Blue Prism Labs

Lab 5: Credential Manager

Document Revision 1.0

Trademarks and copyrights

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom
Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Contents

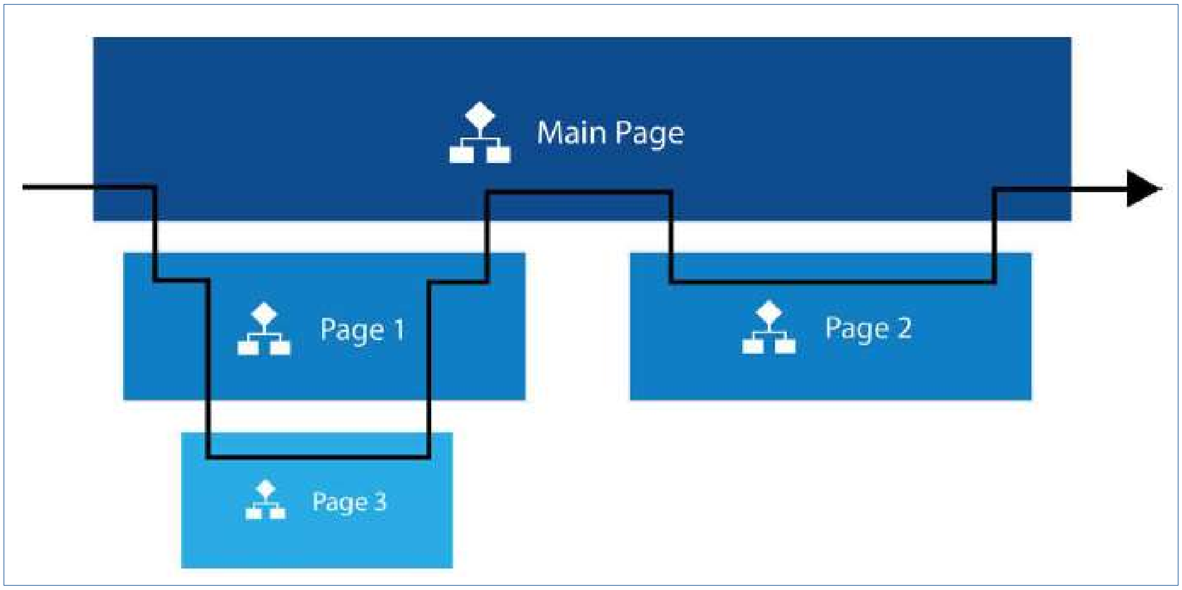
Introduction

Very often a Digital Worker may have to enter credentials to access one or more applications. System access information should always be stored in a secure and encrypted store such as the Blue Prism Credentials Manager. Blue Prism can also integrate with third party credential managers, such as CyberArk.

The Blue Prism Credential Manager provides several functions and features for the secure storage of the user credentials which are used to access target applications. By encrypting and storing credentials securely, Blue Prism can log into applications within a secure runtime environment whilst preventing the casual user or developer from re-using those credentials away from the production environment.

This lab will cover some important concepts around the built in Blue Prism Credential Management. This lab also introduces the concept of breaking a process down into a single main page and sub-pages. We will use a sub-page to retrieve and use credentials to login to Blueprism.com.

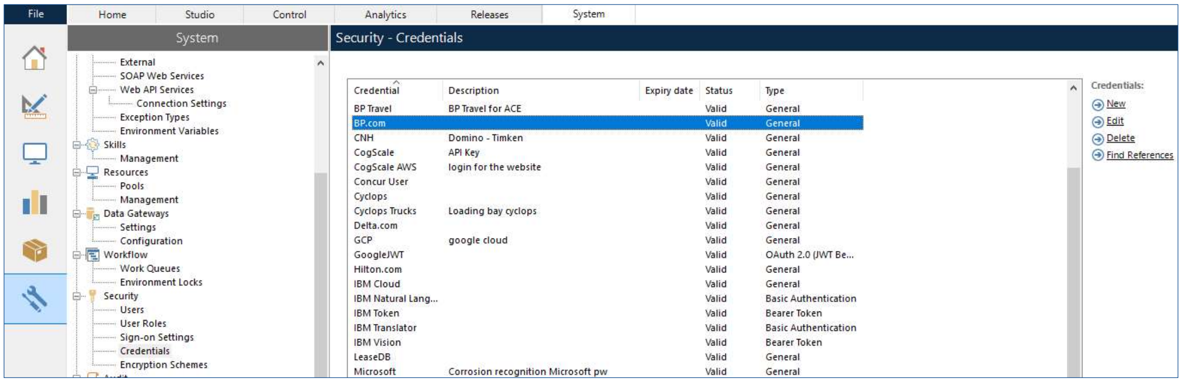
Your process Main page should be a simple high-level flow diagram which uses sub-pages for further task breakdown. This makes it easier to quickly understand what a process does just by looking at the main page. The figure below shows the logical flow through process main pages and sub-pages.



Note: You may need to have pop ups enabled for the site.

Lab 5: Credential Manager

1) Best practice is to never hard code credentials. Instead, we will store our credentials in a secure credential manager. In the interactive client, go to the "System" tab and select "Credentials" under "Security".

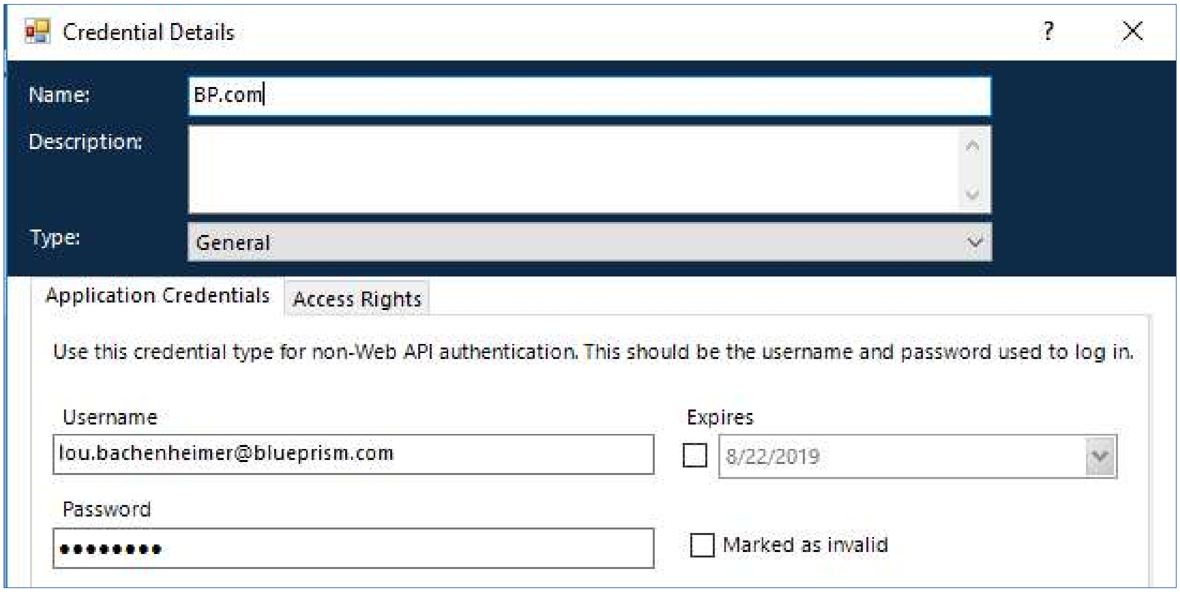


Security - Credentials

Credential	Description	Expiry date	Status	Type
BP Travel	BP Travel for ACE		Valid	General
BP.com			Valid	General
CNH	Domino - Timken		Valid	General
CogScale	API Key		Valid	General
CogScale AWS	login for the website		Valid	General
Concur User			Valid	General
Cyclops			Valid	General
Cyclops Trucks	Loading bay cyclops		Valid	General
Delta.com			Valid	General
GCP	google cloud		Valid	General
GoogleJWT			Valid	OAuth 2.0 (JWT Be...
Hilton.com			Valid	General
IBM Cloud			Valid	General
IBM Natural Lang...			Valid	Basic Authentication
IBM Token			Valid	Bearer Token
IBM Translator			Valid	Basic Authentication
IBM Vision			Valid	Bearer Token
LeaseDB			Valid	General
Microsoft	Corrosion recognition Microsoft pw		Valid	General

NOTE: If this is the first time you have opened/logged in to the Interactive Client, you may need to perform the actions in Appendix A to configure an Encryption Scheme that will be used for credentials stored in the database.

Click "New", located in the top right, to create a new set of credentials. Name the credentials "BP.com" and add a description. Enter the username and password (If you haven't already, sign up for the Blue Prism portal and make credentials). Do NOT click "OK" yet.



Name: BP.com

Description:

Type: General

Use this credential type for non-Web API authentication. This should be the username and password used to log in.

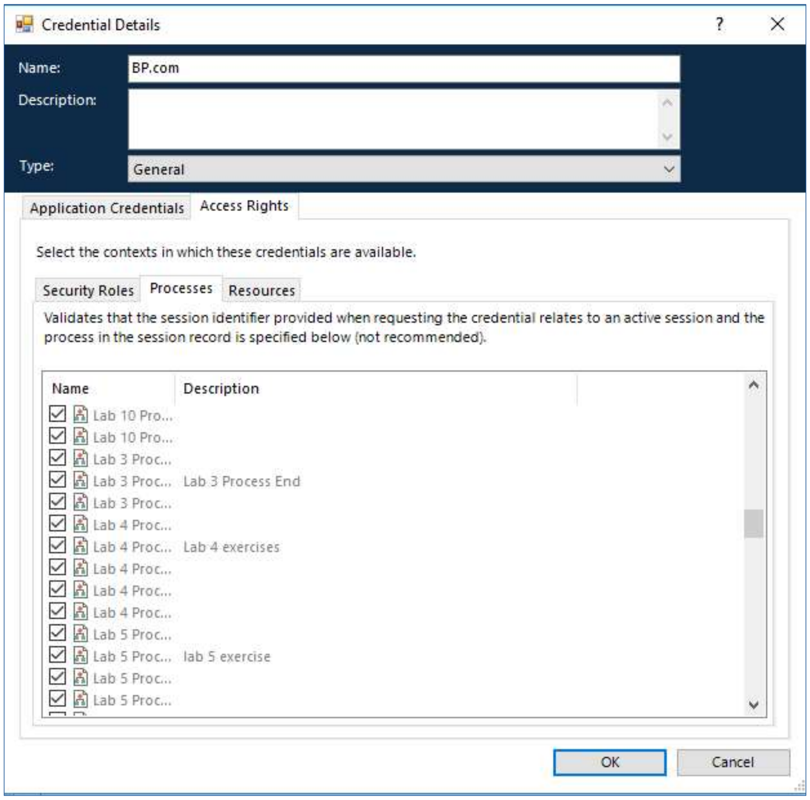
Username: lou.bachenheimer@blueprism.com

Expires: □ 8/22/2019

Password: ••••••••

□ Marked as invalid

2) We still must assign Access Rights. Click the "Access Right" tab. First, under "Security Roles", select your role. Next, under "Processes", select your Process as shown below. Also select all the Lab Processes. Finally, under "Resources", select your machine. If unsure, select all the resources. Now you can click "OK". The ability to control access to Credentials is a crucial security feature for automation platforms being used at scale!


Credential Details

Name: BP.com

Description:

Type: General

Application Credentials | Access Rights

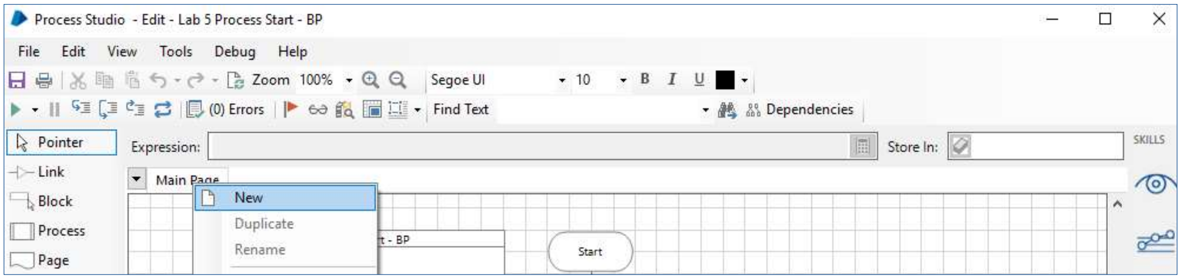
Select the contexts in which these credentials are available.

Security Roles | Processes | Resources

Validates that the session identifier provided when requesting the credential relates to an active session and the process in the session record is specified below (not recommended).

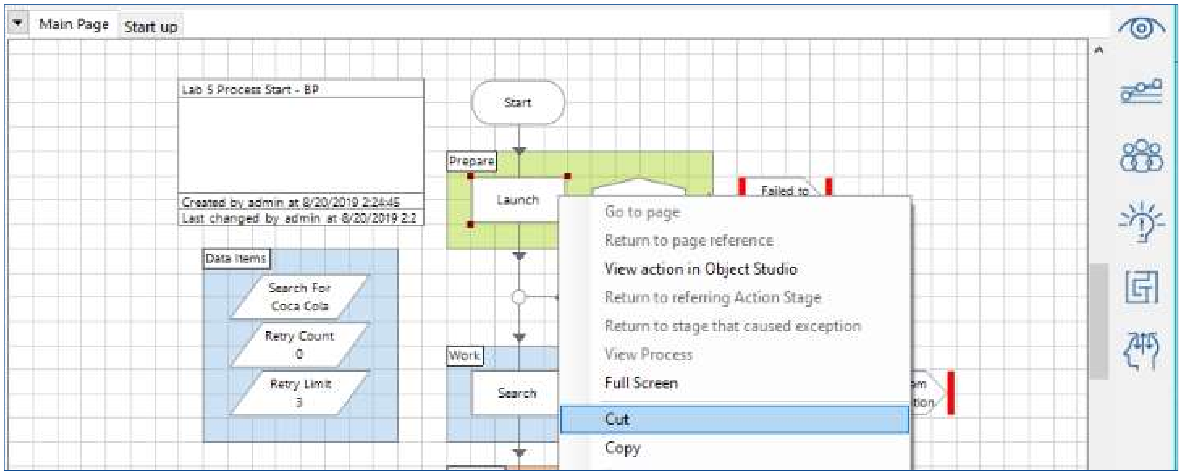
Name	Description
☑ Lab 10 Pro...	
☑ Lab 10 Pro...	
☑ Lab 3 Proc...	
☑ Lab 3 Proc...	Lab 3 Process End
☑ Lab 3 Proc...	
☑ Lab 4 Proc...	
☑ Lab 4 Proc...	Lab 4 exercises
☑ Lab 4 Proc...	
☑ Lab 4 Proc...	
☑ Lab 4 Proc...	
☑ Lab 5 Proc...	
☑ Lab 5 Proc...	lab 5 exercise
☑ Lab 5 Proc...	
☑ Lab 5 Proc...	

3) Now that the credentials exist, we need to set up the process to use them. Open the process called "Lab 5 Process Start - BP". This lab will call an updated Object "Lab 5 Object End - BP" that has a page called "Log In" with credentials set up as inputs. Right click next to the tab where is says "Main Page" and select "New", as shown below.

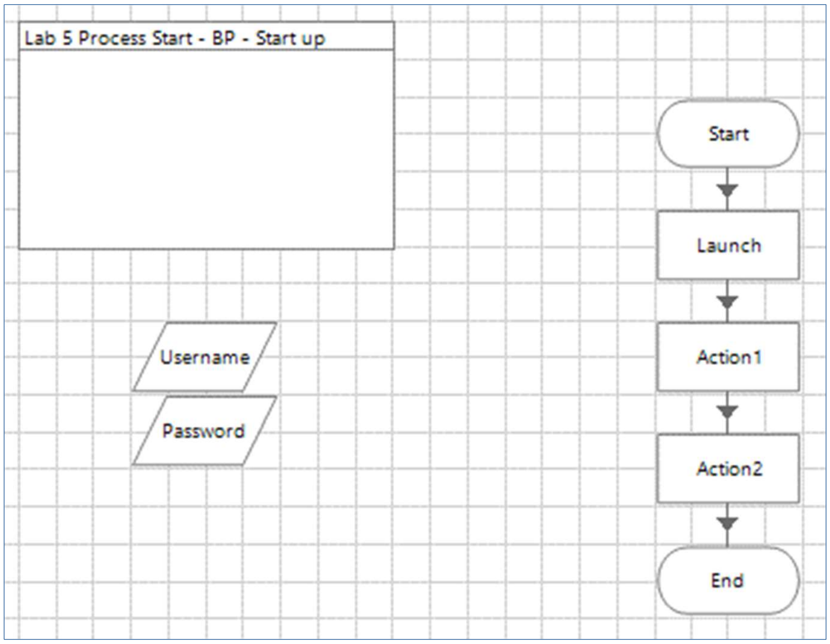

Process Studio - Edit - Lab 5 Process Start - BP

4) Name the page “Start up” and click “OK”. You will be brought to the new page. Breaking up processes into pages makes the process much easier to follow. It also makes it easy to reuse parts!

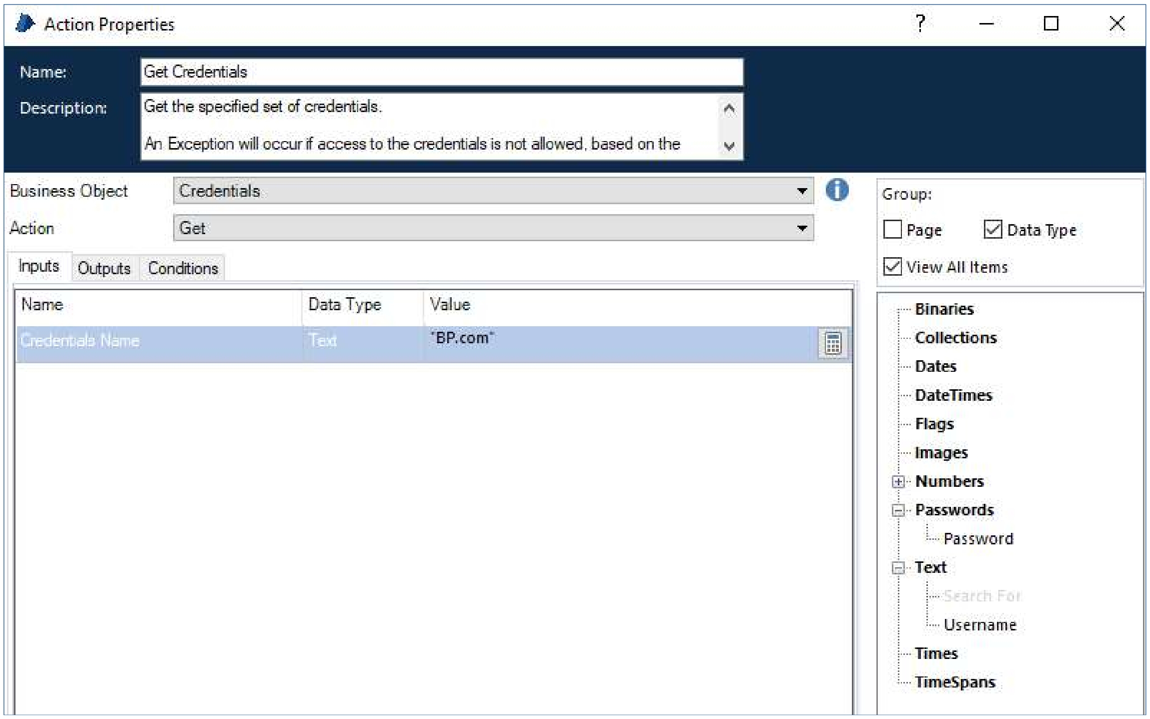
5) On the “Main Page”, right click “Launch” and select “Cut”. Go back to the “Start up” page and paste it under “Start”.



6) Add two actions between “Launch” and “End” and link them all together. Also add two Data Item and name them “Username” and “Password”. Set their types to “Text” and “Password” respectively and don’t enter any initial values.



7) Double click on the first action to open its properties. Change the name to “Get Credentials”. Where it says, “Business Object” scroll to the bottom of the list and select “Credentials”. Where it says “Action”, select “Get”. Under where it says “Value” enter the name you gave to the credentials you added earlier. Make sure to put it in quotes! Finally, click “Outputs” and set “Password” and “Username” to be stored in the Data Items you just created.



Name: Get Credentials

Description: Get the specified set of credentials.

An Exception will occur if access to the credentials is not allowed, based on the

Business Object: Credentials

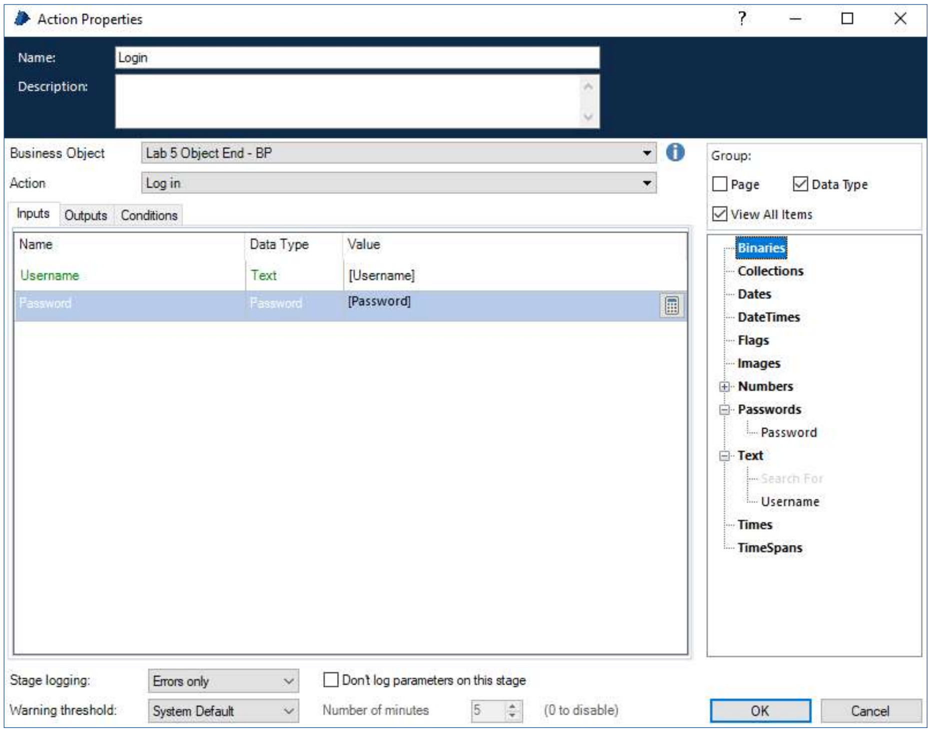
Action: Get

□ Page ☑ Data Type

☑ View All Items

Name	Data Type	Value
Credentials Name	Text	"BP.com"

8) Open the last action's properties. Name it "Log in" and set it up to use the new "Log in" action from the updated Object you imported. It should look like this:



Action Properties

Name: Login

Description:

Business Object: Lab 5 Object End - BP

Action: Log in

Inputs | Outputs | Conditions

Name	Data Type	Value
Username	Text	[Username]
Password	Password	[Password]

Group:

□ Page ☑ Data Type

☑ View All Items

- Binaries
- Collections
- Dates
- DateTimes
- Flags
- Images
- Numbers
- Passwords
  - Password
- Text
  - Search For
  - Username
- Times
- TimeSpans

Stage logging: Errors only

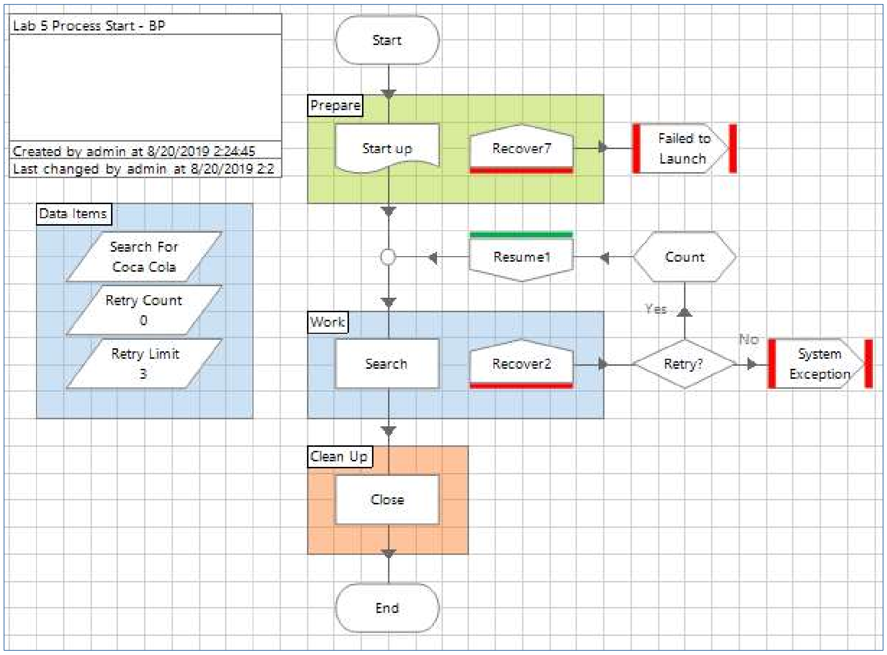
□ Don't log parameters on this stage

Warning threshold: System Default

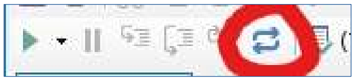
Number of minutes 5 (0 to disable)

OK Cancel

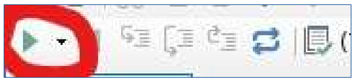
9) Go back to the "Main Page". Add a "Page" block where the "Launch BP" action used to be. Confirm that "Create a reference to an existing page" is selected and click "Next". Choose the Page you just created, "Start up", and click "Finish". Link it together so that it looks like this:



10) Click the "Reset" button in the upper left:



11) Click the "Go" button in the upper left:



12) Watch your process run. What awesome results do you see! When finished, feel free to close both the browser and the process.

Note: You've now learned how to configure and use credentials stored securely in the Credential Manager in Blue Prism. Security policies in your company can leverage this feature to ensure access to target systems is controlled and meets any security requirements or regulations. You've also seen how you can break down processes into a Main page and sub-pages which will help keep processes better organized and easier to understand quickly.

Appendix A: Configuring an Encryption Scheme

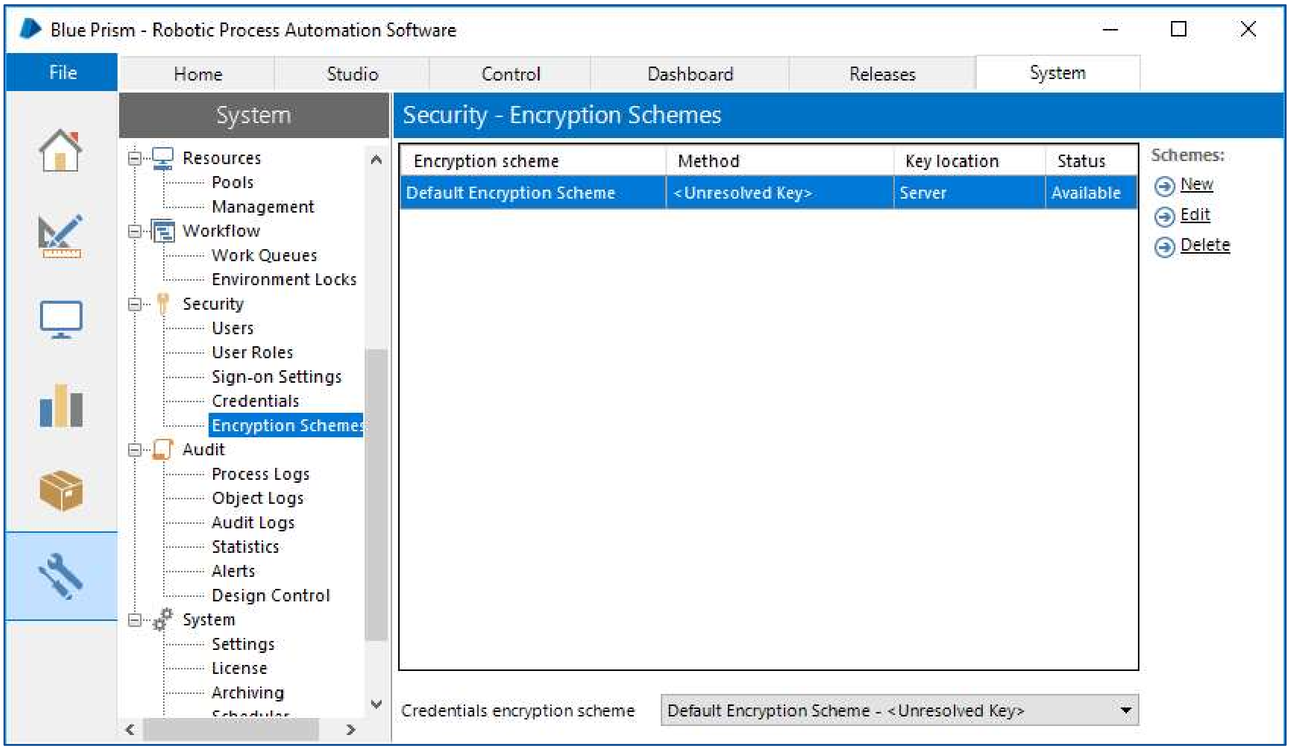
Blue Prism provides the ability to encrypt all data held within the database as it may contain sensitive data. This will protect your data so that it does not show in plain text. It is required when using the Credential Manager to store credentials for the digital workers to use.

There are a few encryption algorithms available which can be used to protect credentials and encrypted work queue information:

Name	Key Length	Notes	Key Generation Info
AES-256 AesCryptoService (5.0.24+)	256-bit	Default implementation leveraging CBC	Blue Prism can be configured to use a manually generated key; or users can use the Generate Key functionality within Blue Prism. Keys generated within Blue Prism are created using RNGCryptoServiceProvider which provides a cryptographically strong sequence of random values.
AES-256 RijndaelManaged	256-bit	Default implementation leveraging CBC	
3DES	192-bit	CBC mode with keying option 1	

There are also options for where to store the key and other options for how keys are managed that can be set for a production environment. The steps below will focus on settings to be used for stand-alone deployments.

1) In the interactive client, go to the "System" tab and select "Encryption Schemes" under "Security".



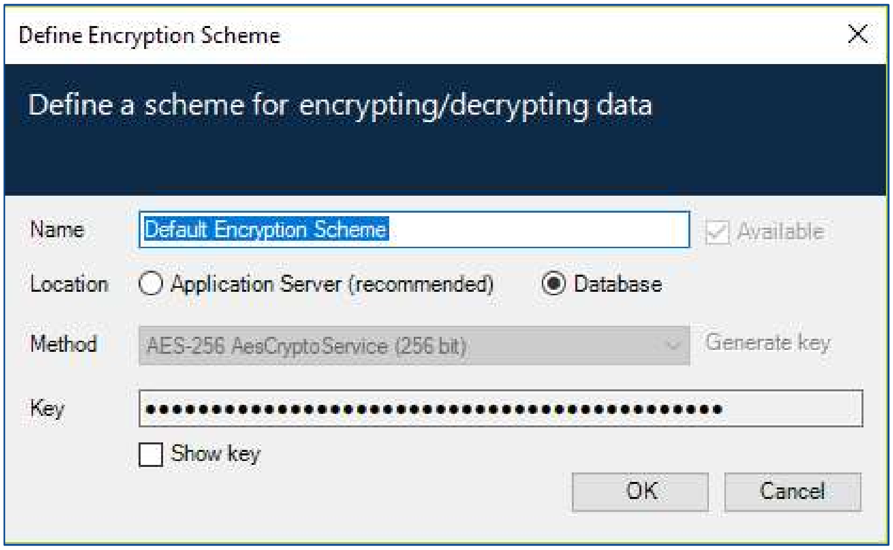
Security - Encryption Schemes

Encryption scheme	Method	Key location	Status
Default Encryption Scheme	<Unresolved Key>	Server	Available

Credentials encryption scheme: Default Encryption Scheme - <Unresolved Key>

Select "Default Encryption Scheme" and click "Edit" in the top right corner to modify.

In the window that opens:



Define Encryption Scheme

Define a scheme for encrypting/decrypting data

Name: Default Encryption Scheme ☑ Available

Location: ○ Application Server (recommended) ● Database

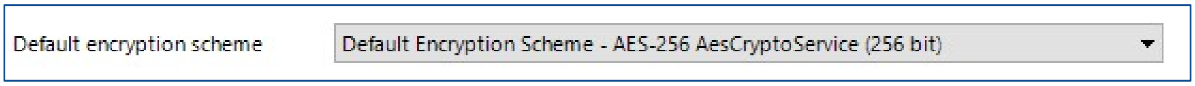
Method: AES-256 AesCryptoService (256 bit) Generate key

Key: ●●

□ Show key

Select the “Database” radio button for “Location”. Select “AES-256 AesCryptoService (256-bit)” for “Method”. Make sure the “Available” check box is checked (it may be greyed out). Then, click “Generate Key” and click “OK”.

Check the bottom of the Encryption Schemes screen to ensure the Default Encryption Scheme now shows “AES-256 AesCryptoService…”



Default encryption scheme: Default Encryption Scheme - AES-256 AesCryptoService (256 bit)