Integrate Automation Anywhere with Password Safe

Automation Anywhere is a leading provider of Robotic Process Automation (RPA) solutions, enabling businesses to automate repetitive and rule-based tasks using software bots. The company's RPA technology is designed to improve operational efficiency, reduce costs, and enhance customer experience.

Automation 360 is Automation Anywhere's web-based automation platform.

This guide covers the steps to integrate Automation 360 with Password Safe to leverage Password Safe credentials.

Setup in Password Safe

Create an API Registration

An API registration must be assigned to the Automation 360 bot, with an IP Filter rule to allow the bot access to the Password Safe API. To create a new API registration:

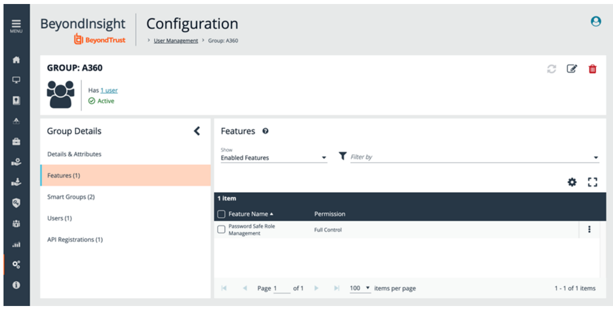
1. In the **BeyondInsight Console**, go to **Configuration** > **General** > **API Registrations**.
2. Click the **Create New API Registration** button.
3. Type a name in the **API Registration Name** field.
4. Click the **Create API Registration** button.
5. Add an IP Rule to allow the bot access to the Password Safe API:
    a. In the **API Registration 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 Automation 360 server or instance.
    d. Click **Create Rule**.

> *For more information, please see Automation 360 IP Address for External Integrations at https://docs.automationanywhere.com/bundle/enterprise-v2019/page/enterprise-cloud/topics/control-room/git-integration/cloud-git-whitelisted-nat-ips.html.*

Create a New Group with API Access

To create a group for the Automation 360 bot in Password Safe:

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**. Check the box next to the Automation 360 API Registration created above to assign it to the group.



Feature Name	Permission
Password Safe Role Management	Full Control

4. Assign the Password Safe Role Management Feature to the new group.
   a. Under **Group Details**, select **Features**.
   b. Under the **Show** dropdown list, select **All Features**.
   c. Filter by **Feature Name**.
   d. Type *Password Safe Role Management* in the **Feature Name** text box.
   e. Check the box next to Password Safe Role Management, and then click the **Assign Permissions** button. Select **Assign Permissions Full Control**.

Assign Smart Rules to the Service Account

The **All Assets** Smart Group with Read Only permissions must be added to the newly created group.

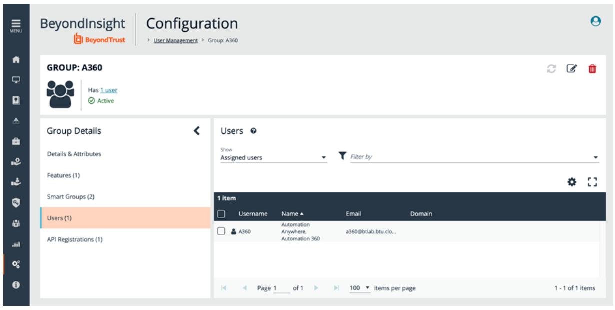
1. Go to **Configuration** > **Role Based Access** > **User Management** > **Groups**. Find the group and click the corresponding ellipsis to the right of the group.
2. Select **View Group Details** from the list.
3. On the next screen, select **Smart Groups**, located under **Group Details**.
4. Under **Smart Group Permissions**, select **All Smart Groups** from the **Show** dropdown list. Check the box next to the **All Assets** Smart Groups to assign it.
5. Once the Smart Group is selected, click the **Assign Permissions** button, and then select **Assign Permissions Read Only**.

Add Information Security Administrator Role for Assets

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

Create a New User and Assign to the Group

A bot service account must be created and assigned to the new group.



Username	Name	Email	Domain
A360	Automation Anywhere, Automation 360	a360@btlab.btu.clo...	

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**, click **Users**.
   d. In the **Show** dropdown list, select **Users Not Assigned**. Filter by the name of the user just created, and then check the box

to the left of the username.

e. Click the **Assign User** button to assign the user to the group.

Select an API-Enabled Local Managed Account

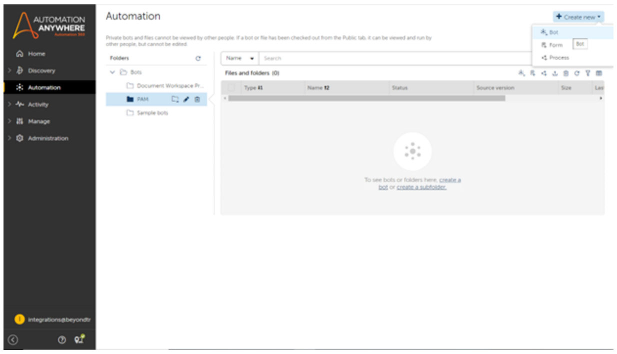
Identify an account that is API-enabled to use as a test account in Automation 360.

1. In the **BeyondInsight Console**, go to **Managed Systems**.
2. Find your managed system, and then right-click the ellipsis to the right of that system. Select **Go To Advanced Details**.
3. Under **Advanced Details**, click **Managed Accounts**.
4. Right-click the ellipsis to the right of the test account and select **Edit Account**.
5. Scroll down to **Account Settings**. Make sure the **API Enabled** toggle button is set to on. Click **Update Account** if required.

Overview of Configuration Steps in Automation 360

The images below demonstrate the steps required by a user to configure Automation 360 for Password Safe.

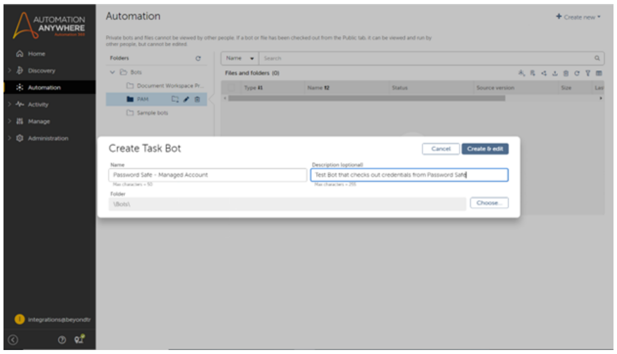
In Automation 360, create a new bot in the appropriate folder.



Private bots and files cannot be viewed by other people. If a bot or file has been checked out from the Public tab, it can be viewed and run by other people, but cannot be edited.

To see bots or folders here, create a bot or create a subfolder.

Provide a name and description. Click **Create and Edit**.



Private bots and files cannot be viewed by other people. If a bot or file has been checked out from the Public tab, it can be viewed and run by other people, but cannot be edited.

Name: Password Safe - Managed Account

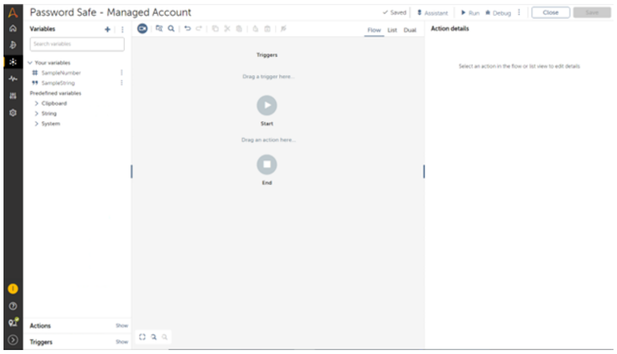
Max characters = 50

Description (optional): Test Bot that checks out credentials from Password Safe

Max characters = 255

Folder: \Bots\

Select **Variables** in the left navigation menu.



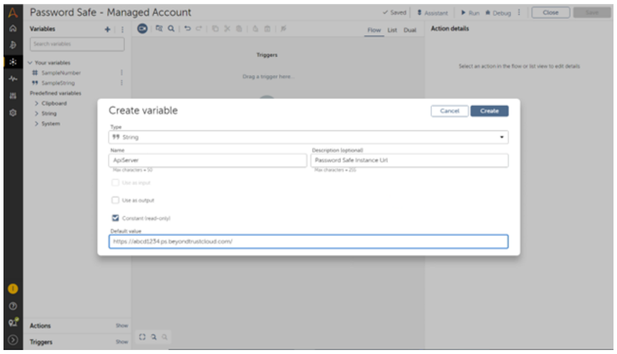
Assign values to the following input variables (string):

- **ApiServer**: Your instance URL (does not include*https://* prefix)
- **Application**: RunAs account for Automation Anywhere in BeyondInsight
- **ApiKey**: API Key for API Registration in BeyondInsight
- **ManagedSystem**: System where managed account is located
- **ManagedAccount**: Account that contains the password to check out, API enabled

Define the following runtime variables:

- **access_output** (dictionary)
- **access_token** (string)
- **checkout_output** (dictionary)
- **ManagedAccount_output** (dictionary)
- **systemID** (string)
- **accountID** (string)
- **password** (string)

Example: **ApiServer** input variable. Replace value with instance URL.



Type: String

Name: ApiServer

Description (optional): Password Safe Instance Url

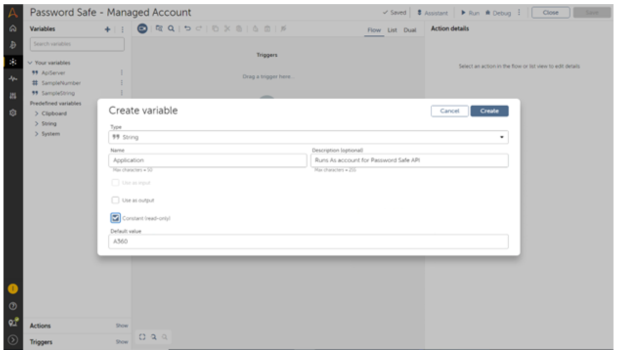
□ Use as input

□ Use as output

☑ Constant (read-only)

Default value: https://abcd1234.ps.beyondtrustcloud.com/

Create the **application** variable that contains the API Run As user account name.



Type: String

Name: Application

Description (optional): Runs As account for Password Safe API

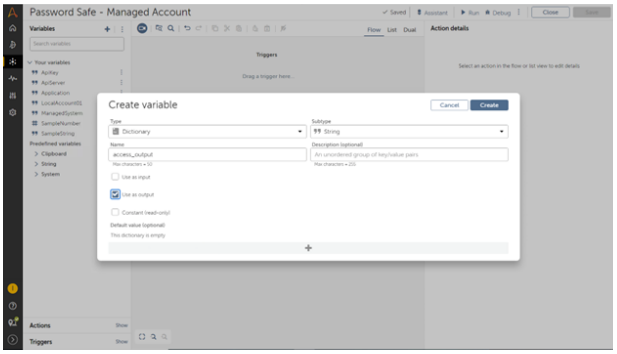
□ Use as input

□ Use as output

☑ Constant (read-only)

Default value: A360

This image displays the **access_output** variable.

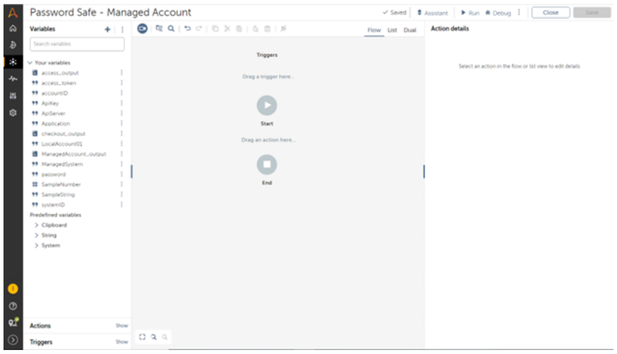


Password Safe - Managed Account

Create variable

Type: Dictionary
Subtype: String
Name: access_output
Description (optional): An unordered group of key/value pairs
☐ Use as input
☑ Use as output
☐ Constant (read-only)
Default value (optional): This dictionary is empty

Ensure that your variables resemble those listed below:



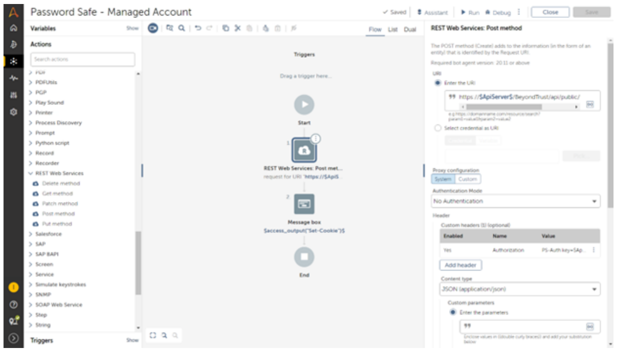
Password Safe - Managed Account

Your variables:

- access_output
- access_token
- accountID
- ApiKey
- ApiServer
- Application
- checkout_output
- LocalAccount01
- ManagedAccount_output
- ManagedSystem
- password
- SampleNumber
- SampleString
- systemID

Add **Actions** from the left menu to allow the bot to check out credentials at run time from Password Safe. Start with **Authentication**, which requires a POST method.

REST Web Services (POST method) for authentication.



Password Safe - Managed Account

REST Web Services: Post method

The POST method (Create) adds to the information (in the form of an entity) that is identified by the Request URI.

Required bot agent version: 20.11 or above

URI
● Enter the URI
https://$ApiServer$/BeyondTrust/api/public/
e.g.https://domainname.com/resource/search?param0=value0&param2=value2
○ Select credential as URI

Proxy configuration: System | Custom
Authentication Mode: No Authentication

Header
Custom headers (1) (optional)

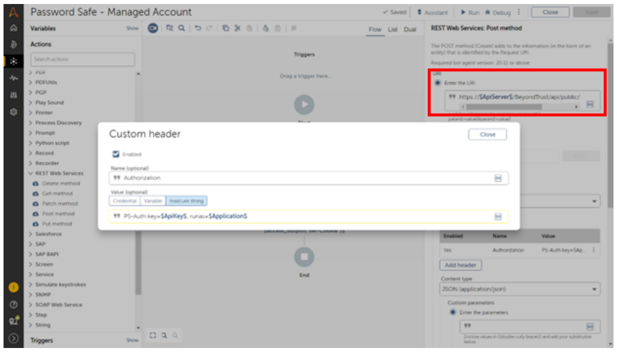
Enabled	Name	Value
Yes	Authorization	PS-Auth key=$Ap...

Content type: JSON (application/json)
Custom parameters
● Enter the parameters
Enclose values in {{double curly braces}} and add your substitution below

1. REST Web Services: Post met... request for URI "https://Api...
2. Message box $access_output{"Set-Cookie"}$

Add the following **URI**: *https://$APIServer$/BeyondTrust/api/public/v3/auth/SignAppin*

Add the following **Header**: *Authorization = PS-Auth key=$ApiKey$; runas=$Application$;*



Password Safe - Managed Account

REST Web Services: Post method

URI
● Enter the URI
https://$ApiServer$/BeyondTrust/api/public/

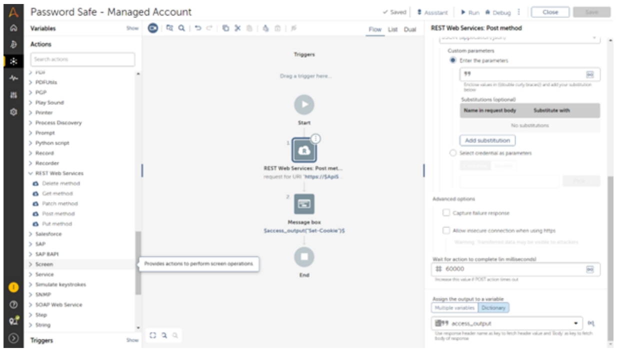
Custom header

☑ Enabled
Name (optional): Authorization
Value (optional): Credential | Variable | Insecure string
PS-Auth key=$ApiKey$; runas=$Application$

Enabled	Name	Value
Yes	Authorization	PS-Auth key=$Ap...

Content type: JSON (application/json)

Assign the output to a variable from the dictionary: **access_output**.



Password Safe - Managed Account

REST Web Services: Post method

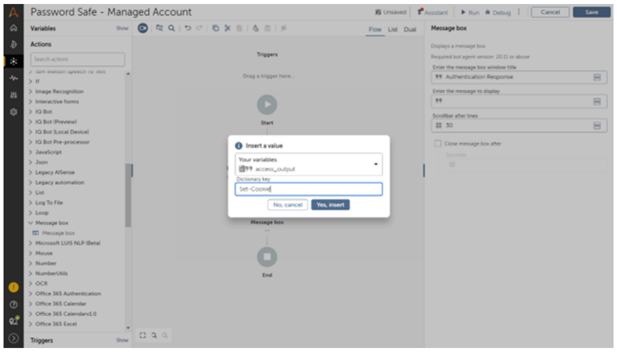
Wait for action to complete (in milliseconds): 60000

Assign the output to a variable: Dictionary

access_output

Message box: $access_output{"Set-Cookie"}$

For troubleshooting purposes, add a message box to display the output of the authentication action. This screen demonstrates the setup to display the session cookie.



Insert a value

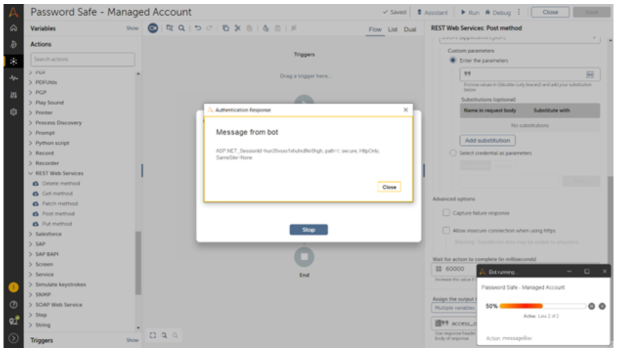
Your variables: access_output

Dictionary key: Set-Cookie

Enter the message box window title: Authentication Response

Scrollbar after lines: 30

This screen displays the message box with the session cookie.



Authentication Response

Message from bot

ASP.NET_SessionId=hun35vsxx1xhuhrdfei5hgh; path=/; secure; HttpOnly; SameSite=None

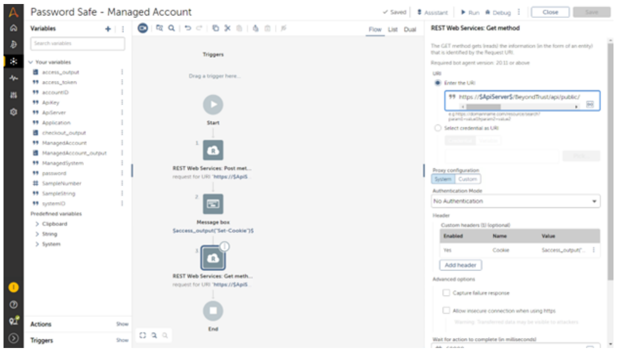
Add an action to retrieve the managed system and account IDs using the GET method.

Add the following **URL**:

https://$ApiServer$/BeyondTrust/api/public/v3/ManagedAccounts?systemName=$ManagedSystem$&accountName=$ManagedAccount$&type=system

Add the following **Header**:

Authorization = PS-Auth key=$ApiKey$; runas=$Application$; Header: Cookie = $access_output{"Set-Cookie"}$

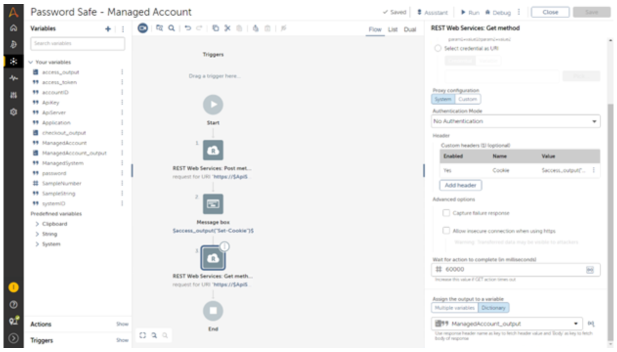


REST Web Services: Get method

Authentication Mode: No Authentication

Custom headers: Yes | Cookie | $access_output{"...

Assign output to dictionary variable **ManagedAccount_output**.



Password Safe - Managed Account

REST Web Services: Get method

Proxy configuration: System

Authentication Mode: No Authentication

Custom headers (1) (optional)

Enabled	Name	Value
Yes	Cookie	$access_output['...

Advanced options

□ Capture failure response

□ Allow insecure connection when using https

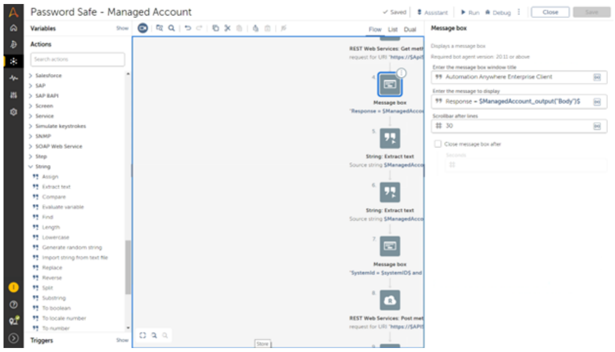
Wait for action to complete (in milliseconds): 60000

Assign the output to a variable: Dictionary

ManagedAccount_output

Use response header name as key to fetch header value and 'Body' as key to fetch body of response

Display the response from GET managed accounts action via a message box.



Password Safe - Managed Account

Message box

Displays a message box

Required bot agent version: 20.11 or above

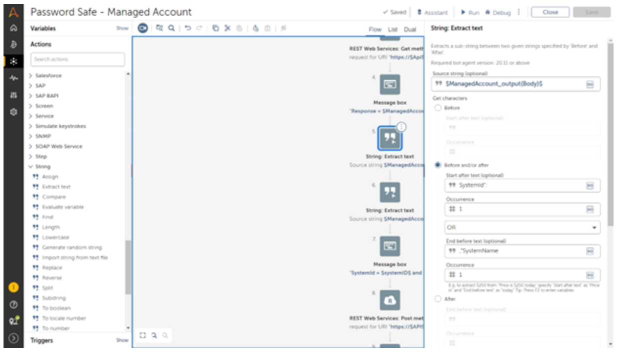
Enter the message box window title: Automation Anywhere Enterprise Client

Enter the message to display: Response = $ManagedAccount_output{"Body"}$

Scrollbar after lines: 30

□ Close message box after

Extract SystemId from ManagedAccount_output and assign the output to variable **systemID**.



Password Safe - Managed Account

String: Extract text

Extracts a sub-string between two given strings specified by 'Before' and 'After'.

Required bot agent version: 20.11 or above

Source string (optional): $ManagedAccount_output{Body}$

Get characters

○ Before

● Before and/or after

Start after text (optional): SystemId":

Occurrence: 1

OR

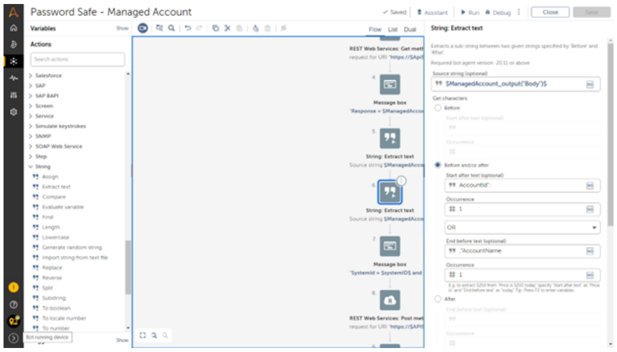
End before text (optional): ,"SystemName

Occurrence: 1

E.g. to extract $250 from 'Price is $250 today' specify 'Start after text' as 'Price is' and 'End before text' as 'today'. Tip: Press F2 to enter variables.

○ After

Extract AccountId from ManagedAccount_output and assign the output to variable **accountID**.



Password Safe - Managed Account

String: Extract text

Extracts a sub-string between two given strings specified by 'Before' and 'After'.

Required bot agent version: 20.11 or above

Source string (optional): $ManagedAccount_output{"Body"}$

Get characters

○ Before

● Before and/or after

Start after text (optional): AccountId":

Occurrence: 1

OR

End before text (optional): ,"AccountName

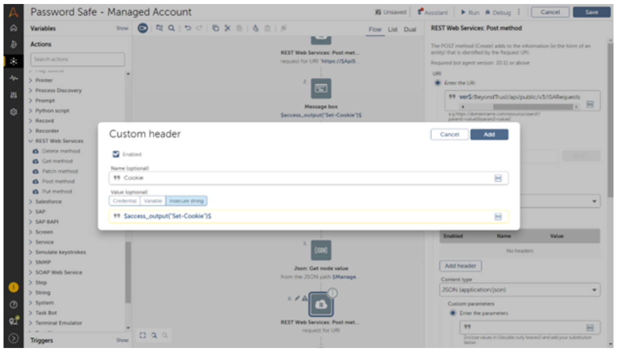
Occurrence: 1

E.g. to extract $250 from 'Price is $250 today' specify 'Start after text' as 'Price is' and 'End before text' as 'today'. Tip: Press F2 to enter variables.

○ After

Now that you have SystemId and AccountId, use the ISA Request call via the POST method to check out credentials for the managed account.

Add the action to check out the credentials for the managed account by ID.


Password Safe - Managed Account
Variables
Actions
Flow
List
Dual
Cancel
Save
REST Web Services: Post met...
Message box
Json: Get node value
REST Web Services: Post met...

REST Web Services: Post method

The POST method (Create) adds to the information (in the form of an entity) that is identified by the Request URI.

Required bot agent version: 20.11 or above

URI

● Enter the URI

ver$/BeyondTrust/api/public/v3/ISARequests

Custom header

☑ Enabled

Name (optional): Cookie

Value (optional): Credential | Variable | [✓ Insecure string]

$access_output{"Set-Cookie"}$

Cancel | Add

Enabled	Name	Value
No headers		

Add header

Content type: JSON (application/json)

Custom parameters

● Enter the parameters

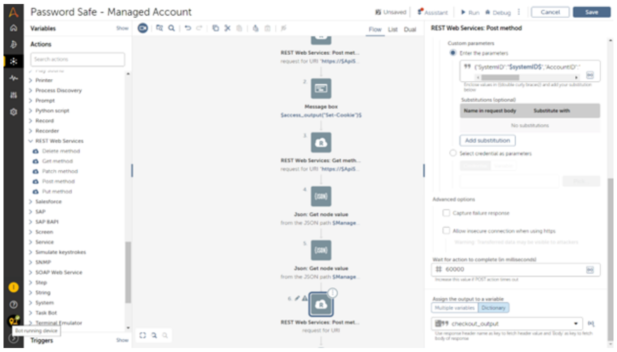
JSON content and output to checkout_output.

Add the following **URI**: *https://$APIServer$/BeyondTrust/api/public/v3/ISARequests*

Add the following **Header**:*Authorization = PS-Auth key=$ApiKey$; runas=$Application$;*

Add the following **Header**:*Cookie = $access_output{"Set-Cookie"}$*

JSON Body: *{"SystemID":"$systemID$","AccountID":"$accountID$"," DurationMinutes":"1","Reason":" AA test"}*


Password Safe - Managed Account
Variables
Actions
Cancel
Save
REST Web Services: Post met...
Message box
REST Web Services: Get meth...
Json: Get node value
Json: Get node value
REST Web Services: Post met...

REST Web Services: Post method

Custom parameters

● Enter the parameters

{"SystemID":"$systemID$","AccountID":"

Enclose values in {{double curly braces}} and add your substitution below

Substitutions (optional)

Name in request body	Substitute with
No substitutions	

Add substitution

○ Select credential as parameters

Advanced options

□ Capture failure response

□ Allow insecure connection when using https

Warning: Transferred data may be visible to attackers

Wait for action to complete (in milliseconds): 60000

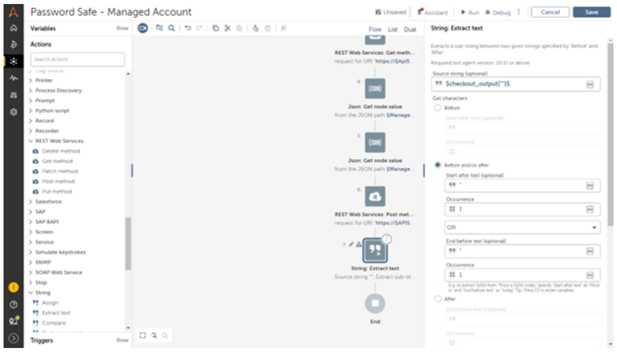
Increase this value if POST action times out

Assign the output to a variable: Multiple variables | [✓ Dictionary]

checkout_output

Use response header name as key to fetch header value and 'Body' as key to fetch body of response

Use a string action to extract text and remove the double quotes from checkout output. Assign the output to variable **password**.


Password Safe - Managed Account
Variables
Actions
Cancel
Save
REST Web Services: Get meth...
Json: Get node value
Json: Get node value
REST Web Services: Post met...
String: Extract text
End

String: Extract text

Extracts a sub-string between two given strings specified by 'Before' and 'After'.

Required bot agent version: 20.11 or above

Source string (optional): $checkout_output{""}$

Get characters

○ Before

● Before and/or after

Start after text (optional): "

Occurrence: 1

OR

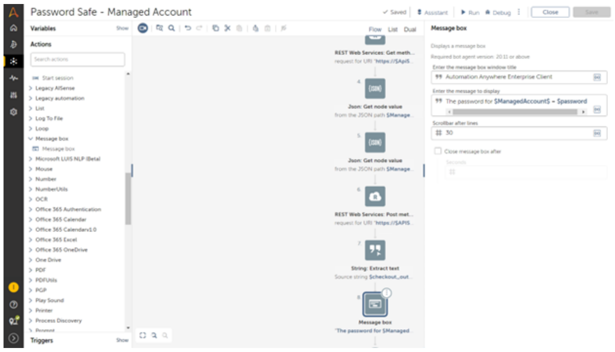
End before text (optional): "

Occurrence: 1

E.g. to extract $250 from "Price is $250 today" specify 'Start after text' as "Price is" and 'End before text' as "today". Tip: Press F2 to enter variables.

○ After

Add a Message action to display the password for the managed account.



Message box

Displays a message box

Required bot agent version: 20.11 or above

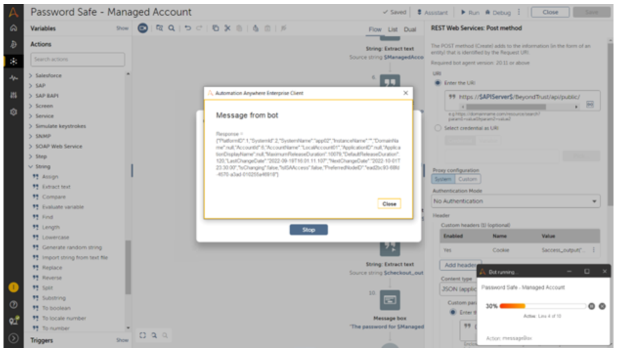
Enter the message box window title: Automation Anywhere Enterprise Client

Enter the message to display: The password for $ManagedAccount$ = $password

Scrollbar after lines: 30

□ Close message box after

The message box displays the response from GET managed accounts action.

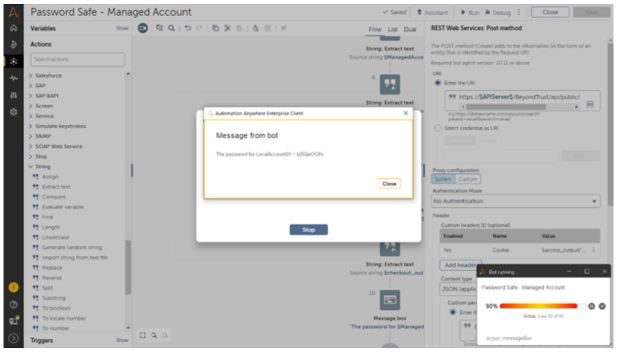


Password Safe - Managed Account
Automation Anywhere Enterprise Client
Close
Stop

Message from bot

```
Response =
{"PlatformID":1,"SystemId":2,"SystemName":"app02","InstanceName":"","DomainName":null,"AccountId":6,"AccountName":"LocalAccount01","ApplicationID":null,"ApplicationDisplayName":null,"MaximumReleaseDuration":10079,"DefaultReleaseDuration":120,"LastChangeDate":"2022-09-19T16:01:11.107","NextChangeDate":"2022-10-01T23:30:00","IsChanging":false,"IsISAAccess":false,"PreferredNodeID":"ead2bc93-68fd-4570-a3ad-010255a46918"}
```

The message box displays the password checked out for the managed account and available to the bot.



Password Safe - Managed Account
Automation Anywhere Enterprise Client
Close
Stop

Message from bot

The password for LocalAccount01 = IzBQeOC6x

For more information, please see Managed Accounts at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/api/password-safe/managed-accounts.htm.