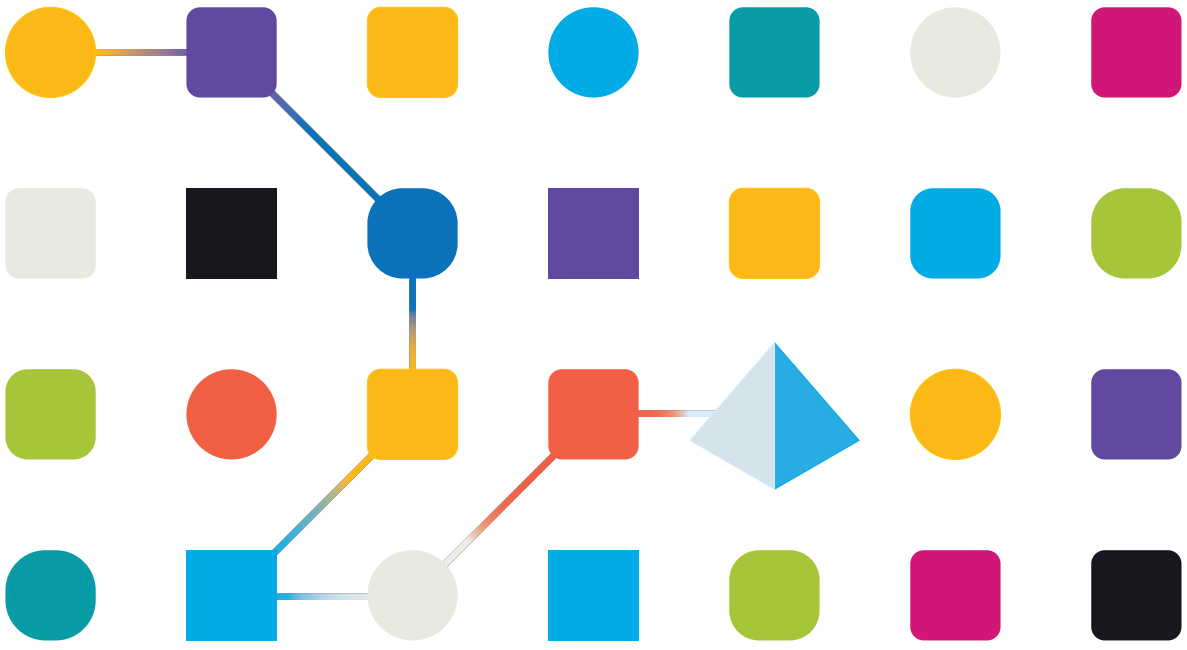
blueprism®

Blue Prism 6

CyberArk Integration User Guide

Document Revision: 1.0



Trademarks and Copyright

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

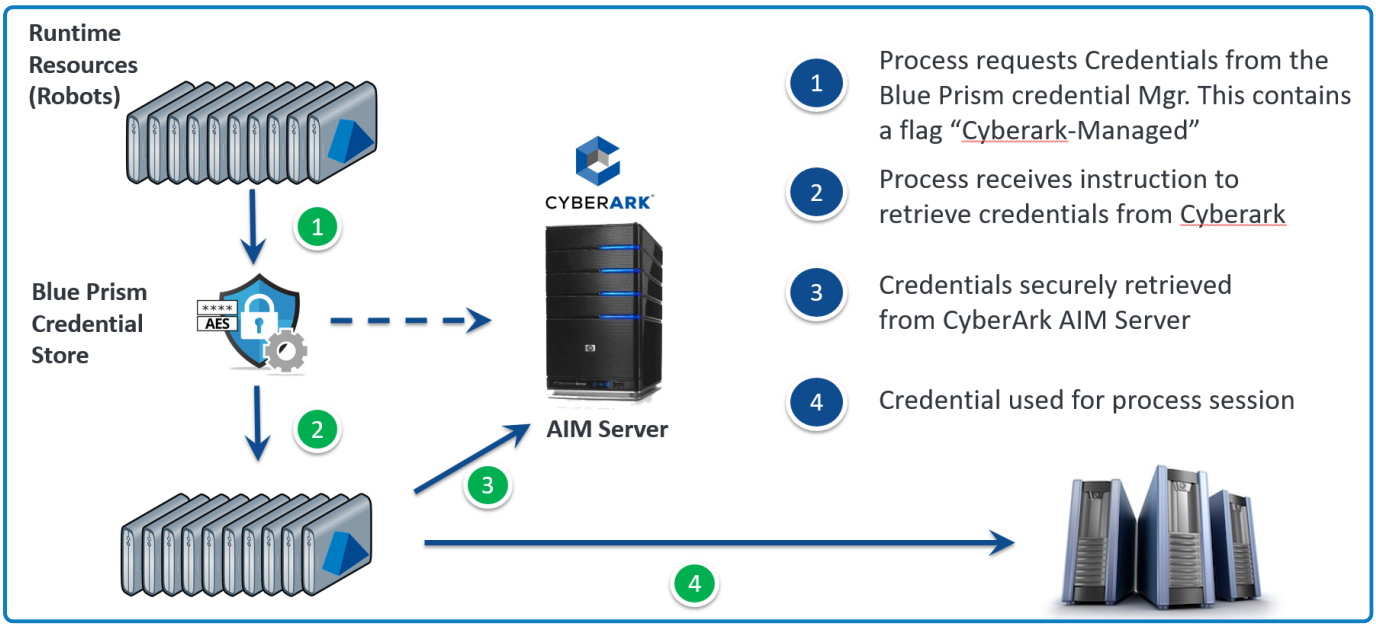
Contents

Introduction

Blue Prism can easily receive credentials stored in CyberArk by utilising CyberArk's SOAP Web Service interface to Application Identity Manager. This guide outlines the steps required to configure AIM and integrate the CyberArk credential workflow into a Business Object.

CyberArk IntegrationSolution Overview

The Blue Prism CyberArk Integration allows for credentials to be retrieved from the CyberArk Credential store, whilst retaining the controls over their context within the Blue Prism environment, using existing functionality. The high level solution approach is outlined below:



There are two stages to the configuration of the solution:

- Configuration of CyberArk AIM server
- Configuration of Blue Prism

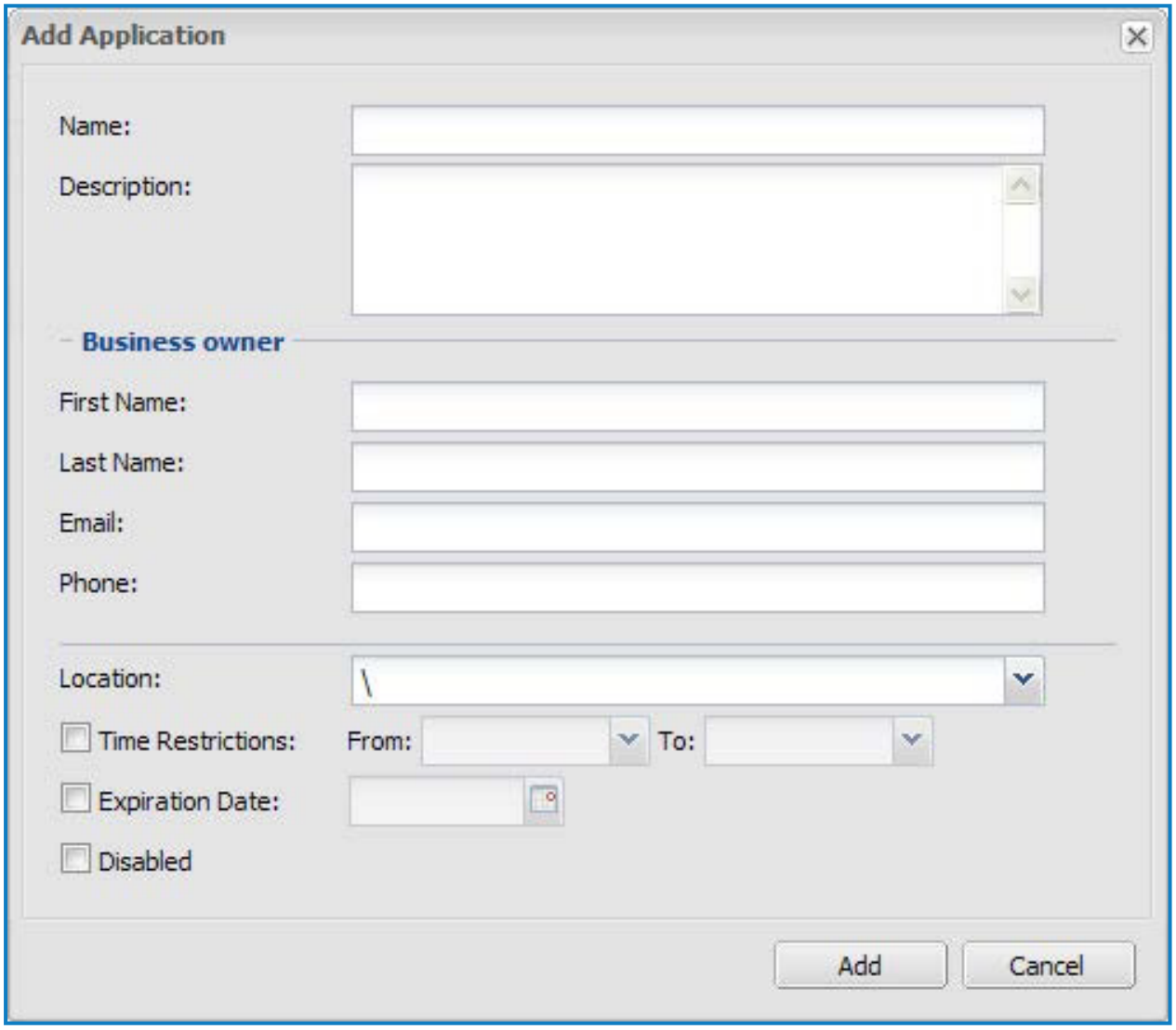
Configuring the CyberArk AIM Server

The following steps outline the specific configuration for the Blue Prism integration. The installation and configuration of AIM is outside the scope of this document.

Defining the Application ID (AppID) and Authentication Details

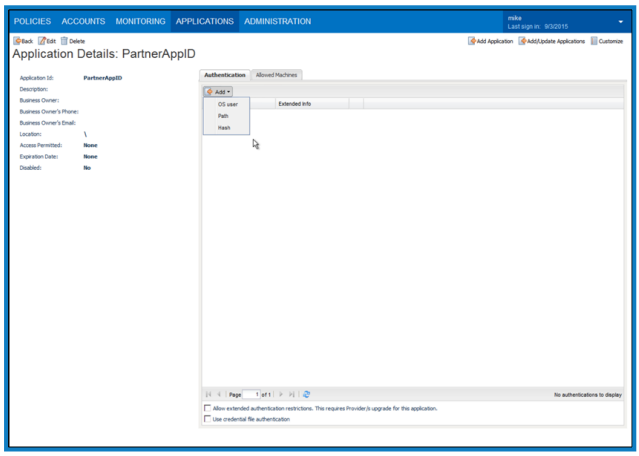
To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click Add Application; the Add Application page appears.



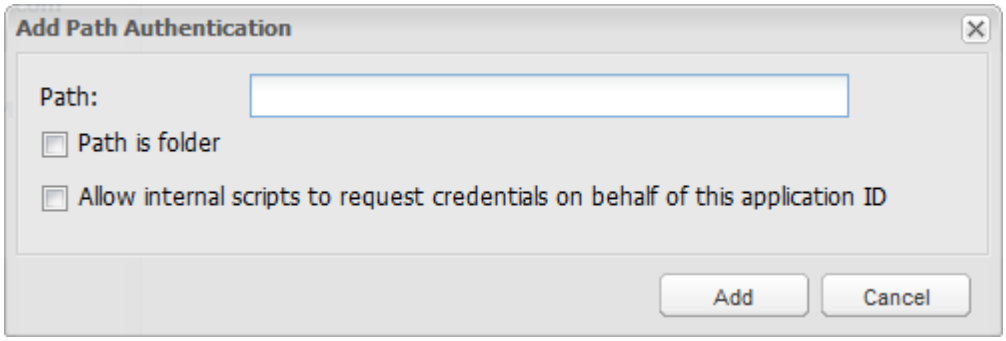
2. Specify the following information:
   - In the Name edit box, specify the unique name (ID) of the application - PARTNER: APP ID = <CyberArk App ID>

     Blue Prism supports a configurable App ID. Whatever CyberArk contains for the necessary credentials can be used, or any appropriate name can be picked for a new one.
   - In the Description, specify a short description of the application that will help you identify it.
   - In the Business owner section, specify contact information about the application's Business owner.
   - In the lowest section, specify the Location of the application in the Vault hierarchy. If a Location is not selected, the application will be added in the same Location as the user who is creating this application.
3. Click **Add**; the application is added and is displayed in the Application Details page.



4. Select the **Allow extended authentication restrictions** check box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
5. Specify the application's Authentication details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Blue Prism will expect to authenticate either via IP white-list or via certificate, and does not provide credentials during the Web Service call.
   - In the Authentication tab, click Add; a drop-down list of authentication characteristics displays.
   - Select the authentication characteristic to specify.
6. Specify the OS user:
   - Select OS user; the Add Operating System User Authentication window displays.
   - Specify the name of the OS user who will run the application, then click Add; the OS user is listed in the Authentication tab.
7. Specify the application path:

8. Select **Path**; the Add Path Authentication window appears.



   - Specify the path where the application will run.
   - To indicate that the specified path is a folder, select **Path is folder**.
   - To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
   - Click **Add**. The path is added as an authentication characteristic with the information that you specified.

9. Specify a hash:
   - Run the AIMGetAppInfo utility to calculate the application's unique hash.
   - Copy the hash value that is returned by the utility.
   - In the PVWA, select Hash; the Add Hash window appears.
   - In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.

     For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2The comment must not include a colon or a semicolon.
   - Click **Add**; the Hash is added as an authentication characteristic with the information that you specified.

10. Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their
11. passwords.
    - In the Allowed Machines tab, click **Add**; the Add allowed machine window is displayed.
    - Specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click Add; the IP address is listed in the Allowed machines tab.

      Make sure the servers allowed include all mid-tier servers or all endpoints where the AIM Credential Providers were installed.

Provisioning Accounts and Setting Permissions for Application Access

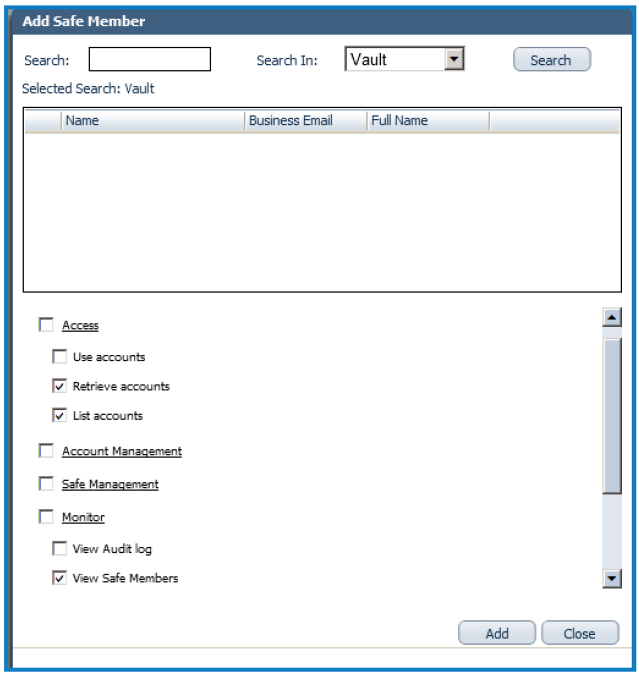
For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault (Step 1). Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - Manually – Add accounts manually one at a time, and specify all the account details.
   - Automatically – Add multiple accounts automatically using the Password Upload feature.

   For this step, you require the Add accounts authorization in the Password Safe.

   For more information about adding and managing privileged accounts, refer to the *Privileged Account Security Implementation Guide*.

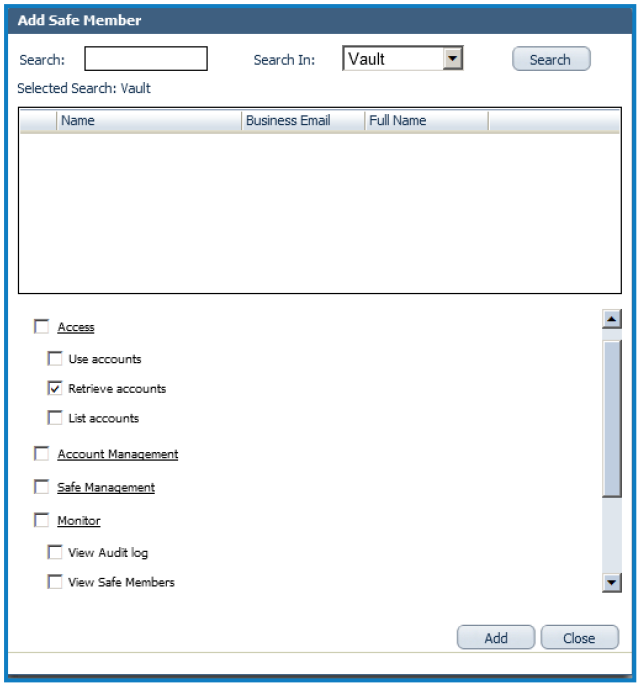
   Because the parameter is required by Blue Prism's current web service call implementation, the Database property must be defined to a known value (e.g. “BluePrism”) on all provisioned accounts that Blue Prism will retrieve.
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.



3. Add the Provider user as a Safe Member with the following authorizations.
   - List accounts
   - Retrieve accounts
   - View Safe Members

   When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

4. Add the application(the APPID) as a Safe Member with the **Retrieve accounts** authorizations.



5. If your environment is configured for dual control:
   - In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the **Access Safe without Confirmation** permission
   - In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
6. If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the *Privileged Account Security Implementation Guide*.

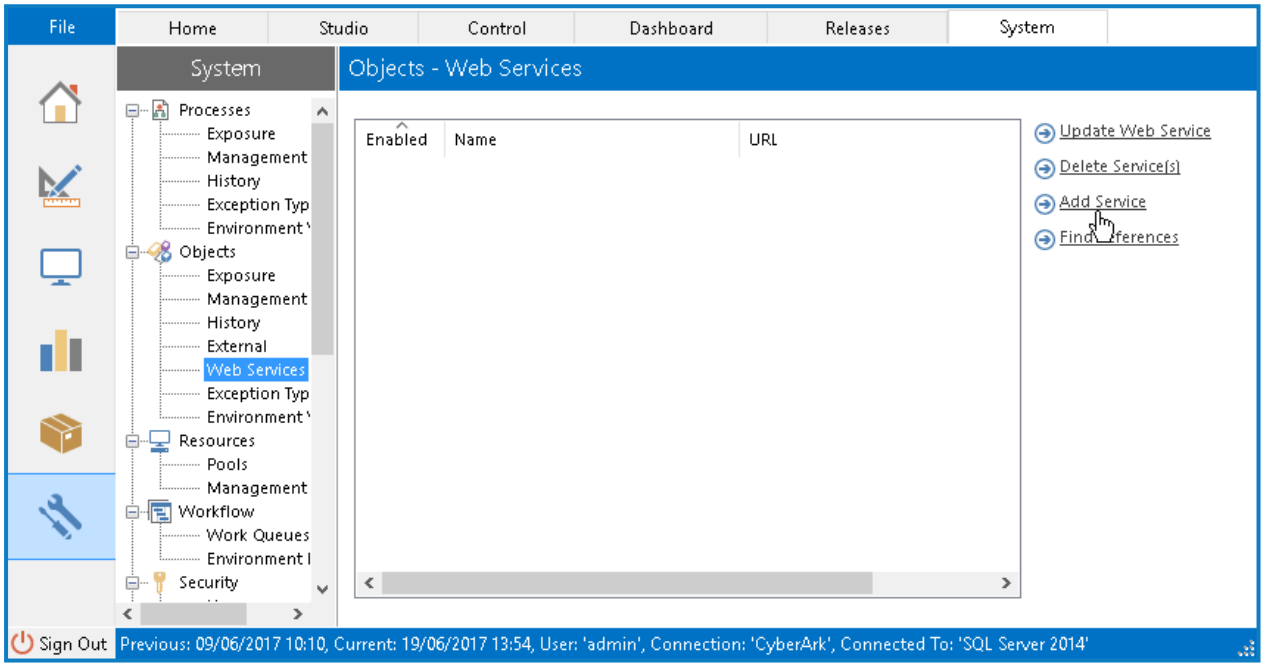
Configuring Blue Prism for CyberArk Integration

Full details of how to set up and consume a 3rd Party SOAP web service in Blue Prism is provided in the Web Services guidance *User Guide – Web Services*, available in the Product Documentation area of the user portal.

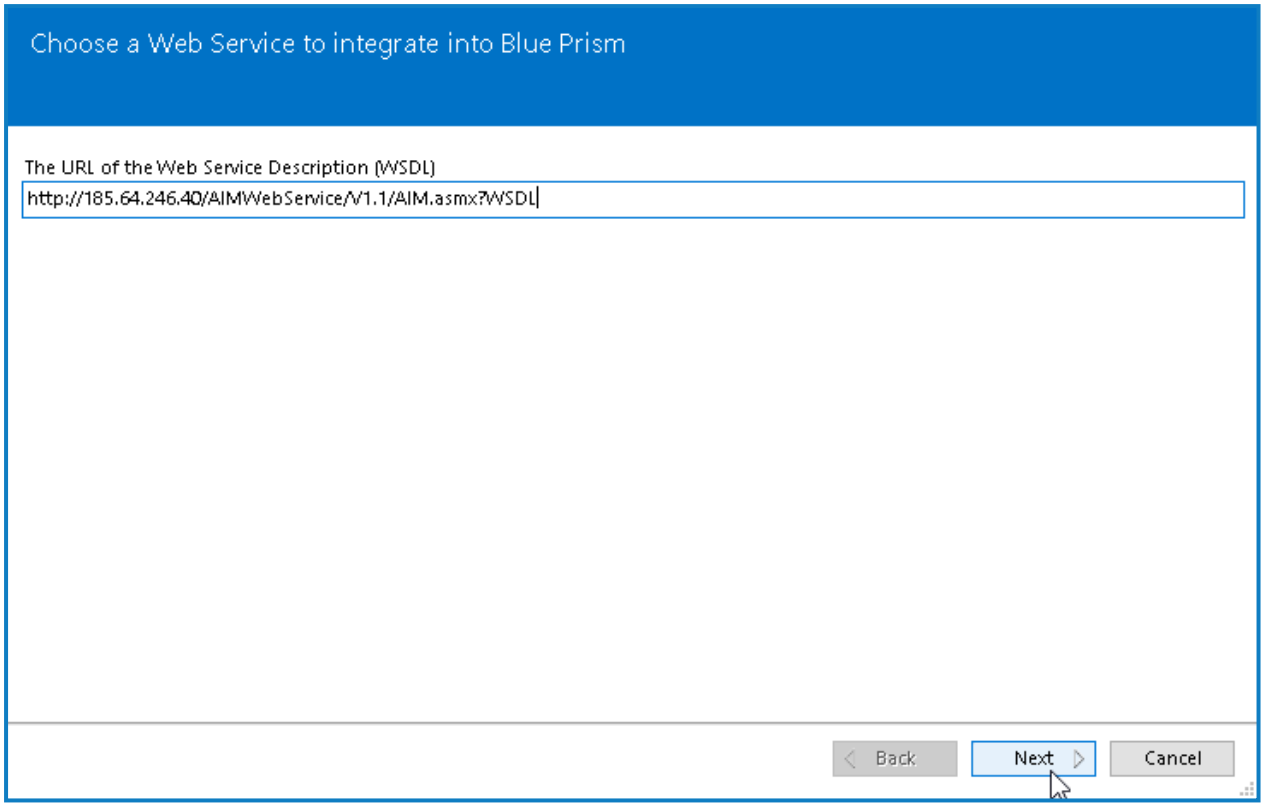
Please refer to CyberArk's own product documentation for details about how to expose a SOAPWeb Service from their product.

The steps required to register a CyberArk Web Service for use in Blue Prism are as follows:

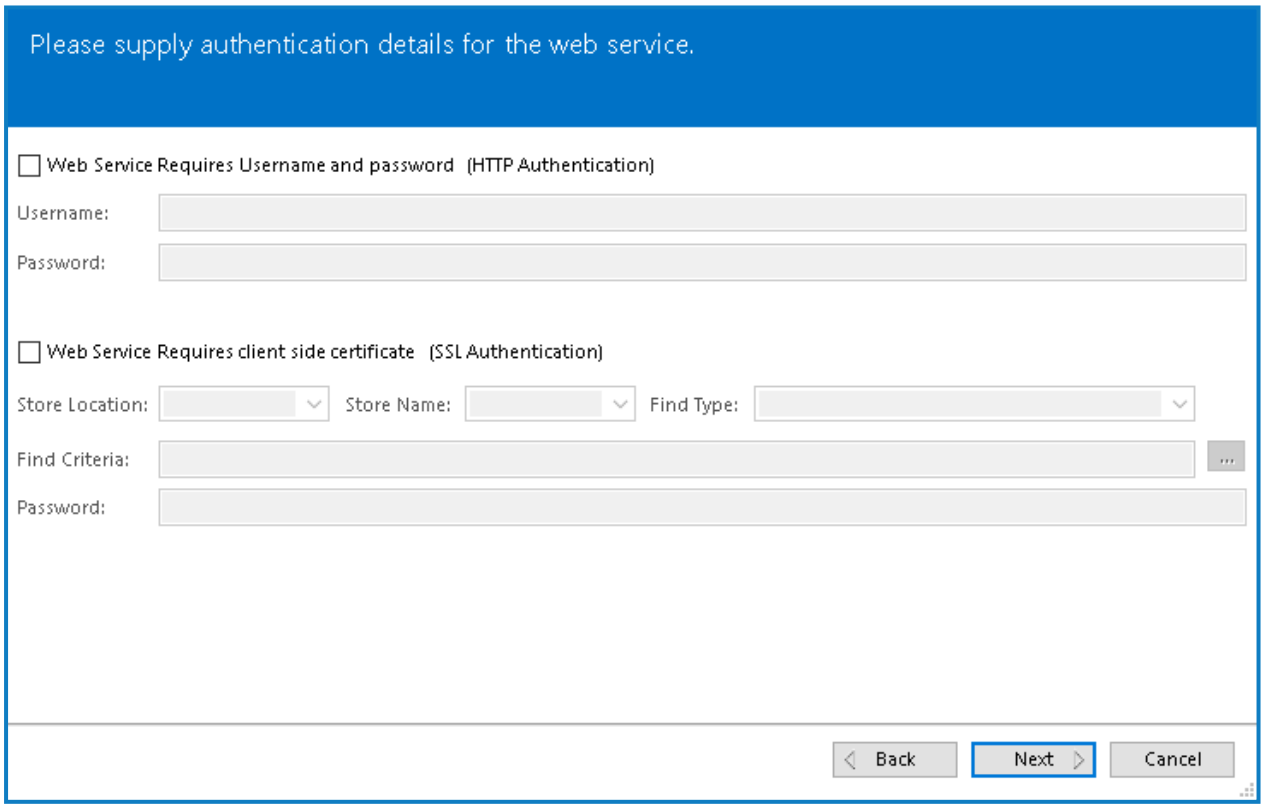
1. Go to the **System** > **Objects** > **Web Services** area of Blue Prism and click on the **Add Service** link.



2. Enter the WSDL URL for the CyberArk Web Service that you want to consume and click **Next**.



3. Enter any HTTP or SLL Authentication details if required by the SOAP Web Service.



4. You can configure the timeout when interacting with the service. It is recommended this is left at the default value of 10000 milliseconds unless there is a known problematic latency issue.
5. Blue Prism will import the web service definitions from the WSDL. Click **Next**.

6. Select the Web Service from the WSDL that you want to include. There should be one CyberArk Web Service, select it and click **Next**.
7. You will be given the option of selecting the Web Service methods you want to use, the **GetPassword** method should exist and already be ticked. Click **Next**.
8. Blue Prism will give a Blue Prism object name to the Web Service based upon the name provided within the WSDL. Click **Finish**.

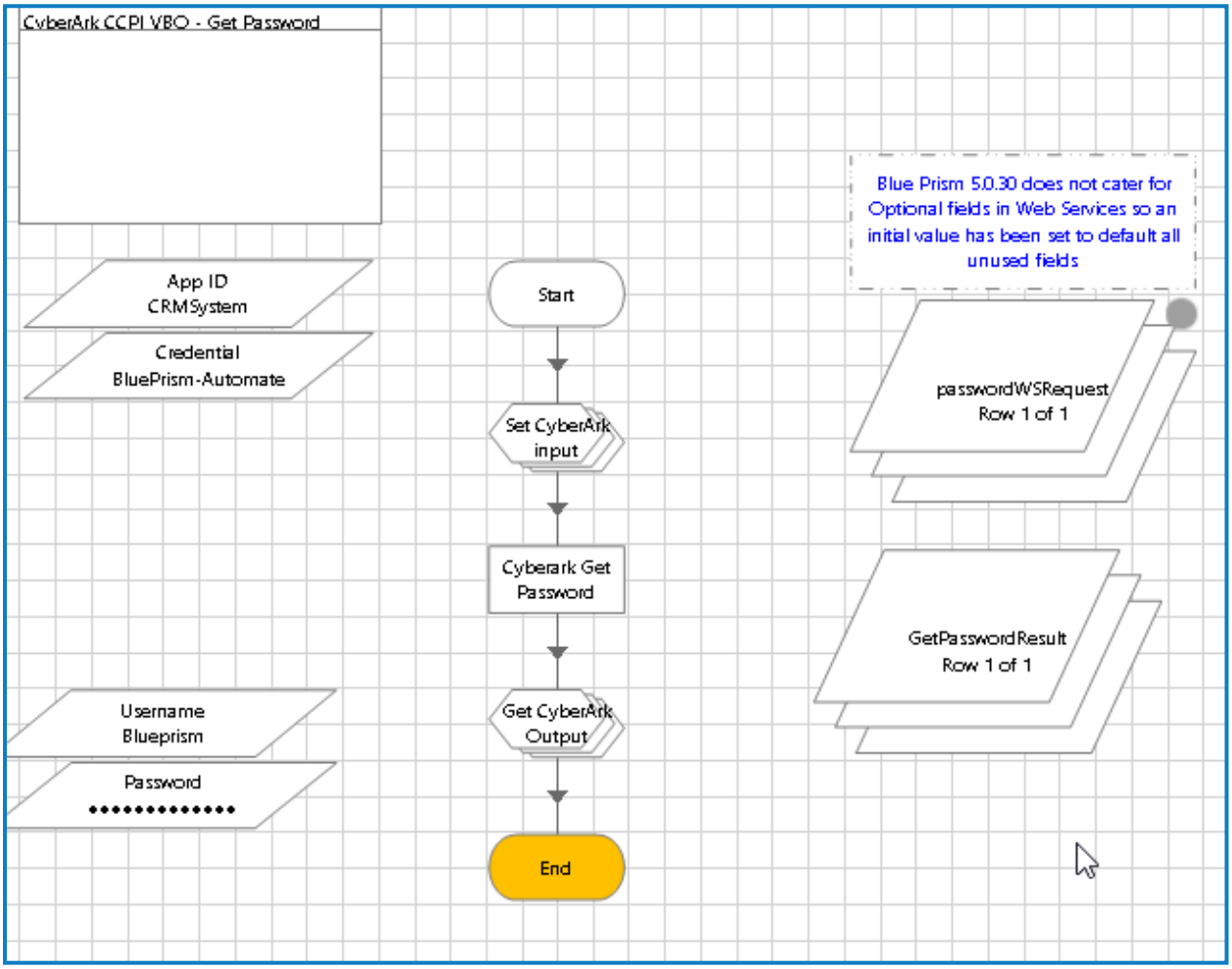
The CyberArk Web Service will now be registered within the Blue Prism product. You will be able to call the GetPassword function in your Process or Object studio flow diagrams using an action stage.

Create a CyberArk VBO

Once the CyberArk Web Service has been registered in Blue Prism it can be used from an action stage within an Object or Process.

The recommendation is that the CyberArk GetPassword method is encapsulated in a Blue Prism object action with input parameters for the AppID and Credential name to retrieve, and output parameters of the Username and Password for that credential.

The object will perform any mapping required between Blue Prism and CyberArk fields. An example CyberArk VBO is available on request or from the Developer Jumpstart section of the Blue Prism Portal. A screenshot of the action is shown below.



For any system or application where CyberArk is used as the credential store instead of Blue Prism, this action can be called from the process to retrieve the credentials from CyberArk.

CyberArk GetPassword input parameters

For this simple VBO implementation only the AppID and Object input parameters are used in the CyberArk GetPassword web service to retrieve credentials.

The CyberArk GetPassword method has numerous other input parameters which are optional inputs. Because the Blue Prism built in SOAP interface does not recognise if a web service input parameter is optional and always passes a value to the web service for every input parameter, a default 'return all' value must be set in Blue Prism for each input parameter in the CyberArk Web Service.

The one input parameter where a default value for the optional field could not be made to work was the 'Database' parameter. For that one field configuration was required within CyberArk to add the database field to the account and set it to a value that could then be used for the CyberArk Database input parameter. For the example object distributed with this document that value was set to be 'Blueprism'

The input parameter values used for the GetPassword Web Service to work when called from Blue Prism were:

CyberArk GetPassword method input Parameter	Default value used	Notes
AppID		AppID is not an optional field. Set to the correct CyberArk AppID for the credentials you want to retrieve.
Safe	".*"	
Folder	".*"	
Object		Object is not an optional field. Set to the correct CyberArk Object name for the credentials you want to retrieve.
UserName	".*"	
Address	".*"	
Database	"Blueprism"	In CyberArk the database field needs adding to the account. The input parameter needs setting to the value used, for our example object "Blueprism" was configured in CyberArk to be a valid database value.
PolicyID	".*"	
Reason	".*"	
ConnectionTimeout	"30"	
Query	""	
QueryFormat	"Regexp"	
Attributes	""	

An enhancement request has been raised with Blue Prism so that optional input parameters are omitted from web service requests. That enhancement, when delivered, will mean that only the AppID and Object input parameters will need to be set.

CyberArk GetPassword output parameters

The GetPassword web service function has numerous output parameters but the only ones utilised for our simple VBO interface were Username and Content. No other output parameters were used by our simple interface. Additional credential fields could be configured in CyberArk and returned in the Properties collection if required.

The output parameters from the GetPassword Web Service are:

CyberArk GetPassword method output parameter	Notes
Content	Used to return the credential Password
UserName	Used to return the credential Username
Folder	Not Used
Address	Not Used
Database	Not Used
PolicyID	Not Used
Properties	Not Used, but if required can be utilised to return additional credential information required by a system.

CyberArk GetPassword Parameters

The GetPassword web service function has numerous output parameters but the only ones utilised for our simple VBO interface were Username and Content. No other output parameters were used by our simple interface. Additional credential fields could be configured in CyberArk and returned in the Properties collection if required.

The output parameters from the GetPassword Web Service are:

CyberArk GetPassword method output parameter	Notes
Content	Used to return the credential Password
UserName	Used to return the credential Username
Folder	Not Used
Address	Not Used
Database	Not Used
PolicyID	Not Used
Properties	Not Used, but if required can be utilised to return additional credential information required by a system.

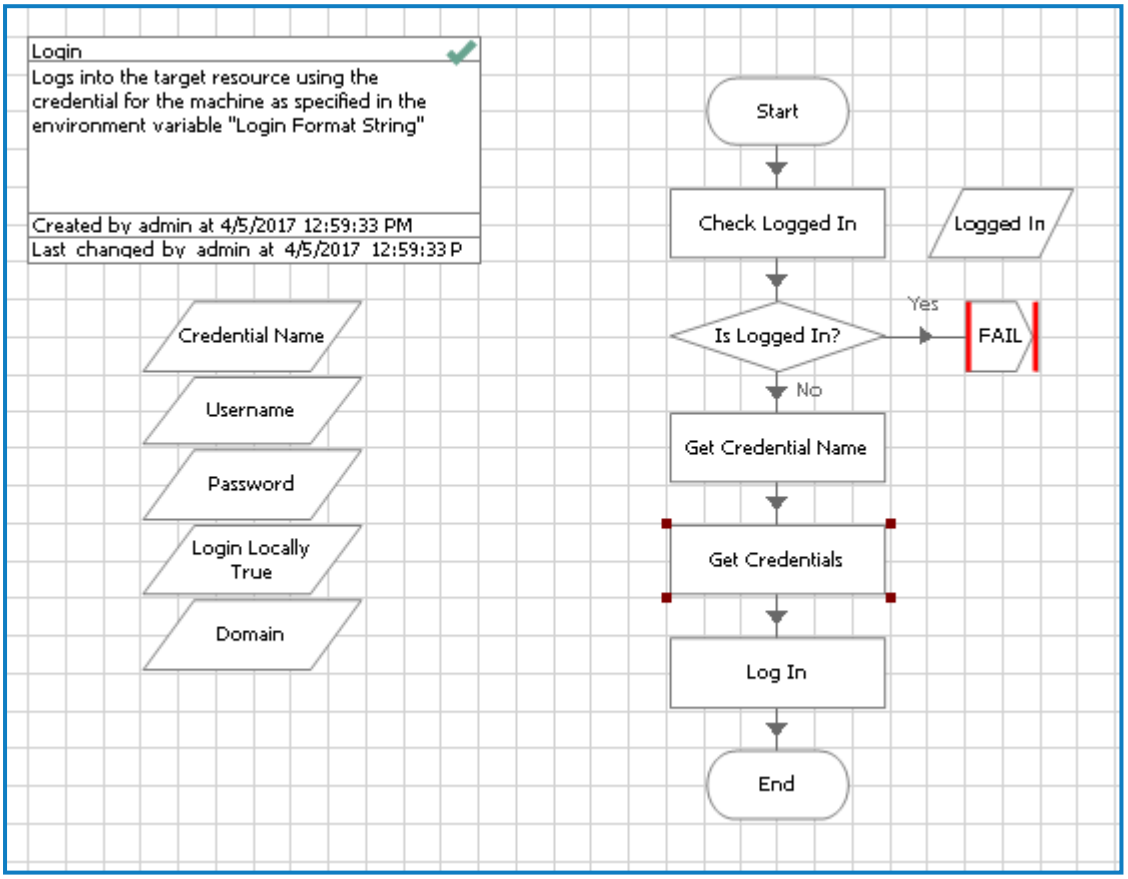
Configure Login Agent to Use CyberArk

Login Agent provides the ability for Blue Prism to log into and out of the Windows Desktop.

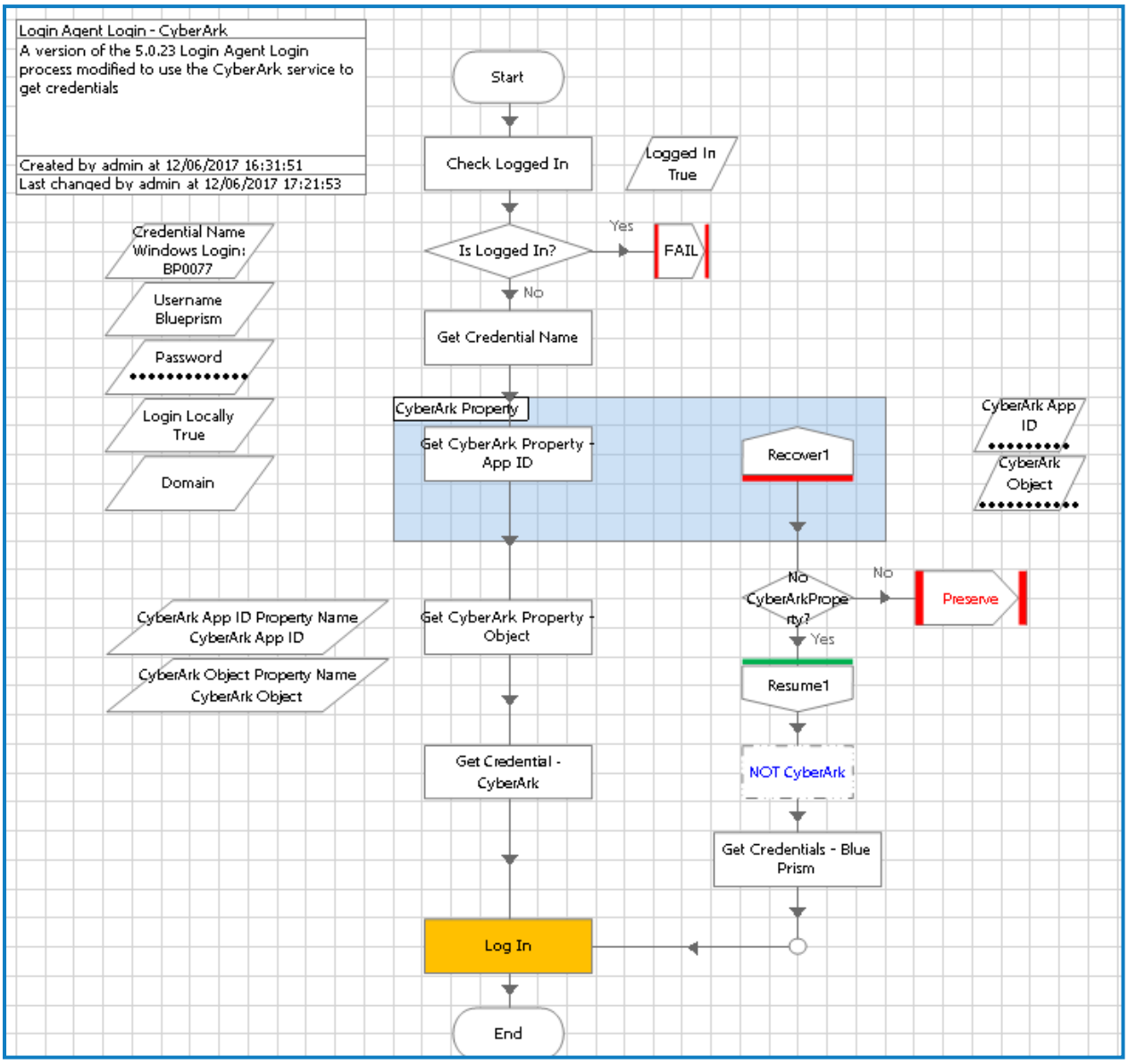
Modify the Login Agent “Login” Process

The Login process provided by the Login Agent must be modified to account for the possibility of calling a credential from CyberArk. This is detected by retrieving the credential from the Blue Prism Credential Manager and looking at its properties. If it is flagged as a CyberArk managed credential, the Login Agent process retrieves the true credential from CA before attempting the log-in operation.

Original logic



Modified Logic



An example of this modified logic is distributed alongside this guide. The main points of note are:

- A Blue Prism credential is still created and used. This allows a mix of CyberArk and Blue Prism credentials to be stored depending upon solution design requirements. It also allows the use of Roles and Permissions in Blue Prism to continue to dictate what Process, Resource, and User can use the credential.
- If the Blue Prism credential includes a Property called CyberArk App ID, then the credentials are stored in CyberArk rather than in the Blue Prism credential.
- If the CyberArk App ID property exists it and a CyberArk Object Property are used as input parameters to the CyberArk VBO object, which was described earlier in this guide.
- If the CyberArk App ID property does not exist it signifies that credentials are not stored in CyberArk.

Blue Prism Authentication with Cyberark

Authentication with Cyberark may be secured via different means, e.g. Client Certificates or Single Sign-On. Consult with your local Cyberark Support team to determine which is the appropriate mechanism to use. The generally accepted best practice is to use Client certificates. This would involve each runtime being configured with the appropriate certificate. The procedure for configuring this is documented within the Cyberark Central Credential Provider Implementation Guide (this is a Cyberark Document and is not supplied or maintained by Blue Prism).