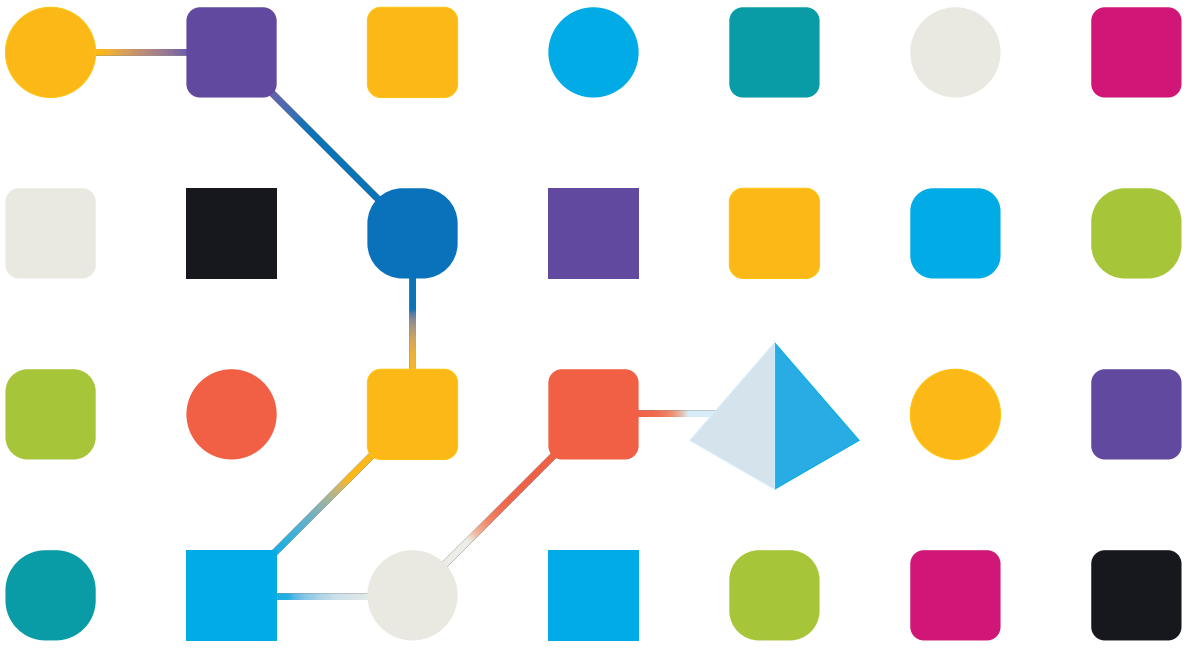
Blue Prism 7.0

Authentication Server Configuration Guide

Document Revision: 2.0



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

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 4.3 or later) if using the Blue Prism API and/or browser-based Control Room with version 7.0 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 only be able to use basic authentication (username and password) and LDAP authentication to log in via Authentication Server.

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 7.0 and configured as a multi-authentication environment. See Blue Prism Enterprise installation guide for guidance.
- A Blue Prism application server that can be configured to integrate with Authentication Server, see Configure RabbitMQ messaging via Blue Prism server on page 15.
- A working Blue Prism Hub deployment running version 4.3 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.

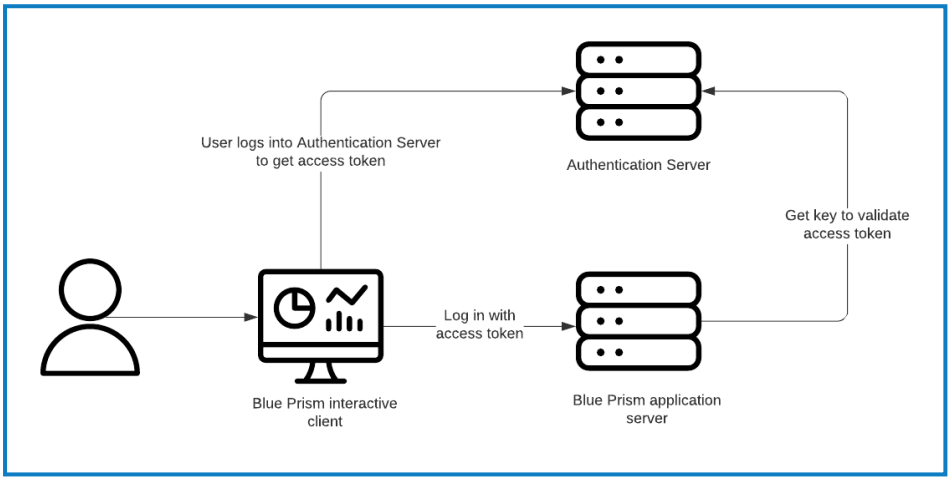
Typical deployment

Blue Prism environments configured to use Authentication Server

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

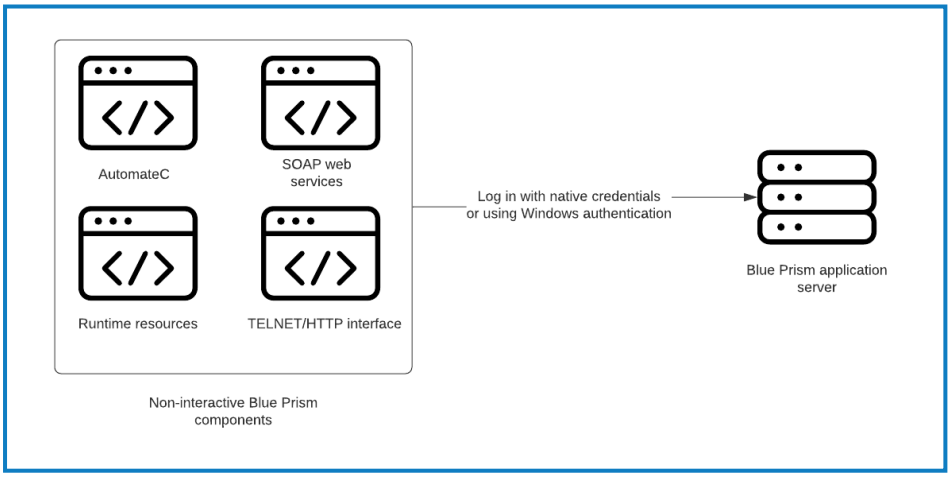
Interactive client authentication

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



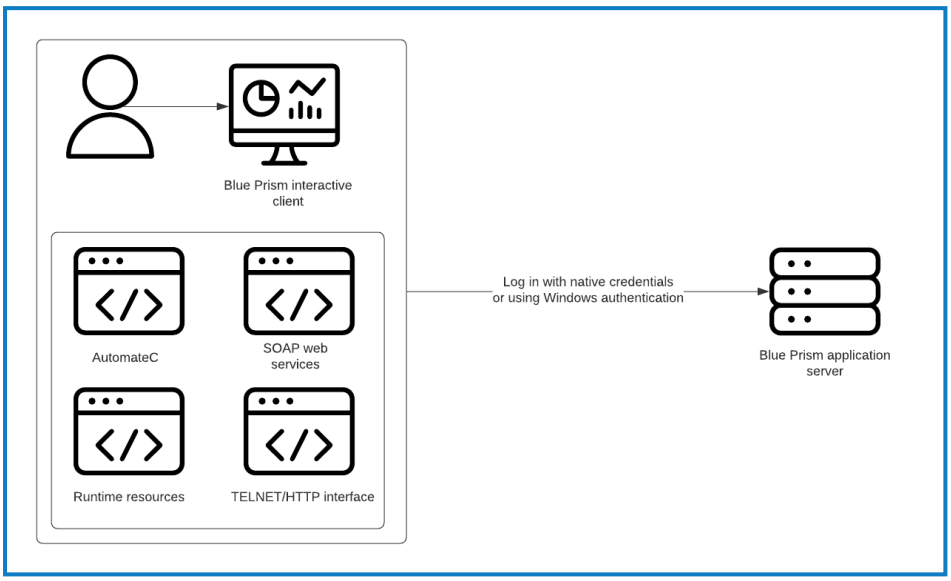
Authentication for other components

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 multi-authentication 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 Blue Prism users to authenticate via Authentication Server.
4. Enable Authentication Server in your Blue Prism environment.
5. Configure the messaging function via the Blue Prism application 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.

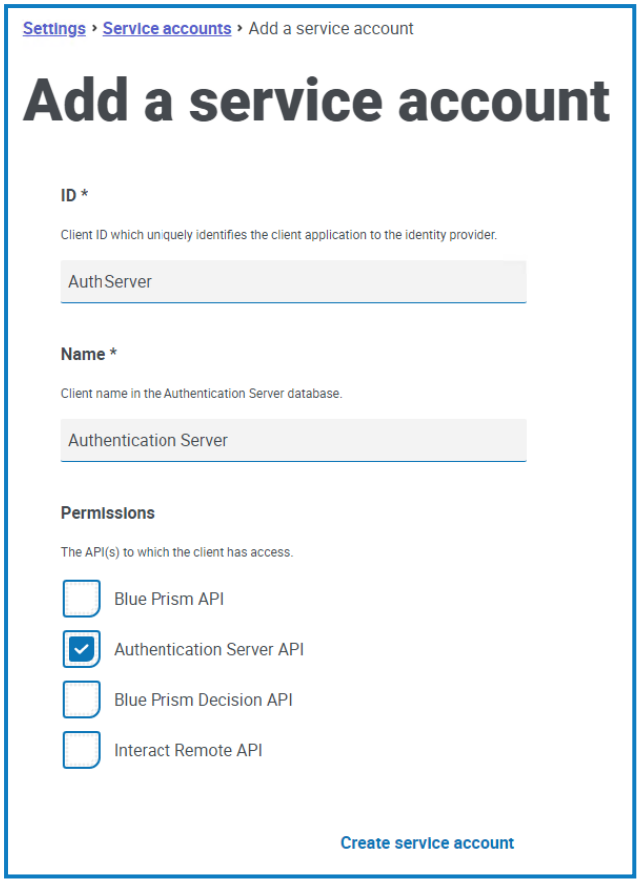
Create a service account in Hub

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 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.

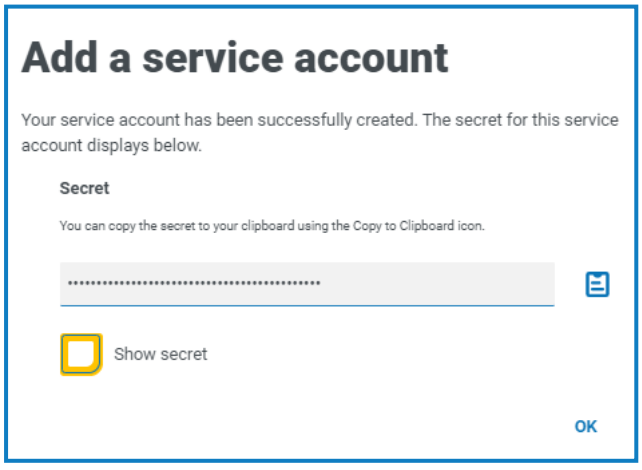
5. Under Permissions, select **Authentication Server API**.



6. Click **Create service account**.

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

> This is used to make authenticated requests to the Authentication Server API and to configure the Authentication Server credential required to enable Authentication Server in the Blue Prism interactive client.



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

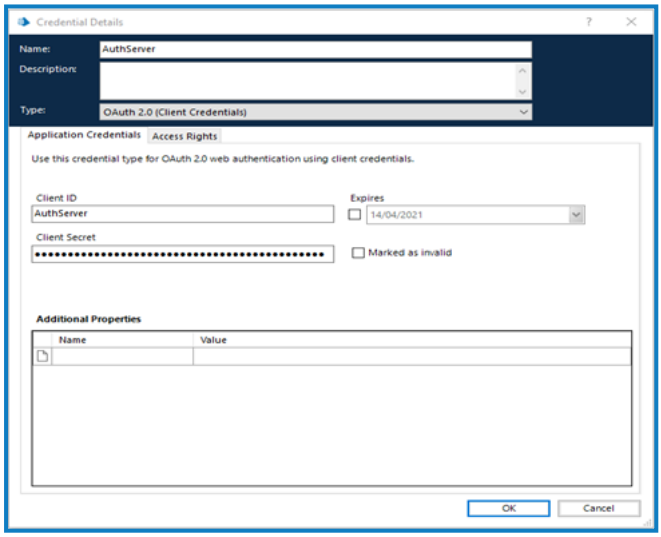
The section below describes how to use a Blue Prism interactive client to configure your Blue Prism environment to use Authentication Server by:

- creating a Blue Prism credential that will be used by Blue Prism to connect to Authentication Server to allow users to be mapped across the two databases. This credential will contain the client ID and secret details of the service account created in Hub.
- adding the Authentication Server credential and the Authentication Server URL on the System > Security - Sign-on Settings screen.

To carry out this configuration, you need to be granted Hub administrator and Blue Prism interactive client system administrator rights.

Create OAuth 2.0 Client Credential

1. Log into the Blue Prism interactive client as an administrator.
2. In the Blue Prism interactive client, navigate to **System** > **Security - Credentials**.
3. In the right-hand side menu, click **New** to create a new credential.
4. In the **Application Credentials** tab, enter a name and a description for the credential, and in the **Type** drop-down, select **OAuth 2.0 (Client Credentials)**.
5. In the **Client ID** field, enter the client ID used for the service account you created in Hub.
6. In the **Client Secret** field, paste the secret generated in Hub from your clipboard.



7. Click **OK** to save.

> No access rights should be granted to this credential as access is not required by process automations.

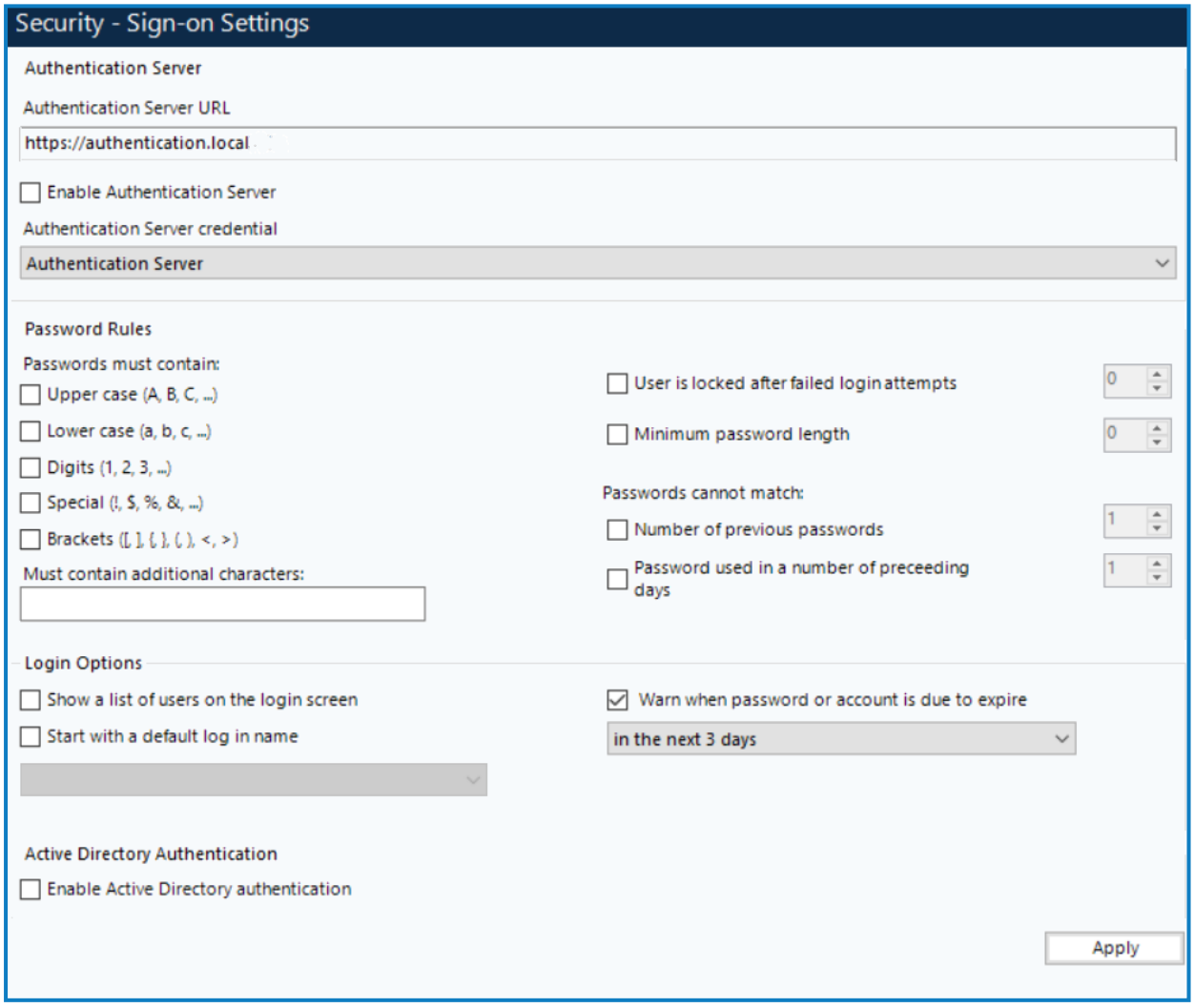
Configure sign-on settings

⚠ The **Enable 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. Navigate to **System** > **Security - Sign-on Settings**.
2. 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.

3. In the Authentication Server credential drop-down, select the credential created on the System > Security - Credentials screen.



4. Ensure that the **Enable Authentication Server** option is unselected.
5. Click **Apply**.

Configure Blue Prism users to authenticate via Authentication Server

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.
- Create Blue Prism native user accounts in Blue Prism for users who already exist in the Authentication Server database but not in the Blue Prism database to allow Hub users to access the Blue Prism environment.
- 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.

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 mapping file

1. Create a CSV file and add the following headings: BluePrismUsername, AuthenticationServerUserID, FirstName, LastName, and Email. A Blue Prism username or an Authentication Server ID are required as a minimum.

   The column order must be preserved as shown in the example below, but the column headings can be customized as required.

2. In the CSV file, add the available user details from the Blue Prism and/or Authentication Server databases, depending on the applicable scenario:
   - If you want to create accounts in the Authentication Server database for existing Blue Prism native users who are not in the Authentication Server database yet – add their Blue Prism username to the CSV file, along with a First Name, Last Name and Email address.

     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.

     You should 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 authenticate runtime resources, AutomateC commands, or web service requests, you should also remove from the file any native user accounts required to authenticate these.
   - If you want to create Blue Prism native accounts in the Blue Prism database for users who already exist in the Authentication Server database but not in the Blue Prism database – add their Authentication Server ID from the PublicId field in the Users table in the Authentication Server database.
   - If you want to link accounts for users who already exist in both databases – add their Blue Prism username and their Authentication Server ID. The Authentication Server ID can be found in the PublicId field in the Users table in the Authentication Server database. To access this, open SQL Management Studio and navigate to the user list in AuthenticationServerDB - Users or run the following query on the Authentication Server database:

     ```
     select username, publicid from Users
     ```

   CSV file example:

	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			

   In Blue Prism 7.0, the Blue Prism username can only contain a sequence of letters, digits, periods, hyphens, or underscores, and without spaces when it is mapped to the Authentication Server database, otherwise the mapping will fail. Please remove any other characters before attempting the user mapping.

3. Save the CSV file.

If there are any instances where an Authentication Server username already exists in Blue Prism, then when the mapping takes place, a random 4-digit number is appended to the new username to ensure it is unique and to differentiate between the users in audit logs.

Use AutomateC to process the mapping file

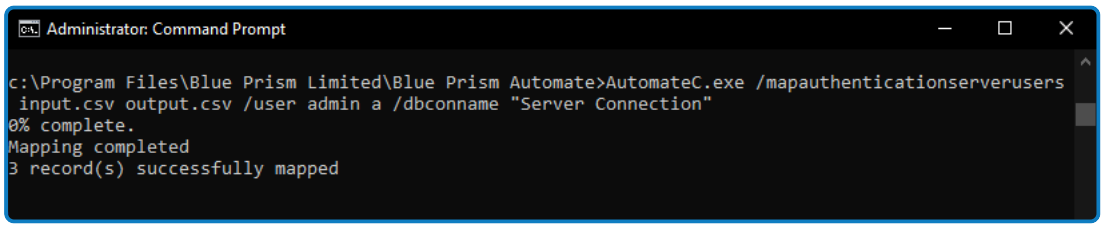
1. Open Command Prompt as an administrator and navigate to the Blue Prism installation directory containing AutomateC.exe (for example `C:\Program Files\Blue Prism Limited\Blue Prism Automate`).
2. Run the following command:

```
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.

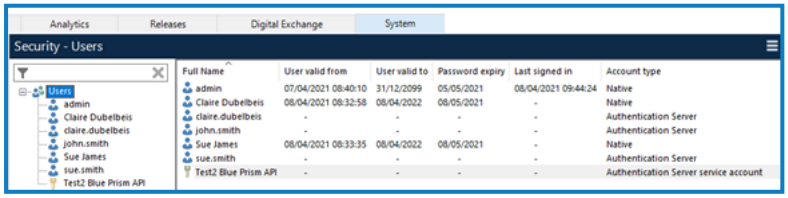
For example:



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

Verify users have been mapped correctly

1. 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.



2. Assign the appropriate roles and permissions to all users mapped from Hub, as described in Manage roles.
3. 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, new users will be created in Hub and synchronized in the Blue Prism interactive client via the messaging server.

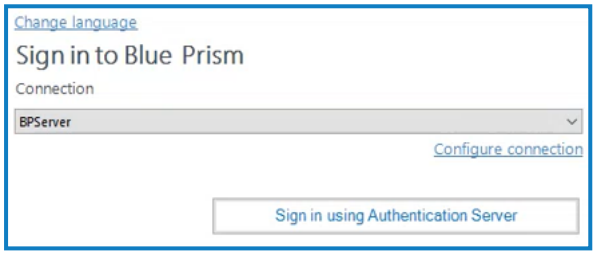
Users created via the mapping tool will be sent an email to set their password manually before logging in for the first time. They will not be able to access Blue Prism until this step has been taken. Users will only receive this email if their email settings have been configured in Hub. For more details,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

Enable Authentication Server in your Blue Prism environment

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

3. Sign out of the Blue Prism interactive client.

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



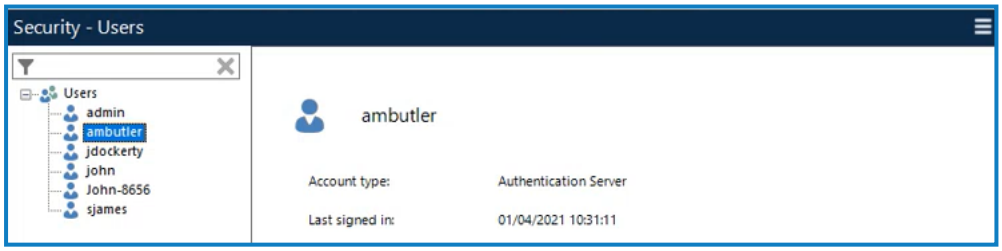
4. Click **Sign in using Authentication Server**.

   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.



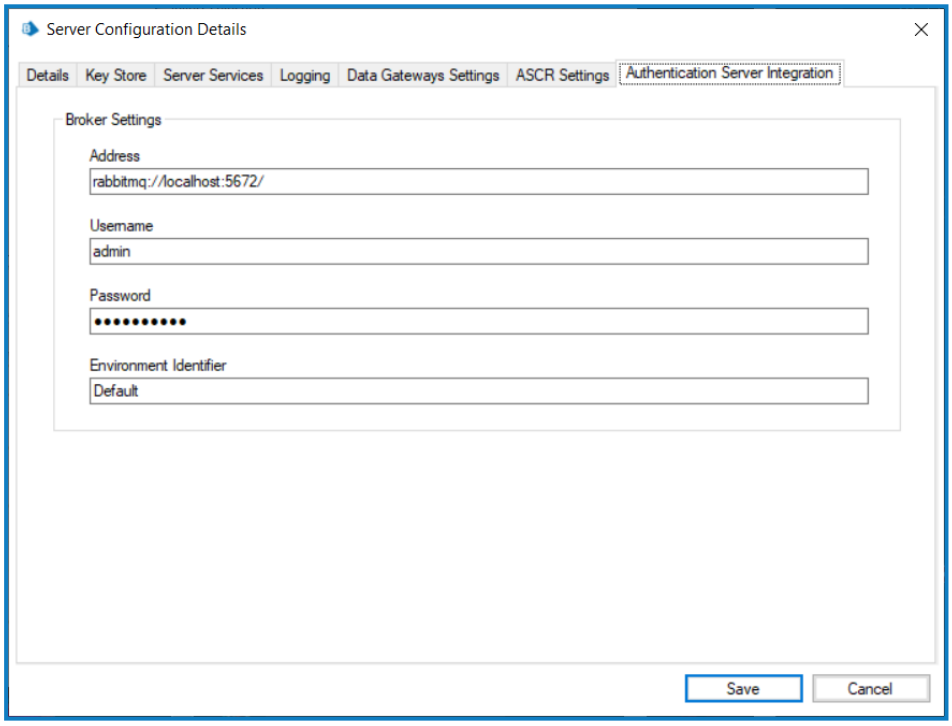
Once Authentication Server has been enabled, native accounts and mapped Active Directory accounts can be added, edited, or deleted locally in Blue Prism, however they can no longer be used to log into the interactive client. These accounts can only be used to authenticate runtime resources, AutomateC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

Configure RabbitMQ messaging via Blue Prism server

For new users created in Hub to be able to sign into the Blue Prism environment via Authentication Server, the Blue Prism application server must be configured to handle user events that are published to a message queue by Authentication 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:
    a. Enter the broker settings as configured in the Blue Prism Hub installation:
        - **Address** – RabbitMQ address in format rabbitmq://<host>:<port>/
        - **Username** – RabbitMQ username
        - **Password** – RabbitMQ password
        - **Environment Identifier** – Used to distinguish between different configured Blue Prism environments if applicable. This value can only contain a sequence of the following characters: letters, digits, hyphens, underscores, periods, and colons.



    b. Click **Save** to apply the settings.
4. Return to the Server configuration screen and click **Start** to start the BPServer.

    To confirm that the message bus has been configured correctly, you should see the following lines:

    [date stamp]: Starting message bus

    [date stamp]: Message bus started

    > If the Blue Prism server is up and running, any users or service accounts created, edited, or deleted in Hub will also be updated in Blue Prism. Should the Blue Prism server go offline or come online later, the synchronization will complete once the connection has been restored.

5. To verify that the message queue has been created, launch the RabbitMQ URL in a browser as configured in the Blue Prism Hub installation, for example, rabbitmq://localhost:15672/.
6. In the **Queues** tab, locate the queue just created via the Authentication Server Integration settings above, for example *blue-prism-app-server.user-synchronization.fresh-install*.

Troubleshooting Authentication Server

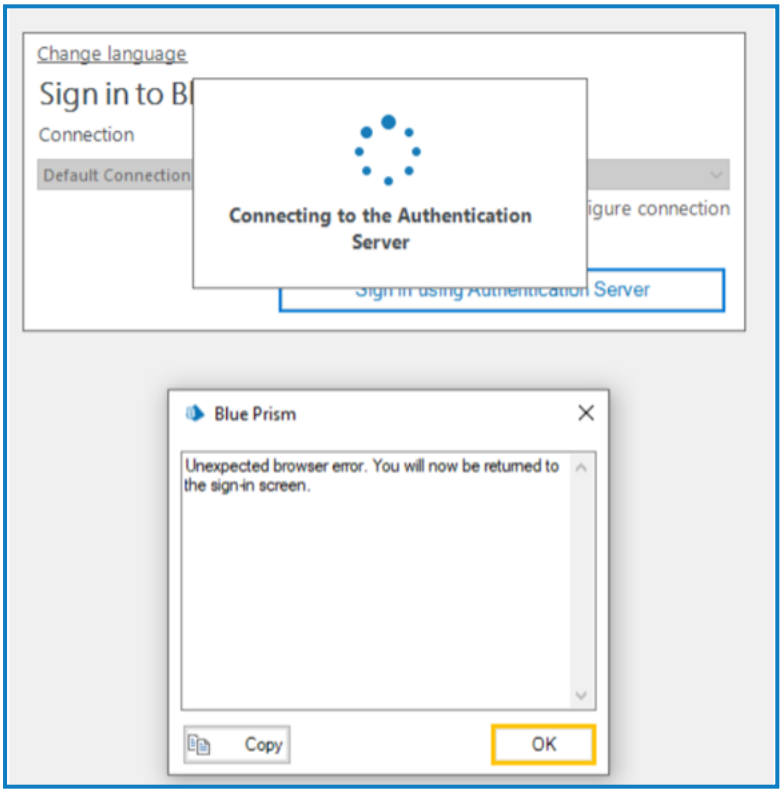
The following sections provide guidance for specific issues that may be experienced while configuring Authentication Server.

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



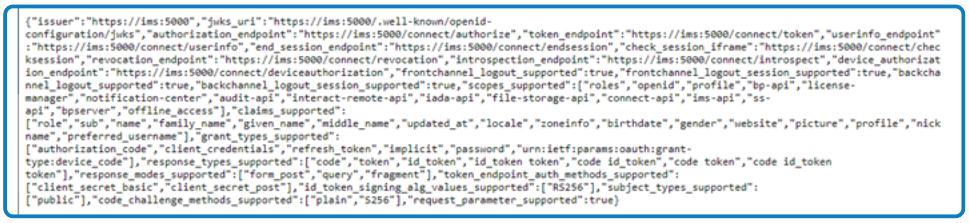
If the message *Unexpected browser error. You will now be returned to the sign-in screen.* displays when a user attempts to sign in using Authentication Server, the following should be checked:

- 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:

    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.

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 key of the service account have not been correctly added to a Blue Prism OAuth2.0 (Client Credential) and configured on the Security - Sign-on Settings page in Blue Prism.

  To verify this:

1. Log into the Blue Prism interactive client and navigate to **System** > **Security - Sign-on Settings**, and check the name of the credential selected in the Authentication Server credential drop-down.
2. Navigate to **System** > **Security – Credentials**, select the credential you have created for Authentication Server and click **Edit**.
3. Check that the client ID entered matches the client ID from the service account in Hub.

- 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. Users that are mapped from Hub to Blue Prism will not have any roles and permissions assigned to them, and a Blue Prism system administrator will need to manually assign the roles and permission for each user after they have been mapped. For more details, see Manage Blue Prism user roles.

Authentication Server settings do not display in your Blue Prism environment

If your Blue Prism environment has been configured to use Authentication Server, the configuration settings should display under System > Security > Sign-on Settings. If they don't, a few reasons could be:

- You haven't upgraded to Blue Prism 7.0, which is the first version in which Authentication Server is available.
- Your Blue Prism environment is a single-authentication (Active Directory SSO) environment, which cannot be configured to use Authentication Server.

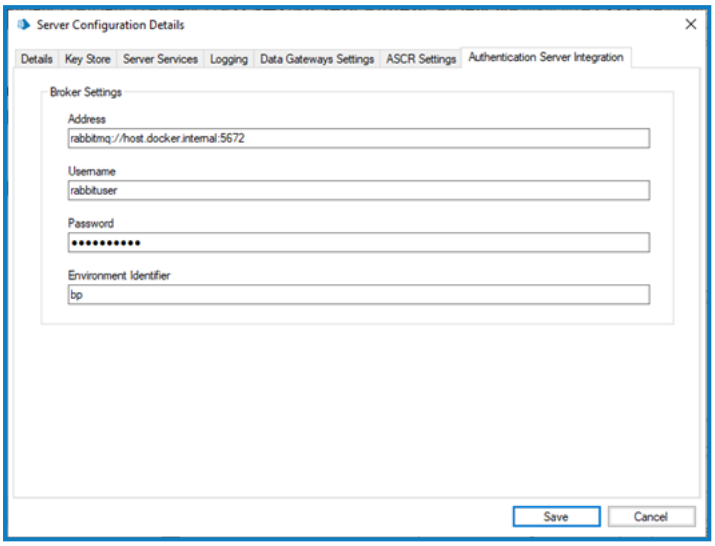
For more details, please refer to this Knowledge Base article.

The RabbitMQ message bus does not start when starting the Blue Prism application server

If the RabbitMQ message bus does not start when starting the Blue Prism application server (a warning will display in the server output window or the server logs), check the following:

- Is RabbitMQ running?
  - Check that the RabbitMQ service is running by locating RabbitMQ in the list of services available on the operating system where RabbitMQ has been installed.
- Are the RabbitMQ address, virtual host and port details correct?
  - The format should be {protocol}://{host}:{port}/{virtual host}, for example, rabbitmq://<rabbitmqserver>:5672/.
- Are the RabbitMQ username and password correct?
  - The guest user only works over a localhost connection. Ensure a new user has been created with the correct virtual host permissions.

The details above can be checked by accessing the RabbitMQ Management Portal from within a browser via https://<rabbitmqserver>:15672/ and logging in with the configured user's credentials.

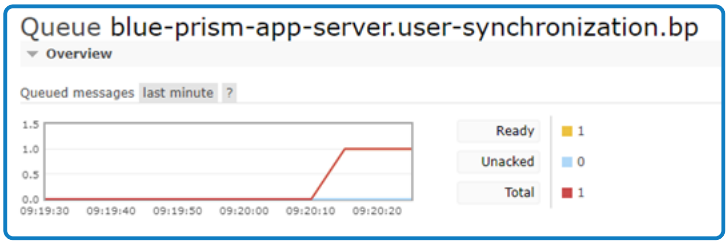


Users created in Authentication Server do not appear in the Blue Prism interactive client

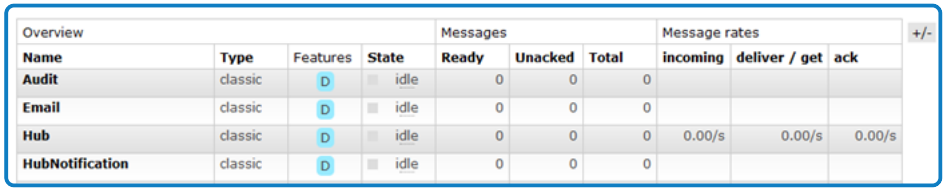
If users created in Authentication Server do not appear in the Blue Prism interactive client after you have configured the message broker settings and started BPServer, check the following:

- Is RabbitMQ running?
  - Check that the RabbitMQ service is running by entering Services into your search bar and and ensuring RabbitMQ displays in the list.

- Check the RabbitMQ Management Portal for the following:
  - Are there any messages on the user synchronization queue?
    - If yes, is BPServer running? BPServer is the only consumer of the user synchronization queue, therefore messages on the queue (indicated by a positive integer in the *Ready* column) mean that BPServer is not running or that the BPServer Authentication Server Integration settings are incorrect.
      - If that is the case, check that the Authentication Server Integration settings in BPServer match the correct queue. Using the example below, the environment identifier should be *bp*.

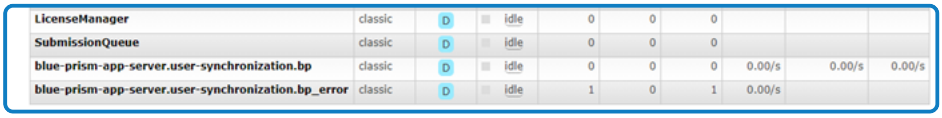


      - Ensure BPServer is started.
    - If there are no messages on the user synchronization queue currently, have there been any messages on the queue? This can be checked by inspecting the message rates for each queue, for example, a queue with activity will have a 0.00/s value, whereas a queue with no messages will be empty.



Overview				Messages			Message rates			+/-
Name	Type	Features	State	Ready	Unacked	Total	incoming	deliver / get	ack	
Audit	classic	D	idle	0	0	0				
Email	classic	D	idle	0	0	0				
Hub	classic	D	idle	0	0	0	0.00/s	0.00/s	0.00/s	
HubNotification	classic	D	idle	0	0	0				

  - Have any messages been consumed on the user synchronization queue?
    - If visible in the RabbitMQ Management Portal, this indicates that the user synchronization function is working end to end and there has been an issue when processing the event.
  - If a user or service account has failed to be created or updated, there will be another queue that will be created which contains application errors (this is known as the error queue). The queue name will be identical, with an additional suffix of *_error*.



LicenseManager	classic	D	idle	0	0	0			
SubmissionQueue	classic	D	idle	0	0	0			
blue-prism-app-server.user-synchronization.bp	classic	D	idle	0	0	0	0.00/s	0.00/s	0.00/s
blue-prism-app-server.user-synchronization.bp_error	classic	D	idle	1	0	1	0.00/s		

- Errors (and any messages) can be inspected to diagnose problems within the application. To do this, first select the queue, and then select the Get Messages option. You can specify how many messages to get. As this is a queue, if we get 1 message then the message at the front of the queue is returned. The message at the front of the queue is the oldest message. Once selected, you can see the contents of the message. In the event of an error message, you can see details such as exception type, message type, and a more detailed stack trace.

- Do your RabbitMQ username and password contain any of the following special characters ? #/:?@\"$'
  - If yes, please change your username or password in the RabbitMQ Management Portal as these characters are not accepted.
  - If these are the user credentials that were specified when installing Hub, then you will need to create a new RabbitMQ connection string and encrypt the value using the Blue Prism Data Protector Tool. Once encrypted, this new value will need to be added to the relevant appsettings files for Hub, and Authentication Server. For more details, see Blue Prism Data Protector Tool.

Using Authentication Server with an existing RabbitMQ instance that uses external certificate-based authentication

If you are using Authentication Server with an existing RabbitMQ instance that uses external certificate-based authentication, credential (PLAIN) authentication will need to be enabled into their instance. More details are available here.

If you have never configured the RabbitMQ function via the Authentication Server Integration tab in the Blue Prism application server, the RabbitMQ Management UI would not have a queue created for that environment, meaning any changes made in Hub would not be queued. However, once that configuration has been set and verified it works successfully, any future updates made in Hub will be queued, whether the Blue Prism application server is running or not.