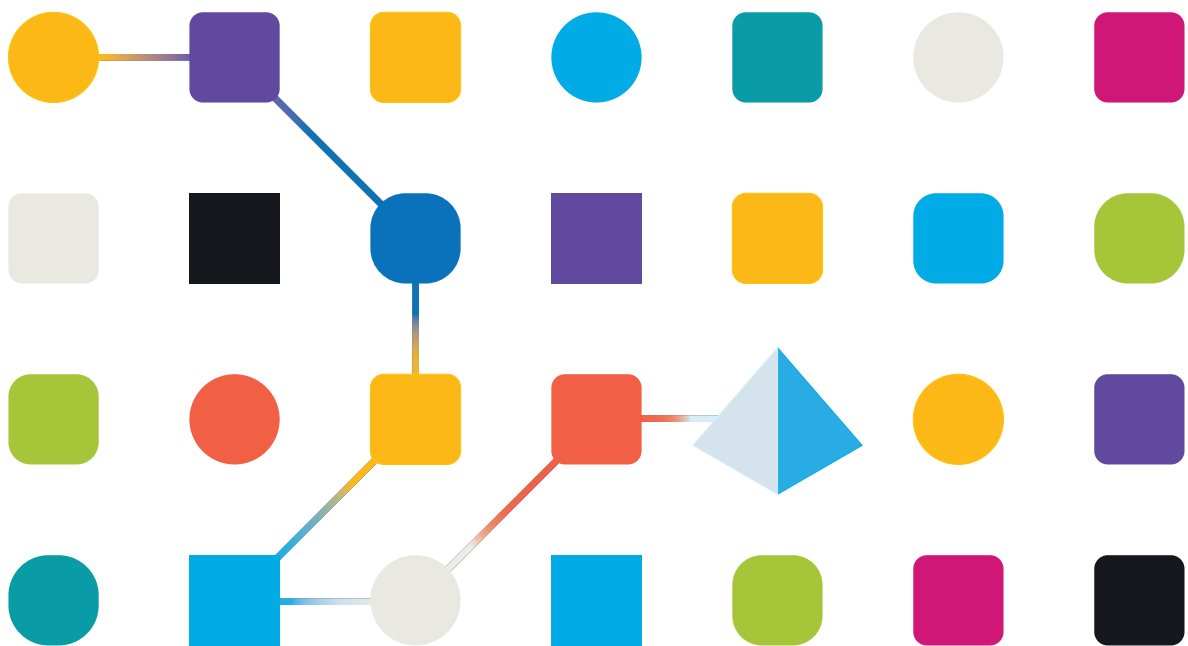




Blue Prism 7.2

Authentication Server Configuration Guide

Document Revision: 3.0



Trademarks and Copyright

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third-party without the written consent of an authorized Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© 2023 Blue Prism Limited

“Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

All trademarks are hereby acknowledged and are used to the benefit of their respective owners. Blue Prism is not responsible for the content of external websites referenced by this document.

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	4
Prerequisites	4
Typical deployment	5
Authentication Server configuration	7
Create a service account in Hub	7
Configure Blue Prism to use Authentication Server	9
Configure the Blue Prism application server	9
Configure Blue Prism users to authenticate via Authentication Server	10
Enable Authentication Server login in your Blue Prism environment	16
Synchronize user and service accounts with Authentication Server	17
Troubleshooting Authentication Server	18
Logging into Blue Prism after enabling Authentication Server	18
Logging into Authentication Server using Active Directory authentication	20
Error message displays in the output CSV file when running the mapping function for the first time	24
Authentication Server users only have access to the Home and Digital Exchange tabs when they sign into the Blue Prism interactive client	24


Introduction

Authentication Server provides centralized common authentication for users across three key components of the Blue Prism platform: Blue Prism Enterprise, Blue Prism API, and Blue Prism Hub.

Authentication Server is installed as part of the Blue Prism Hub installation (version 4.6 or later) if using the Blue Prism API and/or browser-based Control Room with version 7.1 and later. A Blue Prism environment must then be configured to use Authentication Server in order to allow users to log in via Authentication Server only.

Once Authentication Server has been configured and enabled, all user access for Blue Prism Enterprise will be directed via Authentication Server, where users will be able to log in via native, Active Directory, and LDAP authentication. These user accounts must exist both in Hub and Blue Prism.

Blue Prism native and Active Directory authentication can still be used to authenticate runtime resources, AutomateC commands, and when calling web services exposed on runtime resources. These requests cannot be authenticated via Authentication Server.

 The external authentication capability via Authentication Gateway introduced in Blue Prism 6.10 is not supported in Blue Prism version 7.

 For an overview of the configuration, also watch the [Authentication Server configuration video](#).

Prerequisites

The following prerequisites must be met before configuring a Blue Prism environment to use Authentication Server:

- A working Blue Prism Enterprise deployment running version 7.2 . See [Blue Prism Enterprise installation guide](#) for guidance.
- A Blue Prism application server that can be configured to integrate with Authentication Server, see [Configure the Blue Prism application server on page 9](#). This guide assumes one Blue Prism interactive client running on one application server on which the details of the service account created to make authenticated requests to the Authentication Server API are configured.
- A Microsoft Edge WebView2 browser which delivers the embedded Authentication Server login dialog required to enable users to log into Authentication Server from the Blue Prism interactive client. The associated WebView2 runtime must be installed locally on any machine that runs the Blue Prism interactive client. For more details, see <https://docs.microsoft.com/en-us/microsoft-edge/webview2/concepts/distribution>.

 Watch the [installation video](#).

- A working Blue Prism Hub deployment running version 4.6 or later, including Authentication Server, a Message Broker server to host the RabbitMQ Message Broker, and a web server for the Hub installation. See the [Hub installation guide](#) for guidance.

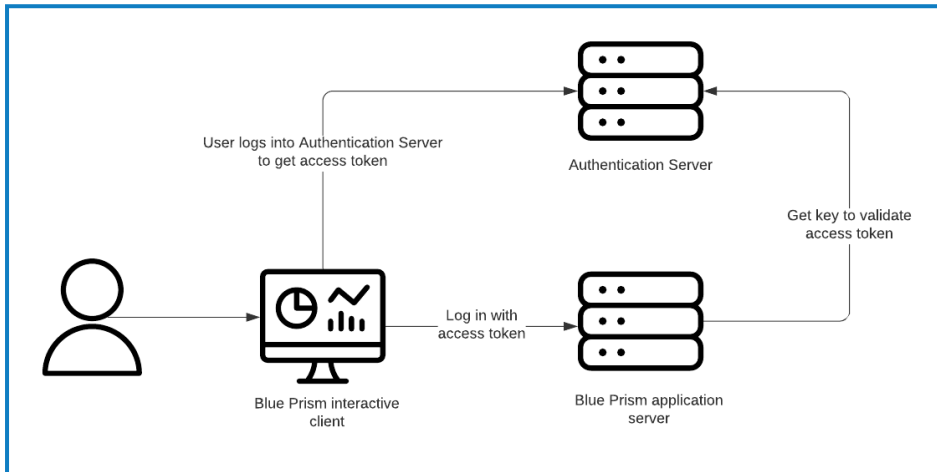
Typical deployment

Blue Prism environments configured to use Authentication Server

The following diagrams show the authentication flow in a Blue Prism environment configured to use Authentication Server.

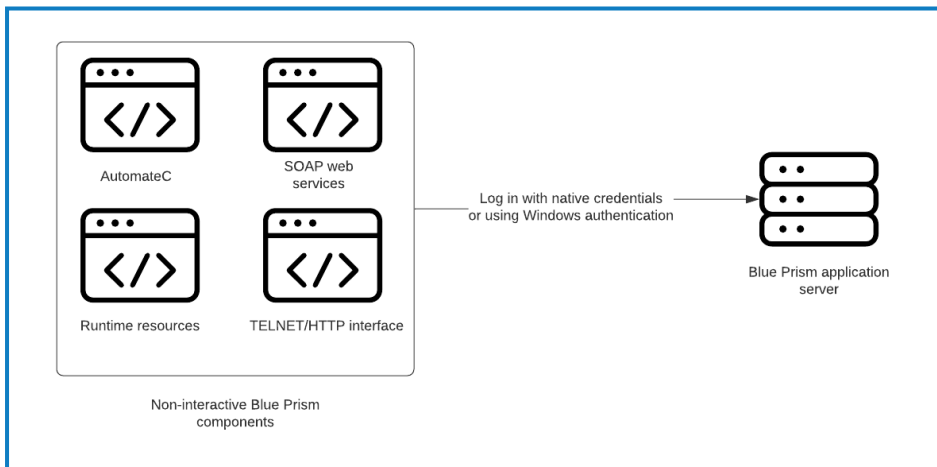
Interactive client authentication

The diagram below shows the authentication flow for a Blue Prism interactive client.



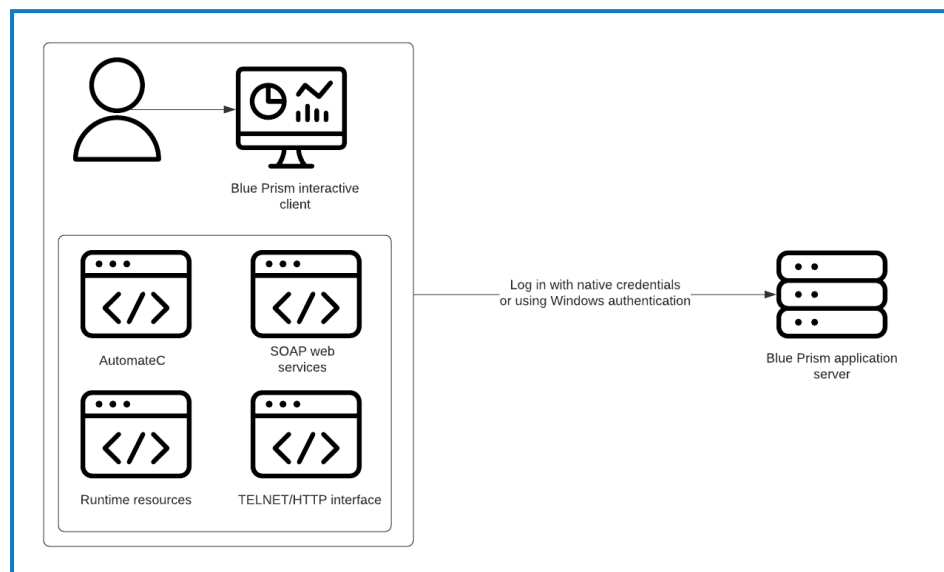
Authentication for other components

The diagram below shows the authentication flow for other components, such as runtime resources, AutomateC commands, and web service requests.



Blue Prism environments not configured to use Authentication Server


The following diagram shows the authentication flow in a Blue Prism environment not configured to use Authentication Server.



Authentication Server configuration

The following is a summary of the steps required to configure Authentication Server:

1. [Create a service account](#) in Hub and grant it permission to the Authentication Server API to issue authentication tokens.
2. [Configure your Blue Prism environment](#) to use Authentication Server.
3. [Configure the Blue Prism application server](#).
4. [Configure Blue Prism users](#) to authenticate via Authentication Server.
5. [Enable Authentication Server login](#) in your Blue Prism environment.
6. [Synchronize user and service accounts](#) with Authentication Server.

 Please ensure you have taken a full and verifiable backup of your Blue Prism database before configuring and enabling Authentication Server for your environment. For more details, see [Back up and restore the full system](#).

Create a service account in Hub

Service accounts provide the ability for applications to obtain access tokens and use them to make authenticated requests to an API. Blue Prism uses a service account to make authenticated requests to the Authentication Server API, and third-party applications can use service accounts to make authenticated requests to the Blue Prism API.

A service account that is used by Blue Prism to communicate with Authentication Server needs to be created and will be used to map and synchronize users between the Blue Prism environment and Authentication Server.

1. Log into Blue Prism Hub as an administrator.
2. Click your profile icon to open the Settings screen, and under User Management click **Service accounts**.
3. On the Service Accounts screen, click **Add account**.
4. Enter an ID for the client application and a name for the client in the Authentication Server database.

5. Under Permissions, select **Authentication Server API**.

Settings > Service accounts > Add a service account

Add a service account

ID *
Client ID which uniquely identifies the client application to the identity provider.

AuthServer

Name *
Client name in the Authentication Server database.

Authentication Server

Permissions
The API(s) to which the client has access.

☐ Blue Prism API

☒ Authentication Server API

☐ Blue Prism Decision API

☐ Interact Remote API

Create service account

6. Click **Create service account**.

The Add a service account screen displays with a generated secret.



This is required when configuring the client details within the Blue Prism application server, to allow this service account to make authenticated requests to the Authentication Server API.

Add a service account

Your service account has been successfully created. The secret for this service account displays below.

Secret
You can copy the secret to your clipboard using the Copy to Clipboard icon.

.....

☐ Show secret


OK

7. Click the Copy to Clipboard icon to copy the generated secret to your clipboard, so you can copy it on the [Blue Prism Server Configuration Details](#) screen later on.


For more details on service accounts, see the [Hub administrator guide](#).

Configure Blue Prism to use Authentication Server

The section below describes how to use a Blue Prism interactive client to configure your Blue Prism environment to use Authentication Server:

 The **User login via Authentication Server** option should only be selected once Blue Prism users have been configured to authenticate via Authentication Server. Once Authentication Server has been enabled, all direct user access for Blue Prism will be directed via Authentication Server and if it has not been configured correctly, users will not be able to log in. Please ensure a [Blue Prism native administrator user](#) still exists in the system who can log into Blue Prism via a direct database connection once Authentication Server has been enabled.

1. Log into the Blue Prism interactive client as an administrator.
2. Navigate to **System > Security - Sign-on Settings**.
3. In the **Authentication Server URL** field, enter https:// followed by the host name configured during the Authentication Server installation.

 The Authentication Server URL can be found in the Internet Information Services (IIS) Manager under Sites > Blue Prism – Authentication Server > Site Bindings > Host Name. This is also the URL you use to log into Blue Prism Hub post installation.


4. Ensure that the **User login via Authentication Server** option is unselected.
5. Click **Apply**.

Configure the Blue Prism application server

To add users from Authentication Server into Blue Prism and to synchronize the user data, the details of the service account created to make authenticated requests to the Authentication Server API must be configured on the Blue Prism application server.

This is configured in the Authentication Server Integration tab on the Blue Prism Server Configuration Details screen.

1. Launch the Blue Prism application server (BPServer.exe from C:\Program Files\Blue Prism Limited\Blue Prism Automate).
2. To open the server configuration, select the relevant environment from the **Current configuration** drop-down and click **Edit**.
3. In the Authentication Server Integration tab, enter the client details of the service account used by Blue Prism to communicate with Authentication Server. These are used for user and service account synchronization and when making calls directly to the Authentication Server API, for example, when adding Authentication Server users to Blue Prism roles, as configured in [Create a service account in Hub on page 7](#).
 - **Client ID** – The client ID of the service account used by Blue Prism to communicate with Authentication Server.
 - **Client Secret** – The client secret key generated by the service account used by Blue Prism to communicate with Authentication Server.

 In Hub 4.7 and later, the client ID is case sensitive. You must ensure you enter the client ID in the same case as defined in the service account.

- Click **Save** to apply the settings.

The screenshot shows the 'Server Configuration Details' dialog box with the 'Authentication Server Integration' tab selected. The 'Client Details' section contains two text input fields: 'Client ID' and 'Client Secret'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Configure Blue Prism users to authenticate via Authentication Server

New Blue Prism environments

If you are configuring a new Blue Prism environment to use Authentication Server, Authentication Server users must be created in Blue Prism Hub first (see the [Hub administrator guide](#) for more details) and then added to Blue Prism by assigning them to a Blue Prism role.

To add one or more Authentication Server users to a Blue Prism role:

- In the Blue Prism interactive client, navigate to **System > Security - User Roles**.
- Select a role from the list and edit the associated permissions if required.
- Click **Manage role membership**.

The Role Membership screen displays.

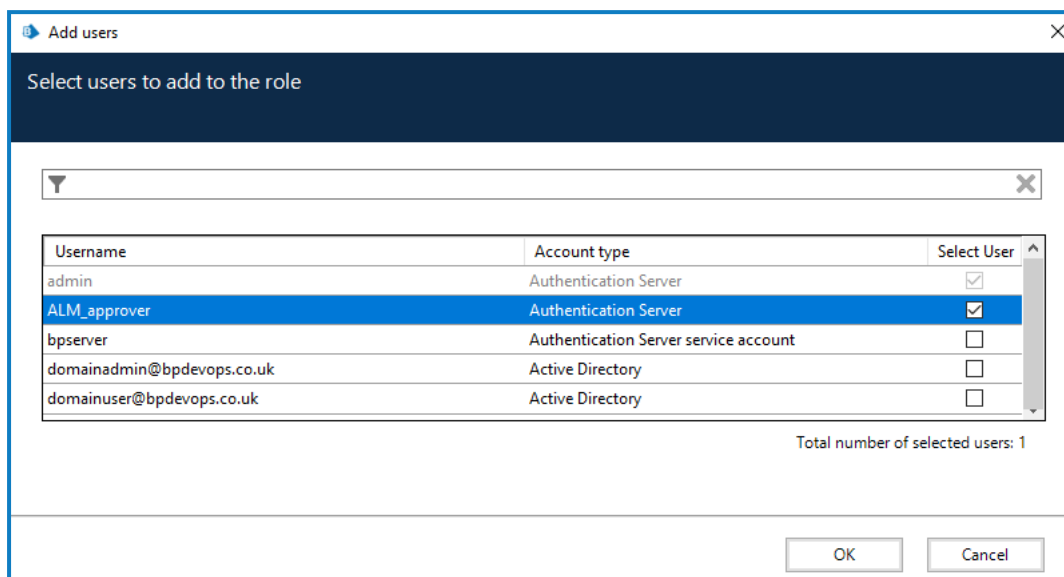
The screenshot shows the 'Role Membership' dialog box. The 'Role Name' field is set to 'System Administrators'. Below it, a message states: 'Members of this role must meet at least one of the following criteria:'. Underneath, it says 'The user is one of the following users:'. A table lists the users:

Full name	Account type	
admin	Authentication Server	

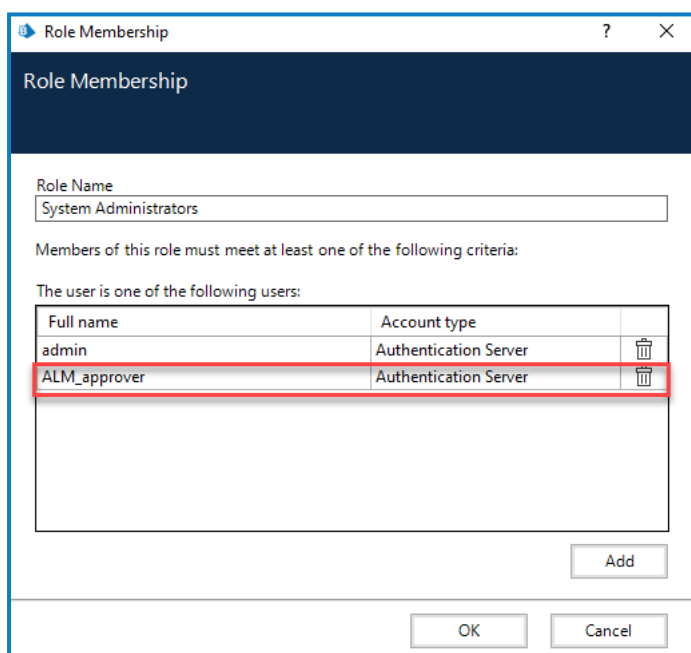
At the bottom right of the table area is an 'Add' button. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

4. Click **Add**.

The Add users dialog displays.

5. Select the Authentication Server user(s) you want to add to the selected role, or search for them using the search box, and click **OK**.

The added Authentication Server user(s) now display on the Role Membership dialog.


6. Click **OK** to save your changes.


Authentication Server users configured to use Active Directory authentication in Hub can also be added to Blue Prism based on their Active Directory security group membership. For more details, see [Add Active Directory users to Blue Prism based on their security group membership](#).

Existing Blue Prism environments

If you are updating a Blue Prism environment, existing Blue Prism native user accounts must be synchronized with the Authentication Server database so that they can continue to log in. To achieve this, a mapping tool must be used to synchronize the existing native users in your Blue Prism and Authentication Server databases with the following scenarios:


- Create native user accounts in Hub for existing Blue Prism native users who do not have a Hub user account yet so Blue Prism native users can use Authentication Server to authenticate in the Blue Prism interactive client.
- Link accounts for native users who already exist in both systems to ensure these are linked together and can access both databases.

 The **Authentication Server – Map users** permission is required to map users using the mapping tool.

 The mapping tool cannot be used in the following scenarios:

- To add Authentication Server users automatically to Blue Prism – Authentication Server users are only added to Blue Prism at the time when they are assigned to a Blue Prism role. For more details, see [New Blue Prism environments on page 10](#).
- To synchronize Blue Prism Active Directory users with Authentication Server – Once Active Directory authentication has been configured in Hub, a Blue Prism user signing in using Active Directory authentication via Authentication Server for the first time will have an account created automatically in Hub, and will be able to continue using Blue Prism with their existing roles. For details on how to manage Active Directory users in Hub, see the [Hub administrator guide](#).

Add users via the mapping tool


 Before starting the mapping, please ensure that a Blue Prism native administrator user exists in the system, and that this user is manually removed from the mapping file before carrying out the mapping process [outlined below](#). This is to ensure that in the event of any issues with the Authentication Server or system configuration, there is always an administrator user available who can log in via a direct database connection.

Create accounts in the Authentication Server database for existing Blue Prism native users who do not have corresponding Hub user accounts yet


1. Open Command Prompt as an administrator and navigate to the Blue Prism installation directory containing AutomateC.exe (for example C:\Program Files\Blue Prism Limited\Blue Prism Automate).
2. Run the following command to get a CSV template file containing a list of all the Blue Prism native users in the database who are available for mapping:

```
automatec /getblueprismtemplateforusermapping <pathtooutputfile> /user <adminuser>  
<adminpwd>
```

3. From Windows Explorer, open the output file and add the first name, last name, and email address for each Blue Prism user you want to add.

 The First Name, Last Name, and Email Address fields do not exist in Blue Prism, so they must be added to create the users in Authentication Server.

4. Delete any users from the file who should not log in via Authentication Server. At least one native administrator user should be removed from the file so they can still log in via a direct database connection.

 If you are using native authentication to also authenticate runtime resources, AutomateC commands, or web service requests, you should also remove from the file any native user accounts required to authenticate these.

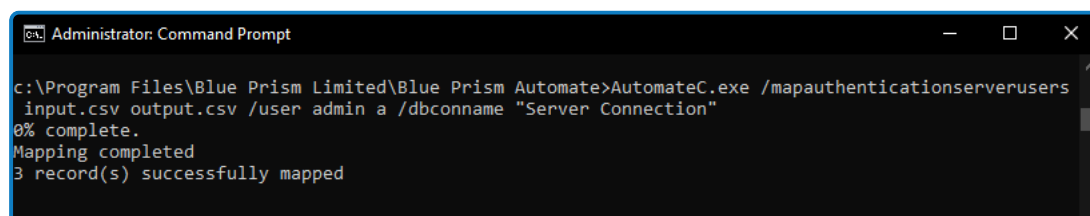
5. Save the CSV file.
6. Open Command Prompt as an administrator and navigate to the Blue Prism installation directory containing AutomateC.exe.
7. Run the following command to complete the user mapping:

```
automatec /mapauthenticationserverusers <input CSV> <output CSV for errors> /user <admin username> <admin password> /dbconname <Blue Prism Server connection name>
```


Where:

- **<input CSV>** – The path to your saved CSV file.
- **<output CSV for errors>** – The path for a file automatically created if there are errors in the mapping process.
- **<admin username>** and **<admin password>** – The credentials for a native admin user in Blue Prism.
- **<Blue Prism server connection name>** – The name of your Blue Prism server connection as set in the [Blue Prism Server settings](#).

For example:



```
Administrator: Command Prompt
c:\Program Files\Blue Prism Limited\Blue Prism Automate>AutomateC.exe /mapauthenticationserverusers
input.csv output.csv /user admin a /dbconname "Server Connection"
0% complete.
Mapping completed
3 record(s) successfully mapped
```

 Ensure the machine you run the command on is able to access the Authentication Server website. For more details, see [Troubleshooting Authentication Server](#).

Map existing Blue Prism users to existing Authentication Server users

1. Open Command Prompt as an administrator and navigate to the Blue Prism installation directory containing AutomateC.exe (for example, C:\Program Files\Blue Prism Limited\Blue Prism Automate).
2. Run the following command to get a CSV template file containing a list of all users available for mapping in the Blue Prism database:

```
automatec /getblueprismtemplateforusermapping <pathtoooutputfile> /user <adminuser>
<adminpwd>
```

3. Run the following command to get a CSV template file containing a list of all users who are available for mapping in the Authentication Server database:

```
automatec /getauthenticationservertemplateforusermapping {outputpath} /dbconname <Blue Prism Server connection name>
```

4. From Windows Explorer, open both output files, and for each Blue Prism user you wish to map, find the corresponding Authentication Server user and copy the Blue Prism username into the Authentication Server output file.



A Blue Prism username and an Authentication Server User ID are required as a minimum. The additional First Name, Last Name, and Email Address fields required in the Authentication Server database should already be present for the Authentication Server users.

5. Delete any users who should not be mapped from the Authentication Server output file. At least one native administrator user should be removed from the file so they can still log in via a direct database connection. You may also want to remove from the file any native user accounts which will be required to authenticate runtime resources, AutomateC commands, or web service requests.
6. Save the Authentication Server output file.
7. Open Command Prompt as an administrator and navigate to the Blue Prism installation directory containing AutomateC.exe.
8. Run the following command to complete the user mapping:

```
automatec /mapauthenticationserverusers <input CSV> <output CSV for errors> /user <admin username> <admin password> /dbconname <Blue Prism Server connection name>
```

Where:

- **<input CSV>** – The path to your saved CSV file.
- **<output CSV for errors>** – The path for a file automatically created if there are errors in the mapping process.
- **<admin username>** and **<admin password>** – The credentials for a native admin user in Blue Prism.
- **<Blue Prism server connection name>** – The name of your Blue Prism server connection as set in the [Blue Prism Server settings](#).

For example:

```
Administrator: Command Prompt
c:\Program Files\Blue Prism Limited\Blue Prism Automate>AutomateC.exe /mapauthenticationserverusers
input.csv output.csv /user admin a /dbconname "Server Connection"
0% complete.
Mapping completed
3 record(s) successfully mapped
```



Ensure the machine you run the command on is able to access the Authentication Server website. For more details, see [Troubleshooting Authentication Server](#).

Authentication Server users cannot be mapped to Blue Prism users that do not exist. If an administrator does not enter a Blue Prism username in the CSV file, but enters an Authentication Server User ID, an error message displays.

For example:

1	BluePrismUsername	AuthenticationServerUserId	FirstName	LastName	Email
2	mbutler	9a45722e-a0fe-4dac-9805-66410bb3c8cc			
3	sjames		Sue	James	sj@email.com
4		f28cfc0a-abdc-4ff2-b77f-a2a1219d66			

Verify that users have been mapped correctly

- In the Blue Prism interactive client, navigate to **System > Security - Users** and check the following:
 - The **Authentication Server** account type displays for native users mapped from the Authentication Server database.
 - The **Authentication Server service account** account type displays for service accounts mapped from the Authentication Server database.

Control

Analytics

Releases

Digital Exchange

System

My Profile

Security - Users

Users

admin

authServerAdmin

authServerAdmin2

authServerAdmin3


testSA2

testSA3

testSA4

User name	Password expiry	Last signed in	Account type
admin	18/01/2022	14/01/2022 15:09:18	Native
authServerAdmin	-	04/01/2022 16:08:37	Authentication Server
authServerAdmin2	-	04/01/2022 16:08:37	Authentication Server
authServerAdmin3	-	04/01/2022 16:08:37	Authentication Server
testSA2	-	-	Authentication Server service account
testSA3	-	-	Authentication Server service account
testSA4	-	-	Authentication Server service account

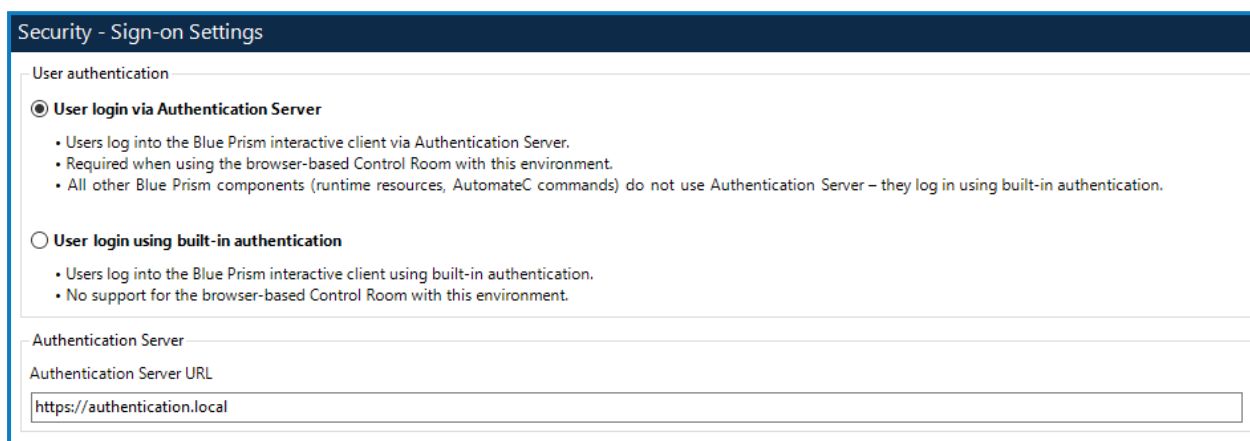
- In Hub, navigate to **Settings > Users** and refresh the users list.
Users mapped from Blue Prism now display in the list.

 You can only perform the mapping once. Once users have been mapped, they cannot be mapped again once Authentication Server has been enabled.

Users created via the mapping tool will be sent an email to set their password manually before logging in for the first time. They will not be able to access Blue Prism until this step has been taken. Users will only receive this email if their email settings have been configured in Hub. For more details, see the [Hub administrator guide](#).

Enable Authentication Server login in your Blue Prism environment

1. In the Blue Prism interactive client, navigate to **System > Security - Sign-on Settings**.
2. Select **User login via Authentication Server** and click **Apply**.



Security - Sign-on Settings

User authentication

☒ **User login via Authentication Server**

- Users log into the Blue Prism interactive client via Authentication Server.
- Required when using the browser-based Control Room with this environment.
- All other Blue Prism components (runtime resources, AutomateC commands) do not use Authentication Server – they log in using built-in authentication.

☐ User login using built-in authentication

- Users log into the Blue Prism interactive client using built-in authentication.
- No support for the browser-based Control Room with this environment.

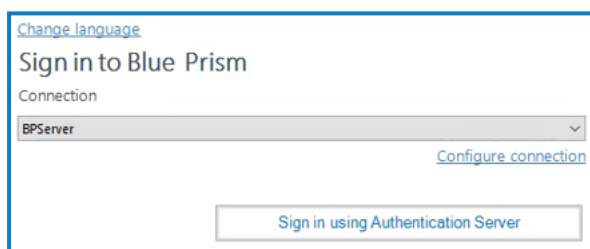
Authentication Server

Authentication Server URL

https://authentication.local

3. Sign out of the Blue Prism interactive client.

The login screen now only displays a **Sign in using Authentication Server** option.



[Change language](#)

Sign in to Blue Prism

Connection

BPSServer

[Configure connection](#)

[Sign in using Authentication Server](#)

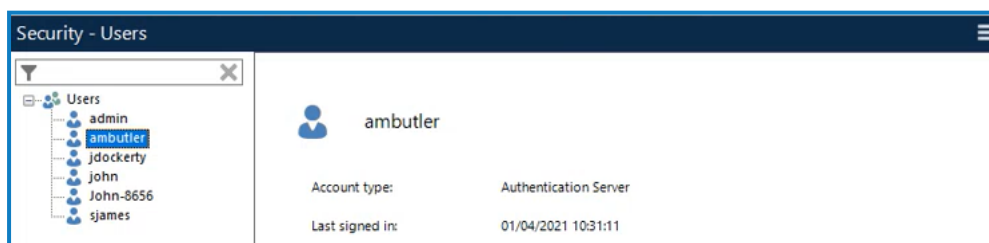
4. Click **Sign in using Authentication Server**.

You will be directed to the Authentication Server login page.

5. Enter your username and password and click **Log in**.

An access token is issued from the Authentication Server in the background which will then be used to automatically log you into the Blue Prism interactive client.

The date and time you last signed in now displays on the **System > Security - Users** screen when right-clicking your username.



Security - Users

Users

- admin
- ambutler**
- jdockerty
- john
- john-8656
- sjames

ambutler

Account type: Authentication Server

Last signed in: 01/04/2021 10:31:11

6. Sign out of Blue Prism and restart the Blue Prism Application Server to ensure the changes are fully applied.

Once Authentication Server has been enabled, native accounts can be added, edited, or deleted locally in Blue Prism, however they can no longer be used to log into the interactive client. These accounts can only be used to authenticate runtime resources, AutomateC commands, and when calling web services exposed on runtime resources.

Synchronize user and service accounts with Authentication Server

User and service account updates can be manually synchronized between the Blue Prism and Authentication Server databases using the **Synchronize users with Authentication Server** option, available from the menu button on the Security - Users screen in the Blue Prism interactive client.

To use this option, the interactive client must be connected via a Blue Prism application server which has been configured with the client details of the service account used to make authenticated requests to the Authentication Server API.



When selected, the following updates will occur:

- Any new Authentication Server service accounts will be added to the Blue Prism database.

Only [service accounts set with the Blue Prism API permission in Hub](#) will display on the Security - Users screen once synchronized with Authentication Server.

Authentication Server users are not added to the Blue Prism environment when using this option, they must be manually assigned to a Blue Prism role on the Role Membership screen, see [New Blue Prism environments on page 10](#). This is to prevent large numbers of Authentication Server users who do need access to Blue Prism, for example, Interact users, from being added into the Blue Prism database.

- Any user and service accounts that have been retired in the Authentication Server database will be retired in the Blue Prism database as well.
- Any user and service accounts that have been unretired in the Authentication Server database will be unretired in the Blue Prism database as well.

When a user account has been deleted in Blue Prism but unretired in Hub, a manual synchronization will be required to reactivate the user account, before they can log into Blue Prism via Authentication Server.

Troubleshooting Authentication Server

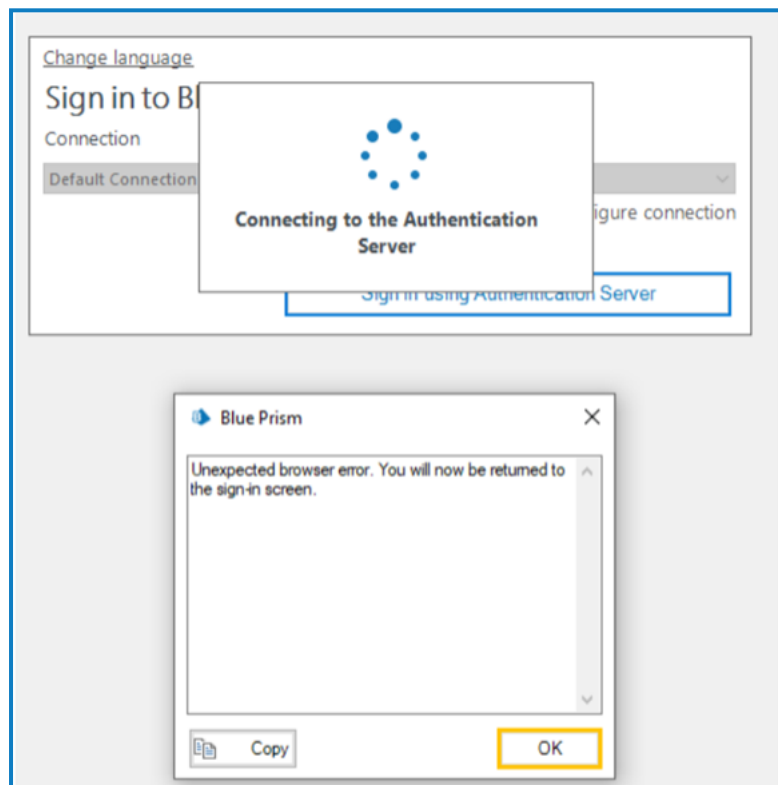
The following sections provide guidance for specific issues that may be experienced while configuring Authentication Server.

Logging into Blue Prism after enabling Authentication Server

Where a Blue Prism deployment has been configured to require all user authentication to be routed via Authentication Server but where Authentication Server is not available, please contact [Blue Prism Support](#) for guidance.

Once Authentication Server has been enabled, you must ensure that a Blue Prism native administrator user remains in the system. Please ensure you have taken a full and verifiable backup of your Blue Prism database before contacting Blue Prism Support.

Error message displays when attempting to sign in using Authentication Server



If the message *Unexpected browser error. You will now be returned to the sign-in screen.* displays when a user attempts to sign in using Authentication Server, the following should be checked:

- Is the Authentication Server URL accessible from the user's device, and has the the correct Authentication Server URL been entered on the Security - Sign-on Settings screen?
 - Validate that the correct Authentication Server URL has been configured in Blue Prism under **System > Security - Sign-on Settings**. If no users can currently log in to view the URL on this page, you can view the URL by running the following query against your Blue Prism database:

```
SELECT authenticationserverurl FROM BPASysConfig
```

- Validate that Authentication Server is running and reachable from the user's machine by entering the URL for the Discovery document in a browser: <authentication server URL>/well-known/openid-configuration

If successful the page will load containing some JSON with details of the Authentication Server as shown below:

```
{
  "issuer": "https://ims:5000/",
  "jwks_uri": "https://ims:5000/.well-known/openid-configuration/jwks",
  "authorization_endpoint": "https://ims:5000/connect/authorize",
  "token_endpoint": "https://ims:5000/connect/token",
  "userinfo_endpoint": "https://ims:5000/connect/userinfo",
  "end_session_endpoint": "https://ims:5000/connect/endsession",
  "check_session_iframe": "https://ims:5000/connect/checksession",
  "revocation_endpoint": "https://ims:5000/connect/revocation",
  "introspection_endpoint": "https://ims:5000/connect/introspect",
  "device_authorization_endpoint": "https://ims:5000/connect/deviceauthorization",
  "frontchannel_logout_supported": true,
  "frontchannel_logout_session_supported": true,
  "backchannel_logout_supported": true,
  "backchannel_logout_session_supported": true,
  "scopes_supported": [
    "roles",
    "openid",
    "profile",
    "bp-api",
    "license-manager",
    "notification-center",
    "audit-api",
    "interact-remote-api",
    "iada-api",
    "file-storage-api",
    "connect-api",
    "ims-api",
    "ss-api",
    "bserver",
    "offline_access"
  ],
  "claims_supported": [
    "role",
    "sub",
    "name",
    "family_name",
    "given_name",
    "middle_name",
    "updated_at",
    "locale",
    "zoneinfo",
    "birthdate",
    "gender",
    "website",
    "picture",
    "profile",
    "nick_name",
    "preferred_username"
  ],
  "grant_types_supported": [
    "authorization_code",
    "client_credentials",
    "refresh_token",
    "implicit",
    "password",
    "urn:ietf:params:oauth:grant-type:device_code"
  ],
  "response_types_supported": [
    "code",
    "token",
    "id_token",
    "id_token token",
    "code id_token",
    "code token",
    "code id_token token"
  ],
  "response_modes_supported": [
    "form_post",
    "query",
    "fragment"
  ],
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post",
    "id_token_signing_alg_values_supported"
  ],
  "subject_types_supported": [
    "public"
  ],
  "code_challenge_methods_supported": [
    "plain",
    "S256"
  ],
  "request_parameter_supported": true
}
```


If the page cannot be reached you may need to restart the site from the application pool in IIS. For more details, click [here](#).

- Validate that you can browse to the correct Authentication Server URL by opening IIS Manager (inetmgr.exe) and locating the Blue Prism - Authentication Server website. Right-click the website and click **Manage Website > Browse**. The Authentication Server website will open in your default browser. For more details on troubleshooting Hub sites such as Authentication Server, click [here](#).
- Is there a network problem?
 - Check that the SSL certificate is valid. For more details, click [here](#).
 - Check that a proxy is not preventing Blue Prism from connecting to Authentication Server. If you need to disable it, you can do so under Internet Properties > Local Area Network (LAN) Settings by deselecting the option **Use a proxy server for your LAN**. For more details on configuring proxy settings, click [here](#).
- Has the WebView2 runtime been installed on the machine that runs the Blue Prism interactive client?
 - For more details, see the [Authentication Server configuration prerequisites](#).


Logging into Authentication Server using Active Directory authentication

If login failures or performance issues are encountered during the login process via Active Directory, system administrators can check if further Active Directory settings need to be added to the Authentication Server appsettings.json file. To edit the appsettings.json file:

1. Open Windows Explorer and navigate to the Authentication Server install location.
To check the install location, open Internet Information Services (IIS) Manager, select the Authentication Server site and click **Explore**.
2. Back up the appsettings.json file.
3. Open the appsettings.json file in a text editor.
4. Locate the lms section of the file.
5. If not already present, add an ActiveDirectory section.

 If the ActiveDirectory section is already present, you might see other settings in that section based on your Active Directory configuration, so the examples in the sections below are only illustrative.

6. Save the file if you have made any changes.

 Authentication Server must be restarted after any changes have been made to the appsettings.json file.

To restart Authentication Server:

1. Open Internet Information Services (IIS) Manager.
2. In the list of connections, select **Blue Prism - Authentication Server**.
This is the default site name – if you have used a custom site name, select the appropriate connection.
3. Click **Restart** from the Manage Website controls.

Check if the Active Directory timeout limit needs to be configured

When Authentication Server attempts to query a Domain Controller, by default it will wait five seconds for a response before triggering a *System.TimeoutException* error. However, this value can be configured if required in the following scenarios:

- If users are experiencing performance issues when logging in via Active Directory and the logs show several instances of *System.TimeoutException: Timeout after 5 seconds*, the value may need to be decreased. The range is between 1 and 60 seconds.
- If users are being prevented from logging in via Active Directory and the logs show several instances of *System.TimeoutException: Timeout after 5 seconds*, the value may need to be increased. The range is between 1 and 60 seconds.

To configure the Active Directory timeout limit:


1. In the ActiveDirectory section of the appsettings.json file, add a QueryTimeoutSeconds setting and a value depending on your scenario, see example below for a decreased value.

```
{
  "Ims" : {
    "ActiveDirectory": {
      "QueryTimeoutSeconds": 3
    }
  }
}
```

2. Save the file.
3. [Restart Authentication Server](#).

Check if the Active Directory domains used during login need to be manually configured

To reduce the time taken for the Active Directory cache to be populated during user login, system administrators can manually configure trusted Active Directory domains that will be queried during the login process. If at least one Active Directory domain is manually configured, these settings will be used during the login process to query only the configured domain(s), rather than programmatically identifying which domains can be queried.

 When a new domain is added to Active Directory, it must also be added to the configuration. Otherwise it will be ignored and users belonging to this domain will not be able to log in until the configuration has been updated.

Any Active Directory domains that meet one or more of the following criteria can be manually configured if using Authentication Server 4.6:

- Contain users that must be able to log in.
- Contain security groups that are assigned directly to Hub or Interact roles in Authentication Server.
- Contain parent security groups which include security groups that are directly assigned to Hub or Interact roles in Authentication Server.

If using Authentication Server 4.7, only Active Directory domains which meet the following criteria should be manually configured:

- Contain users that have an alternative User Principal Name (UPN) suffix that is different to the Domain Name System (DNS) name of the Active Directory domain. For example, corp.dir.company.com (DNS name) and company.com (alias suffix), where john@company.com is the UPN.

The manual configuration requires adding the Active Directory domain name, forest name, and security identifier in the Authentication Server appsettings.json file for each required domain. To do this:

1. In the ActiveDirectory section of the appsettings.json file, add a TrustedDomains section.
2. Add the required information for each domain, for example:
 - DomainName – The name of the Active Directory domain(s) that will be manually configured.
 - ForestName – The name of the forest in which the Active Directory domain resides.
 - Sid – The security identifier for the Active Directory domain.

```
{
  "Ims": {
    "ActiveDirectory": {
      "TrustedDomains": [
        {
          "DomainName": "domain.com",
          "ForestName": "my.domain.com",
          "Sid": "S-1-27-1-3452"
        },
        {
          "DomainName": "company.com",
          "ForestName": "my.company.com",
          "Sid": "S-2-23-1-3458"
        },
        {
          "DomainName": "enterprise.com",
          "ForestName": "enterprise.com",
          "Sid": "S-3-23-1-3459"
        }
      ]
    }
  },
}
```

3. Save the file.
4. [Restart Authentication Server.](#)

Check if cache settings for stored Active Directory domains need to be configured

To further improve performance during the login process, the behavior of the cache that stores the discovered domains can be configured by setting a refresh interval and a maximum cache duration in the Authentication Server appsettings.json file.

- The refresh interval is the interval in minutes at which the cached data will be updated from Active Directory. The value can be set between 5 and 1440 minutes. The default value is 5.
- The maximum cache duration is the amount of time in minutes that the data will be held in the cache before it is invalidated. The value can be set between 5 and 1440 minutes. The default value is 30 if using Authentication Server 4.6. If using Authentication Server 4.7, the default value is 1440.



These two settings must be configured as a pair, and the maximum cache duration should be set higher than the refresh interval. If one or both settings are not configured, the default values will be used.

The cache is populated in Authentication Server when:

- Starting or restarting the Authentication Server site.
- Enabling Active Directory authentication in [Blue Prism Hub > Authentication settings](#).



The cache is not populated in Authentication Server unless Active Directory authentication has been enabled.

To add the cache settings to the Authentication Server appsettings.json file:

1. In the ActiveDirectory section, add the MaxCacheDurationMinutes and CacheRefreshIntervalMinutes settings and their values, for example:

```
{
  "Ims" : {
    "ActiveDirectory": {
      "MaxCacheDurationMinutes": 60,
      "CacheRefreshIntervalMinutes": 10
    }
  }
}
```

2. Save the file.
3. [Restart Authentication Server](#).

Check if Domain Controller name mappings need to be configured

The following error message may display when searching for Active Directory users or security groups, and when adding or editing Active Directory domains: *Invalid credentials. Please check your credentials*. This could occur if the domain of interest is on a different network from the network on which Authentication Server is running.

If you are certain that you have provided the correct credentials when you created an Active Directory domain record, you can configure Domain Controller name mappings in the appsettings.json file so Active Directory queries for the domain specified in DomainName are directed to the endpoint defined in DomainControllerName.

To do this:

1. In the ActiveDirectory section of the appsettings.json file, add a DomainControllerNameMappings section.

2. Add the required information for each domain and Domain Controller, for example:
 - **DomainName** – The name of your Active Directory domain or the DNS name of the domain.
 - **DomainControllerName** – The DNS name of the domain or the FQDN of a Domain Controller in the domain.

```
{
  "Ims": {
    "ActiveDirectory": {
      "DomainControllerNameMappings": [
        {
          "DomainName": "company.com",
          "DomainControllerName": "server-id.company.com"
        },
        {
          "DomainName": "my.company.com",
          "DomainControllerName": "server-id.my.company.com"
        }
      ]
    }
  }
}
```

3. Save the file.
4. [Restart Authentication Server](#).

Error message displays in the output CSV file when running the mapping function for the first time

The message *An error occurred when creating the Authentication Server user record* could display in the output CSV file when running the mapping function for the first time in the following scenarios:

- If the [service account you created in Hub](#) for communication between Blue Prism and Authentication Server has not been granted the Authentication Server API permission.
- If the [client ID and client secret of the service account](#) have not been correctly added in the Client Details section of the **Authentication Server Integration** tab on the Blue Prism Server Configuration Details screen.
- When [mapping users from Blue Prism to Authentication Server](#), if the user you are trying to map already exists in the Authentication Server database, the mapping function will check for the FirstName, LastName and Email details. If one of these already exists in Authentication Server, the user record will not be mapped.
- If the machine you [run the command](#) on is not able to access the Authentication Server website.

Authentication Server users only have access to the Home and Digital Exchange tabs when they sign into the Blue Prism interactive client

Authentication Server manages users' access to Blue Prism and Hub, however, roles and permissions are managed locally in each application. Please contact your Blue Prism system administrators to assign you the necessary roles and permissions to view the entire Blue Prism application.