an asset example for a linked account (Active Directory). Managed systems explicitly specified with a forward slash delimiter (/) indicate that they are configured in Credential Store.



This image shows an example of a Secrets Safe (Team Passwords) credential asset.



This image demonstrates a test workflow to check out and display Password Safe assets credentials.