blueprism®

Robotic Process Automation Software

Installing Enterprise Edition

User Guide

Major version: 6.3

Document Revision: 1.1

For more information please contact:
info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 757 7476
www.blueprism.com

Trademarks and copyrights

Blue Prism Limited, Centrix House, Crow Lane East, Newton-le-Willows, WA12 9UY, United Kingdom

Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Contents

Introduction

This document provides guidance on the process to follow when installing Blue Prism and contains information on how to test that the installation has been successful.

A number of more advanced topics are also included within this guide to provide information on troubleshooting installations and configuring advanced settings and options.

If further assistance is required whilst following this document please contact your Blue Prism Account Manager or Technical Support - support@blueprism.com.

This information relates only to the version of Blue Prism specified in the document title.

It is strongly recommended that the *Blue Prism Infrastructure Reference Guide* is reviewed prior to starting deployment as it contains insight and information for each of the Blue Prism components, and provides guidance and considerations on the main options available.

Related Documents

There are a number of other documents that provide additional information about specific aspects of the implementation of Blue Prism. These can be provided by your Account Manager or via Technical Support.

Document Title	Description
Blue Prism Infrastructure Reference Guide	A detailed overview of Blue Prism infrastructure templates, including architectures, failover and DR strategies, communication methods and virtualization requirements
V6 User Guide - Setting up the Java Access Bridge	A detailed overview of the steps required to install the Access Bridge using the installer and manually, along with methods for verifying the installation.
V6 Data Sheet - Active Directory Integration	A guide to integrating Blue Prism with Active Directory for user authentication
V6.3 Data Sheet - Securing Network Connectivity	A summary of the controls available to enable architects and system implementers to understand how to secure the network connectivity associated with Blue Prism.
V6 Data Sheet - Selecting a BP Server Connection mode	Provides information about the different connection modes that a Blue Prism Server can be configured to use.

Preparation

Prior to undertaking an installation of Blue Prism it is important to consider what type of deployment is required:

- Multi-device Deployment - recommended

  Blue Prism components deployed across a number of devices whereby all database connections are established via an Application Server.

  - Provides an extensible deployment of Blue Prism suitable for a broad range of scenarios.
  - Advanced techniques relating to deploying additional Application Servers, or securing and hardening the environment will commonly require this type of deployment.

- Standalone Deployment – for evaluating Blue Prism

  A single standalone device containing a Blue Prism Interactive Client and Runtime Resource connecting directly to a database server (which can optionally be hosted on an additional device).

  - Simplest deployment of Blue Prism.
    Configuration options are selected based on the ease of install.
  - Suitable only for evaluation, non-production, short-term use.

Both installation types leverage in-product functionality to create and configure the database remotely on the SQL Server. It is therefore necessary to authenticate against the target SQL Server using an account with sysadmin privileges.

Planning

Before carrying out the installation, the following conditions must be met:

- A SQL Server must be available to host the Blue Prism database. Administrator-level access is required. For short-term evaluations a local edition of SQL Server Express may be suitable.
- Administrator access to the devices where Blue Prism is to be installed must be available. All devices must meet in the minimum specifications and the devices must be able to communicate with each other over the network.
- If using Blue Prism Single Sign-on, users' AD accounts, Blue Prism Server(s), and all Blue Prism devices that will be accessed by users (i.e. the Interactive Clients, and possibly the Runtime Resources) must be in domains that directly reside within a common Active Directory forest.

It is also important to ensure that the following decisions have been taken prior to carrying out the installation. The table below outlines which questions are relevant based on the deployment type.

Considerations and their relevance for the type of deployment	Standalone Deployment	Multi-Device Deployment
On what device will the database be hosted?	Relevant	Relevant
What authentication mode is required for the SQL database (SQL Native or Windows Authentication)?	Relevant	Relevant
Do all devices where Blue Prism is to be installed meet the minimum requirements (including an appropriate version of the .NET Framework)?	Relevant	Relevant
Will the Interactive Client be used to create/edit processes?	NA	Relevant
Will all components be deployed within a common Active Directory Forest?	NA	Relevant
Will users authenticate using Blue Prism Native or Blue Prism Single Sign-on?	NA	Relevant
What account will the Blue Prism Server service be configured to logon as?	NA	Relevant

Review the Supported Software section for details of the supported operating systems and .NET Framework versions.

Multi-device deployment considerations

When undertaking a multi-device deployment the following items must be considered prior to undertaking the installation.

	Dev / Test / Pre-Prod Environments	Production Environments
General Connectivity	Connectivity between the various devices must be configure appropriately. Commonly this requires DNS to be configured to allow the devices to resolve each other based on their FQDN; and appropriate firewall rules to be in place to allow the devices to communicate on the required ports.	
Runtime Resources	Fewer Runtime Resources are deployed in comparison to a production environment as execution can be tested locally	The largest number of Runtime Resources are deployed into production environments.
Interactive Clients	Require target applications to be installed to allow processes to be designed and verified.	Do not typically require target applications to be installed as these devices are commonly only used for controlling the environment.
Application Server	A single device can host multiple application servers (on different ports). This may be appropriate for environments of the same type. All services on a given device must use a common version of Blue Prism.	
Database Server instance	Consider if the way that resources are allocated to SQL Server instances make it appropriate to use a single shared instance for deployments of Blue Prism based on their importance and criticality. (E.g. Dev and Production environments are likely to be most business critical).	
WCF Connection Mode	Select which WCF server connection mode will be used to determine whether a server certificate will be required. For information, review: v6 Data Sheet – Selecting a BP Server Connection mode If a certificate is required, this must be manually generated and installed on the Application Server(s). The common name on the certificate must align with the address that the client devices will be configured to use to connect to the server. Additionally, all devices that will connect to the server must trust the Certification Authority that issued the manually generated certificate.	
Runtime Resource Certificates	Decide if there is a requirement to apply certificate-based security to the instructional communications from the Interactive Clients and Application Servers to each Runtime Resource; and to inbound communications received by the Runtime Resources if they are hosting web services. If a certificate is required this must be manually generated and installed on each applicable Runtime Resource. The common name on the certificate must align with the address that Blue Prism will be configured to use when communicating with the devices (E.g. FQDN or machine short name). Additionally, all devices that will connect to the Runtime Resources must trust the Certification Authority that issued the manually generated certificate(s).	

Typical deployment

Suitable for production and non-production use, a typical deployment contains all components of Blue Prism deployed to separate machines and includes the Application Server component which, amongst other things, provides scheduling capabilities.

> Prior to following this guidance, ensure that you have fully considered the information in Preparation.

For production environments, a minimum of four resources are required:

- Application Server
- Interactive Client
- Runtime Resource
- SQL Server

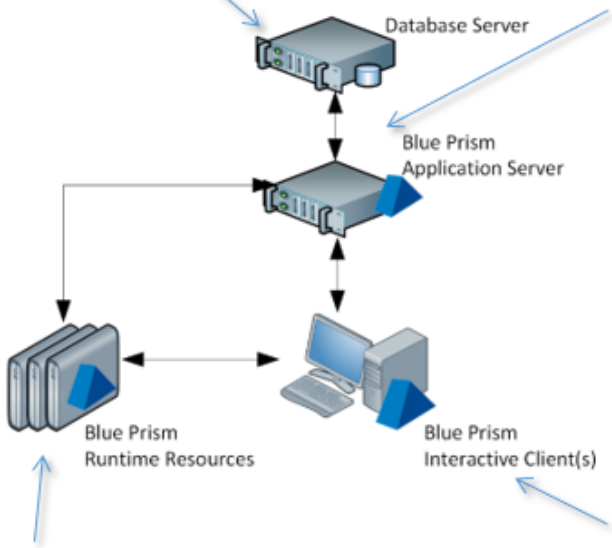
A SQL Server instance must be pre-configured prior to the installation of Blue Prism.

Overview of typical Installation Steps

An overview of the steps required to complete a typical deployment are provided below.

Preparation

1. Ensure that chapter entitled Preparation has been fully considered. It is necessary to ensure that there is an appropriate SQL Server instance available, and that the target device(s) meet the minimum specifications.
2. If using Microsoft SQL Azure, ensure an Azure database is available and that it is configured to accept connections from this platform.



Blue Prism Application Server

3. Install Blue Prism
4. Create/Configure a Blue Prism SQL Server Database
5. Login for the first time
6. Install a Blue Prism License Key
7. Configure an Encryption Scheme
8. Configure common settings
9. Verify the Blue Prism Deployment
10. Configure the Server Profile
    Create a Blue Prism Server Profile which uses the configured SQL connection
11. Configure the Windows Service (including defining the logon and start-up properties of the Blue Prism Server Profile)
12. Validate the Server service logon user
13. Disable the setting to "Start the process engine on this machine automatically"
14. Configure a local Blue Prism Connection to the Blue Prism Application Server

Blue Prism Interactive Client (for each)

15. Install Blue Prism
16. Configure a Blue Prism Connection to the Blue Prism Application Server
17. Optionally disable the setting to start a Runtime Resource when a user logs into Blue Prism
18. If used to develop and configure processes, access will also be required from this device to all appropriate third-party applications that will be automated.

Blue Prism Runtime Resource (for each)

19. Install Blue Prism
20. Configure a Blue Prism Connection to the Blue Prism Application Server
21. Optionally disable the setting to start a Runtime Resource when a user logs into Blue Prism
22. Assign a user account to the device and configure the user profile (including configuring remote access settings).
23. Verify connectivity to line of business applications.
24. Configure the Runtime Resource to start automatically when the device is logged in.
25. Ensure there is a mechanism for Runtime Resources to login following a reboot.

If problems are experienced whilst installing, see Troubleshooting an installation.

Blue Prism Application Server

Install and configure the first Application Server. Includes configuring a new Blue Prism database or connecting to a pre-configured database.

Install Blue Prism

Run the appropriate installer depending on whether you wish to use the 32-bit or 64-bit installer.

- 32-bit Installer: BluePrismx.x.nn_x86.msi
- 64-bit Installer: BluePrismx.x.nn_x64.msi

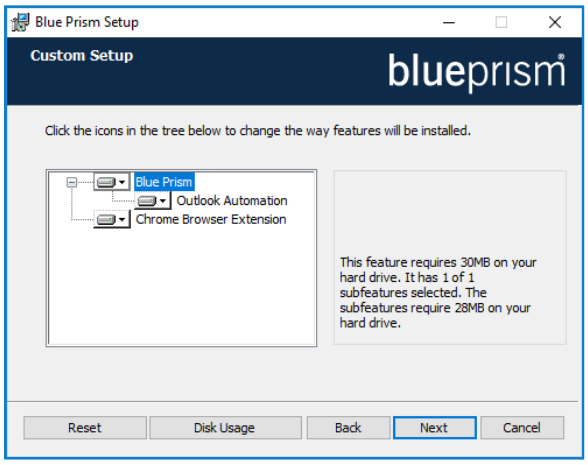
Installers are available from the Blue Prism Portal.

Additional install options

Two additional components are available during a Blue Prism installation:

- **Blue Prism Chrome browser extension** - required on devices that will use this mechanism to automate Chrome
- **Microsoft Outlook Interop DLL** - required on devices where the Blue Prism MS Outlook Email VBO will be executed

Both are installed by default but a custom install is also available, allowing only the required components to be selected.

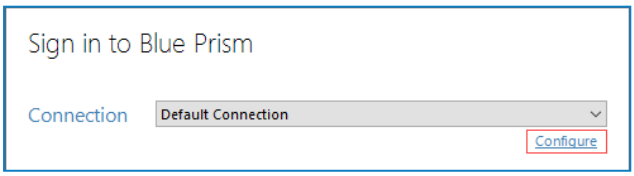


To prevent a component being installed, select **Entire feature will be unavailable** from the appropriate drop-down on the Custom Setup page.

Configure a connection to the SQL Server instance

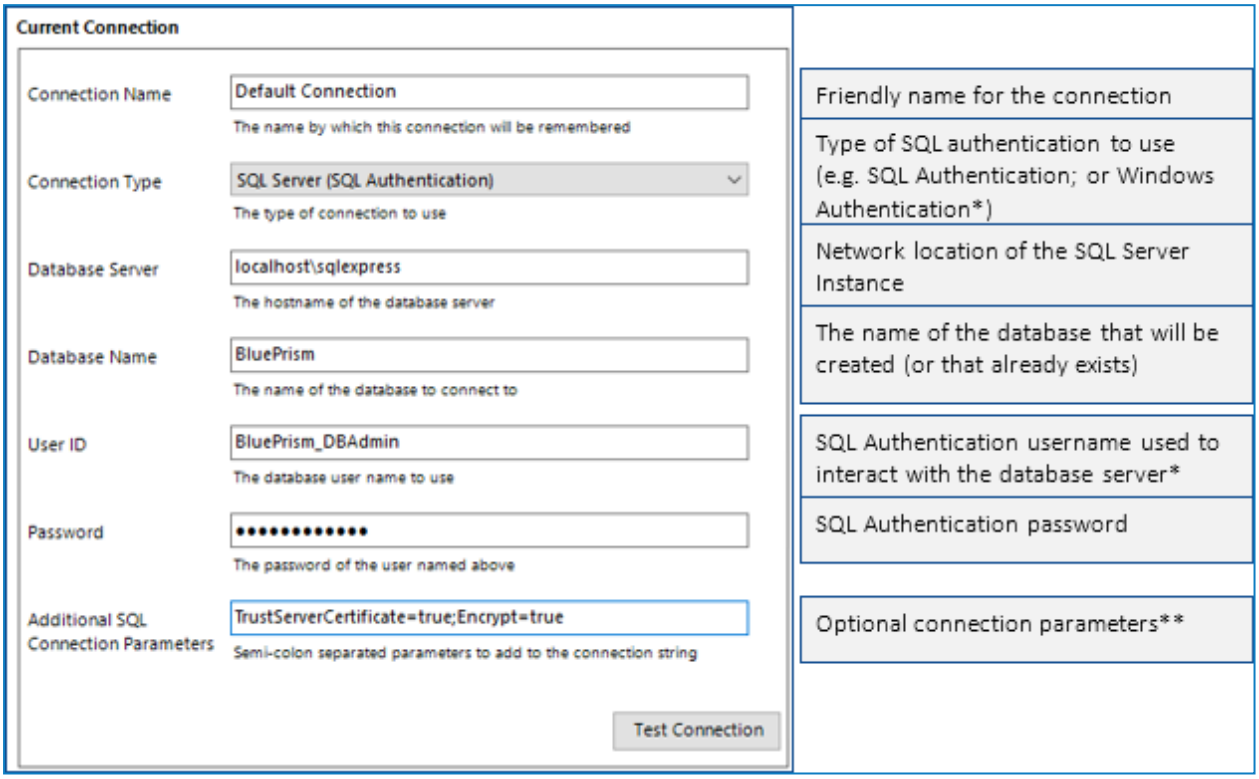
When Blue Prism is launched for the first time it is necessary to define a connection to the SQL Server instance where the database is, or will be, hosted.

1. Click **Configure**. This will launch the wizard that can be used to provide the connection information.



2. Specify the name for this connection, and the settings required to connect to the SQL Server instance.

   The name of the intended database will also be specified on this screen. This is the name that will be used to create a new database; or it can be the name of an existing database.



*If the Connection type applies Windows Authentication, the context of the user currently logged into the device will be used to authenticate against the SQL Server.

Where possible Windows Authentication (rather than SQL Authentication) should be used.

** Can be left blank. Populate if there is a requirement to add custom SQL Connection Parameters such as: encrypt=true; trustservercertificate=true.

See SQL Server Connection Properties information provided by Microsoft for a list of available values.

If connecting to Microsoft SQL Azure, the database must be pre-existing, and the connection details provided within the Azure database configuration area should be used. Example settings (ADO.NET) are provided below:

Connection Type	SQL Server (SQL Authentication)
Database Server:	e12n3456.database.windows.net,1433
Database Name:	BluePrism
User ID:	authUser@e12n3456
Password:	*********

3. Click **Test Connection** to establish if a connection can be established with the SQL Server.

   As the database does not yet exist we expect to be presented with a meaningful error.

   Expected Responses

Database 'Blue Prism' does not exist.	This does not appear to be a valid Blue Prism database.	The database needs configuring before it can be used.
Indicates that a successful connection was established with the server, but that the database does not yet exist.	Indicates that a successful connection was established with the server, but that it cannot be verified as a Blue Prism database. This would typically be the case where the database has been manually created but has not had the Blue Prism schema applied.	Indicates that a successful connection was established with the server, and that a Blue Prism database has been found, but that some further configuration is required.
Click **OK** to clear the message and press Create Database.		Click **OK** to clear the message, and press Configure Database.
Proceed to the next step for further instructions.		

   Alternative Responses

Database Valid	Unable to determine whether database exists - A network-related or instance-specific error occurred whilst establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
Indicates that a successful connection was established with the server and the database. Actions to Create or Configure the database can be bypassed.	Indicates that an error occurred establishing a connection with the SQL Server. Check that the details for the SQL Server instance are correct, and refer to the Troubleshooting an installation.

Create and configure a Blue Prism SQL Server database

There are three stages involved in the creation and preparation of a database for use with Blue Prism.

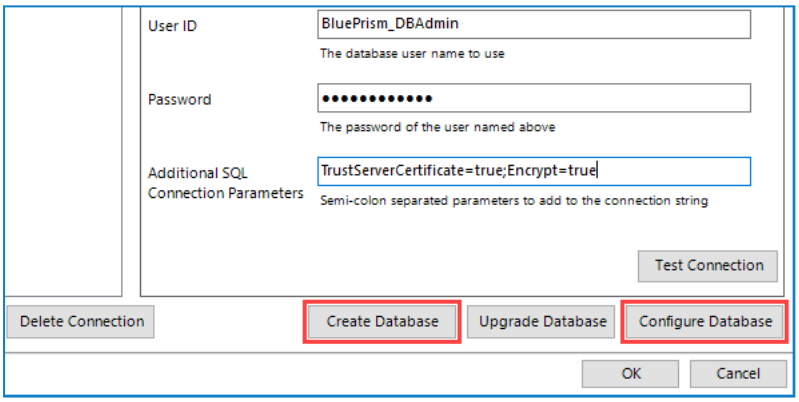
- **Create a SQL Server Database** - This can either be achieved manually or through use of the in-product Create Database action.
- **Apply Blue Prism Schema** - The database schema is applied to the configured database.

  The in-product Create Database action will automatically apply the schema to a database that it creates; or to a specifiable pre-existing blank database.

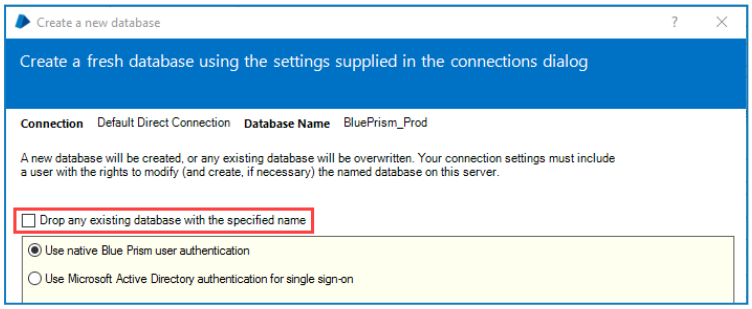
  alternatively the schema can be applied by manually using the CreateScript.sql (from Customer Services) against a pre-existing database.
- **Configure Blue Prism Sign-on Settings** - A number of configuration options are applied to the database. These are applied automatically when using the in-product Create Database action. If the database has been created and had the schema applied manually the Configure Database action must be used.

All of the above stages are completed in a single step when using the in-product Create Database functionality.

1. To launch the in-product utility to create and configure a database, use the **Create** or **Configure** options within Connection Manager.



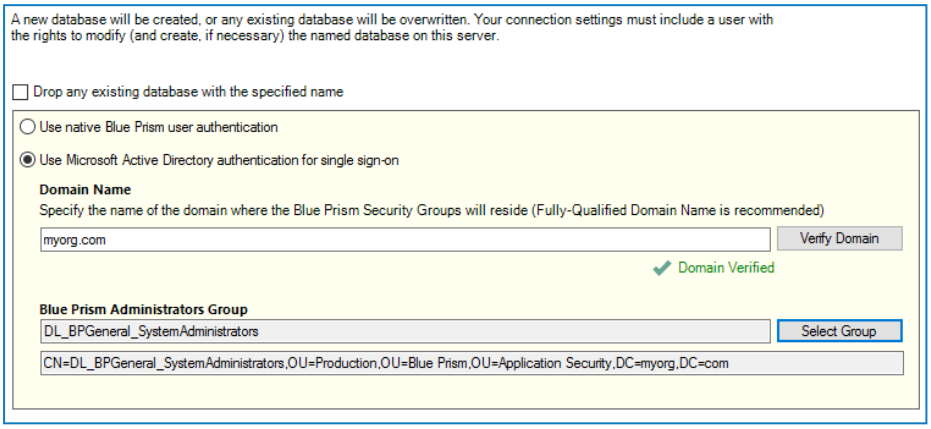
2. Complete the form by selecting:
   - Whether to drop and recreate the database if already exists.



   - If the connection is configured to use SQL native authentication it will also be necessary to re-enter the password.
   - Select the preferred authentication method for users connecting to Blue Prism. Native Blue Prism authentication is the simplest to setup. See following item for information on a single sign-on configuration.

     If the implementation is to be integrated with Active Directory, this must be configured now by selecting the option to **Use Microsoft Active Directory for single sign-on**. Once the authentication mechanism is implemented, it cannot be changed.

3. If using Microsoft Active Directory authentication for single sign-on it is necessary to enter the name of the domain that contains the Active Directory Security Groups that are to be associated with security roles in Blue Prism; and to select the Security Group within that domain whose members will be granted System Administrator access to Blue Prism.



> Only custom security groups should be associated with Blue Prism – do not use built-in groups, or groups with derived membership.

4. Click **OK** to complete the database configuration.

Login for the first time

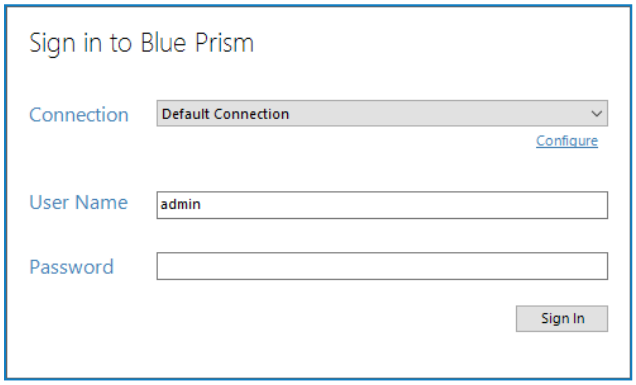
It is now possible to login for the first time and carry out some system-wide configuration.
The steps will differ slightly depending on whether the environment is configured to use Blue Prism Native Authentication or Single Sign-on for Blue Prism.

Blue Prism native authentication

Login using the default credentials:

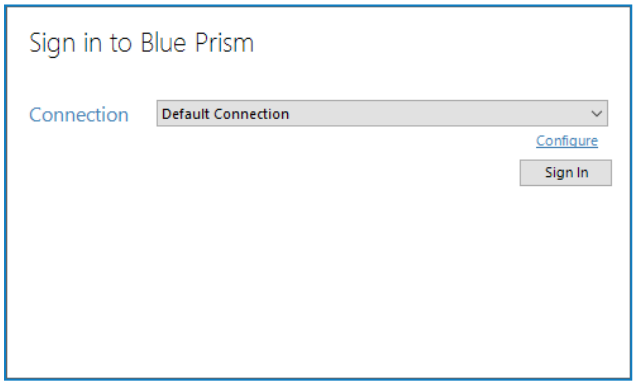
- **Username:** admin
- **Password:** admin

Follow the onscreen instructions to change the administrator's password.



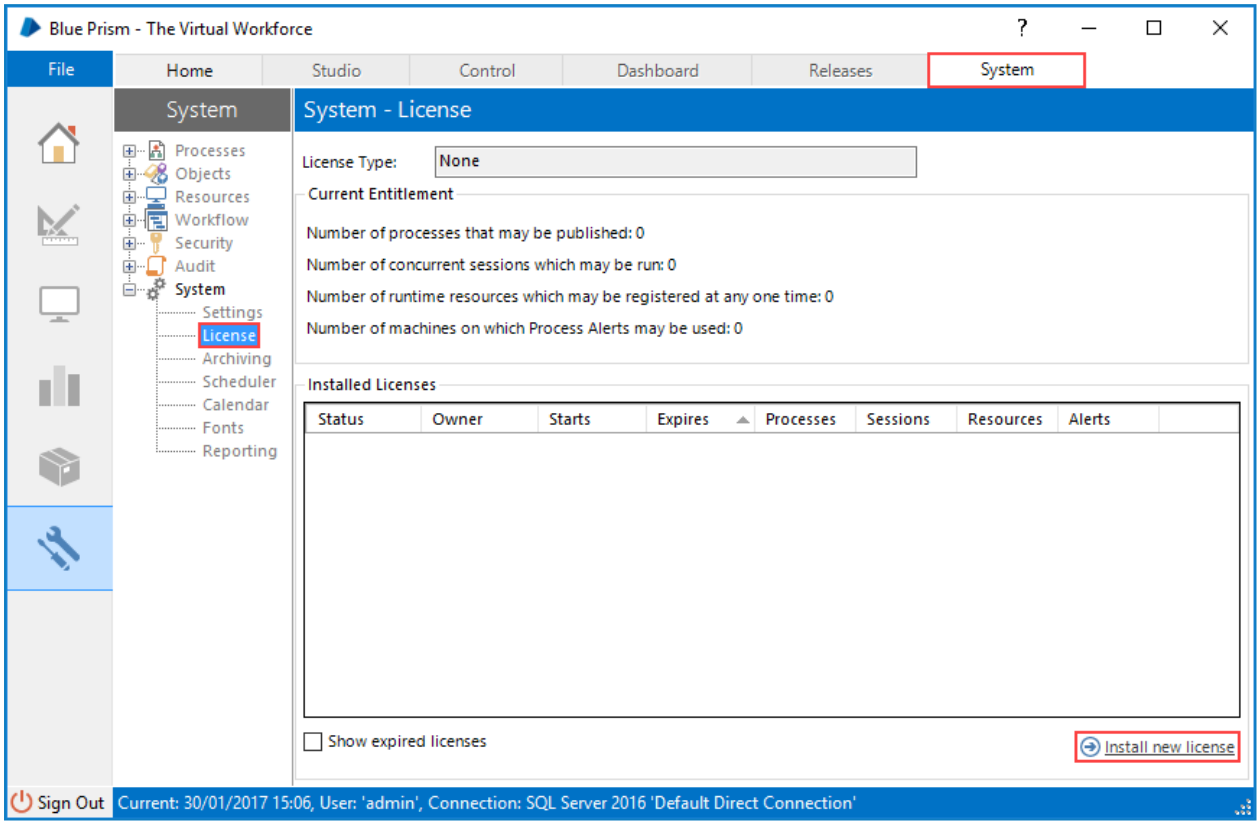
Single Sign-on for Blue Prism

Login by clicking sign in to validate that the configuration has been correctly applied.



Install a Blue Prism license key

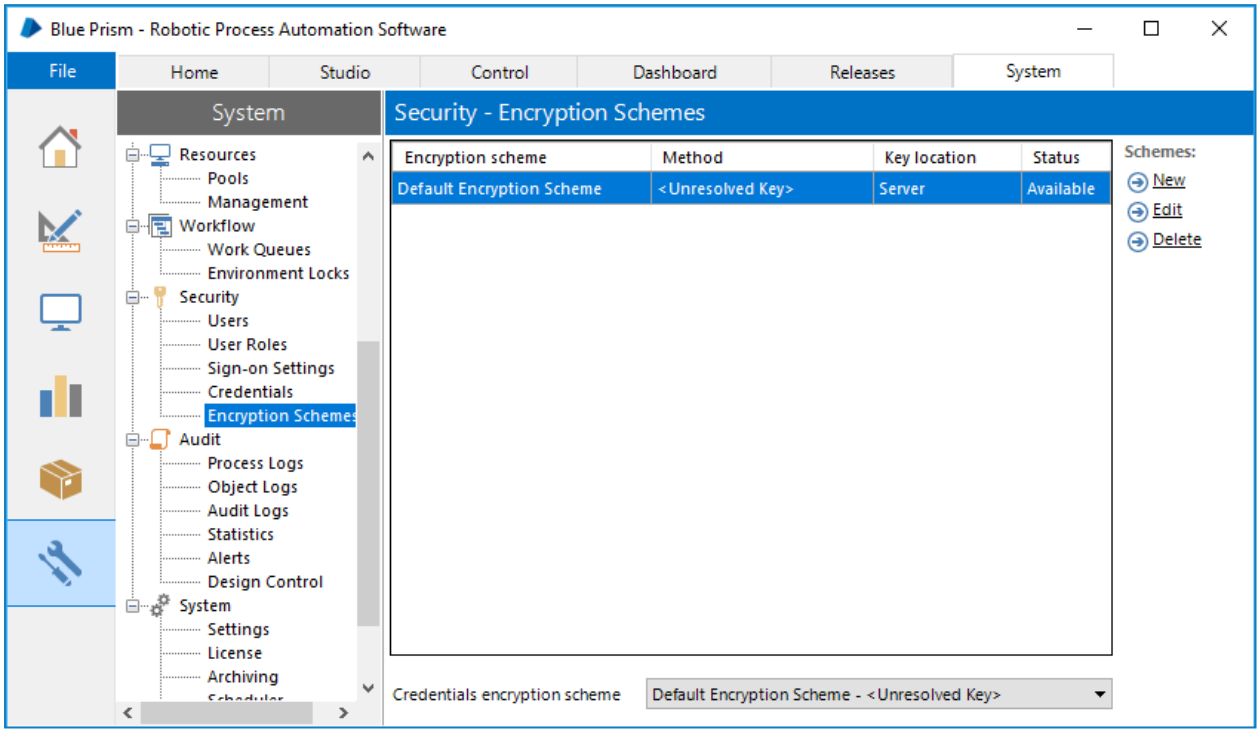
In order to enable the software it is necessary to install a valid license file. License files can be obtained via an Account Manager.



1. Click the **System** tab and select **System** > **License** from the navigation tree.
2. Select **Install new licence**.
3. Select the License file and click **OK**.

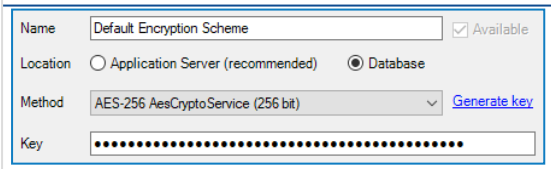
Configure an Encryption Scheme

In order to support the use of Credential Manager (for securely storing credentials), configure the Encryption Scheme that will be used.



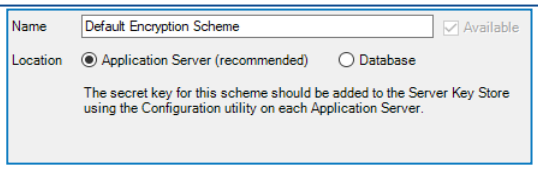
1. Click the **System** tab and select **Security** > **Encryption Schemes** from the navigation tree.
2. Select the scheme listed and click **Edit**.
3. Follow the steps below as appropriate:

Standalone Deployment



a. Select **Database**.
b. Select **AES-256**.
c. Click **Generate Key**.
d. Click **OK**.

Multiple Component (App Server) Deployment

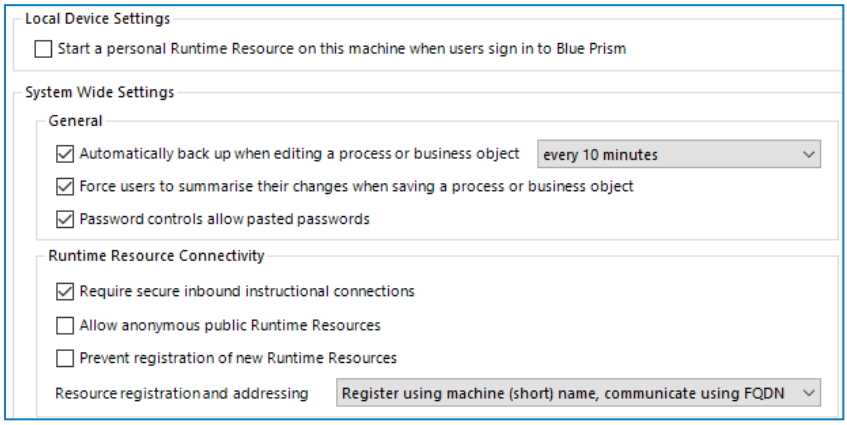


a. Select **Application Server**.
b. Click **OK**.

A copy of each key must be backed up in a secure location

Configure common settings

A number of optional settings are commonly applied. These can be found under **System** > **Settings** on the **System** tab.



Setting	Information
Start a personal Runtime Resource on this machine	Commonly disabled on all devices except for standalone deployments of Blue Prism, provides a local Runtime Resource when a user logs into Blue Prism.
Automatically back up when editing	Indicates the frequency at which auto-save will run. Commonly this settings is only adjusted in environments operating over high-latency networks.
Force users to summarise their changes	Requires users to add a comment when making changes to these records.
Password controls allow pasted passwords	When enabled, users can paste into password controls within the Blue Prism interface. Disable this setting to require users to type (rather than paste) passwords and to increase the security of typed values in memory.
Require secure inbound instructional communications.	Only Runtime Resources which use the /sslcert switch will be able to successfully establish a connection with the platform. The /sslcert switch requires all inbound instructional connections to Runtimes to be subject to certificate-based encryption. This affects programmatically controlled robots such as those hosting Web Services. **Disable** this setting for troubleshooting purposes
Allow anonymous public Runtime Resources	When disabled, requires Runtime Resources to explicitly authenticate when connecting to the platform. This is not appropriate when the environment is configured to use Single Sign-on for user access if Runtime Resources are hosted outside of the common Active Directory Forest. **Enable** this setting for troubleshooting purposes
Prevent registration of new Runtime Resources	When enabled, no new Runtime Resources can be introduced to the platform. This should only be enabled once all required Runtime Resources have connected for the first time. **Disable** this setting for troubleshooting purposes

Setting	Information
Resource registration and addressing	Indicates whether FQDN names will be used to register Runtimes within the database, and for subsequently establishing communications. The appropriate value should be selected from the outset. • Register and communicate using machine short name: Not recommended. Provided only for backwards compatibility. • Register using machine (short) name, communicate using FQDN: Recommended for single network deployments or those which previously used machine short name. • Register and communicate using FQDN: Recommended for new deployments that contain devices from multiple networks.

Verify the Blue Prism deployment

It is recommended that the installation is manually verified by carrying out some simple tasks within the system and confirming that they execute successfully.

For step-by-step instructions, see to Verify an Installation.

Configure the server profile

Blue Prism Application Server services are configured using BPServer.exe. This application is provided as part of the Blue Prism installation and is used to define and configure the services that are available on a given server.

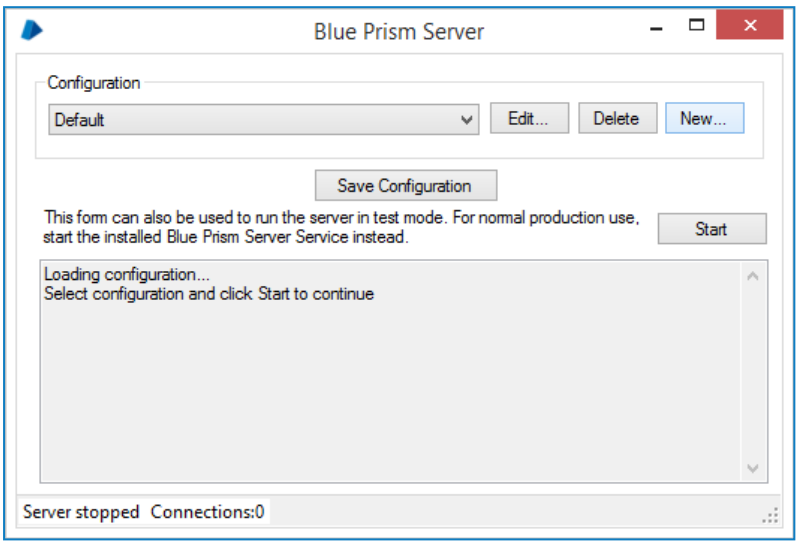
The Blue Prism server configuration utility will be used to configure server profiles which contain the settings that the service will use. Additionally it can be used to create additional Windows Services for situations where the default profile is renamed, or additional profiles are added.

The configuration includes:

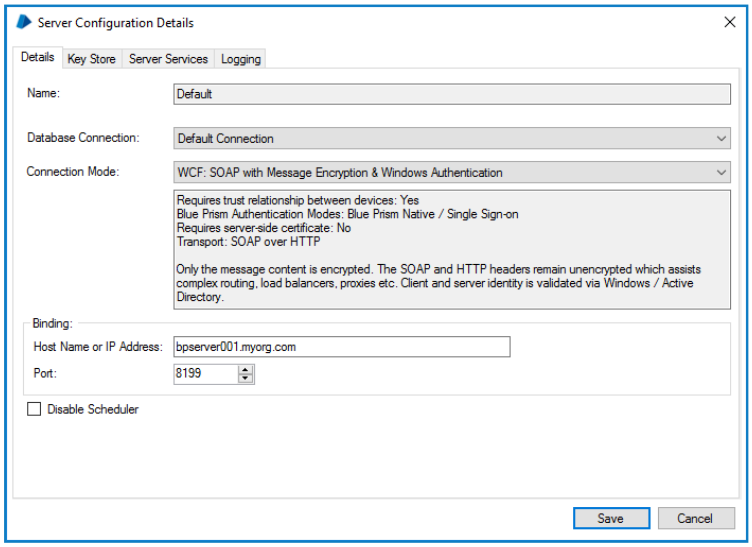
- Selecting the mode that inbound connections will be require to used
- Defining the hostname or IP address binding and port that the service will listen on
- Specifying database connection information.
- Configuring an encryption scheme that will be used for data encryption in that environment.
- Where appropriate, selecting which certificate will be used to secure inbound connections.
- Validating that there is an appropriate Windows Service configured, and that the service logon user has been added to the appropriate access control list (ACL).

Configure the Windows service profile

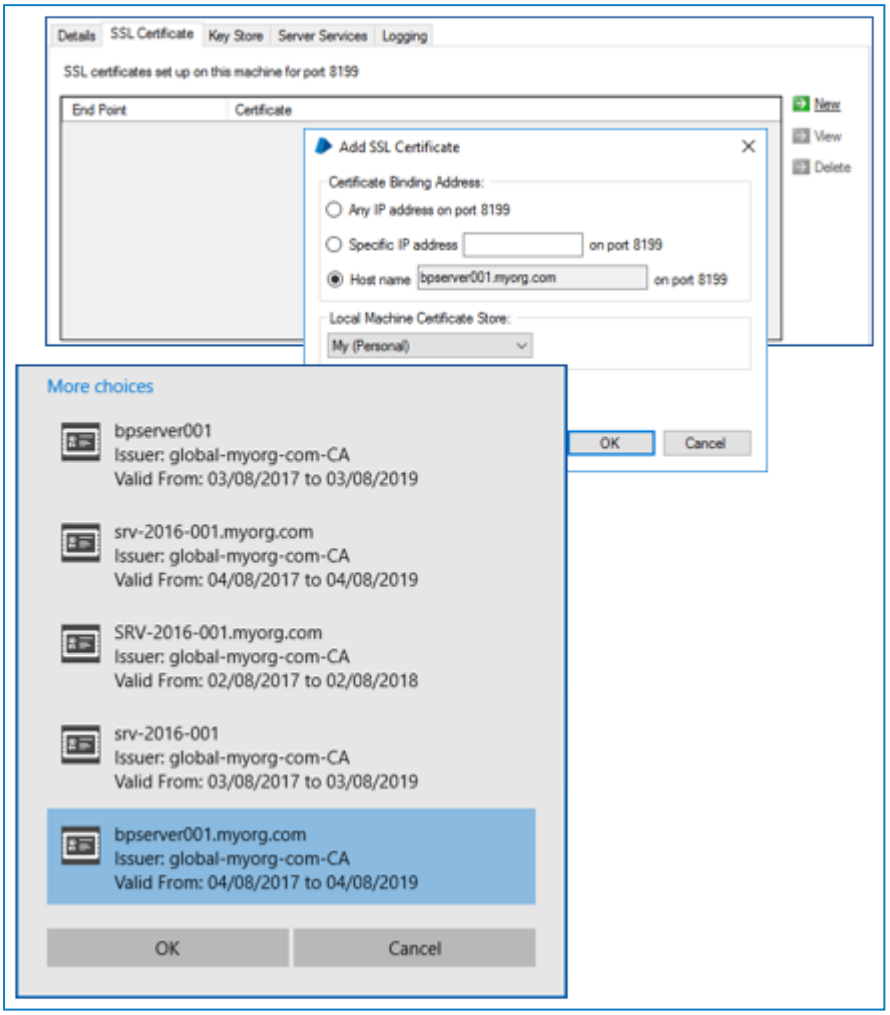
1. Navigate to the Blue Prism installation directory, typically C:\Program Files\Blue Prism Limited\Blue Prism Automate and launch BPServer.exe.
2. Click **New** to create a server configuration.



3. Complete the form ensuring that the connection mode, bindings and listening port are correct.
    - **Name** - Name for the server profile. The first one must be called Default.
    - **Database Connection** - Connection used to connect to the database.
    - **Connection Mode** - Connection mode to be used by connecting devices.
    - **Binding** - Optional binding for the endpoint for scenarios where requests must be received on a specific URL or address.
    - **Port** - Server listening port.
    - **Disable Scheduler** - Indicates whether this server should have the scheduler enabled.



4. If a connection mode has been selected which requires a certificate to be configured, a message will be displayed and the Certificates tab will become available. This allows a certificate that has been configured as a Computer certificate on the local device to be associated with the server service.



If the certificates tab is not displayed, progress to the next step.

   a. Select to add a new certificate binding and enter the binding information and which store on the local device the certificate has been installed in.
   b. Click **OK** to launch the Windows certificate selection utility and pick the appropriate certificate.
   c. It is necessary to select a certificate that matches the binding on the details tab.

5. Select the **Key Store** tab and click **New**.

   An entry must be made for each Encryption Scheme defined via the Blue Prism client that is configured to use a key stored on the Application Server.

   The name of the Encryption Schemes must be an exact match of those configured in the client.

   When using a default configuration only one Encryption Scheme will be required named *Default Encryption Scheme*.

6. If this is the first Application Server that is being configured for the environment, select **AES-256** as the encryption method.

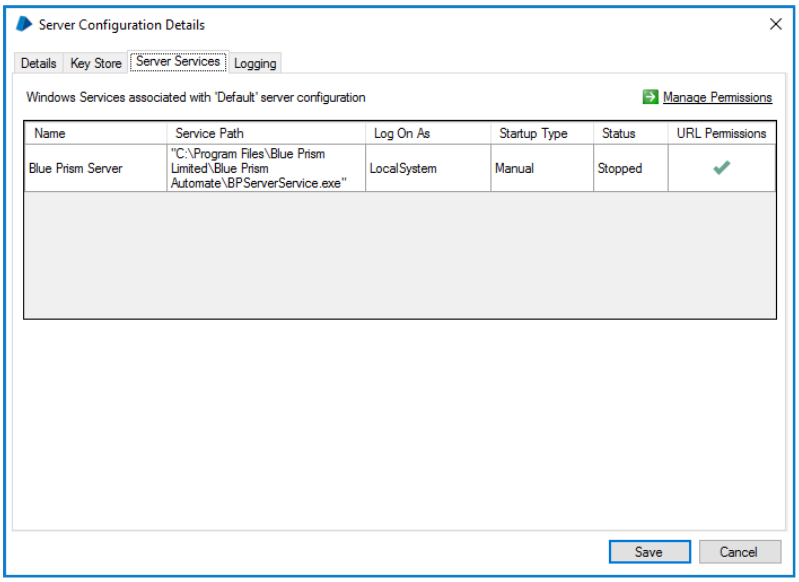
7. Click **Generate Key** followed by **OK**.

   If this is an additional Application Server instance for an existing Blue Prism deployment, the algorithm and key must match that on the pre-existing server.

   Commonly security conscious users will also select to store keys separately in individual files so that the target locations can controlled.

   A copy of each key must be backed up in a secure location - it will be needed to retrieve encrypted data if the server fails.

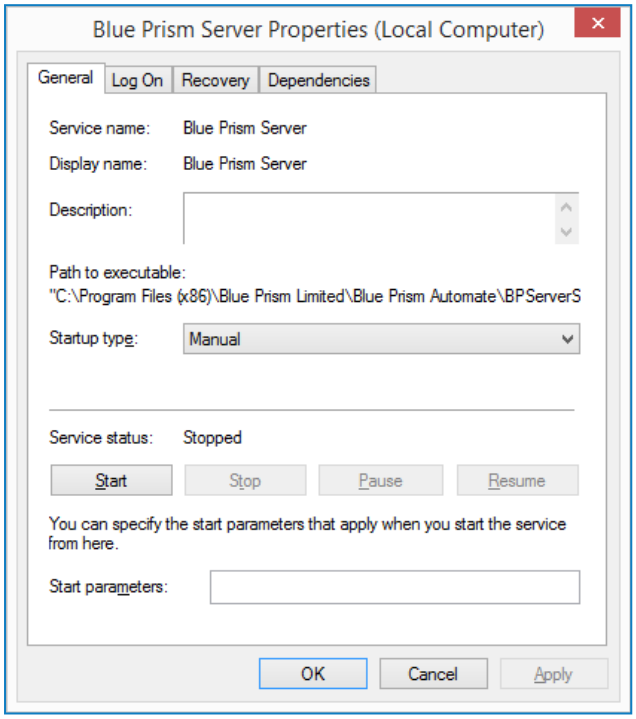
8. Review the settings on the Server Services tab to ensure that no problems have been identified so far.



9. Click **Save**.

Configure the Windows service

The default installation of Blue Prism creates a Blue Prism Server service which is configured to use the server settings profile named Default. If a profile of a different name has been used, the server configuration utility can be used to create a Windows service associated with the custom profile.



The Windows service should be configured from the Windows Services management console on the local device. The main settings to be configured are:

- **Startup type** - By default this is set to Manual however it is recommended that for most environments it should be set to Automatic.
- **Log On** - The default account used by Blue Prism is Local System however this can be configured to be custom account. Where Windows Authentication is used for the Blue Prism Server profile to communicate with the database, it is the account specified here that will be used by the service when connecting to the database.

When SQL is secured using Windows Authentication, the configured Windows Service account will need to have appropriate (minimum) access to the SQL database.

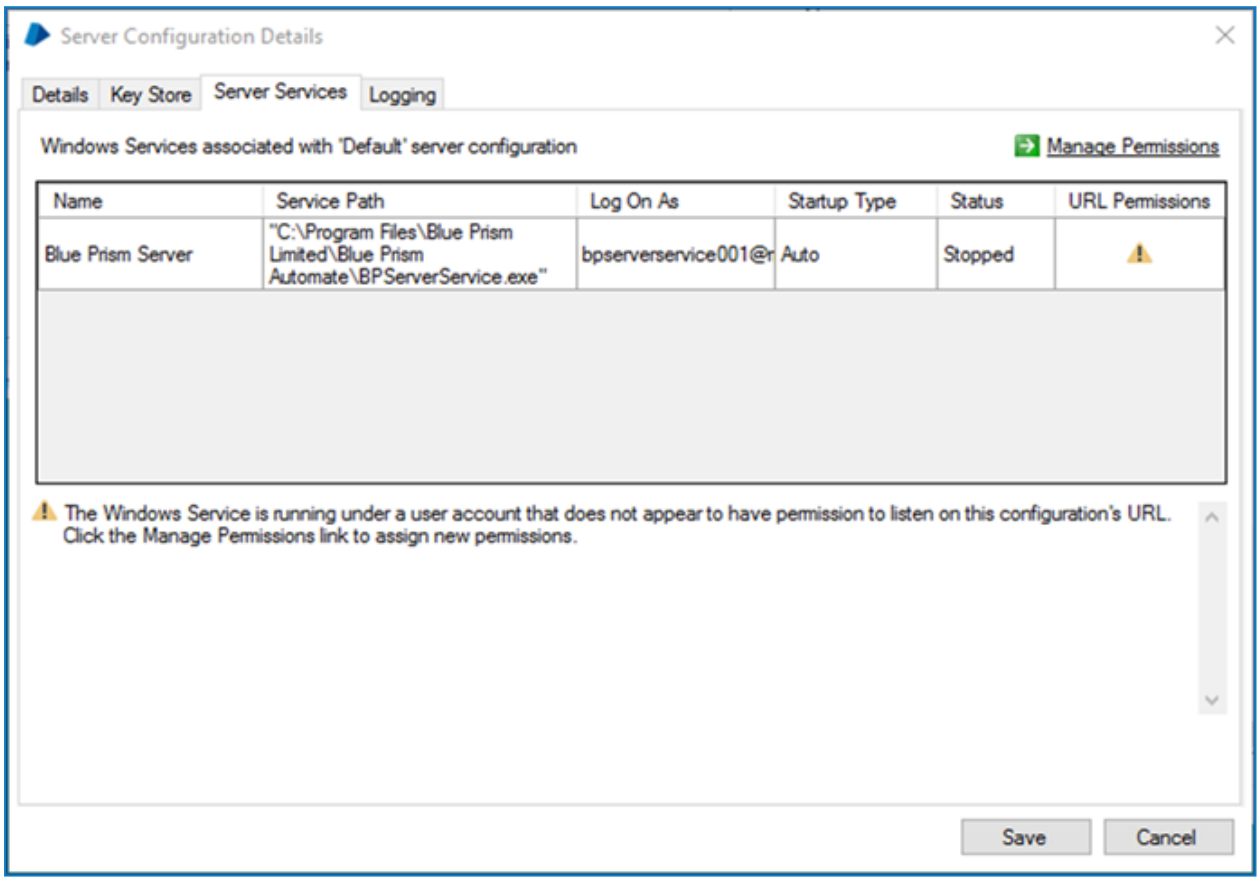
When Blue Prism is configured to use Single Sign-On, the configured Windows Service account will need to have appropriate permissions to access the directory services provider and query users and group membership. The specific permissions that are required in relation to Active Directory will be dependent on environmental factors and therefore assistance from the Active Directory administrator team within the target environment is likely to be required.

When starting the service, if it won't start or if it stops immediately, it can indicate a configuration problem. Check the Blue Prism Application Log within Windows Event Viewer for additional information about the problem.

Validate the Server service logon user

Use the Blue Prism Server configuration utility to re-validate the service configuration.

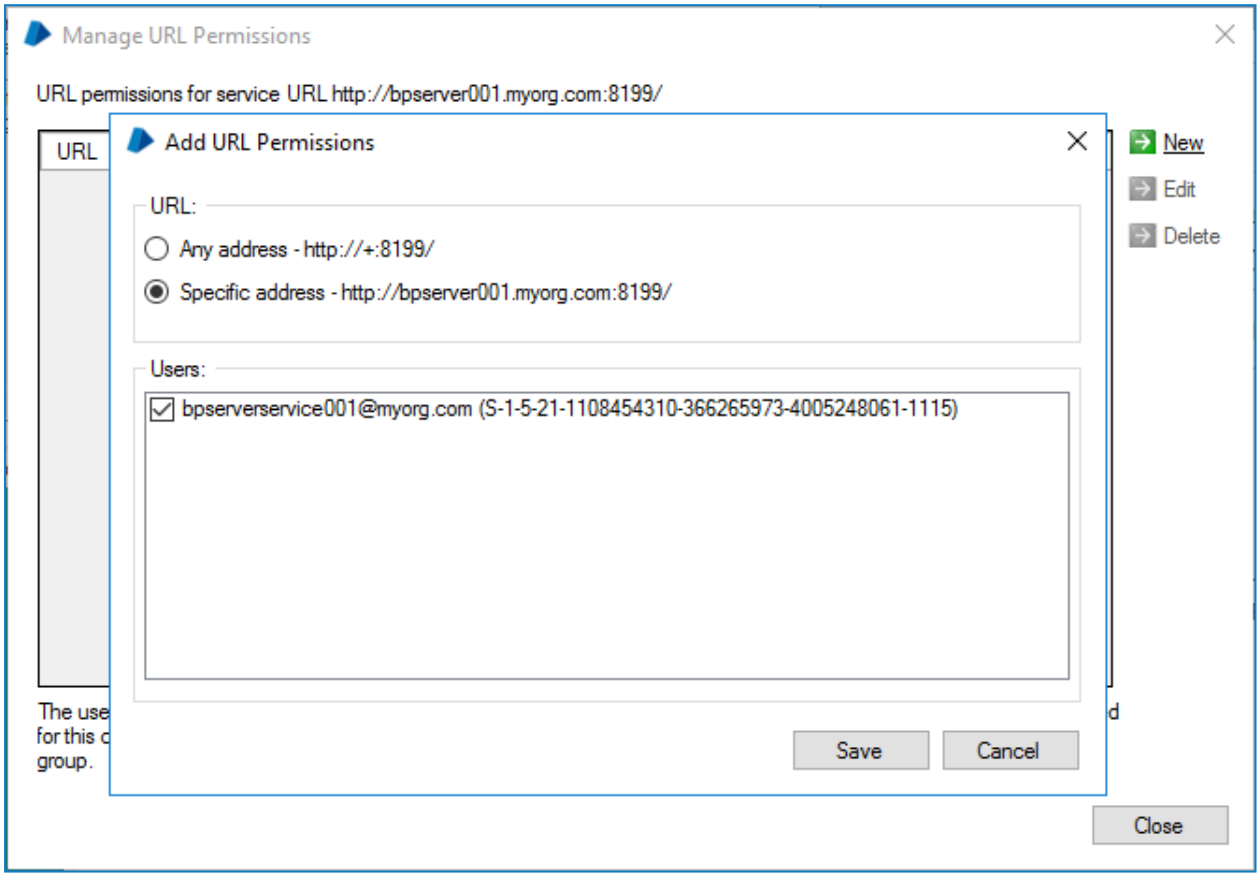
Common configurations such as where Blue Prism is configured to use Windows Authentication to authenticate against SQL may result in an error. This can occur if a non-admin user has been configured as the service log on account. In such situations, alerts similar to the below may be presented:



The Manage Permissions functionality can be used to grant the service account the appropriate permissions to listen on the defined port. The following rules must be considered:

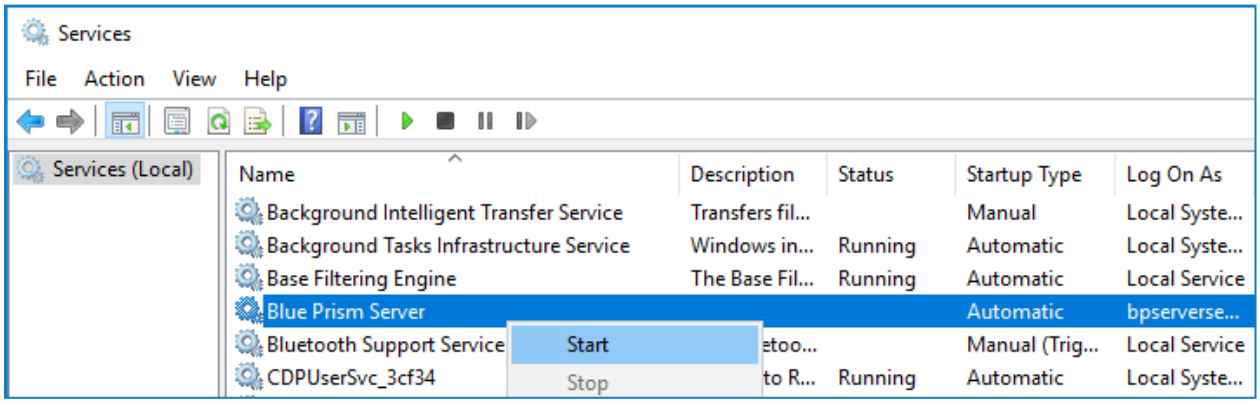
- If the service is configured to use a binding, a specific address permission must be created.
- If the service is not configured to use a binding, a non-specific address permission must be used.

It is not possible to use an address containing a strong wildcard if the service will be using a defined binding.



Start the Windows service

Use the Windows Services management console to start the service.

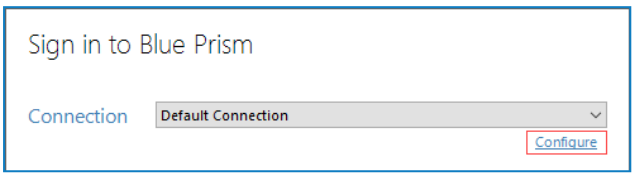


If the service will not start, or starts and then immediately stops there is a problem with the configuration of the service. For more information, review Troubleshooting an installation.

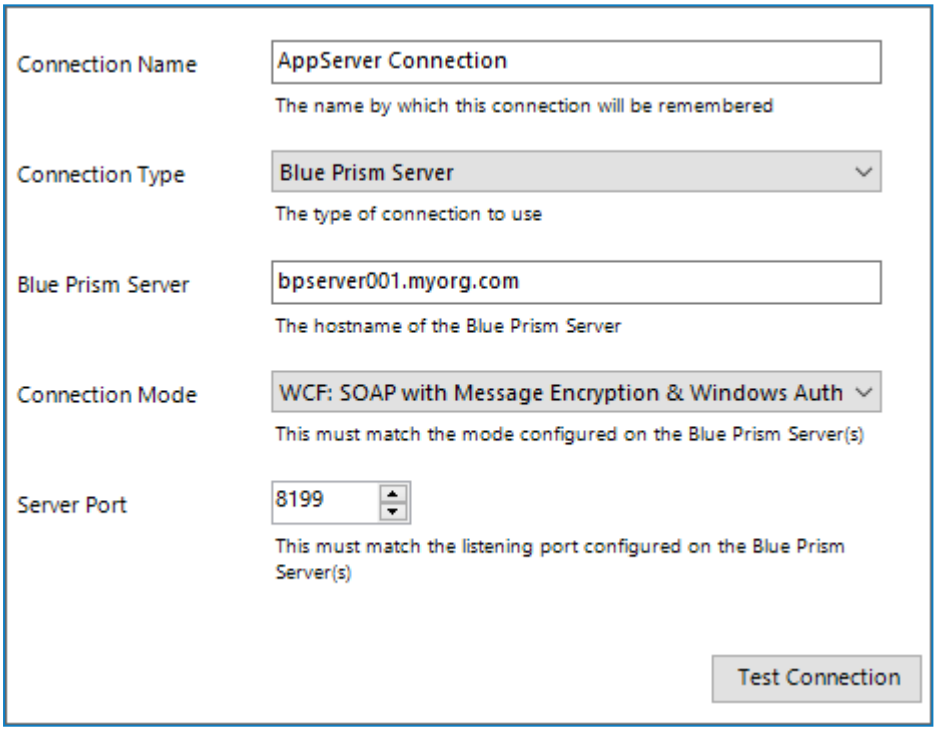
Configure a Blue Prism connection to the Blue Prism Application Server

The server service can be tested locally be configuring an additional Blue Prism connection on the local device that is configured to connect via the newly configured server service.

1. Launch Blue Prism and click **Configure**.



2. This will launch the wizard that can be used to provide the connection information:
   - **Connection Name** - Friendly name for the connection
   - **Connection type** - The type of connection to use
   - **Blue Prism Server** - Address of the server. Must match the server binding, and be resolvable.
   - **Connection Mode** - Connection mode to use. Must match the setting on the Server
   - **Server port** - The port that the server is listening on.



3. Click **Test Connection** to verify that a connection can be established.

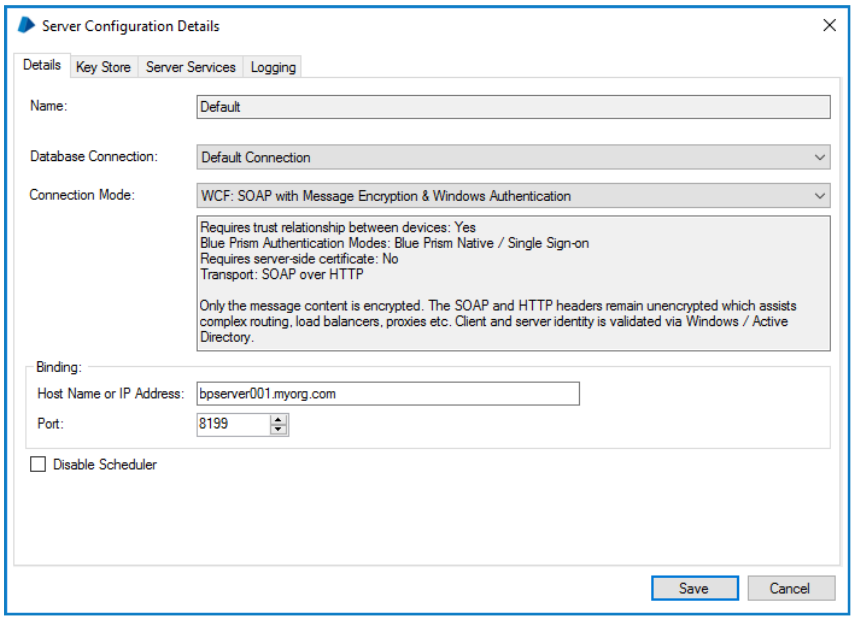
   If the connection cannot be verified, this indicates that there is a problem with establishing a connection with the Application Server. For more information, review Troubleshooting an installation.

Administrators can now use the two connections configured in the local Blue Prism client to validate:

- Direct connections to the Blue Prism database.
- Connections to the environment via the Application Server.

Blue Prism Interactive Client

For each device of this type that will be configured, Blue Prism will be installed and configured with a connection to the Blue Prism Application Server.



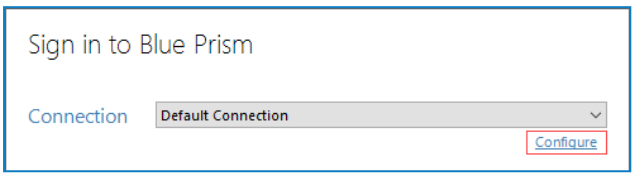
The following should be noted:

- It is necessary to use some settings from the server configuration on each client such as:
  - Connection mode
  - Bind to address (if specified)
  - Port
- If the server is configured to use a WCF mode that uses transport encryption, it will be necessary to ensure that the certification authority that issued the server certificate is trusted by all clients.
- If the device will not be used for locally executing automated processes, the optional step to prevent a local runtime resource from starting when a user logs into to Blue Prism will be followed.

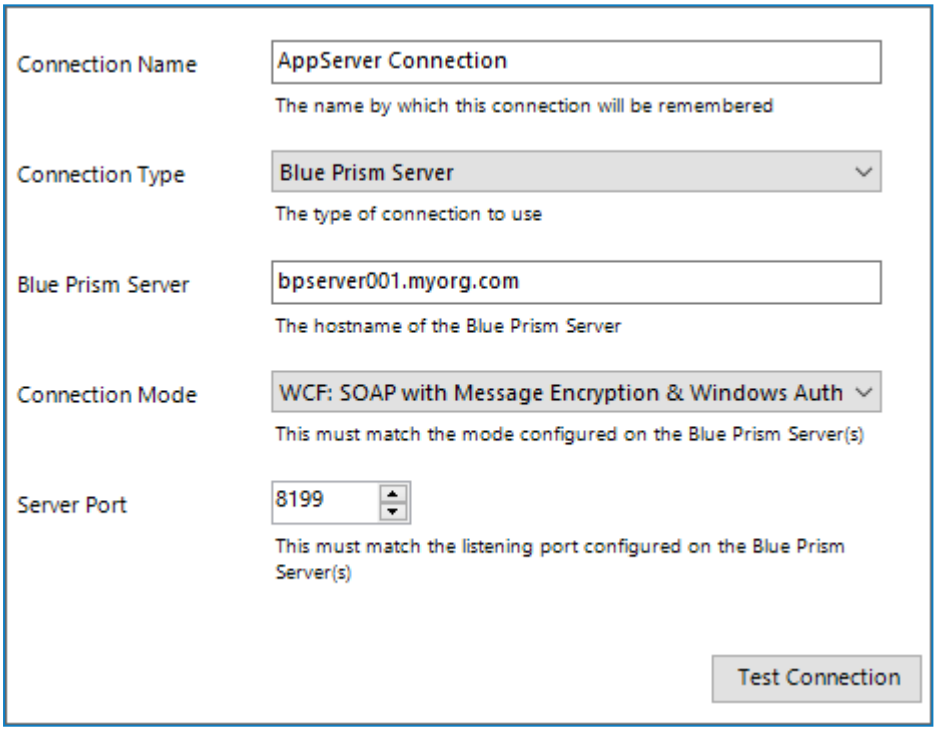
Configure a Blue Prism connection to the Blue Prism Application Server

The server service can be tested locally be configuring an additional Blue Prism connection on the local device that is configured to connect via the newly configured server service.

1. Launch Blue Prism and click **Configure**.



2. This will launch the wizard that can be used to provide the connection information:
   - **Connection Name** - Friendly name for the connection
   - **Connection type** - The type of connection to use
   - **Blue Prism Server** - Address of the server. Must match the server binding, and be resolvable.
   - **Connection Mode** - Connection mode to use. Must match the setting on the Server
   - **Server port** - The port that the server is listening on.



3. Click **Test Connection** to verify that a connection can be established.

   If the connection cannot be verified, this indicates that there is a problem with establishing a connection with the Application Server. For more information, review Troubleshooting an installation.

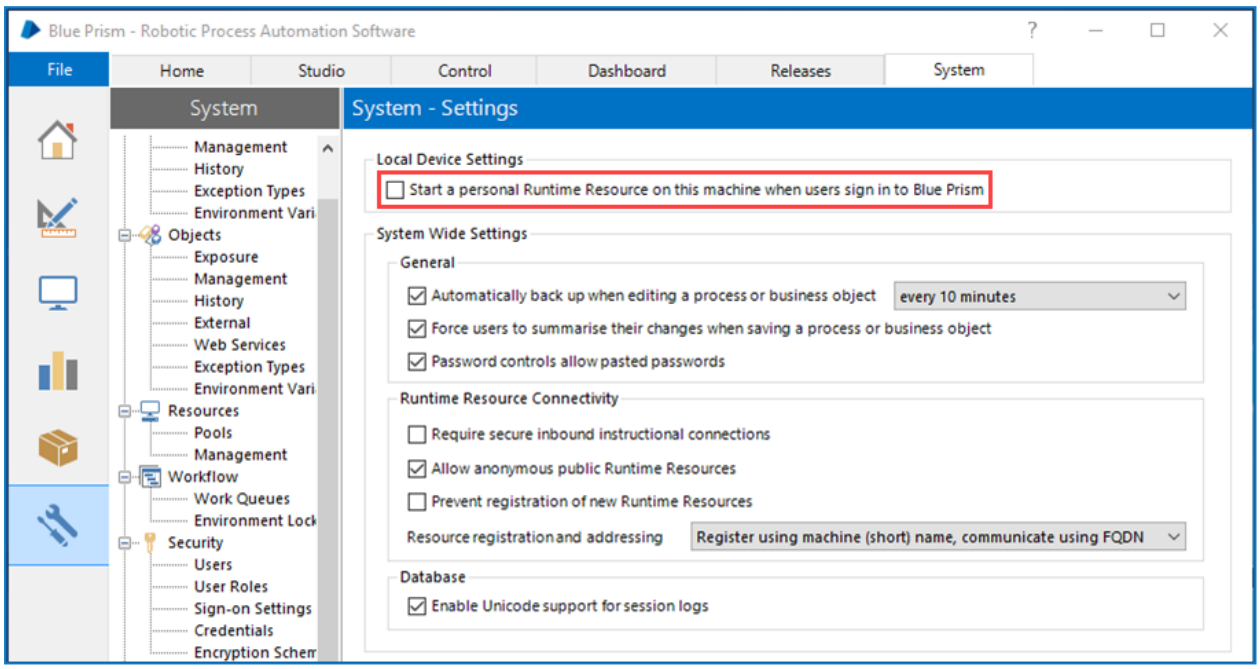
Administrators can now use the two connections configured in the local Blue Prism client to validate:

- Direct connections to the Blue Prism database.
- Connections to the environment via the Application Server.

Configure local device settings

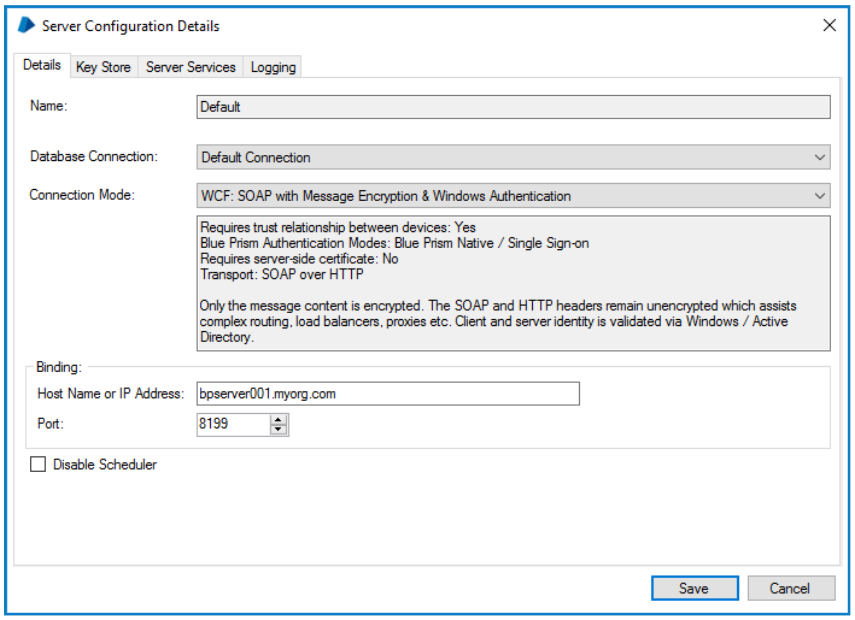
In most cases it is recommended to disable the setting that starts a personal Runtime Resource when a user logs in to the Blue Prism client on the current device. Enabling this feature is commonly only required for demo and UAT purposes.

This setting can be disabled within the **System** tab.



Blue Prism Runtime Resource

For each device of this type that will be configured, Blue Prism will be installed and configured with a connection to the Blue Prism Application Server.



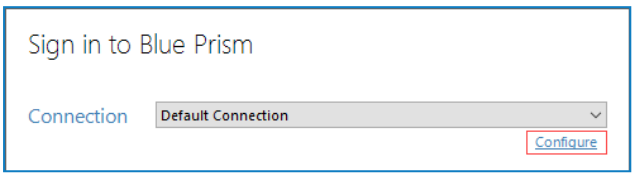
The following should be noted:

- It is necessary to use some settings from the server configuration on each client such as:
  - Connection mode
  - Bind to address (if specified)
  - Port
- If the server is configured to use a WCF mode that uses transport encryption, it will be necessary to ensure that the certification authority that issued the server certificate is trusted by all clients.
- If the device will not be used for locally executing automated processes, the optional step to prevent a local runtime resource from starting when a user logs into to Blue Prism will be followed.

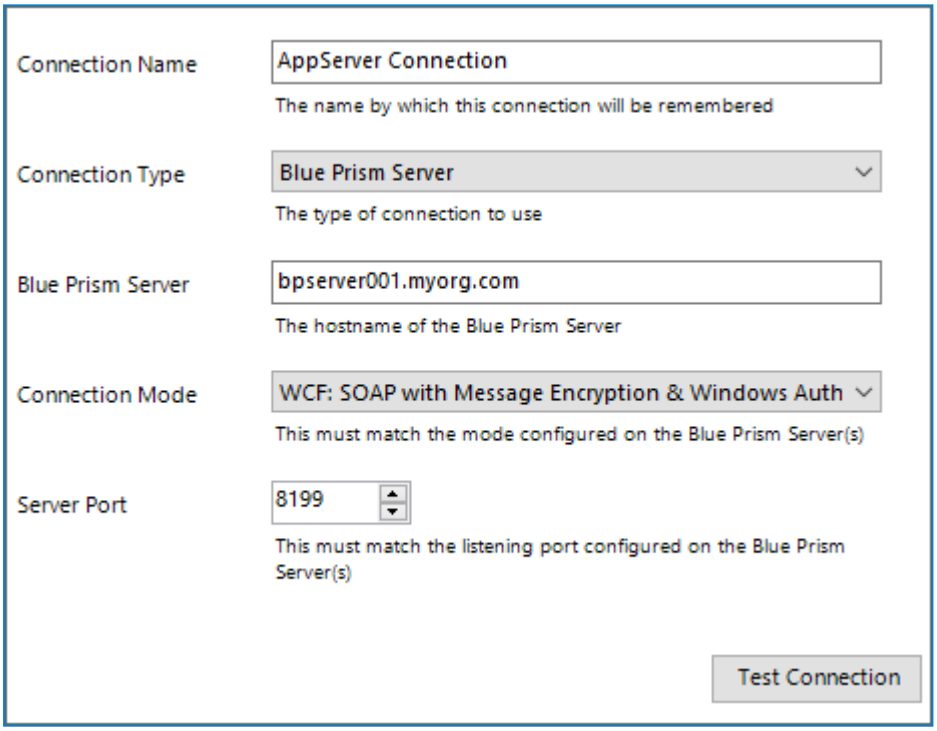
Configure a Blue Prism connection to the Blue Prism Application Server

The server service can be tested locally be configuring an additional Blue Prism connection on the local device that is configured to connect via the newly configured server service.

1. Launch Blue Prism and click **Configure**.



2. This will launch the wizard that can be used to provide the connection information:
   - **Connection Name** - Friendly name for the connection
   - **Connection type** - The type of connection to use
   - **Blue Prism Server** - Address of the server. Must match the server binding, and be resolvable.
   - **Connection Mode** - Connection mode to use. Must match the setting on the Server
   - **Server port** - The port that the server is listening on.



3. Click **Test Connection** to verify that a connection can be established.

   If the connection cannot be verified, this indicates that there is a problem with establishing a connection with the Application Server. For more information, review Troubleshooting an installation.

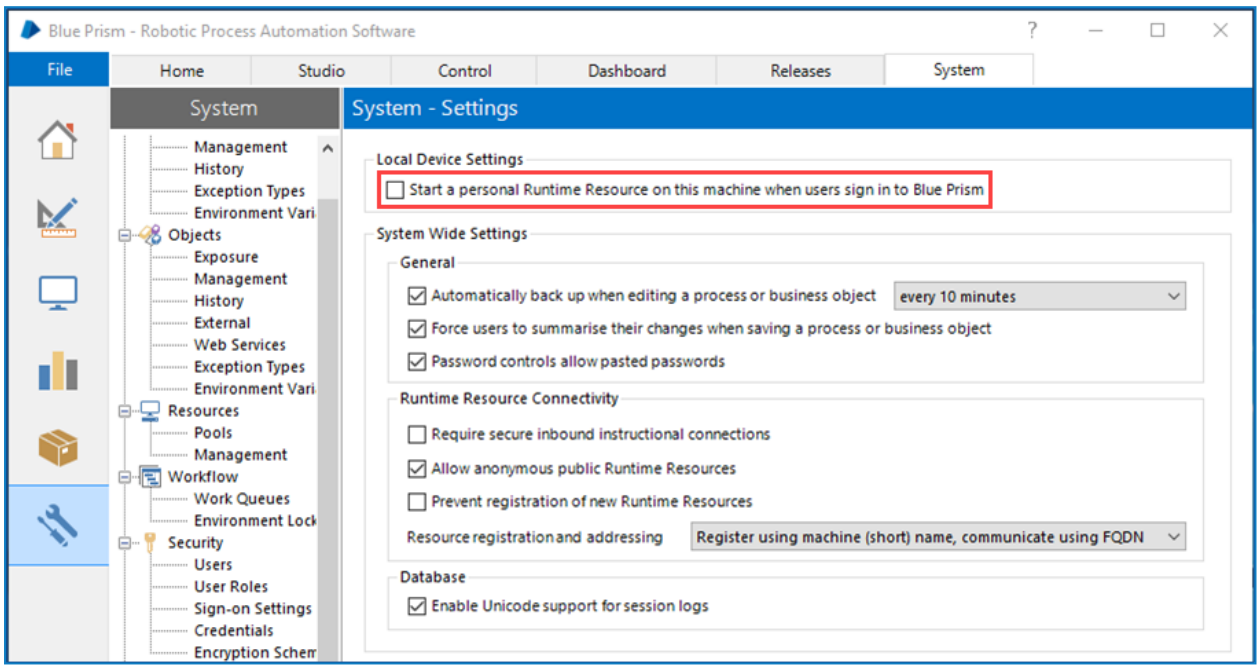
Administrators can now use the two connections configured in the local Blue Prism client to validate:

- Direct connections to the Blue Prism database.
- Connections to the environment via the Application Server.

Configure local device settings

In most cases it is recommended to disable the setting that starts a personal Runtime Resource when a user logs in to the Blue Prism client on the current device. Enabling this feature is commonly only required for demo and UAT purposes.

This setting can be disabled within the **System** tab.



Assign a user account to the device and configure the user profile

Blue Prism Runtime Resources operate on devices that are logged in, either locally or using a domain account. Commonly a domain account is used to provide network administrators with central control over the user accounts and to allow the Runtime Resources to use single sign-on to access business applications.

Although many devices can theoretically share a single network login, in most cases it is more appropriate for each device on which a Runtime Resource is to be logged in to have a unique set of credentials.

Once selected, the user profile settings should be configured to address the considerations referenced in the Blue Prism Infrastructure Overview NHS Data Sheet. These include:

- Screensaver and auto-lock
- Regional Settings
- Power Saver options
- Default remote access settings

Verify connectivity to line of business applications

The Blue Prism Runtime Resources must be configured with the appropriate client installs and connectivity to allow interaction with the user interface of the applications that are to be automated as part of Blue Prism processes.

For further information, such as the requirement for Blue Prism to interact with Java based applications, see Advanced Configuration.

Configure the Runtime Resource to start automatically at device login

When the device is logged in, it is advisable that the Runtime Resource be configured to automatically start with the selected configuration.

This can be achieved through use of a login script, a scheduled task, or through use of adding a batch file to the start-up folder. The commands required to launch are below, along with optional configuration that may be required based on restrictions enforced within the platform:

The command line to start a Runtime Resource is:

[Blue Prism Install Location]\automate.exe /resourcepc /public

"C:\Program Files\Blue Prism Limited\Blue Prism Automate\automate.exe" /resourcepc /public

Configure robot authentication

The Runtime Resource can be configured to authenticate with the environment for security purposes.
This is required where anonymous public Runtime Resources are prevented from connecting. The user account will need to be granted the Runtime Resource role within the Blue Prism environment prior to being used.

- Use the /sso switch to authenticate as the logged on user against a single sign-on Blue Prism environment.

  ```
  automate.exe /resourcepc /public /port 8181 /sso
  ```

- Use the /user [username] [password] switch to authenticate against a native Blue Prism environment.

  ```
  automate.exe /resourcepc /public /port 8181 /user jbloggs pa55w0rd1
  ```

Configure a specific port

Runtime Resources listen for instructional communications from the Scheduler, Control Room and potentially 3rd Party systems (e.g. web service calls) on a defined port. If no port is explicitly specified, port 8181 will be used.

To set a custom port the /port switch can be used:

```
automate.exe /resourcepc /public /port 8182
```

Configure encrypted inbound connections

If an appropriate certificate has been deployed locally on the Resource the /sslcert switch can be used to apply certificate-based encryption to all communication received on the nominated port. This would, for example, require that all instructional information be subject to certificate-based encryption. In addition, HTTP requests such as inbound web service calls would need to be directed to use HTTPS:

```
automate.exe /resourcepc /public /sslcert [Certificate Thumbprint]
automate.exe /resourcepc /public /sslcert 33a4d8aa6a3d57b04c10eb32278d8a8612ffae9d
```

Override the selected connection

By default when Runtime Resources connect to the Blue Prism environment they will use the default connection configured within the Blue Prism client on the local machine. They can be configured to use any configured connection by using the /dbconname switch and providing the friendly name of the connection:

```
automate.exe /resourcepc /public /port [port] /dbconname [Connection Name]
automate.exe /resourcepc /public /port 8001 /dbconname "Production 001"
```

Ensure there is a mechanism for Runtime Resources to login following a reboot

The devices that host Blue Prism Runtime Resources must be started in order for a conventional Runtime Resource to start and be able to receive instructions that allow it to execute automated processing. In order to allow this is it is necessary to consider how Runtime Resource devices will be logged on following a reboot.

Options may include manually logging into these resources following a reboot, using auto-login, or using Blue Prism Login Agent.

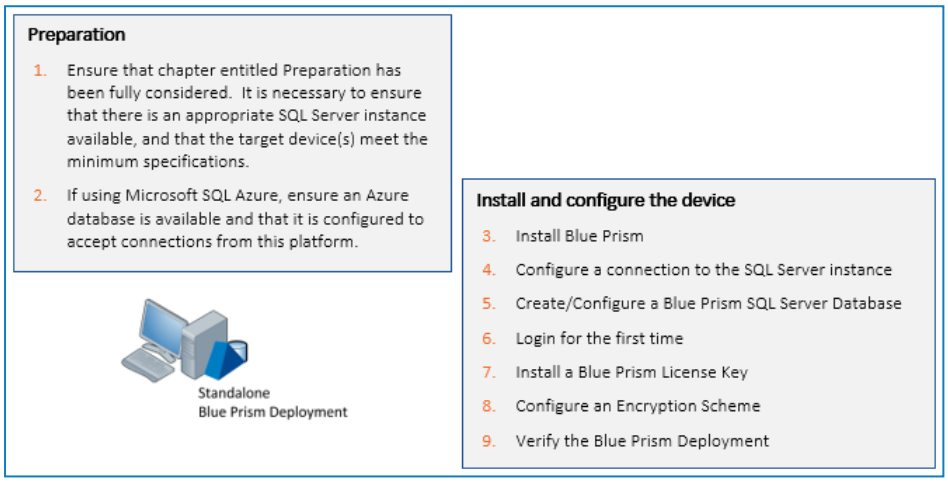
Information on using Blue Prism Login Agent can be found within the *Blue Prism User Guide – Login Agent*.

Standalone deployment

Prior to following this guidance, ensure that you have fully considered the information in Preparation.

Overview of installation steps

An overview of the steps typically required to complete a standalone deployment are provided below.



If problems are experienced whilst installing, review Troubleshooting an installation.

Install Blue Prism

Run the appropriate installer depending on whether you wish to use the 32-bit or 64-bit installer.

- 32-bit Installer: BluePrismx.x.nn_x86.msi
- 64-bit Installer: BluePrismx.x.nn_x64.msi

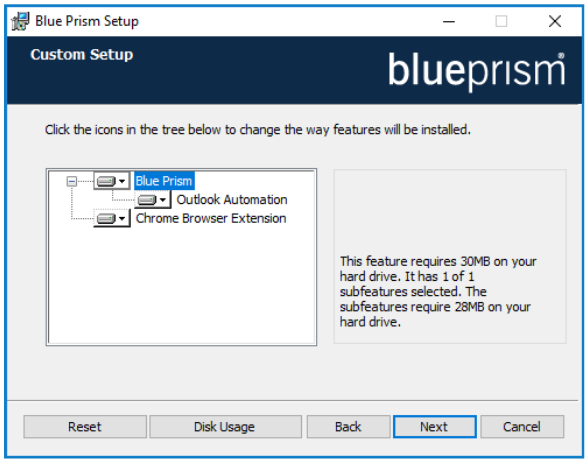
Installers are available from the Blue Prism Portal.

Additional install options

Two additional components are available during a Blue Prism installation:

- **Blue Prism Chrome browser extension** - required on devices that will use this mechanism to automate Chrome
- **Microsoft Outlook Interop DLL** - required on devices where the Blue Prism MS Outlook Email VBO will be executed

Both are installed by default but a custom install is also available, allowing only the required components to be selected.

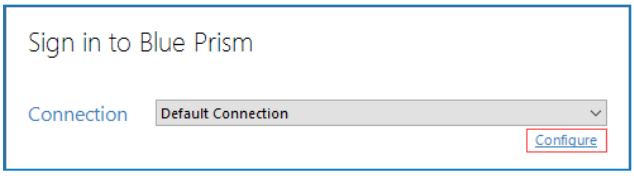


To prevent a component being installed, select **Entire feature will be unavailable** from the appropriate drop-down on the Custom Setup page.

Configure a connection to the SQL Server instance

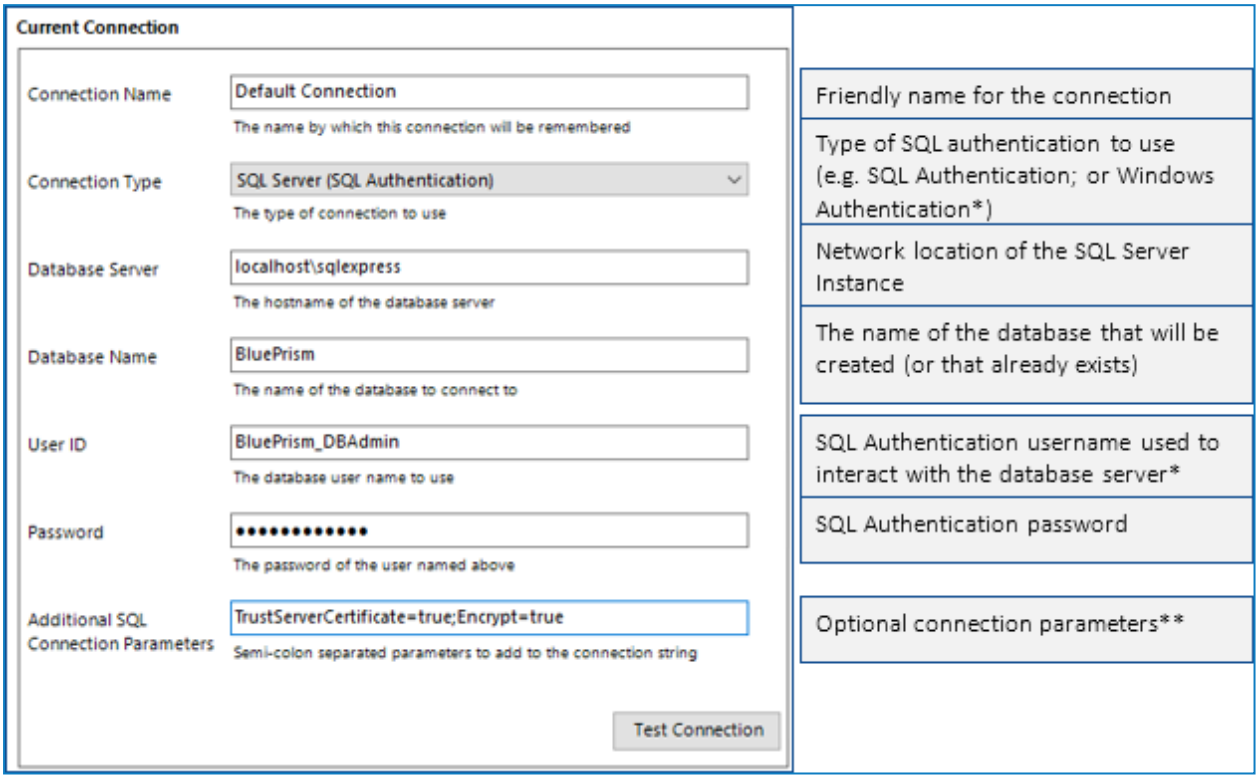
When Blue Prism is launched for the first time it is necessary to define a connection to the SQL Server instance where the database is, or will be, hosted.

1. Click **Configure**. This will launch the wizard that can be used to provide the connection information.



2. Specify the name for this connection, and the settings required to connect to the SQL Server instance.

   The name of the intended database will also be specified on this screen. This is the name that will be used to create a new database; or it can be the name of an existing database.



*If the Connection type applies Windows Authentication, the context of the user currently logged into the device will be used to authenticate against the SQL Server.

Where possible Windows Authentication (rather than SQL Authentication) should be used.

** Can be left blank. Populate if there is a requirement to add custom SQL Connection Parameters such as: encrypt=true; trustservercertificate=true.

See SQL Server Connection Properties information provided by Microsoft for a list of available values.

If connecting to Microsoft SQL Azure, the database must be pre-existing, and the connection details provided within the Azure database configuration area should be used. Example settings (ADO.NET) are provided below:

Connection Type	SQL Server (SQL Authentication)
Database Server:	e12n3456.database.windows.net,1433
Database Name:	BluePrism
User ID:	authUser@e12n3456
Password:	*********

3. Click **Test Connection** to establish if a connection can be established with the SQL Server.

   As the database does not yet exist we expect to be presented with a meaningful error.

   Expected Responses

Database 'Blue Prism' does not exist.	This does not appear to be a valid Blue Prism database.	The database needs configuring before it can be used.
Indicates that a successful connection was established with the server, but that the database does not yet exist.	Indicates that a successful connection was established with the server, but that it cannot be verified as a Blue Prism database. This would typically be the case where the database has been manually created but has not had the Blue Prism schema applied.	Indicates that a successful connection was established with the server, and that a Blue Prism database has been found, but that some further configuration is required.
Click **OK** to clear the message and press Create Database.		Click **OK** to clear the message, and press Configure Database.
Proceed to the next step for further instructions.		

   Alternative Responses

Database Valid	Unable to determine whether database exists - A network-related or instance-specific error occurred whilst establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
Indicates that a successful connection was established with the server and the database. Actions to Create or Configure the database can be bypassed.	Indicates that an error occurred establishing a connection with the SQL Server. Check that the details for the SQL Server instance are correct, and refer to the Troubleshooting an installation.

Create and configure a Blue Prism SQL Server database

There are three stages involved in the creation and preparation of a database for use with Blue Prism.

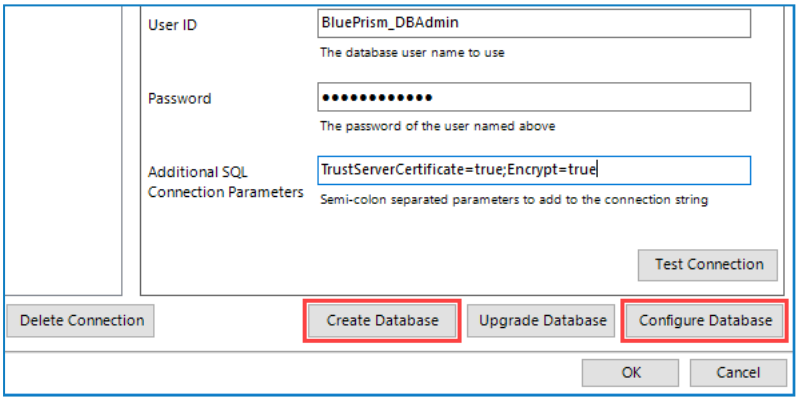
- **Create a SQL Server Database** - This can either be achieved manually or through use of the in-product Create Database action.
- **Apply Blue Prism Schema** - The database schema is applied to the configured database.

  The in-product Create Database action will automatically apply the schema to a database that it creates; or to a specifiable pre-existing blank database.

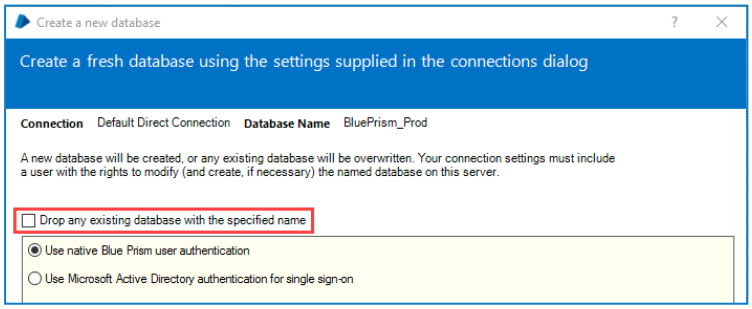
  alternatively the schema can be applied by manually using the CreateScript.sql (from Customer Services) against a pre-existing database.
- **Configure Blue Prism Sign-on Settings** - A number of configuration options are applied to the database. These are applied automatically when using the in-product Create Database action. If the database has been created and had the schema applied manually the Configure Database action must be used.

All of the above stages are completed in a single step when using the in-product Create Database functionality.

1. To launch the in-product utility to create and configure a database, use the **Create** or **Configure** options within Connection Manager.



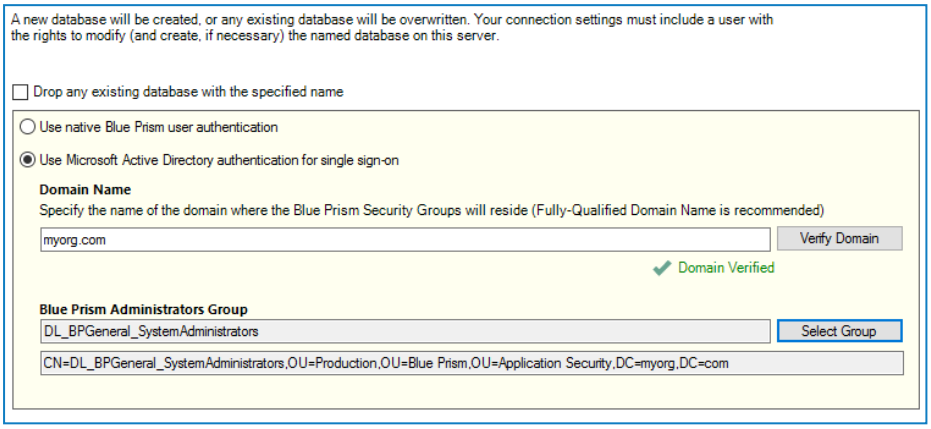
2. Complete the form by selecting:
   - Whether to drop and recreate the database if already exists.



   - If the connection is configured to use SQL native authentication it will also be necessary to re-enter the password.
   - Select the preferred authentication method for users connecting to Blue Prism. Native Blue Prism authentication is the simplest to setup. See following item for information on a single sign-on configuration.

     If the implementation is to be integrated with Active Directory, this must be configured now by selecting the option to **Use Microsoft Active Directory for single sign-on**. Once the authentication mechanism is implemented, it cannot be changed.

3. If using Microsoft Active Directory authentication for single sign-on it is necessary to enter the name of the domain that contains the Active Directory Security Groups that are to be associated with security roles in Blue Prism; and to select the Security Group within that domain whose members will be granted System Administrator access to Blue Prism.



> Only custom security groups should be associated with Blue Prism – do not use built-in groups, or groups with derived membership.

4. Click **OK** to complete the database configuration.

Login for the first time

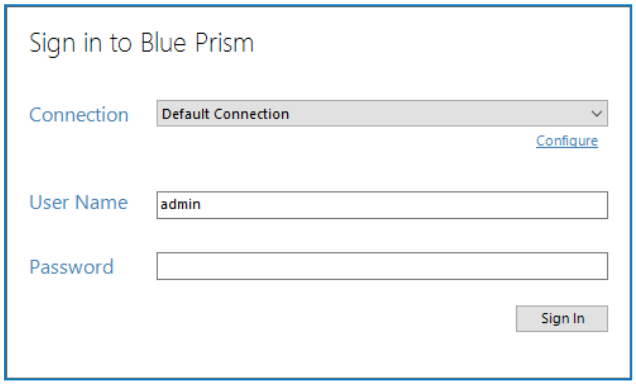
It is now possible to login for the first time and carry out some system-wide configuration.
The steps will differ slightly depending on whether the environment is configured to use Blue Prism Native Authentication or Single Sign-on for Blue Prism.

Blue Prism native authentication

Login using the default credentials:

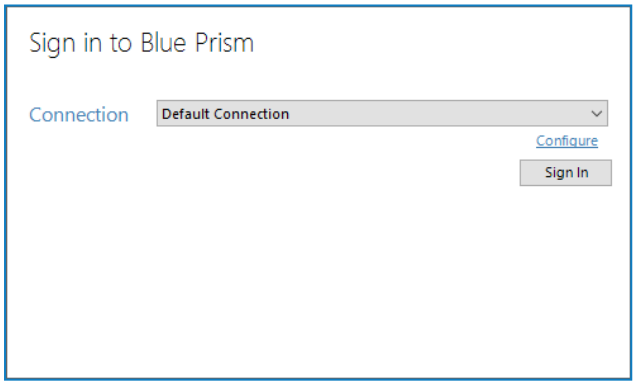
- **Username:** admin
- **Password:** admin

Follow the onscreen instructions to change the administrator's password.



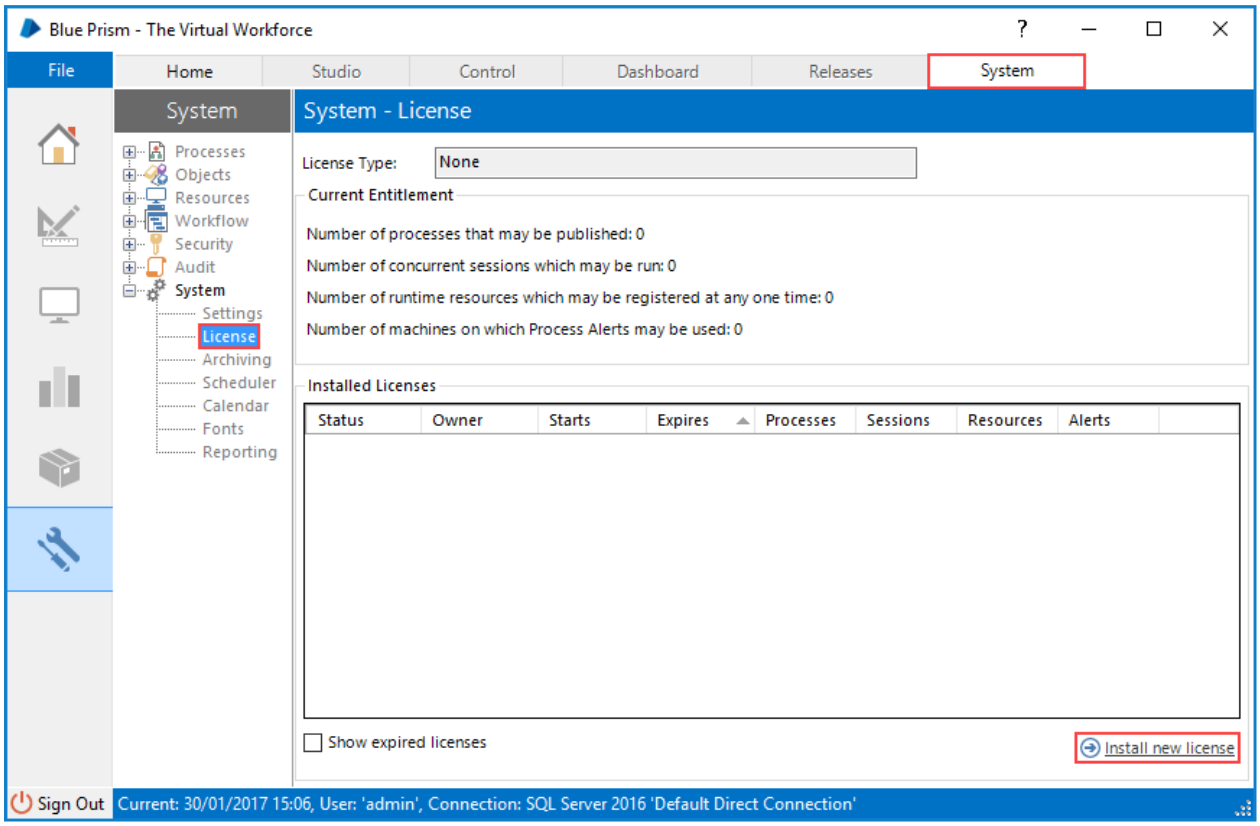
Single Sign-on for Blue Prism

Login by clicking sign in to validate that the configuration has been correctly applied.



Install a Blue Prism license key

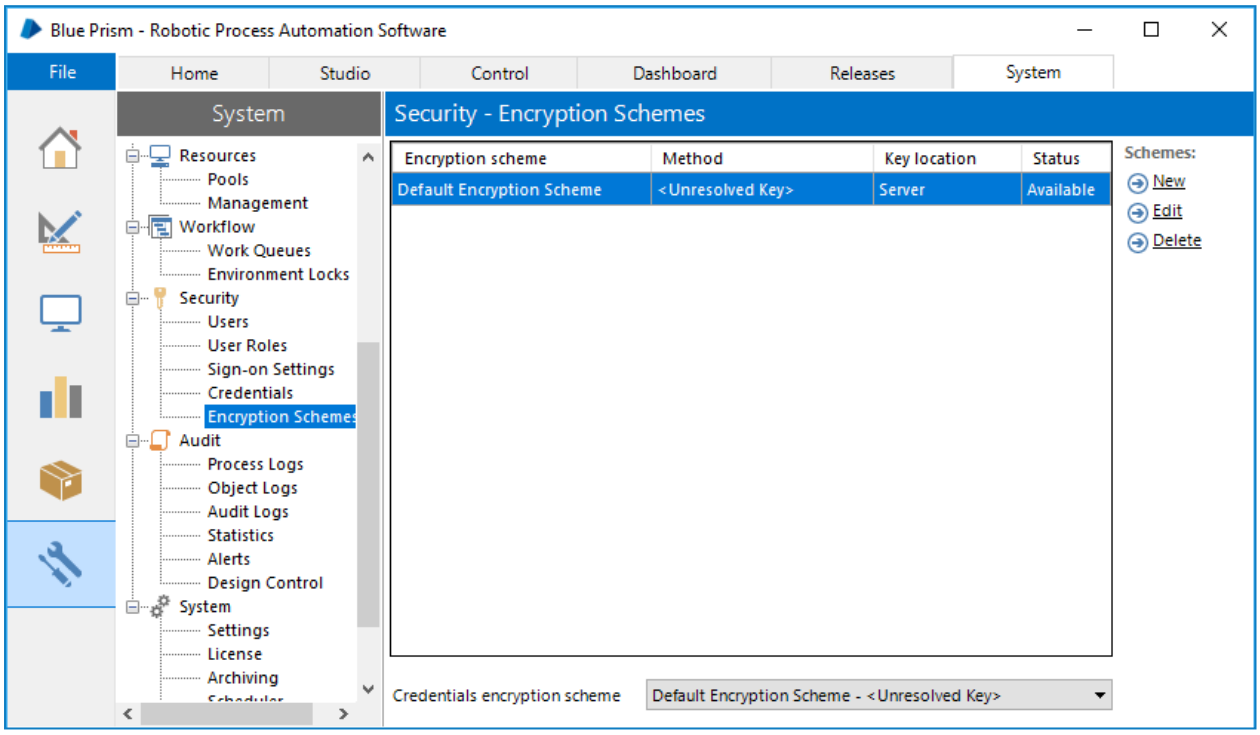
In order to enable the software it is necessary to install a valid license file. License files can be obtained via an Account Manager.



1. Click the **System** tab and select **System** > **License** from the navigation tree.
2. Select **Install new licence**.
3. Select the License file and click **OK**.

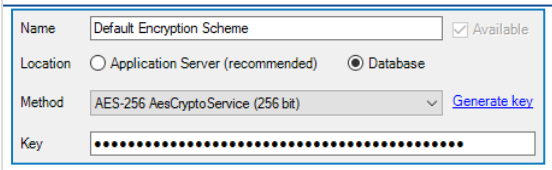
Configure an Encryption Scheme

In order to support the use of Credential Manager (for securely storing credentials), configure the Encryption Scheme that will be used.



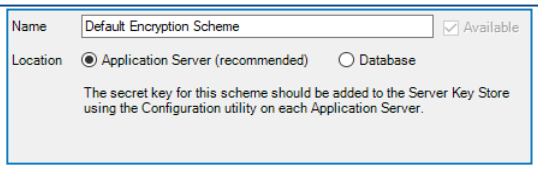
1. Click the **System** tab and select **Security** > **Encryption Schemes** from the navigation tree.
2. Select the scheme listed and click **Edit**.
3. Follow the steps below as appropriate:

Standalone Deployment



a. Select **Database**.
b. Select **AES-256**.
c. Click **Generate Key**.
d. Click **OK**.

Multiple Component (App Server) Deployment



a. Select **Application Server**.
b. Click **OK**.

A copy of each key must be backed up in a secure location

Verify the Blue Prism deployment

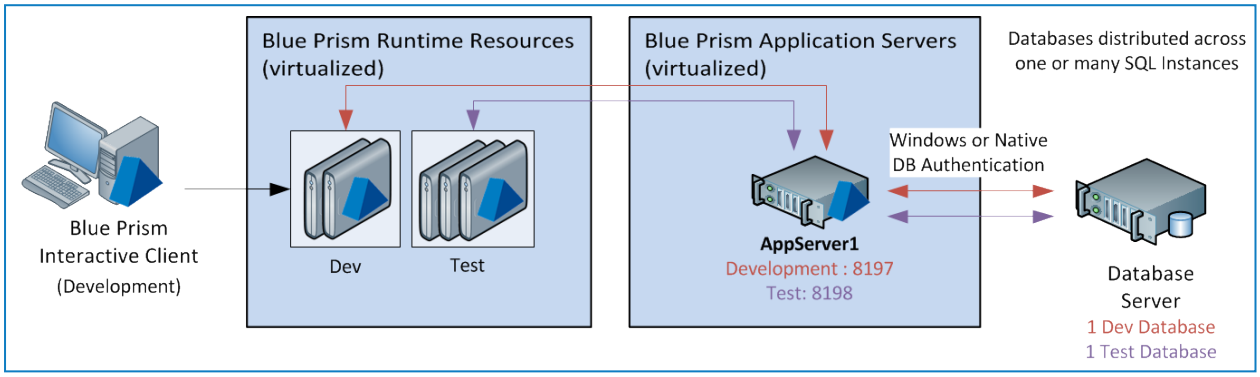
It is recommended that the installation is manually verified by carrying out some simple tasks within the system and confirming that they execute successfully.

For step-by-step instructions, see to Verify an Installation.

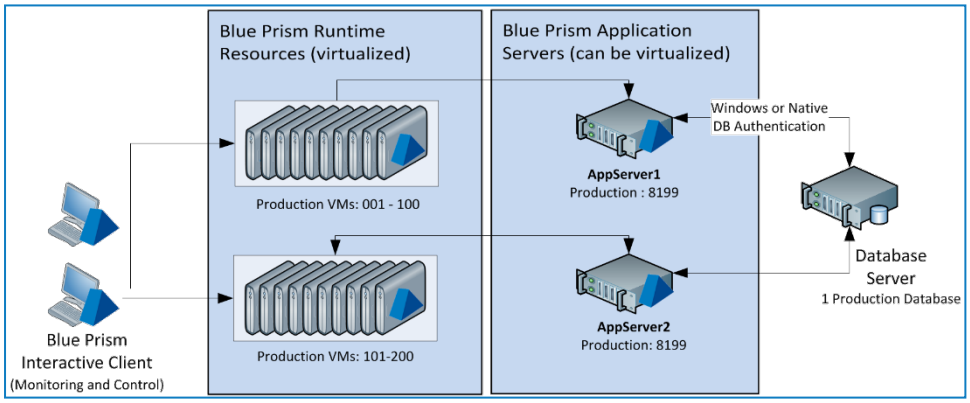
Advanced Configuration

Multiple and co-hosted Application Servers

See Blue Prism Application Server for the steps required to configure multiple Blue Prism Application Servers for various environments on a single device. Instructions about setting up an independent service connected through to a dedicated database are also included.



Where there is a requirement to have multiple Application Servers for a single environment it is important that the profile for each Blue Prism Server service across the different devices have the same information. Each profile for a given environment must use the same credential key and connect through to the same database.



Where there is a desire to implement network load balancing to provide Application Server failover it is recommended that this is only implemented once the deployment has been installed and verified.

DNS Resolution

Blue Prism installations communicate with each other using their respective machine names - it is therefore necessary to ensure that these can be resolved successfully, and that firewall rules allow appropriate communication on the defined ports.

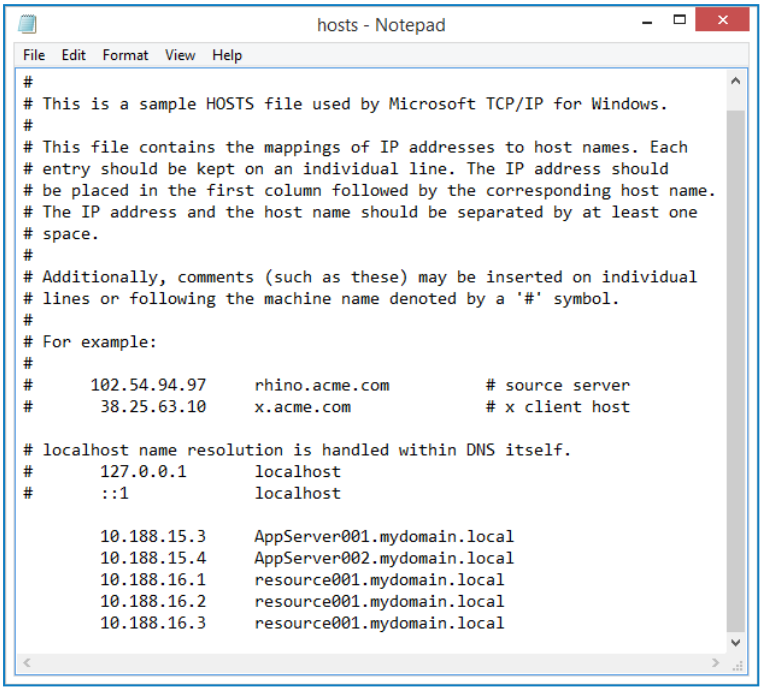
It may be necessary to set up DNS servers, Windows DNS search suffixes or local Host files to support this.

Enterprise organizations often use formal DNS management utilities, however for tactical or experimental configurations it may be appropriate to use local host files to manipulate DNS.

1. Open the host file on the local machine using a text editor such as Notepad - administrator level access is required.

   C:\Windows\System32\drivers\etc\hosts

2. Enter the IP addresses and host names that are relevant to the deployment.



3. Save and exit the text editor.

Java Access Bridge

If any of the target applications, including browser plug-ins, are deployed using the Java Runtime Environment, the Java Access Bridge must be installed on each Blue Prism client desktop.

> Information about obtaining the appropriate installers can be provided to the Blue Prism Support team by your Account Manager.

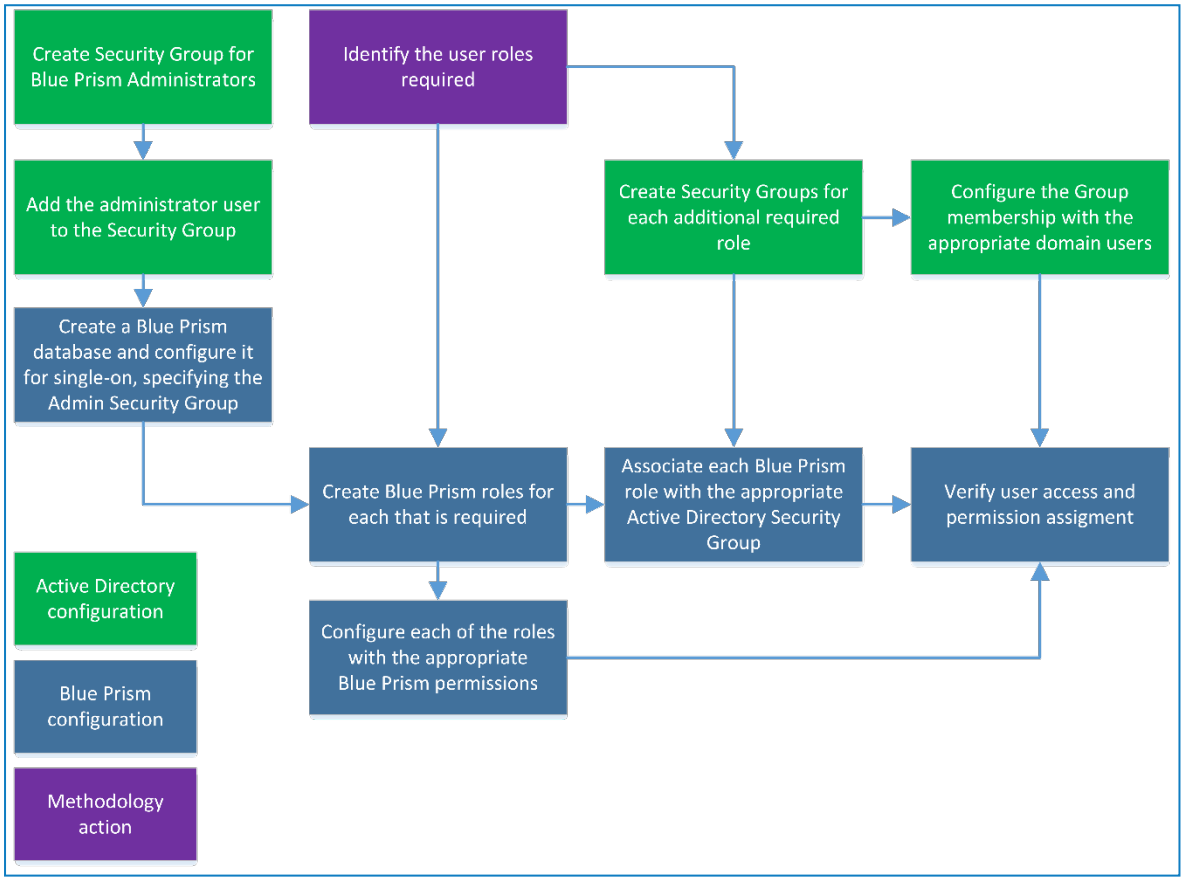
Blue Prism uses Java Access Bridge to access a series of specialised techniques for interfacing with applications written in the Java Programming Language.

For further information about the Java Access Bridge and Blue Prism, see *Java Access Bridge - User Guide*.

Active Directory configuration

Where Blue Prism is deployed within a single Active Directory Forest, it can be configured to allow users to authenticate against the platform using Single Sign-on. It essentially requires an Active Directory Security Group to be mapped to each relevant Blue Prism security role after which users will be granted access to the platform based on their Active Directory Security Group membership.

The steps required to configure Blue Prism integration with Active Directory for single sign-on are illustrated in the diagram below:



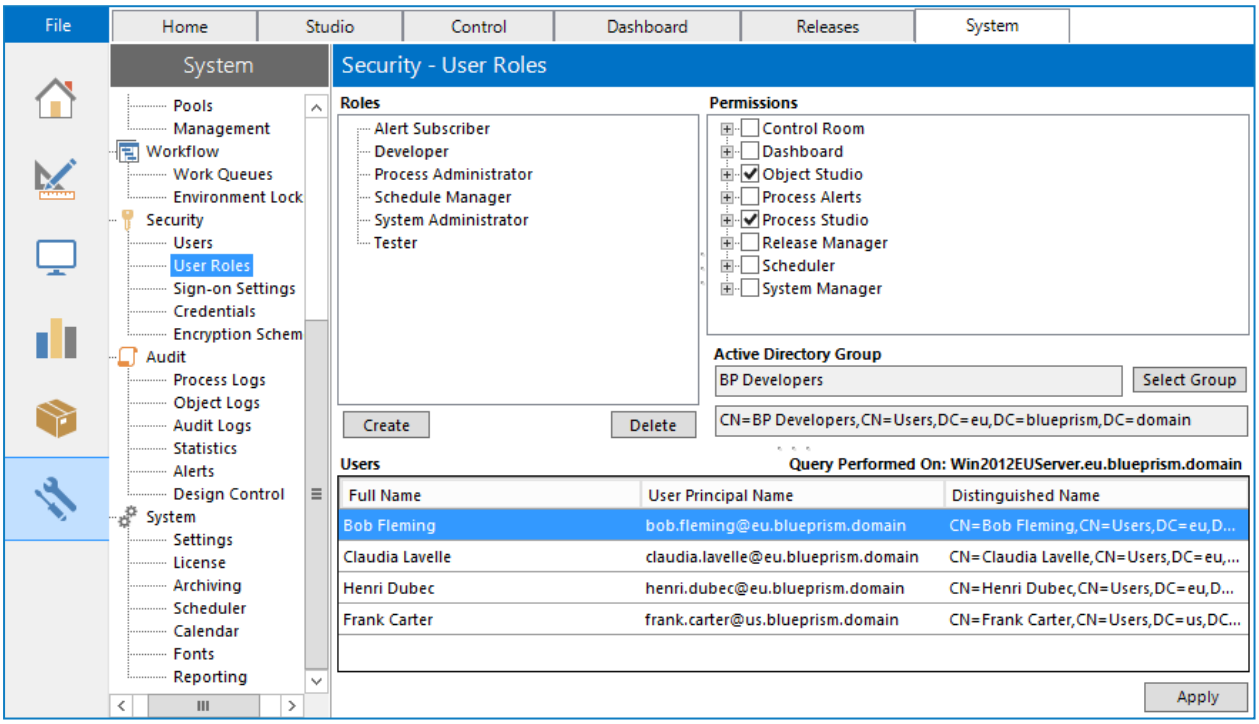
When configuring Blue Prism to use Active Directory for authentication, the database must be configured at the time of creation to use Microsoft Active Directory Authentication of Single Sign-On.

For further information, see Create/Configure a Blue Prism SQL Server Database.

Configure Active Directory users and roles

After the database has been created with the appropriate settings to indicate that Active Directory authentication should be used for the Blue Prism platform, the users and roles must be configured within the Blue Prism product.

1. Click **System** and select **Security** > **User Roles** from the navigation tree.
2. For each Role, configure the permissions that should be granted and select the Active Directory Security Group whose members should be assigned to this role.



> Blue Prism Security Roles must be associated with Security Groups created in Active Directory. Single sign-on for Blue Prism does not support built-in Groups or those with derived membership such as Domain Users or Authenticated Users. It is also recommended that the Security Groups used do not contain Foreign Security Principals.

3. Once complete, click **OK**.

Users who belong to the groups that have been configured should now be able to log in to Blue Prism and perform the actions permitted by the corresponding Blue Prism role (as indicated by the tree on the right).

Users may have to log out of windows and log back in again for Active Directory changes to take effect.

Scripted installation

The installation of the pre-requisite software and Blue Prism software can be scripted. These instructions illustrate how a single device can be scripted to be configured with:

- SQL Server
- Blue Prism Application Server connected to the SQL Server
- Blue Prism Interactive Client connected to the Application Server

The examples provided within this section are for illustrative purposes only and should be tested prior to being used in a production environment.

Information on the scripting capabilities can be found in the In-Product help (automate.exe /help), and by using the automatec /? Switch.

SQL Server

To install SQL Server Express 2012 the command below can be used:

```
Sqlexprwt_x64_ENU.exe /qs /UpdateEnabled=0, /ACTION=Install, /FEATURES=SQL, SSMS,
/INSTANCENAME=SQLExpress, /SECURITYMODE=SQL, /SQLSVCACCOUNT="NT AUTHORITY\\SYSTEM",
/AGTSVCACCOUNT="NT AUTHORITY\\Network Service", /SAPWD=saPassword_123,
/SQLSYSADMINACCOUNTS="BUILTIN\\ADMINISTRATORS", /IACCEPTSQLSERVERLICENSETERMS=1
```

This installs and configures SQL server for mixed mode authentication with a password of saPassword_123.

The parameters used when configuring this or other editions of SQL Server should be reviewed for their appropriateness.

> Production environments should be configured to connect to SQL Server using Windows Authentication where possible.

Blue Prism

Core application

To install Blue Prism use the command:

```
msiexec /i "BluePrism6.3.0_x64.msi" /QB- ALLUSERS=1
```

This command performs a full install of Blue Prism including all optional components, such as the Chrome browser extension.

Custom install options

To install Blue Prism without the optional components, use the ADDLOCAL parameter with the BluePrism and BPServer components:

```
msiexec /i BluePrism6.3.0_x64 ADDLOCAL=BluePrism,BPServer /qn
```

> The *BluePrism* and *BPServer* components must both be specified to install or upgrade Blue Prism using the ADDLOCAL parameters. They cannot be used in isolation.

The ADDLOCAL parameter can also be used to install the following optional components:

Component	Description
ChromePlugin	Installs the Blue Prism Chrome browser extension required on devices that will use this mechanism to automate Chrome.
OutlookAutomation	Installs the Microsoft Outlook Interop DLL required on all devices on which the Blue Prism MS Outlook Email VBO will be executed.

To install Blue Prism with the Chrome browser extension, use the command:

```
msiexec /i BluePrism6.3.0_x64 ADDLOCAL=BluePrism,BPServer,ChromePlugin /qn
```

To install Blue Prism and the Microsoft Outlook Interop DLL:

```
msiexec /i BluePrism6.3.0_x64 ADDLOCAL=BluePrism,BPServer,OutlookAutomation /qn
```

Configure the database connection

Once Blue Prism is installed, the Blue Prism database connection can be configured.

For SQL native authentication mode, use:

```
Automate.exe /dbconname "Friendly name" /setdbname "DB Name" /setdbserver "DB Server"
/setdbusername "DB User" /setdbpassword "********"
```

For SQL windows authentication mode use:

```
Automate.exe /dbconname "Friendly name" /setdbname "DB Name" /setdbserver "DB Server"
```

Create a Blue Prism database

Once a database connection has been defined a Blue Prism Database can then be created. The parameters that must be used will depend on whether Blue Prism Native, or Single Sign-on will be used to secure access to Blue Prism.

Configuring a database for an environment to be secured using Blue Prism Native Authentication

Database secured using SQL Authentication

```
AutomateC.exe /createdb "*******"
```

Database secured using Windows Authentication

```
AutomateC.exe /createdb ""
```

Configuring a database for an environment to be secured using Single Sign-on for Blue Prism

Database secured using SQL Authentication

```
AutomateC.exe /createdb "*******" /setaddomain "Domain Name" /setadadmingroup "Group
Name"
```

Database secured using Windows Authentication

```
AutomateC.exe /createdb "" /setaddomain "Domain Name" /setadadmingroup "Group Name"
```

The current user must belong to the AD Group specified as the /setadmingroup.

The configuration of additional Blue Prism security roles including associating with Active Directory Security Groups must be completed via the User Interface.

Register the License

The license can be added to the deployment by specifying the path of the license file in the command below:

```
AutomateC.exe /license "Path of License File"
```

Create the server service profile

Create a server service that uses the created connection. An encryption scheme named Default Encryption Scheme will be created by default.

```
AutomateC.exe /serverconfig "Profile Name" "Connection Name" "Port"
AutomateC.exe /serverconfig "Default" "Default Connection" "8199"
```

> Do not use this method to create a server for an existing environment as the encryption scheme must match existing schemes.

Configure a connection to the Application Server

Configure the devices to connect to the environment via the Blue Prism Server.

```
Automate.exe /dbconname "Friendly name" /setbpserver "Server Name" "Port"
```

Import Processes

If there are a Business Objects or Processes to be imported the XML files can be imported individually using the command(s):

```
AutomateC.exe /import "C:\My Process.xml" /user admin admin
AutomateC.exe /import "C:\My Object.xml" /user admin admin
```

The user credentials supplied here (username "admin" and password "admin") are the sample options for native authentication; these have not yet been changed but will be changed later. Where Active Directory authentication is being used, the option "/user admin admin" should be replaced with "/sso"; this assumes that the Active Directory groups have already been configured.

Publishing Processes

Any processes which need to be published can be published as follows:

```
AutomateC.exe /publish "My Process" /user admin admin
```

Publishing a process makes it available to be run or scheduled.

Scripting references

The following table provides references to further information on the command line examples printed above.

Topic	Help Reference	Download Location
Msiexec	http://technet.microsoft.com/en-us/library/cc759262%28WS.10%29.aspx	N/A
SQL 2012	https://technet.microsoft.com/en-us/library/ms144259(v=sql.110).aspx	https://www.microsoft.com/en-gb/download/details.aspx?id=29062
Blue Prism	AutomateC.exe /help or Contact your Account Manager or the Technical Support Team	N/A

Generate manual SQL Create and Upgrade Scripts

For scenarios where it is necessary for database creation or update operations to occur manually, the SQL scripts for the operation can be generated.

- **Create Script** - AutomateC.exe can be used to generate a script and save it on a local device which, when run against a blank database, generates the Blue Prism schema and carries out essential configuration.

  ```
  Automatec.exe /getdbscript > "c:\temp\CreateScript.sql"
  ```

- **Upgrade Script** - AutomateC.exe can be used to generate a script and save it on a local device which, when run against an existing Blue Prism database, updates the schema and configuration to be appropriate for the version of Blue Prism.

  ```
  Automatec.exe /getdbscript /fromrev 10 > "c:\temp\UpgradeScript.sql"
  ```

Advanced scripted techniques

Setup the Windows services

For each server configuration (excluding Default which is configured automatically), a windows service can be created using SC.exe. This is the service control program typically distributed within resource kits by Microsoft.

```
sc create {SERVICENAME} binPath= "[Blue Prism Install Location]\BPServerService.exe {CONFIGURATIONNAME}"
```

Please note that in the below examples that there is a space between binPath= and the opening quote, and also that the configuration name is within the same quotes as the location as the BPServerService.

```
sc create "Blue Prism Dev Server" binPath= "C:\Program Files\Blue Prism Limited\Blue Prism Automate\BPServerService.exe Development"
sc create "Blue Prism Test Server" binPath= "C:\Program Files\Blue Prism Limited\Blue Prism Automate\BPServerService.exe Test"
```

Where the server configuration name contains spaces, it is necessary to use a backspace as an escape character. The example below shows the setup where the server configuration name is “Development Environment”

```
sc create "Blue Prism Dev Server" binPath= "\"C:\Program Files\Blue Prism Limited\Blue Prism Automate\BPServerService.exe\" \"Development Environment\""
```

Configuring the Access Control List (ACL) for non-administrators

When the Blue Prism Server service is configured to use a WCF connection mode, if the Service logon account is not a local administrator, it will be necessary to grant the logon account user permissions to start the listener using the defined settings.

The command to setup the ACL will differ based on the WCF connection mode and the binding configured on the associated server profile settings.

```
netsh http add urlacl url=[http | https]://[Server Binding]/bpserver user=[Service User]
```

The following should be considered when constructing the command:

- When using a WCF mode that uses message encryption select http.
- When using a WCF mode that uses transport encryption select https.
- When a binding is specified this must be explicitly stated in the command
- When not using a binding, a strong wildcard should be used in the binding

WCF mode that uses message encryption where no server binding is specified on the server profile

```
netsh http add urlacl url=http://+:8199/bpserver user=Domain\UserName
```

WCF mode that uses message encryption where a server binding is specified on the server profile

```
netsh http add urlacl url=http://bpserver001.mydomain:8199/bpserver user=Domain\UserName
```

WCF mode that uses transport encryption where no server binding is specified on the server profile

```
netsh http add urlacl url=https://+:8199/bpserver user=Domain\UserName
```

WCF mode that uses transport encryption where a server binding is specified on the server profile

```
netsh http add urlacl url=https://bpserver001.mydomain:8199/bpserver user=Domain\UserName
```

Associating a Certificate with the network interface

When the Blue Prism Server service is configured to use a WCF connection mode that requires a deployed certificate, these steps provide the commands to associate a locally deployed certificate with the listening IP address and port.

The certificate must be deployed for the computer account. Likewise ensure that the issuing certificate authority is trusted by this device and that the certificate, and its issuing authority, are trusted by all client devices.

```
netsh http add sslcert ipport=[IP Address:Port] certhash=[Thumbprint] appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

For example:

```
netsh http add sslcert ipport=10.0.2.15:8199 certhash=bac31cc4094793d275167cf02b31bbac2718f3c7 appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

Supported software

The following technologies are supported for use with the software.

Operating system

Version	Blue Prism Client	Blue Prism Server
Windows 7 SP1 (32-bit / 64-bit)	✓	✓
Windows 8.1 (32-bit / 64-bit)	✓	✓
Windows 10 Anniversary Update (32-bit / 64-bit)	✓	✓
Windows Server 2008 R2 SP1 (64-bit)	✓	✓
Windows Server 2012 (64-bit)	✓	✓
Windows Server 2012 R2 (64-bit)	✓	✓
Windows Server 2016 (64 bit)	✓	✓

Where the Blue Prism client is installed on a 64-bit operating system, it will run as a 32-bit application.

> 64-bit application integration using invasive techniques is not supported.

Microsoft SQL Server

The following Microsoft SQL Server versions are supported for locating the Blue Prism database.

	Express	Standard	Enterprise
SQL 2012 (32-bit / 64-bit) (inc. R2)	✓	✓	✓
SQL 2014 (32-bit / 64-bit) (inc. R2)	✓	✓	✓
SQL 2016 (64-bit)	✓	✓	✓
SQL 2017 (64-bit)	✓	✓	✓

SQL Express versions are only appropriate for non-production environments such as for the purposes of Proof of Concept exercises.

SQL Azure is also supported.

Microsoft .NET Framework

To install Blue Prism, Microsoft .NET Framework 4.7 is required.

Microsoft .NET applications built on the specified .NET Framework Version or below can be automated by Blue Prism.

See Verifying the .NET Framework Version(s) for additional guidance.

Web browser

Where Blue Prism is required to interact with Web Applications, the following browsers are supported:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

Java Access Bridge (JAB) and Runtime Environments (JRE)

If java components are to be automated by Blue Prism, the following considerations should be taken into account in relation to JAB and JRE:

- When installed on 32-bit operating systems, Java Access Bridge 2.0.0 and above can be used to launch relevant applications in embedded or external 32-bit mode.
- When installed on 64-bit operating systems, the minimum supported Java Access Bridge is 2.0.2.
- Business objects that model 64-bit applications must be set to external 64-bit mode.

Minimum SQL permissions

The minimum SQL permissions required on the Blue Prism database for normal operation are:

- Datareader
- Datawriter
- All roles prefixed with bpa_

  For example:

  - bpa_ExecuteSP_DataSource_bpSystem
  - bpa_ExecuteSP_DataSource_custom
  - bpa_ExecuteSP_System

The roles prefixed “bpa_” are only available once the database has been configured using the in-product Create Database functions or manually using the CreateScript.

The minimum SQL permissions do not provide appropriate privileges to carry out Create, Configure or Upgrade database actions from within the product, therefore an appropriate administrator account will need to be used when any of these actions are required:

- Create Database: dbcreator (server role) or sysadmin (server role)
- Configure Database: sysadmin (server role) or dbowner (database role)
- Upgrade Database: sysadmin (server role) or dbowner (database role)

To manually execute the Create or Upgrade database scripts (available via Blue Prism Support) against an existing database, the following SQL permissions are required by the user carrying out the actions:

- DBCreate: sysadmin (server role) or dbowner (database role)
- DBUpgrade: sysadmin (server role) or dbowner (database role)

Verifying software versions

Verify the Blue Prism version

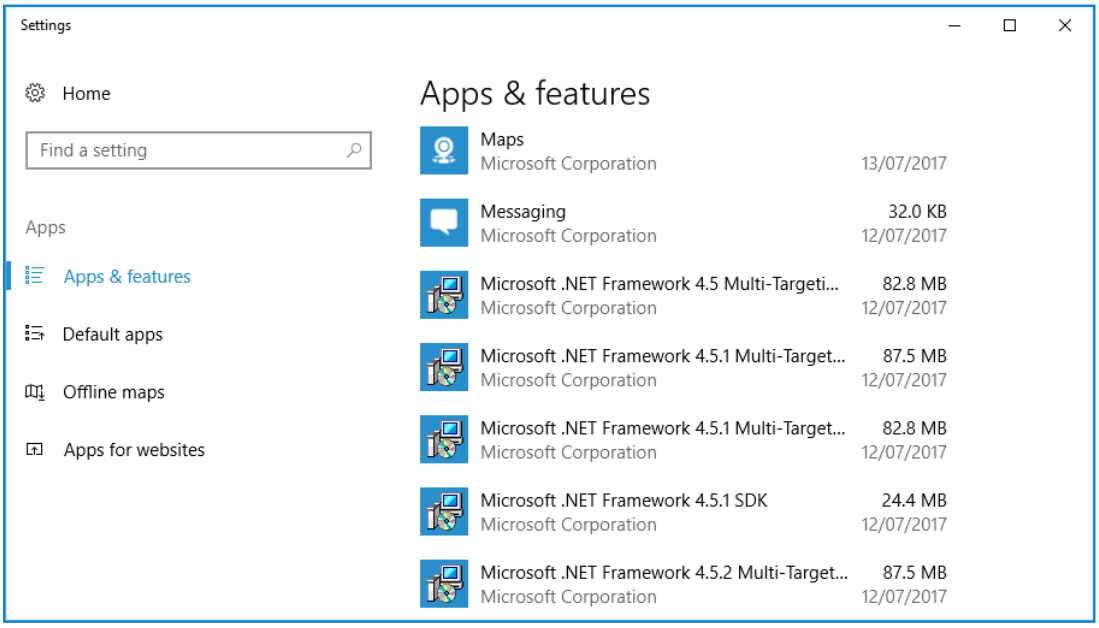
The Blue Prism version information is contained in the application under **Help** > **About**. The example below shows Blue Prism version 6.0.0.

Verify the .NET Framework version(s)

Multiple versions of .NET Framework can be installed as some versions do not supersede earlier releases.

To determine which .NET Framework versions are installed on a machine:

1. Access the programs list



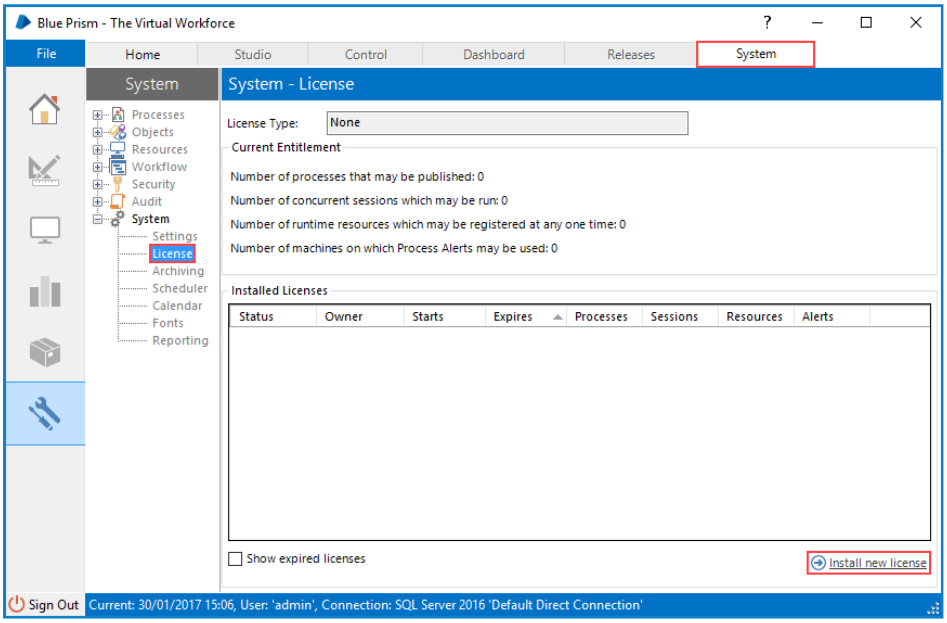
2. Read the following article to determine which versions are installed: Determine Which .NET Framework Versions Are Installed.

Update the license

Apply the license using the instructions below based on the version of the software that is installed.

To install or update a Blue Prism license file follow the steps below:

1. Launch Blue Prism.
2. Click the **System** tab and select **System** > **License**.
3. Select **Install new licence**.
4. Select the License file and click **OK**.



All Blue Prism components on each Interactive Client, Resource and Server must be restarted for the changes to be fully recognized.

Verify an installation

This section provides a simple automation scenario to test that the basic components of the Blue Prism installation are operating as expected.

The verification steps include:

- Creating a new Process using the Microsoft Word Object.
- Test the Process.

These instructions assume that the Blue Prism database is empty and that Microsoft Word has been installed on the device. If that is not the case, process names which conflict with existing processes must be changed.

If problems are experienced whilst verifying the installation, see Troubleshooting an installation.

Import the Microsoft Word Object

A Microsoft Word automation object is included with the release package and is required for the verification process.

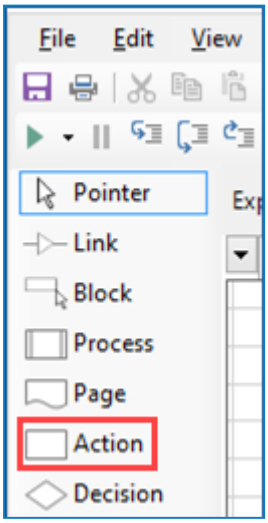
1. Launch Blue Prism and sign in using the *admin* username.
2. Select **File** > **Import**.
3. Select the *BPA Object – MS Word.xml* file. For the default install location, this is in C:\Program Files\Blue Prism Limited\Blue Prism Automate\VBO.
4. Complete the wizard to import the object.

> Optionally the above steps can be repeated to import the Microsoft Excel Object - *BPA Object – MS Excel.xml*.

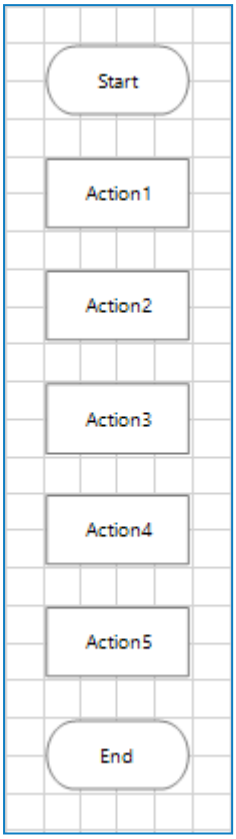
Create a new Process

1. Select the **Studio** tab.
2. Right-click in the navigation pane and click **Create Process**to display the New Process wizard.
3. Enter *Letter Writing Test* as the process name and click **Next**.
4. Enter *Evaluation test* as the process description and click **Finish**.

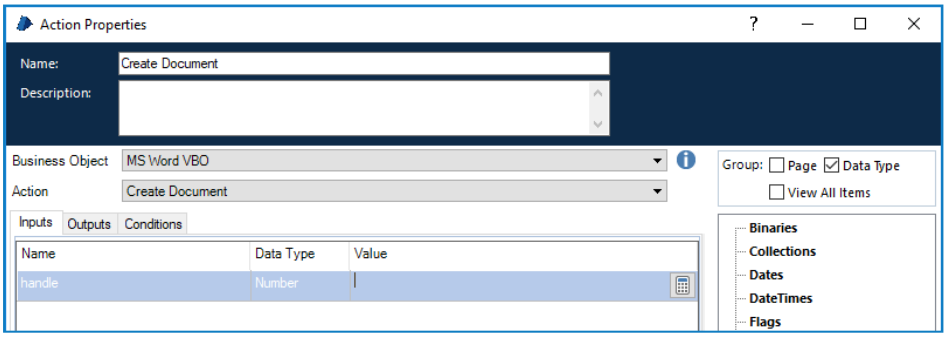
   The new process is listed under Processes in the navigation tree.
5. Double-click the process to open it in Process Studio.
6. Add four actions to the process. To add an action, select **Action** and from the toolbar and click in the process diagram.



7. Place the action stages between the Start and End stages.



8. Double click the first action stage to open the Action Properties dialog.
9. Enter *Create Document* as the action name and select **MS Word VBO** and **Create Document** as the Business Object and Action.

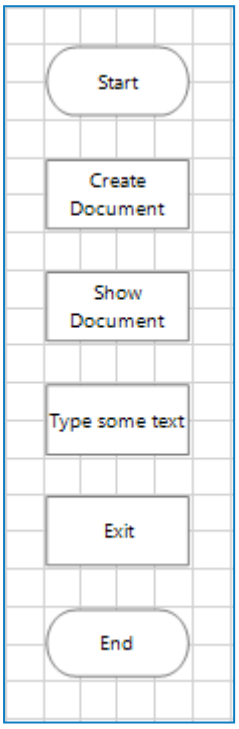


Leave the input blank.

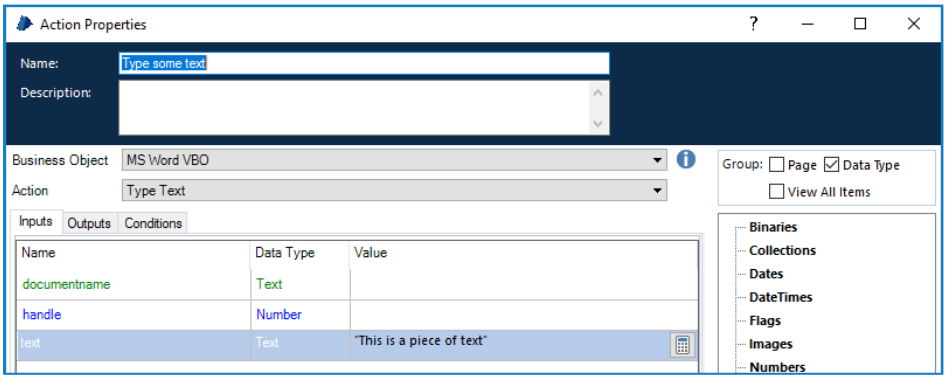
10. Click **OK** to save the changes.

11. Repeat these steps for each for the remaining three stages using the following details.

Original Name	New Name	Business Object	Action
action2	Show Document	MS Word VBO	Show
action3	Type some text	MS Word VBO	Type Text
action4	Exit	MS Word VBO	Exit

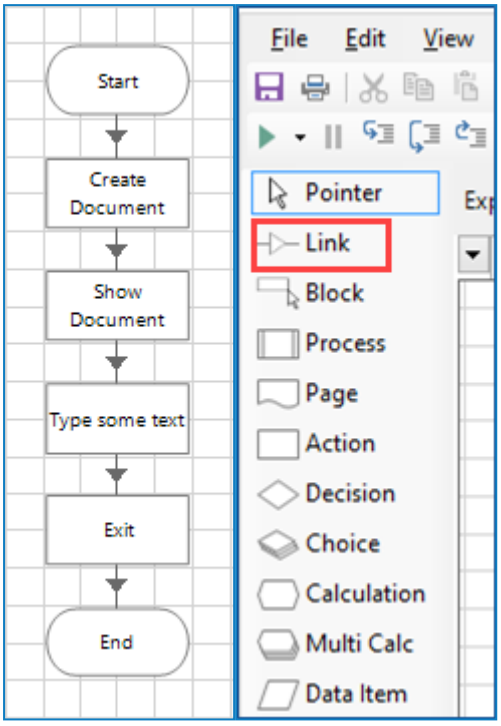


12. Double click **Type some text** stage.
13. Select the **Inputs** tab.
14. For the *text* input parameter, enter some text into the Value field. The text must be enclosed in quotation marks. It will be added to a Word document when the process runs.



15. Click **OK** to return to Process Studio.

16. From the toolbar select the Link tool and connect each of the stages in turn by dragging from one stage to the next.

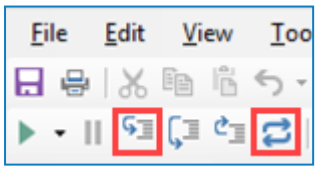


17. Save the process. A confirmation message should be displayed in the status bar at the bottom of the window.

Test the Process

The following buttons are required to test the process in Process Studio.

- **Step** - Highlighted on the left
- **Reset** - Highlighted on the right



1. Once the process has been saved, click the reset button.
2. Click the step button. This highlights the first stage in the process diagram and indicates that this is the next stage to be run. Next time the step button is clicked, the actions within that stage are performed.
3. Click step again perform the actions in the first stage. A new Microsoft Word document is created but it will not yet be visible.
4. Continue to click step to move from the stage to stage.
5. Verify that the expected action takes place with each step - the new Microsoft Word document is shown, the correct text is typed into the document, and the document closes on Exit.
6. If you wish to run the process again, click the reset button and repeat.

Troubleshoot an installation

The following sections seek to provide guidance if specific issues are experienced either during the install or when verifying that the installation has been successful.

Installing Blue Prism

Error Message 2869 on installation

Some versions of Blue Prism that are not intended for general availability will present an error when:

- Installed over a pre-existing installation of Blue Prism
- A newer version of Blue Prism is being installed

In order to proceed it is necessary to remove the previous installation of Blue Prism.

Database connectivity

There are a number of checks that can be performed when a connection cannot be made to a SQL Server over the LAN:

- **Verify Network Connectivity** - Ensure that all relevant devices are connected to the same network and are able to communicate.
- **SQL Credentials** - Verify the SQL credentials and that the user has appropriate permissions on the SQL Server.
- **Firewall** - Check that the firewalls on the servers themselves or within the network are not preventing communication.
- **SQL Browser Service** - Ensure the SQL Browser Service on the SQL Server is enabled to allow for a SQL Instance to be found. For SQL Server Express this service is typically disabled by default.
- **Enabling TCP/IP Connectivity** - Where remote connectivity is required for SQL, check that TCP/IP connectivity is enabled for the SQL Instance. Microsoft provide articles specific to each version of SQL that provide instructions to Enable the TCP/IP Network Protocol for SQL Server.

The following sections provide information on common errors.

Unable to determine whether database exists

When testing a SQL connection an error message is displayed:

Unable to determine whether database exists - A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error:26 - Error Locating Server/Instance Specified)

This is a common error when working with SQL 2008 R2 or later as the server is set up by default to not accept remote connections. TCP/IP connectivity needs to be enabled for the given instance of SQL Server.

Microsoft provide articles specific to each version of SQL that provide instructions to Enable the TCP/IP Network Protocol for SQL Server.

Failed to create database

When creating a SQL database through Blue Prism an error message may display:

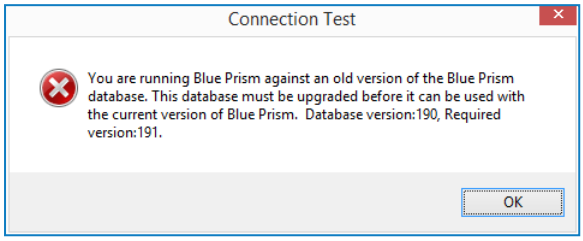
Failed to create database – A network-related or instance-specific error occurred while establishing a connection to SQL server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 – Could not open a connection to SQL Server)

This is a common error when working with SQL 2008 R2 or later as the server is set up by default to not accept remote connections. TCP/IP connectivity needs to be enabled for the given instance of SQL Server.

Microsoft provide articles specific to each version of SQL that provide instructions to Enable the TCP/IP Network Protocol for SQL Server.

Incorrect database version

You are running Blue Prism against an old version of the Blue Prism database. The database must be upgraded before it can be used with the current version of Blue Prism. Database version: xxx, Required version: xxx



This message indicates that the database does exist but it is not currently valid for this version of Blue Prism and is commonly received after upgrading the Blue Prism software, prior to having applied the database upgrade.

Commonly the database version will be a lower number than the required version – the ability to Upgrade Database to the appropriate version is provided within the Connections interface. Ensure that you have a database backup before applying a database upgrade.

If the current database version is greater than the required version, this version of Blue Prism cannot be used with this database and a newer version of the product is required.

Insufficient permissions error message is displayed

A message is displayed:

Failed to create database - CREATE DATABASE permission denied in database 'master'

This indicates that the SQL user does not have permission to create a new database. This typically happens with Windows Authentication, but may occur with a SQL authenticated user with restricted permissions.

A number of options are available for working around this issue:

- Re-attempt the action under the context of a SQL administrator, or provide elevated database permissions for the user attempting the action
- A DBA (Database Administrator) can create the database manually, and then manually run a Blue Prism provided SQL script to define the schema. Following this a Blue Prism user can use the Configure database option to determine whether the environment should be configured for Blue Prism Native or Single Sign-on authentication.

Configuring a Blue Prism Application Server

The Windows Service cannot start

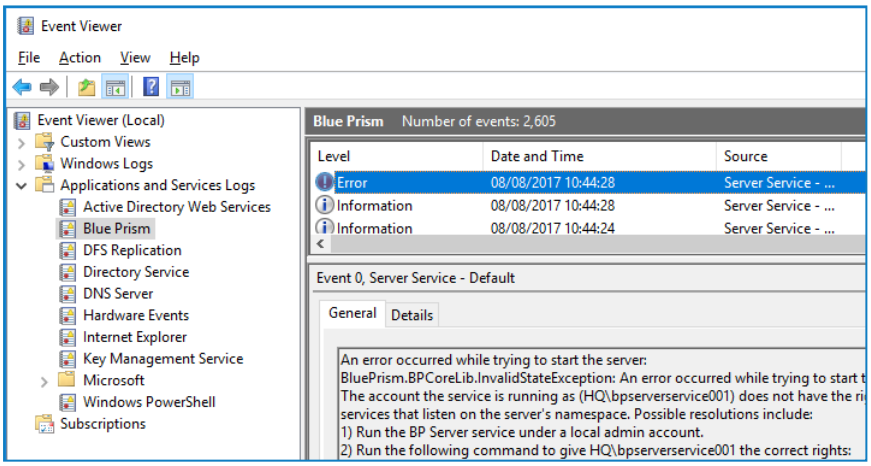
If the Windows service will not start or starts and immediately stops, this indicates that there is a problem with the configuration of the server.

When the server service is starting a number of checks occur including, but not limited to, the following:

- Appropriate access to the SQL database, and expected DB updates have been installed.
- Encryption scheme keys are held on the server for those records in the database that indicate the key should be held there.
- The server connection mode supports the Blue Prism authentication mode.
- The user has appropriate rights to start the listener on the device.
- Valid license is installed.

In order to identify the cause of issues, the following steps should be followed:

- **Check the profile for warning messages within the BPServer.exe utility** - This will highlight issues such as if a server service is not configured for this profile; or if an encryption certificate is required but cannot be found; or if the service logon user does not have appropriate rights to start the listener.
- **Review messages within Event Viewer** - This will highlight issues such as if the server service profile cannot be found; if the server cannot authenticate with the database; if an encryption certificate is required but there are issues with it; if expected encryption schemes cannot be found within the service profile; or if the service logon account does not have appropriate rights to start the listener.



- **Attempt to start the service using the BPServer.exe utility** - Using this utility in this way is only suitable for troubleshooting purposes as it attempts to start the service under the context of the currently logged in user. If the locally logged on user has different permissions to the service logon account the behaviour seen here can differ in comparision to when the service is started from the Services management console. For example, if the service is configured to connect to SQL using windows authentication this will require the currently logged in user to have appropriate minimum rights to the Blue Prism database on the target SQL server.

Connecting to the database

Review the troubleshooting section entitled Database Connectivity for general connectivity advice.

When troubleshooting, consider that the account being used to authenticate with SQL will depend on SQL authentication mode that has been configured on the connection used by the server:

- SQL Authentication - The credentials specified on the connection will be used.
- Windows Authentication - The context of the server service will be used. If starting the service from the Windows Services console, this will be the service logon account; if starting the service directly from BPServer.exe, this will be the currently logged in user.

Database does not exist

Service cannot be started. BluePrism.BPCoreLib.InvalidStateException: Connection not valid: Server is unavailable

Database 'BP_Prod_Native' does not exist

This error indicates that the database cannot be found.

Verify that the database server, and database name are correct. If a Blue Prism database has not yet been created, a user with appropriate SQL permissions can achieve this through use of the in-product Create Database action, or manually through use of a CreateScript.sql.

Incorrect permissions

Service cannot be started. BluePrism.BPCoreLib.InvalidStateException: Connection not valid: Server is unavailable

Cannot open database "BP_Prod_Native" requested by the login. The login failed.

This error indicates that the user used to authenticate against the database does not have permissions to access it.

The user will need to be granted at least SQL permissions on the target database that meet or exceed the minimum permissions.

Incorrect credentials

Service cannot be started. BluePrism.BPCoreLib.InvalidStateException: Connection not valid: Server is unavailable

Unable to determine whether database exists - Login failed for user

This error indicates that the user credentials used to access the database are incorrect (e.g. invalid username or password).

Verify the user credentials being used, and that the user's SQL permissions on the target database meet or exceed the minimum permissions.

A valid license could not be detected

Service cannot be started. System.NotSupportedException: A valid license could not be detected.

A valid license must be configured for the environment in order for a Blue Prism server to be able to start.

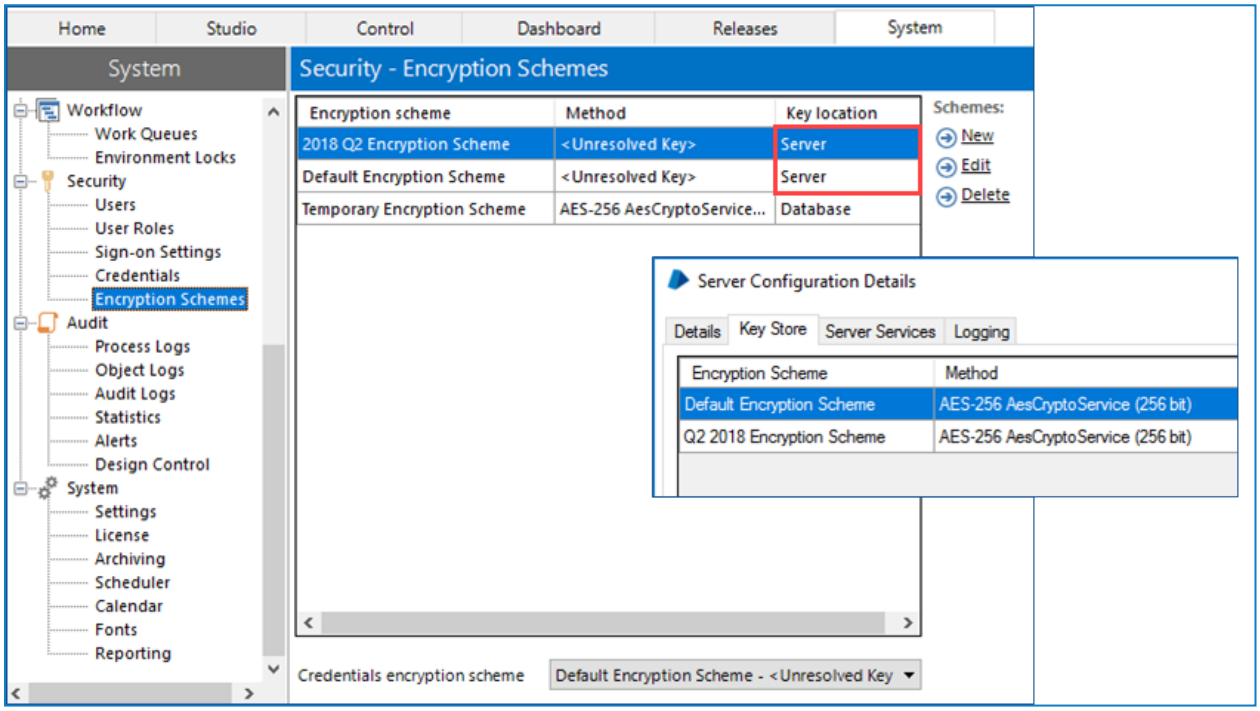
A new license key can be installed via the Blue Prism user interface. It may be necessary to use a client that has a direct database connection to carry out this action.

The following encryption keys could not be resolved

Service cannot be started. BluePrism.BPCoreLib.InvalidStateException: The following encryption keys could not be resolved: 2018 Q2 Encryption Scheme, Default Encryption Scheme

This error indicates that there are encryption scheme keys that are expected to be on the server, but which cannot be found. The error above indicates that it can't find two schemes which should be defined locally on the Blue Prism Server named: "2018 Q2 Encryption Scheme" and "Default Encryption Scheme".

It is necessary to review the Encryption Scheme records configured within the database, and ensure that for each with a Key location of Server, that there is an appropriate encryption scheme record created on the Blue Prism Server. An example of comparing the settings within the Client against the settings within the Blue Prism server configuration utility.



The account the service is running as does not have the right to create services

Errors such as the following indicate that the account that the service is being run as, does not have appropriate permissions to configure the service to listen on the configured settings:

BluePrism.BPCoreLib.InvalidStateException: An error occurred while trying to start the server. The account the service is running as (AD\bpserverservice001) does not have the right to create services that listen on the server's namespace.

This is a common message when the Blue Prism Server is being started as a user which is not a local administrator; or if the Access Control List (ACL) has not been configured appropriately.

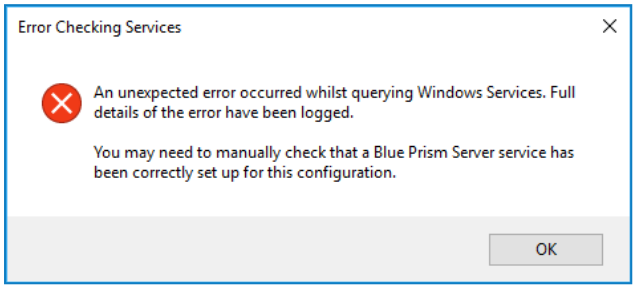
To resolve the issue either:

- Use the Blue Prism Server configuration utility to setup permissions for the configured user to start the service; or
- Execute the command provided within the event viewer message.

It is important to ensure that the ACL permission is created specifically for the user that will be starting the service, and that it is configured with either a generic URL if no server binding is specified; or a URL that directly aligns with a specified server binding.

Error checking services

If this error is presented when editing the Blue Prism server profile it indicates that an error has occurred when validating if the currently logged in user is a local administrator.



This is known to occur when a local user account is used to access a device that is a member of an Active Directory Domain, and where a Domain Controller cannot be contacted. It is necessary to ensure that a Domain Controller can be contacted.

Connecting to the Application Server

Errors connecting a Blue Prism device to the Application Server can be caused by a large number of factors, it is strongly recommended that the following are verified:

- Blue Prism Server service is started
- The address being used for the Server service is resolveable (i.e. via DNS) and that network connectivity is not being prevented. (e.g. verify that firewalls are configured appropriately).
- The connecting device is configured with the correct settings:
  - The server connection mode, and port match those defined on the server
  - If the server is configured with an address binding, that the device is connecting using that address
- If the server is configured to use transport encryption, the certification authority that issued the server certificate must be trusted by the connecting the device.

Configuring a Runtime Resource

Runtime will not start

Commonly misconfiguration of start-up command is the main reason for a Runtime Resource failing to start such as incorrect use of switches or settings.

Before trying to start a Runtime Resource using the command line, verify that if the Blue Prism client is launched on the device, that it is possible to login to Blue Prism using the default connection. By default – the Runtime Resource will use the same connection settings when started via the command line.

Using the client to validate that a connection can be achieved will help to validate that the appropriate network connections can be established and that the appropriate configuration has taken place.

Configurable settings can prevent connections

There are a number of configurations that can restrict whether Runtime Resources can connect.

Require secure inbound instructional connections

If this settings is enabled, only Runtime Resources that are correctly configured to use the /sslcert start-up command will be able to connect to the Blue Prism environment.

Allow anonymous public Runtime Resources

If this setting is disabled, only Runtime Resources that are configured with appropriate details to authenticate against the environment as part of the start-up command will be able to connect.

The configuration required differs depending on the mode users authenticating against Blue Prism are required to use:

- Single sign-on for Blue Prism - The start-up command will need to include an /sso switch, and the user context that the Runtime Resource runs as will need to be configured with appropriate Blue Prism permissions.
- Blue Prism native authentication - The start-up command will need to include the /user “username” “password” parameters, and the user credentials specified will need to match a valid Blue Prism user configured with appropriate permissions.

Runtime will not accept connections/control room cannot connect to a Runtime

There are a number of situations where a Runtime Resource can be started, but subsequently fails to successfully accept connections. It is useful to review the dialog within the Runtime Resource dialog and within Control Room. Also review the system and application specific event logs on the Runtime device.

General issues

The following issues may occur both for any Runtime Resource.

Runtime Resource does not receive connections or an operation was attempted on something that is not a socket

Situations where the Runtime Resource appears to be online, but where it is not contactable from Control Room, are indicative of scenarios where the network communication cannot be established. Common reasons for this are:

- The Runtime Resource is not online
- Firewalls (or similar) are preventing the communication
- The network is not operating as expected

Runtime Resource appears online in some Control Rooms but not others

Situations where the Runtime Resource appears to be online, but independent Control Room installations show different information about whether the Runtime can be contacted are indicative of network connectivity issues.

Each Blue Prism Server and Control Room attempts to directly connect to each Runtime Resource, therefore if a given Control Room cannot connect to a Runtime Resource but others can, it suggests a network or device configuration issue is preventing the Control Room from establishing the connection.

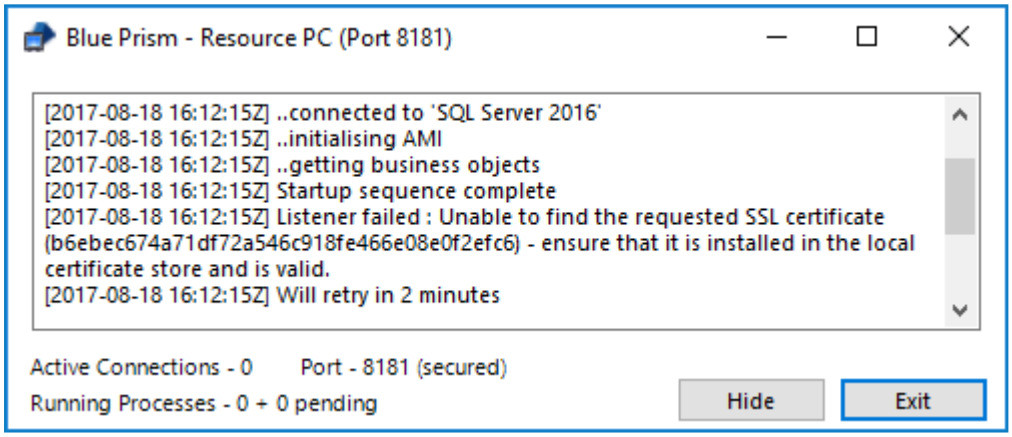
Blue Prism may also forcibly prevent a connection if the Runtime is connected to one environment (such as Production: Finance), but the Control Room is connected to a different environment (such as Production: Ops)

Issues when the /sslcert switch is being used

The following issues are only relevant to Runtime Resources that are configured to use a certificate to encrypt inbound instructional communications such as through use of the /sslcert switch.

Unable to find the requested SSL certificate

Unable to find the requested SSL certificate – ensure that it is installed in the local certificate store and is valid



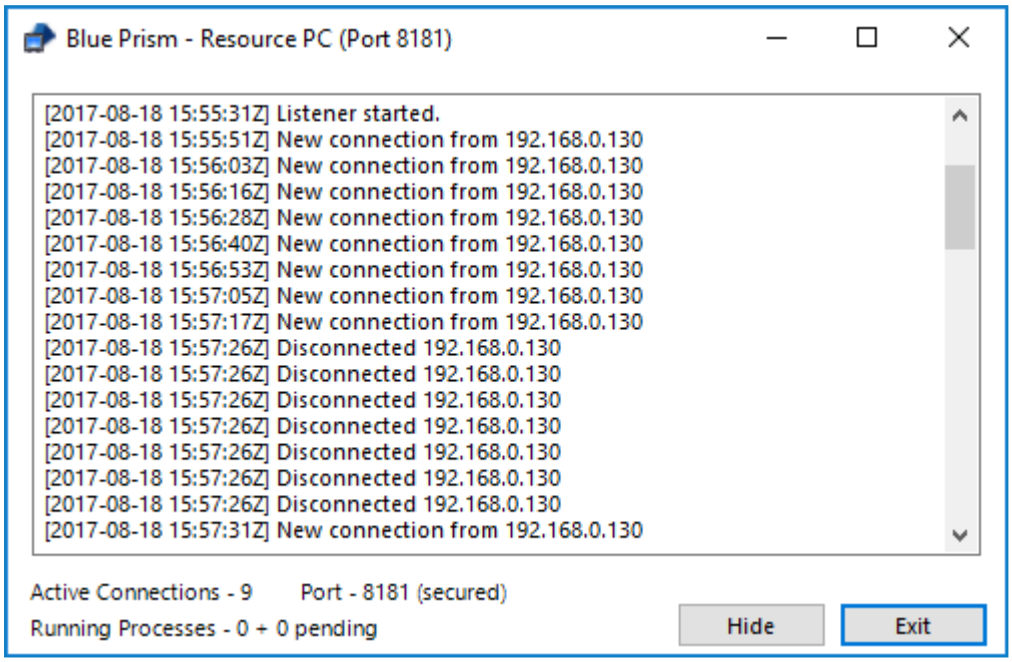
In order to address errors that state that the certificate cannot be found, it is necessary to ensure that the certificate has been installed on the local machine (within the computer account) and that the thumbprint has been set correctly.

This message is commonly received when a hidden character is present at the beginning of the thumbprint. It is therefore strongly recommended that a utility such as notepad is used to delete any non-visible characters from the beginning of the thumbprint.

The remote certificate is invalid according to the validation procedure

Commonly where there are validation issues with the certificate it is expected that the Runtime Resource will be able to start, and it may be seen to accept connections, but those connections are likely to cease within a short time frame as shown. Likewise the Control Room user interface is likely present a message such as:

Error establishing a secure connection – The remote certificate is invalid according to the validation procedure



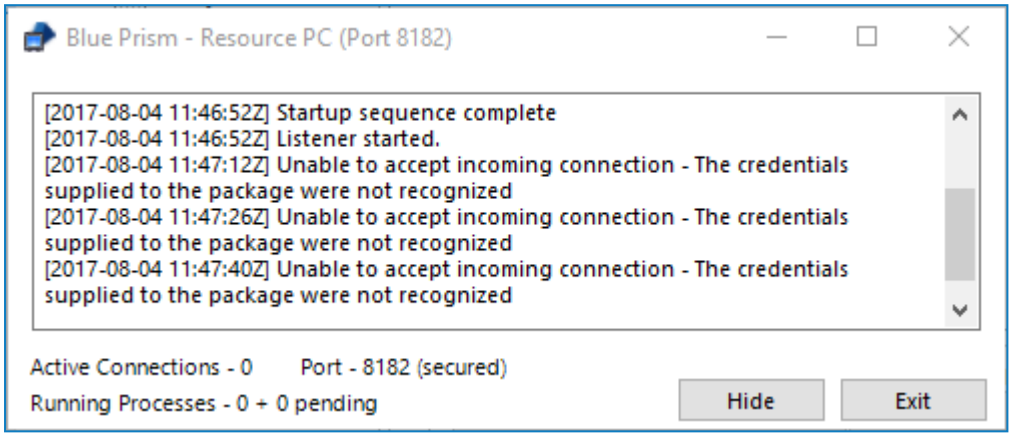
To address this type of issue is necessary to ensure that:

- The address used by Blue Prism to contact the Runtime Resource matches the name on the certificate.
- The certificate has not been revoked.
- The certificate has been trusted by the device on which Control Room is running.

Unable to accept incoming connection – the credentials supplied to the package were not recognized

Commonly this error is coupled with a message in Control Room that states:

Unable to accept incoming connection because the certificate (/sslcert) cannot be used for inbound connections. Ensure the logged in user has permission to read the certificate private key.



This is indicative of situation where the user context used to start the Runtime Resource does not have sufficient rights to configure the listener correctly. It is most commonly found where the applied local security policy of the device results in user accounts being run in admin approval mode.

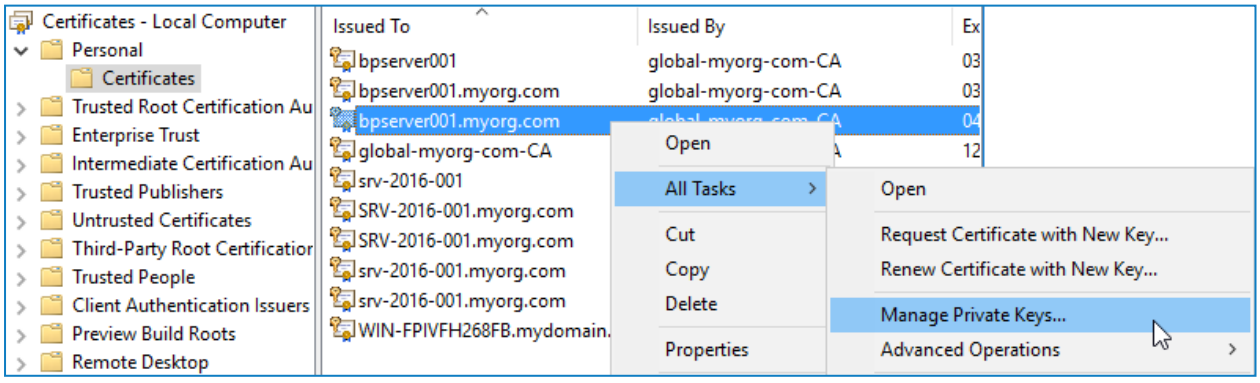
To diagnose and resolve this issue, start the Runtime Resource from an elevated command prompt. For example: start command prompt as an administrator and use it to launch a Runtime Resource using the same switch configuration.

To address this issue it is necessary to ensure that:

- The Windows Logs (System) have been reviewed for further information.
- The private keys for the certificate specified using the /sslcert switch are available on the device.
- The starting user of the Runtime Resource has read access to the private keys.

The steps below provide instructions to configure access to the private keys for a given certificate:

1. Open the certificates interface on the specified device (e.g. Manager Computer Certificates, or via the Certificates snap-in for MMC).
2. Find the appropriate certificate, access the context menu and select to Manage Private Keys.
3. Grant read permissions to the user that is responsible to starting the Runtime Resource.



When on a device that enforces Admin Approval Mode it is necessary to ensure that the user is explicitly named as having permission to the key (rather than being granted permission through membership of an administrators group).