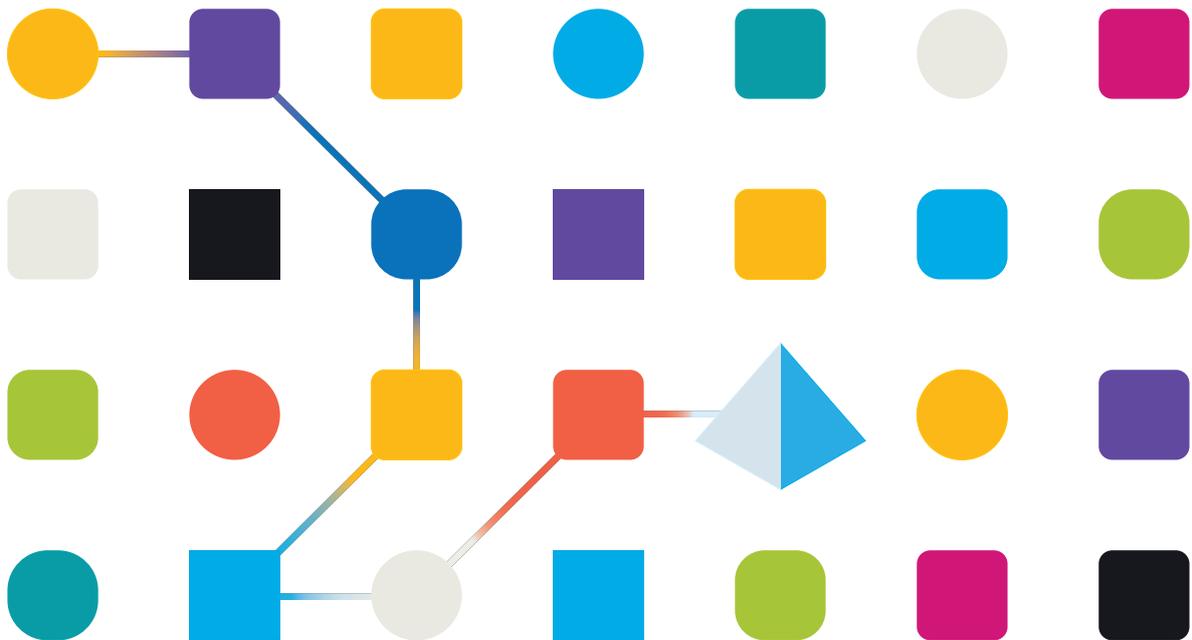




# Blue Prism 7.0 Enterprise Edition Installation Guide

Document Revision: 6.0



## Trademarks and Copyright

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

### © 2024 Blue Prism Limited

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

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

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

# Contents

<b>Introduction</b> .....	<b>4</b>
Intended audience .....	4
Related documents .....	4
<b>Enterprise preparation</b> .....	<b>5</b>
Planning .....	6
Multi-device deployment considerations .....	7
<b>Components and minimum requirements</b> .....	<b>9</b>
Interactive client .....	9
Runtime resources .....	10
Application server .....	11
Database server .....	12
<b>Minimum SQL permissions</b> .....	<b>14</b>
<b>Multi-device deployment</b> .....	<b>15</b>
Blue Prism application server .....	17
Blue Prism interactive client .....	41
Blue Prism runtime resource .....	44
<b>Standalone deployment</b> .....	<b>48</b>
<b>Advanced configuration</b> .....	<b>57</b>
Advanced installation options .....	57
Multiple and co-hosted application servers .....	58
DNS resolution .....	59
Java Access Bridge .....	60
Active Directory configuration .....	60
Silent installation .....	66
Contained databases .....	73
Deploying to a virtualized or cloud environment .....	74
Service Principal Name (SPN) configuration for Kerberos authentication .....	78
<b>Update a license</b> .....	<b>82</b>
<b>Verify an installation</b> .....	<b>83</b>
1. Import the Microsoft Word object .....	83
2. Create a new process .....	83
3. Test the process .....	87
<b>Verify software versions</b> .....	<b>88</b>
Verify the Blue Prism Enterprise version .....	88
Verify the .NET Framework version(s) .....	88
<b>Troubleshoot an installation</b> .....	<b>89</b>
Installing Blue Prism .....	89
Database connectivity .....	89
Application server .....	90
Runtime resources .....	96

## Introduction

This guide provides guidance on the process to follow when installing SS&C | Blue Prism® Enterprise 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.

 This guide provides details of how to configure Blue Prism Enterprise in a secure enterprise environment. However, it is advised that you also consult the Robotic Operating Model (ROM) Security information on the [SS&C | Blue Prism Portal](#) for recommendations of best practice.

It is also 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 Enterprise components and provides guidance and considerations on the main options available.

 For an overview of the installation, also watch the [Blue Prism Enterprise installation video](#).

## Intended audience

This guide is aimed at IT professionals with experience in configuring and managing networks, servers, and databases. The installation process requires familiarity with installing and configuring web servers and databases.

## Related documents

There are a number of other documents that provide additional information about specific aspects of the implementation of Blue Prism Enterprise.

Document Title	Description
<a href="#">Blue Prism Infrastructure Reference Guide</a>	A detailed overview of Blue Prism Enterprise infrastructure templates, including architectures, failover and disaster recovery strategies, communication methods, and virtualization requirements
<a href="#">Blue Prism Java Access Bridge User Guide</a>	A detailed overview of the steps required to install the Java Access Bridge using the installer and manually, along with methods for verifying the installation.
<a href="#">Blue Prism Active Directory Integration Guide</a>	A guide to integrating Blue Prism Enterprise with Active Directory for user authentication.

## Enterprise preparation

Before installing Blue Prism Enterprise, 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 Enterprise).

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 the minimum specifications and the devices must be able to communicate with each other over the network.
- If using Active Directory Single Sign-on (SSO), the users' Active Directory accounts, the Blue Prism application server(s), and all Blue Prism devices that will be accessed by users (such as, interactive clients and runtime resources) must reside in Active Directory domains that directly reside within a common Active Directory forest. For more information, see [Active Directory domains](#).

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 <a href="#">minimum requirements</a> (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 authentication or Active Directory Single Sign-on?	NA	Relevant
What account will the Blue Prism Server service be configured to logon as?	NA	Relevant

For details about the supported software versions and operating systems, see [Software and hardware requirements](#).

## 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 configured 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 more details, see <a href="#">Selecting a BP Server connection mode</a> .  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).	

	Dev/Test/Pre-Prod Environments	Production Environments
User role permissions	<p>To strengthen Blue Prism network security, role-based access control (RBAC) should be utilized and only specific users, such as infrastructure administrators, should be granted access to application servers and network communication configuration. All other users should be denied access by default. Explicit allow/deny access should be configured for all users and the principle of ‘Least Privilege’ followed.</p> <p>These controls should also extend to the users of Blue Prism, so that only those who need access to the platform are allowed and are only given the level of authority required to carry out their role, while all others are denied access by default.</p> <p>It is advised that you also consult the Robotic Operating Model (ROM) security information on the <a href="#">Blue Prism Portal</a> for recommendations of best practice.</p> <div data-bbox="368 674 1461 831" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Please be aware that starting and running a runtime resource with elevated permissions might affect the interaction with the application that is being automated. Generally, the permissions of the runtime resource must match those of the user context of the target application.</p> </div>	

## Components and minimum requirements

For details about supported software versions and operating systems, see [Software and hardware requirements](#).

### Interactive client

Blue Prism interactive clients are used to configure and control the environment and to monitor the Blue Prism resources as processes are executed - they can be thought of as Development or Administration machines.

Each Blue Prism interactive client requires the installation of Blue Prism along with the necessary software prerequisites.

In development environments the interactive clients are used to develop and maintain the processes - therefore access to each of the target applications and any associated pre-requisites or thick clients will also need to be deployed and configured on these devices.

These pre-requisites may include the Java Access Bridge, SAP Scripting, Adobe Acrobat Professional and certified Terminal Emulator software for mainframe automation. Local Administrator privilege is usually required in order to install these pre-requisites and the Blue Prism runtime.

Processes and objects are stored in the database server (or, for non-production use, in a local copy of SQL Express).

interactive clients communicate with each connected runtime resource in order to ascertain its' status.

Typically interactive clients communicate with the database via the Blue Prism Server using a Windows Communication Framework (WCF) connection, however there is the option to configure a direct database connection as is required when a Blue Prism Server is not available.

## Runtime resources

Blue Prism runtime resources are responsible for executing the processes that are allocated to them - they are run unattended and are often referred to as digital workers.

This commonly requires process definitions to be retrieved from the central repository; interacted with, automating various third-party applications via the user interface, and generate the necessary log information.

Each runtime resource requires the installation of Blue Prism along with the necessary software prerequisites. In addition, each will need to be configured with access to each of the target applications and any associated pre-requisites. Relevant thick clients will also need to be deployed.

Typically runtime resources communicate with the database via the Blue Prism Server using a Windows Communication Framework (WCF) connection, however there is the option to configure a direct database connection as is required when a Blue Prism Server is not available.

 The specification of the interactive clients (used for development) and the runtime resources must meet the collective recommendations of the in-scope target applications. (for example, SAP, Office, Kana)

A useful indicator is to base the specification on an equivalent PC used by an end-user to automate those same applications.

## Application server

The Blue Prism Server is an optional but important component that marshals database connections and removes the need to configure direct connections between the various Blue Prism components and the database.

When implemented, all Blue Prism components (interactive clients and runtime resources) connect to the Blue Prism Server service.

Additional Blue Prism Servers can be added to an environment to provide increased scale and capacity. Typically Blue Prism Servers are deployed to dedicated, virtual servers however there are options to co-host Blue Prism Servers that service different environments on the same devices. For example, a single virtual server could host Blue Prism Servers for the Dev and Test environment.

The Blue Prism Server is responsible for the key used by encrypted work queues and credentials, and also manages the execution and allocation of scheduled processes.

Where multiple Blue Prism servers are deployed for the same environment, all of them must be configured with the same encryption scheme information, and those which have the scheduler enabled must be configured to use the same time zone.

## Database server

Underpinning the Blue Prism platform is a Microsoft SQL Server database which holds not only the process and object repository, but also user credentials, audit information and production process log data - a transaction log of each production process running in the environment.

Communication between the Blue Prism runtime resources, application servers and database is typically moderate to high in volume, and transactional in nature as records are frequently inserted into the session log, along with look-ups and updates being performed within workflow tables.

Consideration should be given to the proximity of the database server to the Blue Prism application server and runtime resources, particularly when implemented across large or multi-site networks. Where network latency is an issue, it will be made more prominent by the frequency of the queries performed.

Commonly the Blue Prism database will receive direct connections only from each Blue Prism application server within a given environment.

In some circumstances, such as where application servers are not deployed, any Blue Prism component can be configured to establish a direct database connection. This will be subject to the application of appropriate routing, authorization and access settings.

The number of connections that will be established by each directly connecting device is managed by the .NET Framework through use of SQL connection pools.

As with many database applications, Blue Prism can occupy shared space in a data center should suitable database servers already be available. Likewise where there are multiple segregated Blue Prism environments such as for Dev, Test, Production, or for different parts of the business (HR, Finance, Operations), each will have its own dedicated database. If required, these schemas can co-exist within the same SQL Server instance and the Blue Prism application server is then responsible for directing the communications to the relevant database.

See also the specific data sheets available for Provisioning and Maintaining a Blue Prism Database Server.

## Database collation

The collation of the Blue Prism database must be one that is case-insensitive and that supports the 1252 codepage. The case-insensitive feature is typically denoted by the presence of CI within the collation name, for example:

- Latin1\_General\_CI\_AS
- SQL\_Latin1\_General\_CP1\_CI\_AS
- Chinese\_PRC\_CI\_AS
- Japanese\_CI\_AS
- Arabic\_CI\_AS
- Greek\_CI\_AS
- Cyrillic\_General\_CI\_AS

## Database disk space requirements

Best-practise should be followed in relation to the performance and allocation of disk arrays and their use by both Microsoft SQL Server and the underlying operating system.

The amount of disk space that is required by Blue Prism in the database is largely dependent on the number of connected runtime resources, although it will also be dependent on the data retention policy. For production environments the amount of space required is:

- Minimum 10 GB data file per connected runtime resource
- Minimum 5 GB log file per connected runtime resource (50% of the value allocated to the data file)

In addition to the above metrics, the minimum amount of disk space allocated to the database data file for a production environment should be no less than 100 GB (+ 50 GB for logs). For Dev/Test environments this minimum should be no less than 50 GB (+25 GB for logs)

Regular archiving of the Blue Prism logs, as well as frequent database server maintenance and housekeeping can be used to control the amount of space used overtime.

## High availability and redundancy

The platform can be connected to SQL databases which are configured for SQL high-availability or redundancy.

This includes those that are configured for clustering or mirroring and those hosted by SQL Availability Groups.

## Minimum SQL permissions

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

- db\_datareader
- db\_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 command.

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:
  - When deleting the existing database - sysadmin (server role)
  - When not deleting the existing 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: dbcreator (server role) or sysadmin (server role)
- DBUpgrade: sysadmin (server role) or dbowner (database role)
  - When deleting the existing database - sysadmin (server role)
  - When not deleting the existing database - sysadmin (server role) or dbowner (database role)

Additionally, it is recommended to grant the execute permission to the SQL user running the Blue Prism database to the custom table type `<schemaname>.IntIdTableType`. See [Blue Prism application server, step 12: Configure the Windows service](#) for details on the SQL user. An example of the SQL command is shown below where [dbo] is the <schemaname> and [User] is the SQL user running the Blue Prism database:

```
GRANT EXEC ON TYPE::[dbo].[IntIdTableType] TO [User]
GO
```

If this permission is not granted, users will be unable to view session logs from Control Room, unless they are an admin user. The Session Logs table will display blank and an error message will show in the Blue Prism Event Logs for the application server, for example:

*System.Data.SqlClient.SqlException (0x80131904): The EXECUTE permission was denied on the object 'IntIdTableType', database 'BPv7', schema 'dbo'.*

## Multi-device deployment

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

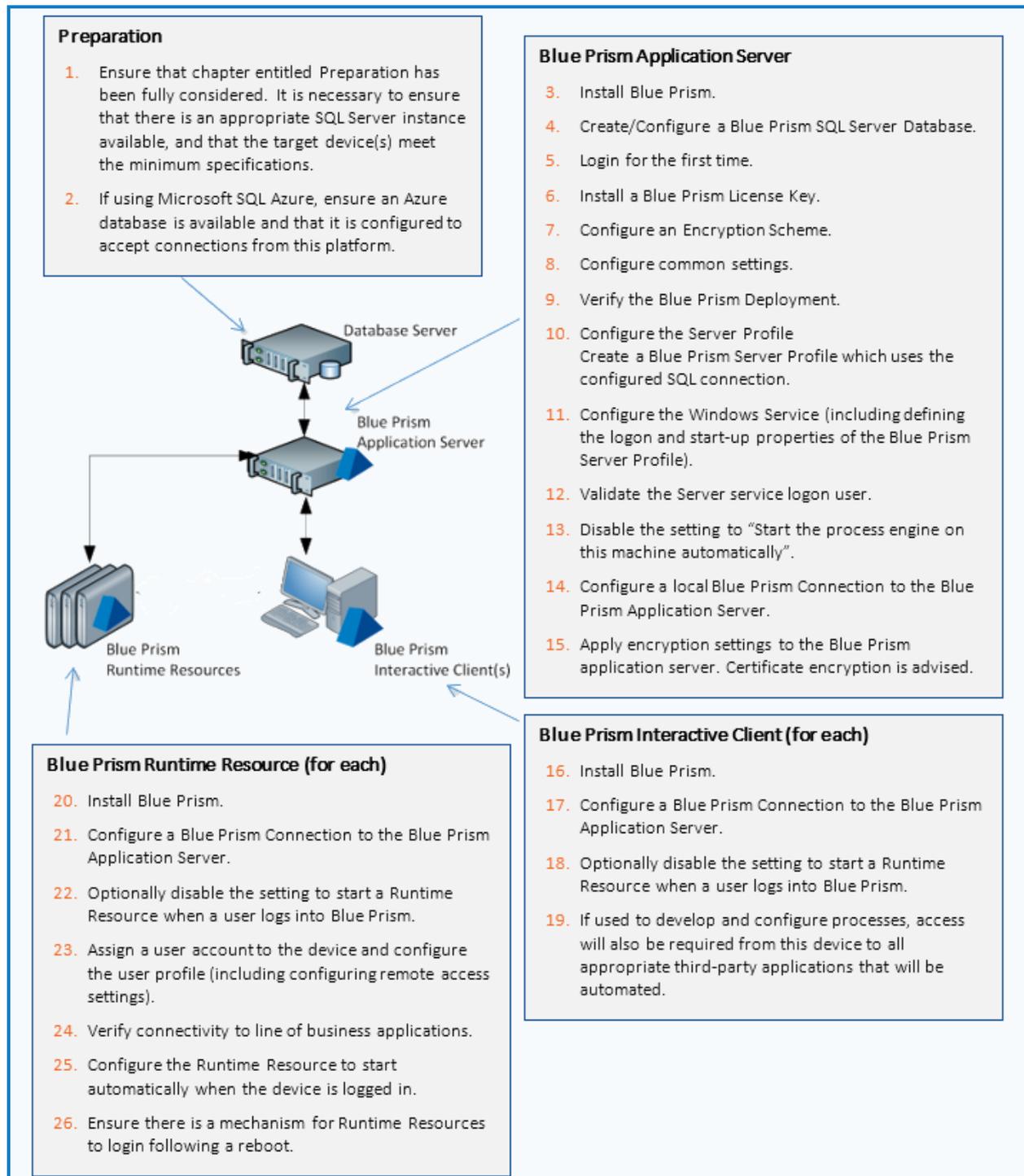
 Prior to following this guidance, ensure that you have fully considered the information in [Preparation](#).

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.

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



If problems are experienced whilst installing, see [Troubleshooting an installation](#).

## Blue Prism application server

**!** Blue Prism application servers should not be installed on any domain or network where there is internet facing access. The Blue Prism platform should be implemented into your environment as a separate entity. This can be achieved through network segregation, for example, using jump servers for cross-domain travel, or other similar methods. It is advised that you also consult the Robotic Operating Model (ROM) Security information on the [Blue Prism Portal](#) for recommendations of best practice.

Install and configure the first application server by either configuring a new Blue Prism database or connecting to a pre-configured database.

### 1. Install Blue Prism

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

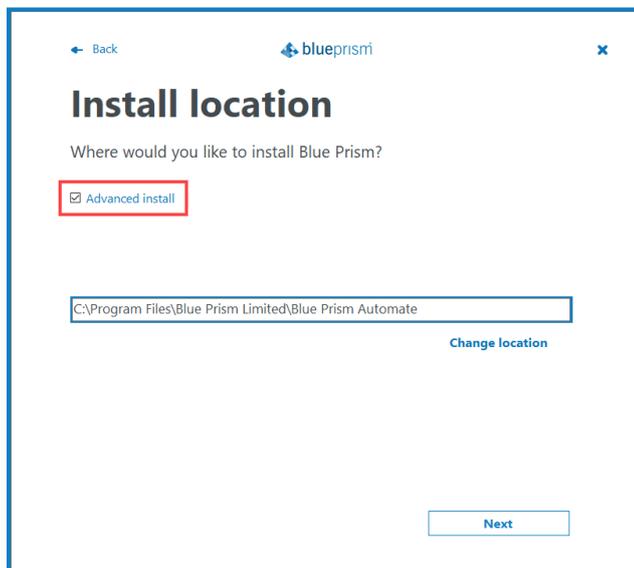
- 32-bit Installer: BluePrismx.x.nn\_x86.msi
- 64-bit Installer: BluePrismx.x.nn\_x64.msi

Installers are available from the [Blue Prism Portal](#).

Click **Get started** to follow the steps in the installation wizard and complete the installation. If required, you can change the language in the wizard by clicking **Choose language** at the top of the first screen.

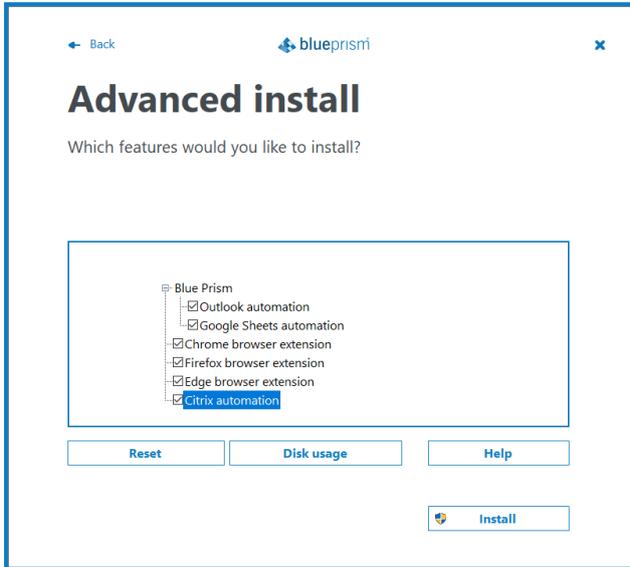
### Advanced install options

The following additional components are available during a Blue Prism installation if the **Advanced install** option is enabled on the Install location screen. Components selected by default that are not required must be deselected before proceeding with the installation.



- **Outlook automation** - Required on devices where the Blue Prism MS Outlook Email VBO will be executed.
- **Google Sheets automation** - Required on devices where the Blue Prism Google Sheets VBO will be executed.
- **Chrome browser extension** - Required on devices that will be used to automate Chrome.
- **Firefox browser extension** - Required on devices that will be used to automate Firefox.
- **Edge browser extension** - Required on devices that will be used to automate Chromium-based Edge.

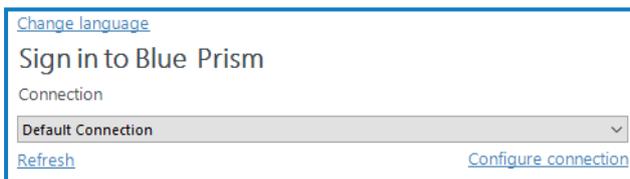
- **Citrix automation** - Required on devices that will be used to automate applications natively via a Citrix Virtual Desktop Environment (VDE). This option is only available for selection if Citrix Workspace has been installed. For more details, see [Citrix integration](#).



## 2. 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. On the Blue Prism login screen, click **Configure connection**.



2. In the Connection Configuration dialog, specify the connection details as outlined in the image below:

\*If the Connection type selected includes 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.

- **SQL Server (SQL Authentication)** - Connection Name (must be unique), Database Server, Database Name, User ID
- **SQL Server (Windows Authentication)** - Connection Name (must be unique), Database Server, Database Name
- **Availability Group (SQL Authentication)** - Connection Name (must be unique), Database Server, Database Name, User ID
- **Availability Group (Windows Authentication)** - Connection Name (must be unique), Database Server, Database Name
- **SQL Server (Custom Connection String)** - Connection String (the complete SQL connection string must 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:

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

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

As the database does not yet exist, one of the following messages will display:

**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 <b>OK</b> to clear the message and then click <b>Create Database</b> .		Click <b>OK</b> to clear the message and then click <b>Configure Database</b> .
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 <a href="#">Troubleshooting an installation</a> .

### 3. Create and configure a Blue Prism SQL Server database

There are threestages 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 by using the Create Database action.
- **Apply Blue Prism schema** - The database schema is applied to the configured database.

The 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 against a pre-existing database. The CreateScript.sql can be obtained via request from Blue Prism Customer Support or generated using the Blue Prism client - Click **Generate Script** at the bottom of the Create a new database or Upgrade the database screens.

- **Configure Blue Prism sign-on settings** - A number of configuration options are applied to the database. These are applied automatically when using the 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 is completed in a single step when using the Create Database functionality.

1. To create and configure a database, click **Create Database** or **Configure Database** in the Connection Configuration dialog.

2. In the Create a new database dialog, enable the **Drop any existing database with the specified name** option if you want to purge and recreate a database that already exists.

3. Select the preferred authentication method for users connecting to Blue Prism. You can choose between two types of environments:
  - **Multi-authentication environment** - This environment supports three types of authentication, where roles and permissions are mapped to individual users in Blue Prism. The authentication type is configured when a [user is created](#) and cannot be changed later.
    - **Blue Prism native authentication** - User accounts are individually created and maintained in Blue Prism and user login attempts are processed by verifying the supplied credentials configured in the Blue Prism database. For more details, see [Authentication in Blue Prism](#).
    - **Active Directory authentication** - If Active Directory authentication has been configured in Blue Prism, Active Directory user accounts can be created by retrieving users from the Active Directory and assigning them to Blue Prism user roles.
    - **Native authentication via Authentication Server** - An Authentication Server configuration is required when using the Blue Prism API and/or browser-based Control Room from version 7.0 onwards. Authentication Server user accounts can be created directly in Blue Prism Hub (version 4.3 and later), or by mapping users between the Authentication Server and Blue Prism databases, and assigning them to Blue Prism user roles. For more details, see [Authentication Server](#).
  - **Single-authentication environment** - referred to as *Active Directory Single Sign-On* prior to Blue Prism 6.8, this environment supports Active Directory authentication where users log in via Active Directory only and roles are mapped to Active Directory security groups. To set up a single-authentication environment, 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 select the security group within that domain whose members will be granted system administrator access to Blue Prism. For more details, see [Single sign-on](#).
4. Click **OK** to complete the database configuration.

### Support for contained databases

Blue Prism supports the use of contained databases, hosted on Microsoft SQL Server. To use a contained database, it is necessary to manually create the database and apply the Blue Prism CreateScript.sql.

For more information, see [Contained databases](#).

## 4. Log in for the first time

It is now possible to log in for the first time and carry out some system-wide configuration.

You will first need to log in using the default Blue Prism native credentials to configure the system for the required authentication methods.

Default credentials:

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

Follow the onscreen instructions to change the administrator password.

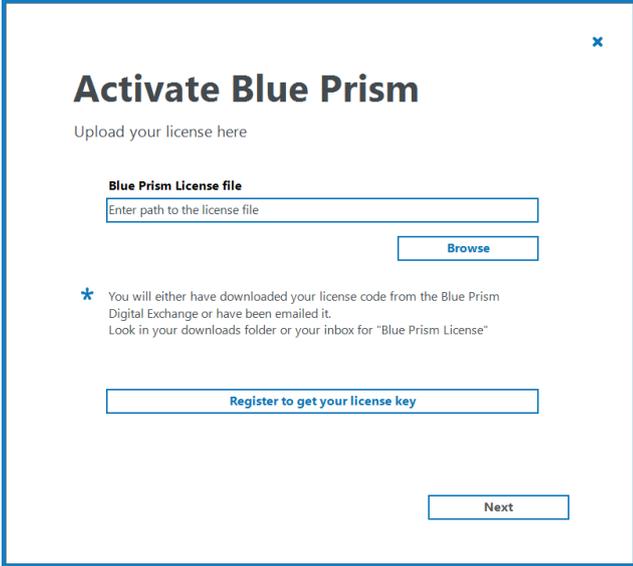
 This [video](#) shows you how to recover your admin password.

See [Authentication in Blue Prism](#) for more details.

## 5. Install a Blue Prism license key

A license file containing a valid license key is required to activate the software. License files can be obtained from a Blue Prism Account Manager. Your license and EULA are emailed to you from [digitalworker@blueprism.com](mailto:digitalworker@blueprism.com). Save the files to your hard-drive.

After logging into Blue Prism, if a license is not already installed, you will be prompted to enter your license key.



1. Click **Browse**, select the required License (.lic) file and click **Next** to start the license activation wizard.
2. Follow the steps in the wizard and save or copy the generated activation code.
3. When prompted, click to open the Blue Prism Portal.

You will be directed to [portal.blueprism.com/products/activation](https://portal.blueprism.com/products/activation).

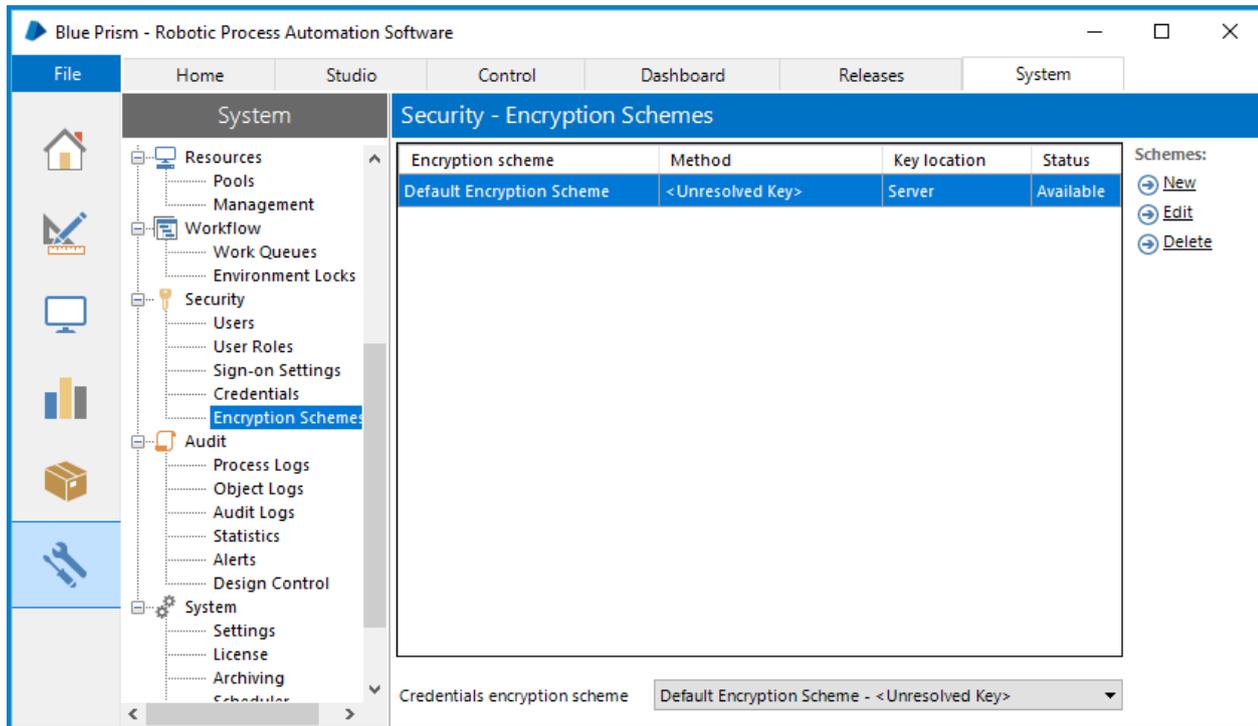
 If you are not already logged into the Blue Prism Portal, you will be prompted to log in.

4. Paste or import the generated activation code and click **Submit license activation**.
5. Copy the activation key, paste it back into the Blue Prism license activation wizard, and click **Next**.  
Your Blue Prism license is activated.

For information on how to manage your license after activation, see [Licensing](#).

## 6. Configure an encryption scheme

In order to support the use of Credential Manager (for securely storing credentials), you must 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:

It is not recommended practice for enterprise customers operating at scale to store the encryption scheme keys in the database.

Standalone Deployment	Multiple Component (App Server) Deployment
<div style="border: 1px solid #0070C0; padding: 5px; margin-bottom: 10px;">                     Name: <input type="text" value="Default Encryption Scheme"/> <input checked="" type="checkbox"/> Available                      Location: <input type="radio"/> Application Server (recommended) <input checked="" type="radio"/> Database                      Method: <input type="text" value="AES-256 AesCryptoService (256 bit)"/> <a href="#">Generate key</a>                      Key: <input type="password" value="....."/> </div> <ol style="list-style-type: none"> <li>a. Select <b>Database</b>.</li> <li>b. Select <b>AES-256</b>.</li> <li>c. Click <b>Generate Key</b>.</li> <li>d. Click <b>OK</b>.</li> </ol>	<div style="border: 1px solid #0070C0; padding: 5px; margin-bottom: 10px;">                     Name: <input type="text" value="Default Encryption Scheme"/> <input checked="" type="checkbox"/> Available                      Location: <input checked="" type="radio"/> Application Server (recommended) <input type="radio"/> Database                      The secret key for this scheme should be added to the Server Key Store using the Configuration utility on each Application Server.                 </div> <ol style="list-style-type: none"> <li>a. Select <b>Application Server</b>.</li> <li>b. Click <b>OK</b>.</li> </ol>

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

## 7. Configure common settings

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

The screenshot shows the 'System - Settings' window with the following sections and options:

- Local Device Settings:**
  - Start a personal Runtime Resource on this machine when users sign in to Blue Prism
- System Wide Settings - General:**
  - Automatically back up when editing a process or business object (every 10 minutes)
  - Force users to summarise their changes when saving a process or business object
  - Password controls allow pasted passwords
  - Allow latest Runtime Resource screen capture
  - Hide the Digital Exchange tab
  - Default session warning time (mins) (0 = disable warnings): 5
- Runtime Resource Connectivity:**
  - Require secure inbound instructional connections
  - Allow anonymous public Runtime Resources
  - Prevent registration of new Runtime Resources
  - Resource registration and addressing: Register and communicate using machine (short) name
- Database:**
  - Enable Unicode support for session logs
  - Save environment data for clients, runtime resources and servers to the database
- Application Manager Settings:**
  - Tesseract engine: 3 Default, based on what is available
- Environment Themes:**
  - Choose a name for this environment and select the colours to use for title and status bars
  - Name: Home
  - Background: [Dark Blue]
  - Foreground: [Light Blue]
  - Environment Theme Preview: [Preview]
  - Apply
- Offline Help:**
  - Enable Offline Help
  - Base URL: [Empty text box]

For more information, see [System settings](#).

## 8. Verify the installation

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 [Verify an Installation](#).

## 9. 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:

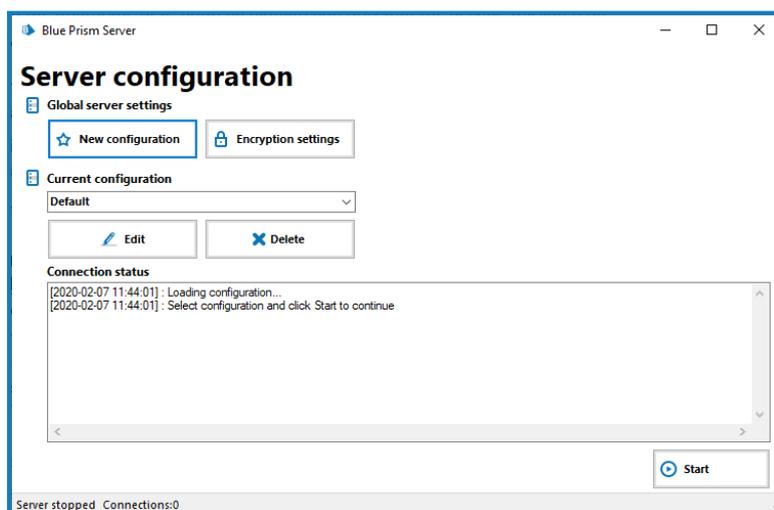
- Selecting the mode that inbound connections will be required to use.
- Defining the hostname or IP address binding and port that the service will listen on.
- Specifying database connection information.
- Configuring an encryption scheme that will be used for data encryption in that environment.
- 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).

For more information on additional server settings you might need to configure post installation, see [Blue Prism Server](#).

## 10. 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 configuration** to create a server configuration.

 The recommended approach for a brand new installation is to edit the default configuration. A new configuration is typically only required for additional server configuration on the same server, or if you decide to create a new configuration from scratch.



3. Add the required details in the Server Configuration Details dialog. Ensure 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.

Server Configuration Details

Details | Key Store | Server Services | Logging | Data Gateways Settings | ASCR Settings | Authentication Server Integration

Name: Default

Database Connection: Connection 7.0

Connection Mode: WCF: SOAP with Message Encryption & Windows Authentication

Requires trust relationship between devices: Yes  
Blue Prism Authentication Modes: Blue Prism Native / Single Sign-on  
Requires server-side certificate: No  
Transport: SOAP over HTTP

Only the message content is encrypted. The SOAP and HTTP headers remain unencrypted which assists complex routing, load balancers, proxies etc. Client and server identity is validated via Windows / Active Directory.

Binding:

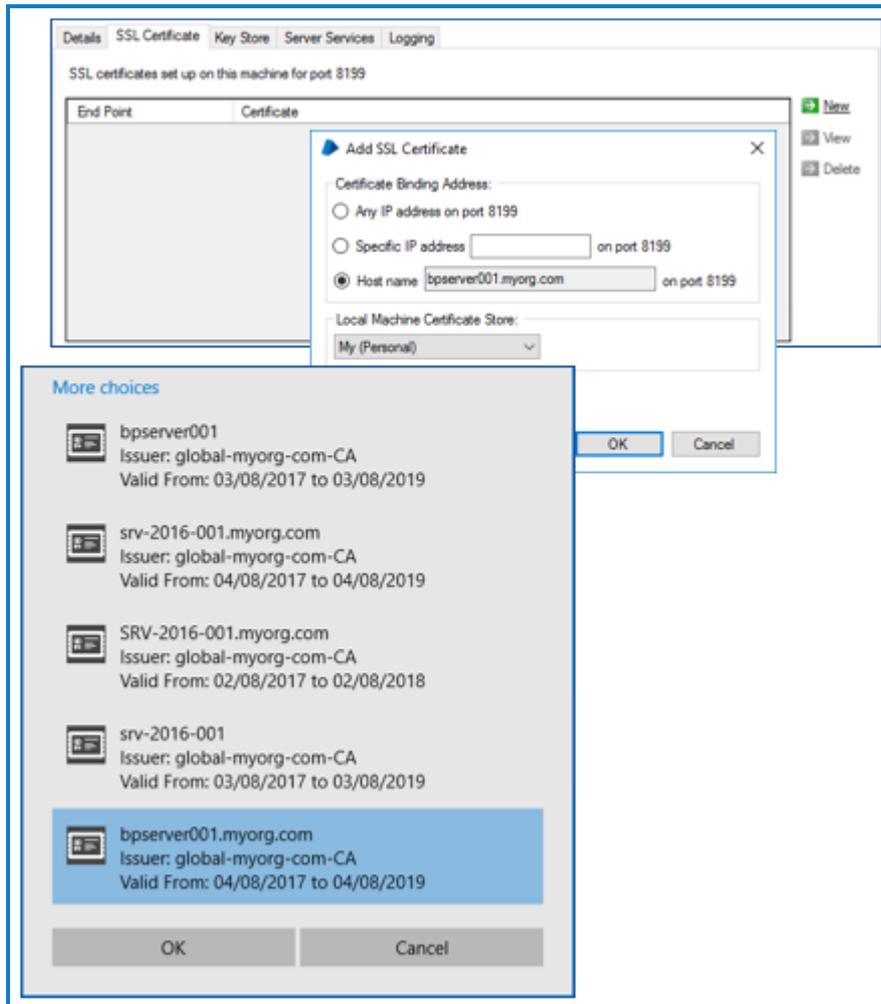
Host Name or IP Address: localhost

Port: 8199

Disable Scheduler

Save Cancel

- 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.

- 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.
  - Click **OK** to launch the Windows certificate selection utility and pick the appropriate certificate.
  - It is necessary to select a certificate that matches the binding on the details tab.
- 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*.

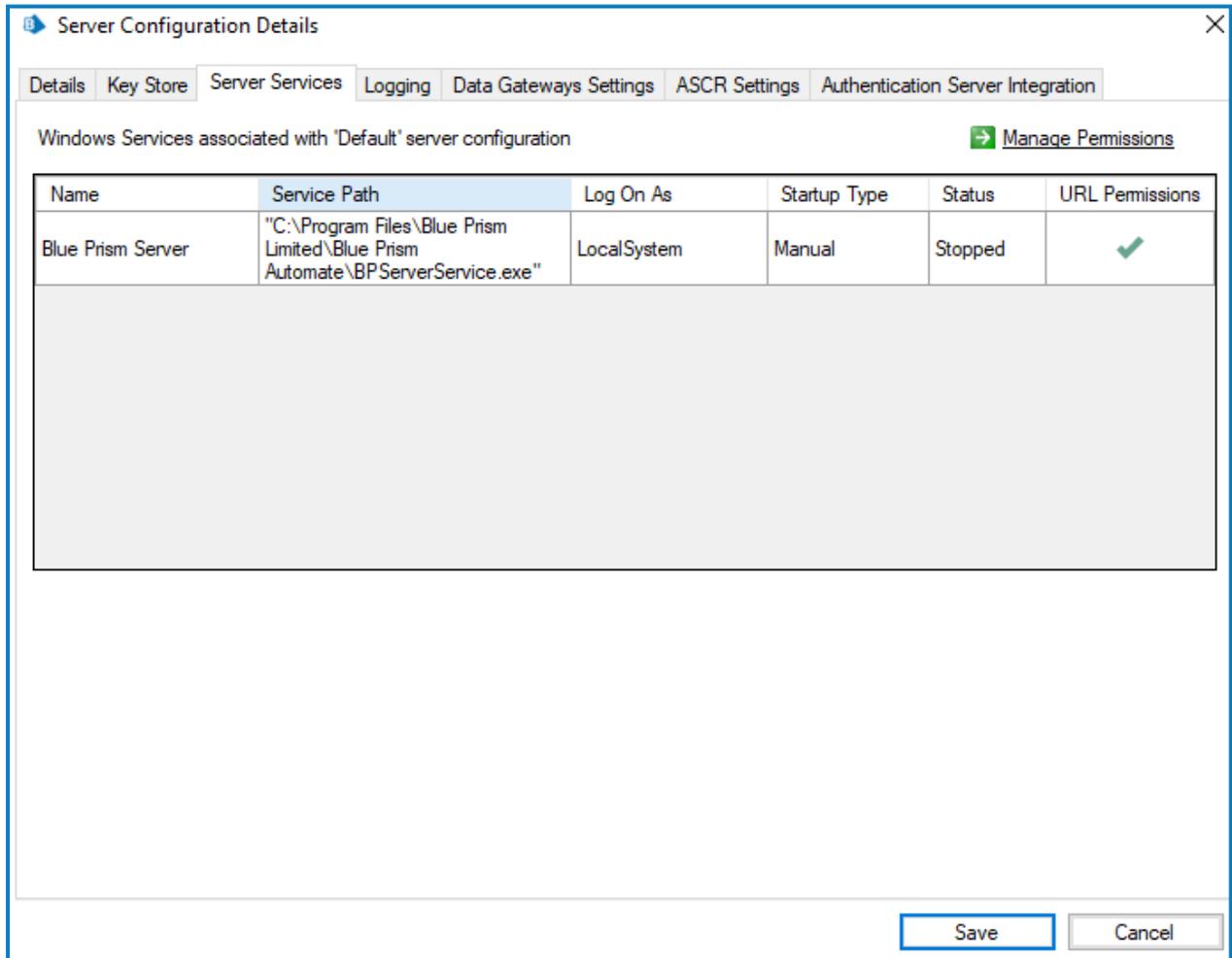
- Click **Generate Key** and then click **OK**.

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 be 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.

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



- Click **Save**.

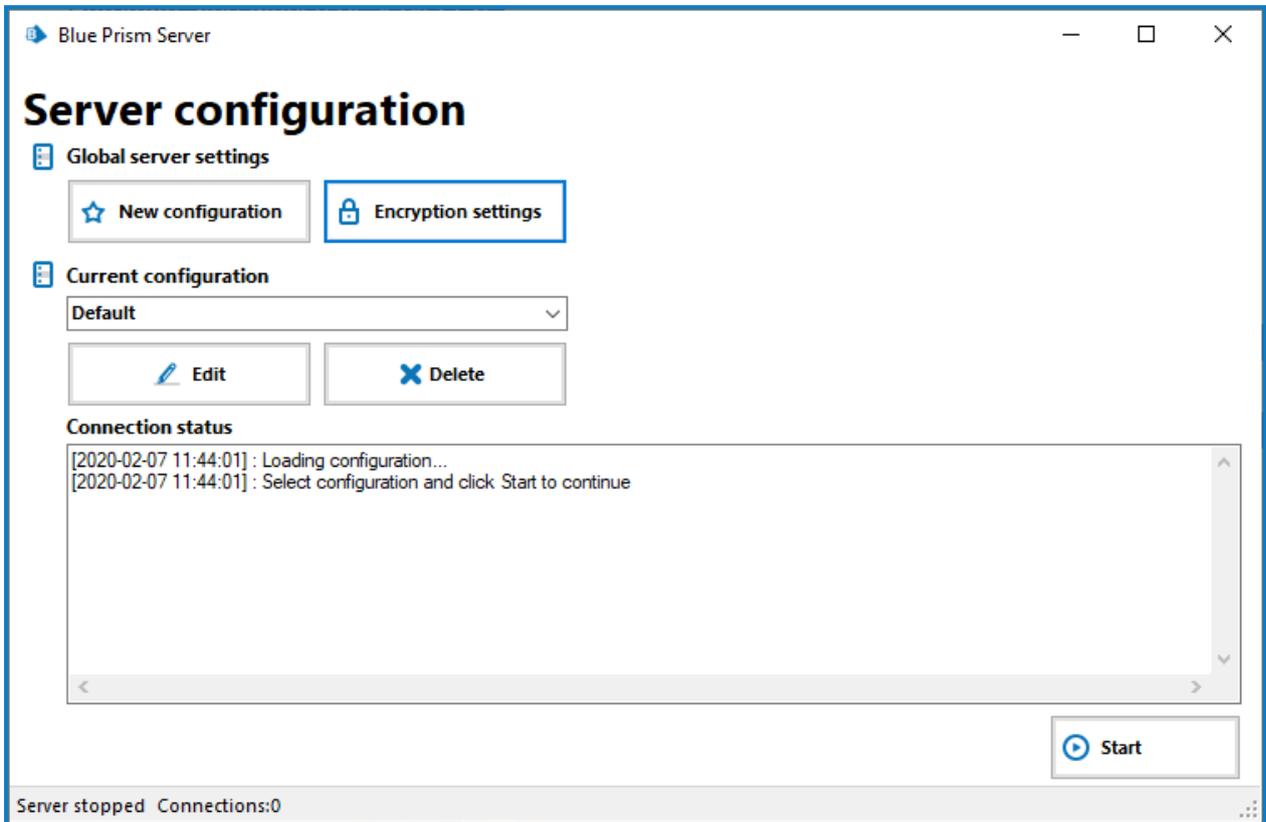
For more information on additional server settings you might need to configure post installation, see [Blue Prism Server](#).

### 11. Configure server configuration file encryption settings

The encryption settings of the BP server can be configured to protect the server's encryption keys when they are stored in the application server.

Certificate encryption of server configuration files is recommended for deployments that need to be the most secure and it requires a locally-deployed certificate with an associated private key to be available. See [Using certificate encryption](#) for details.

1. Navigate to the Blue Prism installation directory, by default C:\Program Files\Blue Prism Limited\Blue Prism Automate and launch BPServer.exe.
2. Click **Encryption settings** to configure the encryption settings that will be applied to the information stored in the local configuration files used by the Blue Prism application server.



3. In the Select Encryption Method dialog, select to use either the default Blue Prism encryption or your own certificate. We recommend using your own certificate.

 We recommend using your own certificate. See [Using certificate encryption](#).

When selecting to use your own certificate, enter the thumbprint from your certificate, which is the automatically generated ID for the certificate.



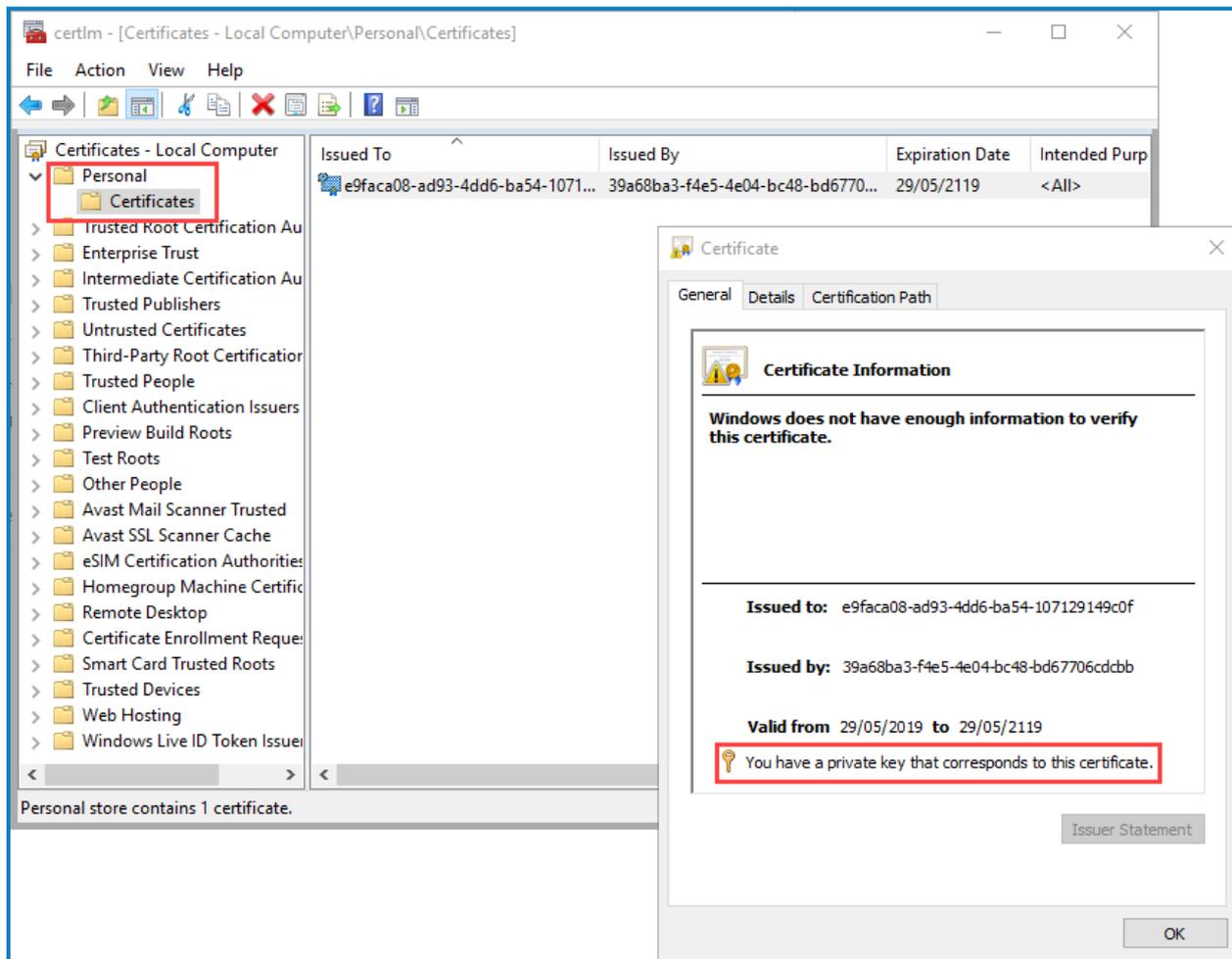
4. Click **OK**.

### Using certificate encryption

If you have chosen to use certificate encryption for the application server configuration data, the following elements must be considered to ensure access for all relevant components and for continued successful encryption.

#### Certificate storage

The certificate used to encrypt server configuration data must use RSA encryption and contain a public/private key pair. The certificate must also be stored on the local machine in the following location: [Certificates - Local Computer\Personal\Certificates].

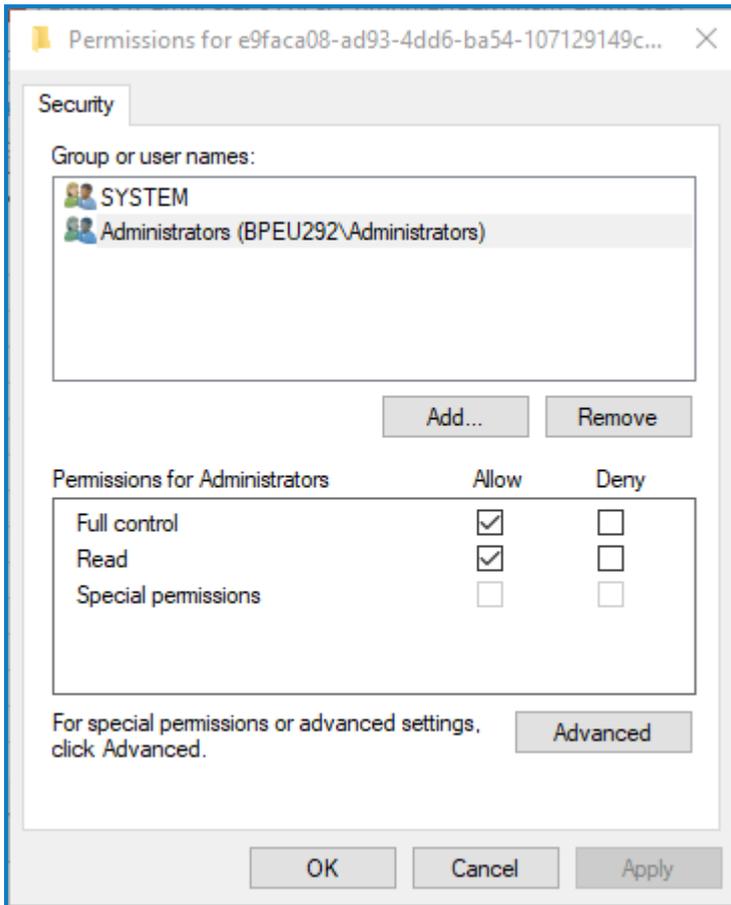


#### Certificate access

To ensure that the user configuring the Blue Prism server and the user account on which the server service runs have read access to the private keys on the certificate:

1. In the Manage Computer Certificates window select the certificate to which you need to give read access.
2. From the shortcut menu select **All Tasks > Manage Private Keys**.

- In the Permissions dialog ensure the user account on which the server service is running has read access to the certificate. Add any users or groups that also need read access to the certificate.



 If you have chosen to store encryption scheme keys in separate files, the certificate encryption will be applied to the separate files. If the location of the separate files is shared with other application servers, they will all need the same certificate to be stored locally and have a minimum of read access to the private key.

### Encrypting server configuration data

When you use certificate encryption, all encrypted data from the server configuration is decrypted and held in protected memory. When a new encryption method or certificate thumbprint is selected, the file is saved, encrypting the secret data as they are read from protected memory and written to the file.

When you select certificate encryption, the following application server configuration data is encrypted:

- The encryption scheme key that is used to encrypt and decrypt sensitive information from the database for the Blue Prism server connection.
- The password used to connect to the database if using SQL Authentication for database connections.

### Expired and missing certificates

The expiry date for custom encryption certificates for Blue Prism application server configuration files can be found in the *Environment Summary* report, they are also written to Blue Prism event logs. In addition, when logging into Blue Prism, users are notified if a certificate used to encrypt the Blue Prism application server configuration files is due to expire within the next seven days.

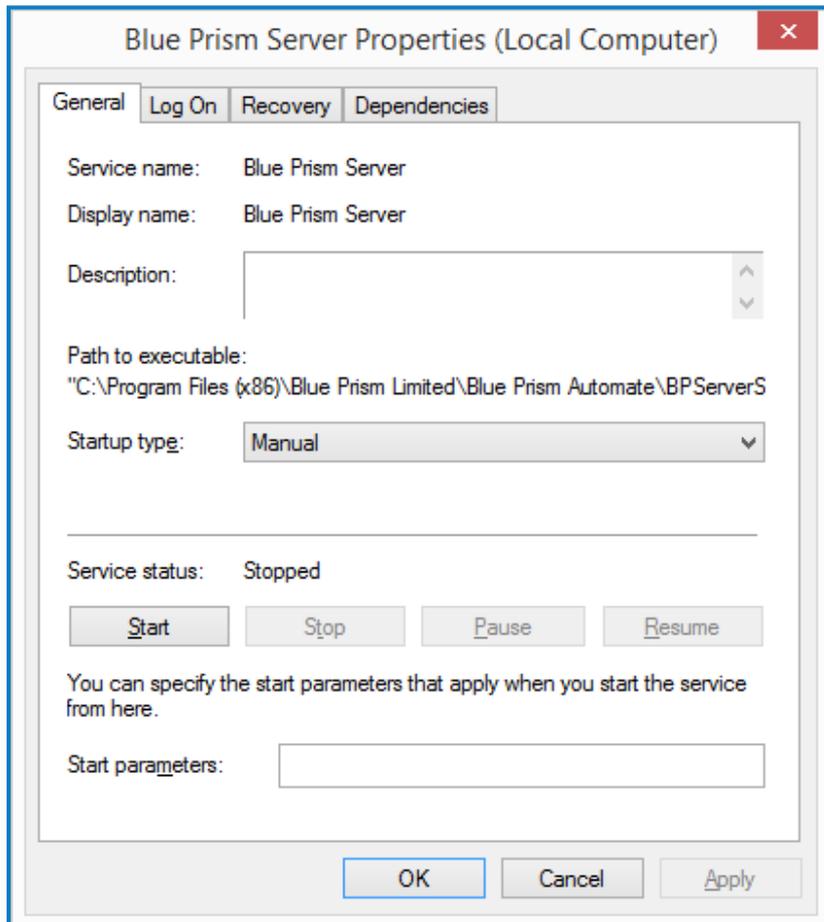
If a certificate expires it will stop working with the Blue Prism application server. Certificate encryption may also stop working in the following circumstances:

- The user account running the server doesn't have access to the public and/or private key. In this instance, a message displays asking the user to reset the configuration.
- The certificate used for encryption is now missing from the certificate store.
- The user account no longer has access to the local computer certificate store. In this instance, an error will display at start up when trying to load the certificate.

 If the certificate used for encryption cannot be accessed or restored the user configuring the Blue Prism server will need to recreate the server configuration profiles. To do this, delete the Automate.config file, which is located in: ProgramData\Blue Prism Limited\Automate V3. A new Automate.config file will be automatically created when the BPServer.exe is launched. An encryption scheme and new certificate can then be applied to the new server configuration file.

## 12. 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.

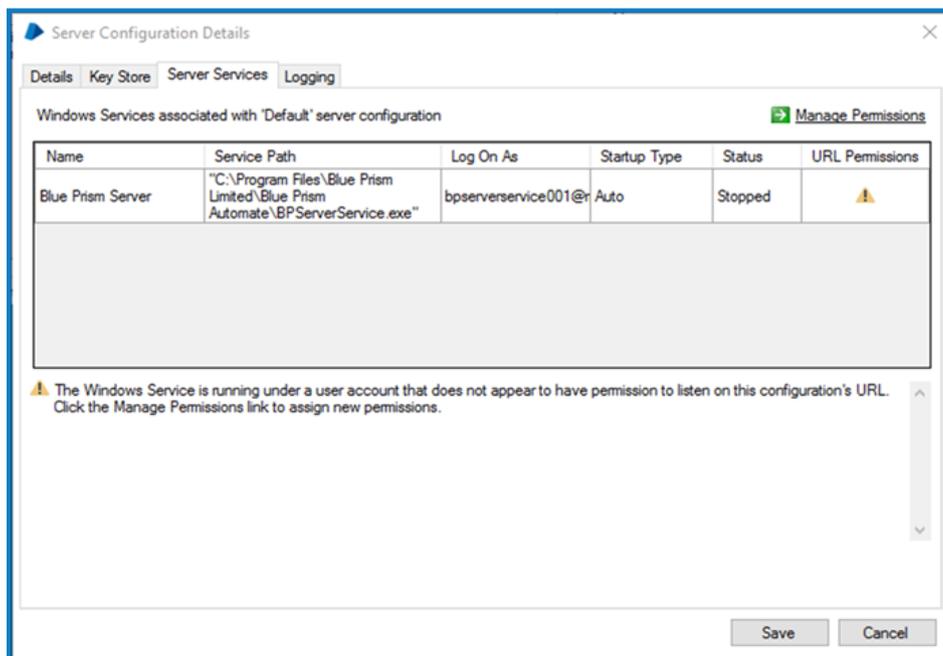
When Blue Prism is configured to use Single Sign-On, the configured Windows service account will need to have appropriate permissions to access the directory services provider and query users and group membership. The specific permissions that are required in relation to Active Directory will be dependent 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.

### 13. Validate the Server service logon user

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

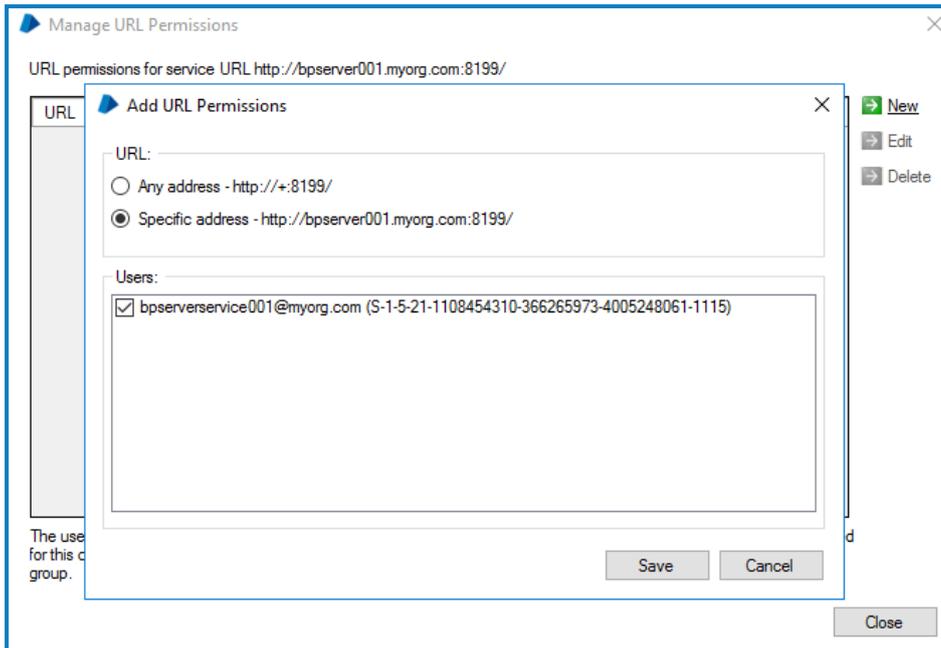
Common configurations such as where Blue Prism is configured to use Windows Authentication to authenticate against SQL may result in an error. This can occur if a non-admin user has been configured as the service log on account. In such situations, alerts similar to the below may be presented:



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:

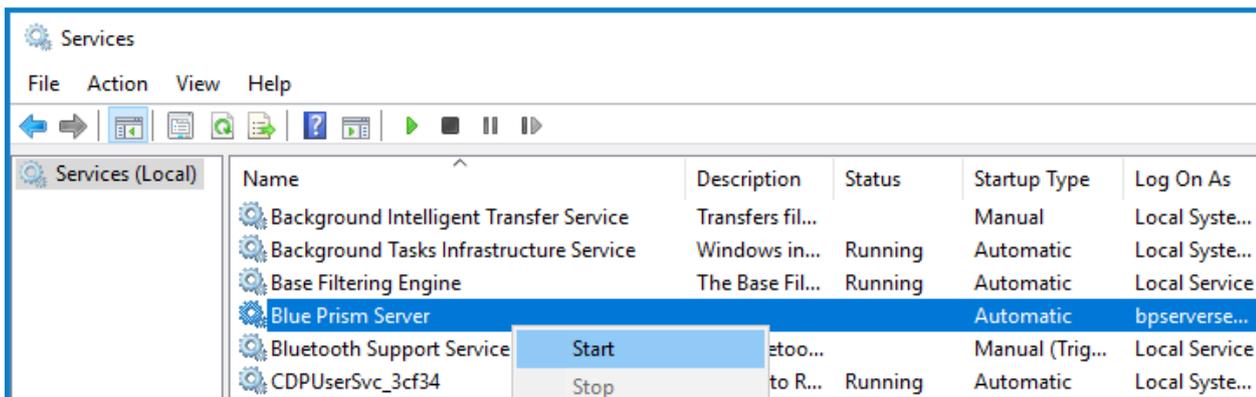
- If the service is configured to use a binding, a specific address permission must be created.
- If the service is not configured to use a binding, a non-specific address permission must be used.

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



#### 14. Start the Windows service

Use the Windows Services management console to start the service.

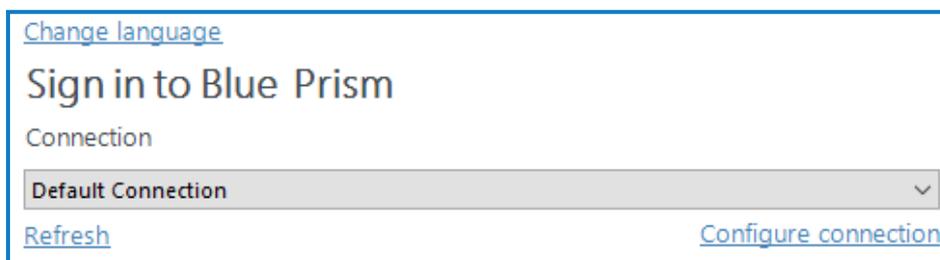


If the service will not start, or starts and then immediately stops there is a problem with the configuration of the service. For more information, review [Troubleshooting an installation](#).

#### 15. Configure a Blue Prism connection to the Blue Prism application server

The server service can be tested locally by 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 connection**.



2. This will open the Connection Configuration Dialog where you can provide the connection information:

- **Connection Name** - Friendly name for the connection.
- **Connection Type** - Select **Blue Prism Server** from the drop-down.
- **Blue Prism Server** - Hostname of the Blue Prism server. Must match the server binding, and be resolvable.
- **Connection Mode** - Connection mode to use. This must match the mode configured on the [Blue Prism Server](#).
- **Server Port** - The port that the server is listening on.
- **Ordered Sessions** - This is enabled by default and controls whether WCF connection sessions must be transmitted in order or not. Disabling this setting will reduce the amount of time a Blue Prism interactive client takes to connect to a large number of runtime resources.

The screenshot shows a 'Connection Configuration Dialog' window. It contains the following fields and values:

- Connection Name:** BP server (The name by which this connection will be remembered)
- Connection Type:** Blue Prism Server (The type of connection to use)
- Blue Prism Server:** localhost\\SQLExpress (The hostname of the Blue Prism Server)
- Connection Mode:** WCF: SOAP with Message Encryption & Windows Authentication (This must match the mode configured on the Blue Prism Server(s))
- Server Port:** 8199 (This must match the listening port configured on the Blue Prism Server(s))
- Ordered Sessions:**

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 see [Troubleshooting an installation](#) and [Troubleshooting the application server connection](#).

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.

## 16. Configure a Service Principal Name (SPN) on the Blue Prism application server (if applicable)

If using the following connection modes with a Blue Prism Server connection, a Service Principal Name (SPN) must be configured against the Active Directory (AD) account under which each Blue Prism Server service instance is running:

- WCF: SOAP with Message Encryption & Windows Authentication
- WCF: SOAP with Transport Encryption & Windows Authentication
- .NET Remoting Secure

This is because when a Blue Prism interactive client or a runtime resource connects to an application server using one of the connection modes above, the Microsoft Negotiate Security Package is used to select the best Security Support Provider (SSP) to authenticate the connection. The internal code of the Blue Prism interactive client provides the expected SPN to the Microsoft Negotiation Security Package,

which prompts Microsoft Negotiation to select the Kerberos SSP over New Technology LAN Manager (NTLM) SSP, provided the SPN is present in Active Directory. If the SPN is not present in Active Directory, Kerberos authentication will fail. See [this Knowledge Base article](#) for more details on the Windows security update for CVE-2022-21920 which affects this behavior. From Blue Prism 7.0.2, if the SPN is not present in Active Directory, and if the `/forcentlm <flag>` is set in Automate C, the NTLM SSP will be used.

It is recommended to contact your organization's IT team for assistance with this configuration, and that you first test the configuration in a non-production environment.

This configuration applies to all Blue Prism environments, however, if the Active Directory account under which your BP Server instances are running resides in a different domain to the Active Directory account used for the Blue Prism interactive client and runtime resource, we recommend you do not install the Windows security update for CVE-2022-21920. If you have already installed it, we recommend that you uninstall it. From Blue Prism 7.0.2, the additional configuration in Automate C outlined [below](#) is required.

To configure the SPN, follow the steps below on each Blue Prism Server Service instance:

1. Log into the Blue Prism Server using a Privileged Windows User Account that is a member of the Domain Admins or Enterprise Admins group.

See [the Microsoft documentation](#) in this topic for further details including required permissions. This is an essential step to review with your organization's IT team to ensure that the `Setspn` command does not fail to execute due to missing account permissions.

2. Open Command Prompt as an administrator on the application server and run the command below.

If the Blue Prism Server is running as a Local System account:

```
Setspn -S HTTP/SERVER_FQDN:SERVER_PORT/BPServer COMPUTER_HOSTNAME
```

If the Blue Prism Server is running as a user account:

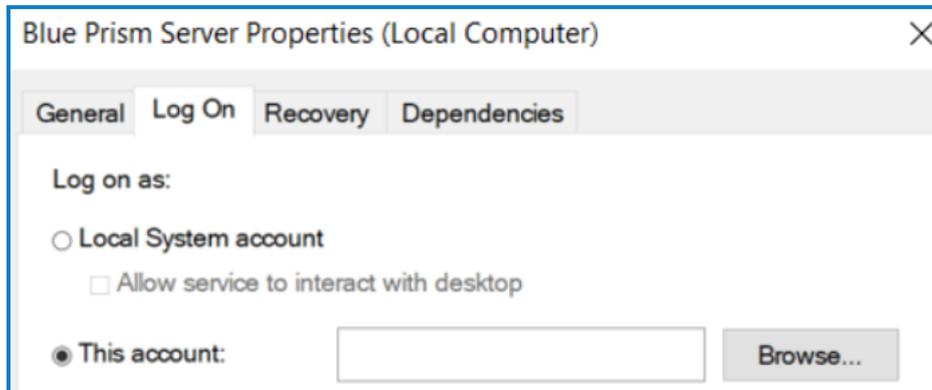
```
Setspn -S HTTP/SERVER_FQDN:SERVER_PORT/BPServer DOMAIN\Username
```

Where:

- HTTP accounts for both HTTP and HTTPS. Do not change the command to include HTTPS specifically as the configuration will fail.
- SERVER\_FQDN:SERVER\_PORT must be the Fully Qualified Domain Name (FQDN) of the Blue Prism application server.
- COMPUTER\_HOSTNAME is the hostname of the computer if BP Server Service is running as a Local System account.

- DOMAIN\Username is the domain username if BP Server Service is running as a user account.

This should match the **Log on as** setting in the Blue Prism Server Properties (Local Computer) window.



Example with local system:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>setspn -S HTTP/BPWINS2016.orgdomain.local:8199/BPServer BPWINS2016
```

Example with DOMAIN\Username:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>setspn -S HTTP/BPWINS2016.orgdomain.local:8199/BPServer orgdomain\mmb-adm
```

3. After setting the SPN you will need to wait for the Kerberos ticket cache to renew (the default setting is 15 minutes, but it can be changed via Group policy). For more details, see the [Kerberos authentication documentation](#).

Alternatively, you can either:

- Restart the Blue Prism interactive client or runtime resource; or
- On the machine running the interactive client or runtime resource, open Command Prompt and run `klist purge` to refresh the Kerberos tickets.

This command should not be performed within an elevated Command Prompt as it will not purge all the user Kerberos tickets.

4. Check that this is working as expected by connecting to the Blue Prism Server from a Blue Prism interactive client running on another machine.
5. Repeat the steps above on each instance of the Blue Prism Server Service running on every Blue Prism Server.

### Check SPN entries and remove an incorrect SPN

1. To check SPN entries for troubleshooting purposes, you can see a list of the added SPNs on the application server using the following command:

```
Setspn -L ACCOUNTNAME
```

Example of SPN list:

```

Administrator: Command Prompt
C:\Users\qauser103>setspn -L BPWINS2016
Registered ServicePrincipalNames for CN=BPWINS2016,OU=Domain Controllers,DC=orgdomain,DC=local:
HTTP/BPWINS2016.orgdomain.local:9898/BPServer
Dfsr-12f9a27c-bf97-4787-9364-d31b6c55eb04/BPWINS2016.orgdomain.local
MSSQLSvc/BPWINS2016.orgdomain.local:49716
MSSQLSvc/BPWINS2016.orgdomain.local:SQLEXPRESS
TERMSRV/BPWINS2016
TERMSRV/BPWINS2016.orgdomain.local
ldap/BPWINS2016.orgdomain.local/ForestDnsZones.orgdomain.local
ldap/BPWINS2016.orgdomain.local/DomainDnsZones.orgdomain.local
DNS/BPWINS2016.orgdomain.local
GC/BPWINS2016.orgdomain.local/orgdomain.local
RestrictedKrbHost/BPWINS2016.orgdomain.local
RestrictedKrbHost/BPWINS2016
RPC/349cbbcb-0c5a-41be-8b47-b4cbdf74c742._msdcs.orgdomain.local
HOST/BPWINS2016/ORGDOMAIN
HOST/BPWINS2016.orgdomain.local/ORGDOMAIN
HOST/BPWINS2016
HOST/BPWINS2016.orgdomain.local
HOST/BPWINS2016.orgdomain.local/orgdomain.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/349cbbcb-0c5a-41be-8b47-b4cbdf74c742/orgdomain.local
ldap/BPWINS2016/ORGDOMAIN
ldap/349cbbcb-0c5a-41be-8b47-b4cbdf74c742._msdcs.orgdomain.local
ldap/BPWINS2016.orgdomain.local/ORGDOMAIN
ldap/BPWINS2016
ldap/BPWINS2016.orgdomain.local
ldap/BPWINS2016.orgdomain.local/orgdomain.local
C:\Users\qauser103>
    
```

2. Check the entries for the SPNs you added for the BP Server Service. You can remove the one added in error using the command listed below:

```
Setspn -D SPN_NAME ACCOUNTNAME
```

Where SPN\_NAME is the name displayed in the SPN entries list, for example, HTTP/SERVER\_FQDN:SERVER\_PORT/BPServer.

### Additional configuration for Blue Prism application servers in load balanced environments

It is essential that all instances of the Blue Prism Server Service in the same load balancer pool are running under the same service account and the SPN is registered to this account.

Additionally, it is recommended to register SPNs for the application server's FQDNs to the same service account, as this will allow for testing of a direct connection to the application servers. For more information, see [SPN troubleshooting](#).

### Additional configuration for Active Directory authentication in multi-forest environments

 This functionality is only available from Blue Prism 7.0.2 onwards.

To support Kerberos authentication in Blue Prism environments configured to use Active Directory authentication in multiple forests, the following settings must be configured in Automate C:

- **/setkerberosrealm** - For example, `/setkerberosrealm mycompany.com`. This must be configured for each BP Server connection in the interactive client where the user's Kerberos realm is different to that of the user account configured to run BP Server.

 The Kerberos realm is usually the same as the domain name, however, please check with your IT team for the correct value. This should be the realm of the service account running the Blue Prism Server service. In some environments, it may be necessary to apply the same configuration where the service account exists in another domain within the same forest. You can verify whether the Kerberos realm must be specified by running a `klist get` command against an SPN. For more information, see [SPN troubleshooting](#).

- `/forcentlm <flag>` - For example, `/forcentlm true`. Forces Microsoft Negotiate Security Package to select New Technology LAN Manager (NTLM) as the Security Support Provider (SSP) for the last used or specified connection (using the `/dbconname` switch) when authenticating the Blue Prism server connection. This option is provided so that NTLM can be used when Kerberos is unavailable or not configured.



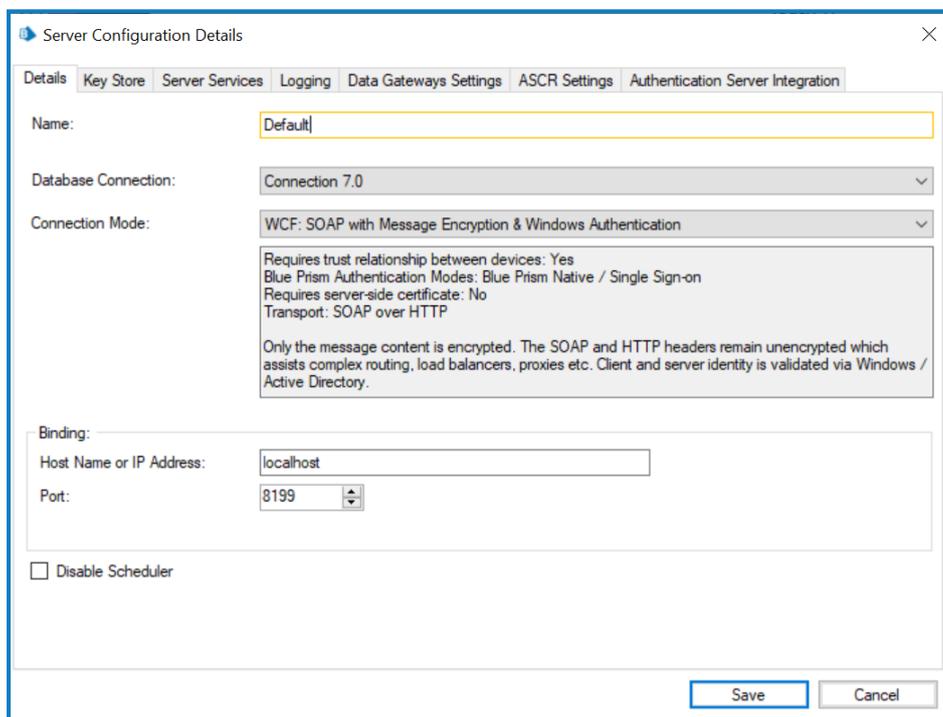
Please consult with your security team before enabling this option as NTLM is considered a less secure protocol.

## 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:

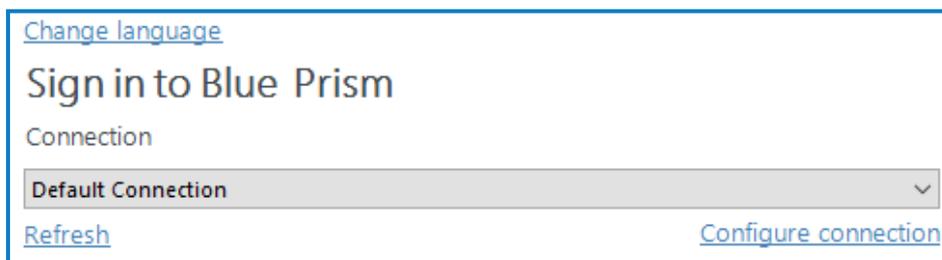
- It is necessary to use some settings from the server configuration on each client such as:
  - Connection mode
  - Bind to address (if specified)
  - Port
- If the server is configured to use a WCF mode that uses transport encryption, it will be necessary to ensure that the certification authority 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.



### 1. Configure a Blue Prism connection to the Blue Prism application server

The server service can be tested locally by 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 connection**.



2. This will open the Connection Configuration Dialog where you can provide the connection information:

- **Connection Name** - Friendly name for the connection.
- **Connection Type** - Select **Blue Prism Server** from the drop-down.
- **Blue Prism Server** - Hostname of the Blue Prism server. Must match the server binding, and be resolvable.
- **Connection Mode** - Connection mode to use. This must match the mode configured on the [Blue Prism Server](#).
- **Server Port** - The port that the server is listening on.
- **Ordered Sessions** - This is enabled by default and controls whether WCF connection sessions must be transmitted in order or not. Disabling this setting will reduce the amount of time a Blue Prism interactive client takes to connect to a large number of runtime resources.

The screenshot shows a 'Connection Configuration Dialog' with the following fields and values:

- Connection Name:** BP server (The name by which this connection will be remembered)
- Connection Type:** Blue Prism Server (The type of connection to use)
- Blue Prism Server:** localhost\SQLExpress (The hostname of the Blue Prism Server)
- Connection Mode:** WCF: SOAP with Message Encryption & Windows Authentication (This must match the mode configured on the Blue Prism Server(s))
- Server Port:** 8199 (This must match the listening port configured on the Blue Prism Server(s))
- Ordered Sessions:**

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 see [Troubleshooting an installation](#) and [Troubleshooting the application server connection](#).

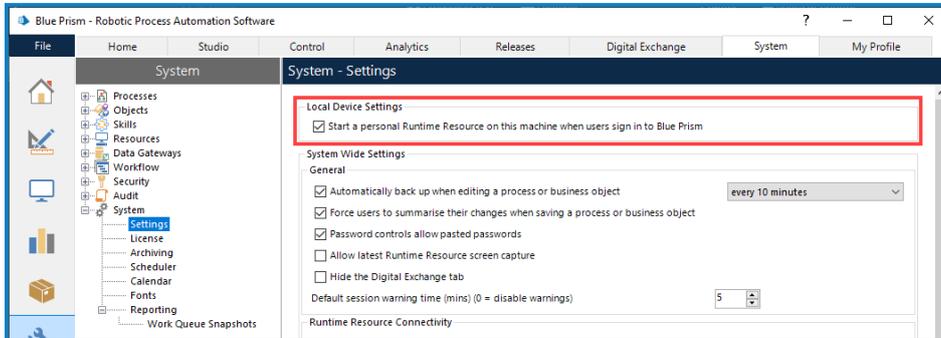
Administrators can now use the two connections configured in the local Blue Prism client to validate:

- Direct connections to the Blue Prism database.
- Connections to the environment via the application server.

## 2. 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 under System > System - Settings.



## 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.

Server Configuration Details

Details | Key Store | Server Services | Logging | Data Gateways Settings | ASCR Settings | Authentication Server Integration

Name: Default

Database Connection: Connection 7.0

Connection Mode: WCF: SOAP with Message Encryption & Windows Authentication

Requires trust relationship between devices: Yes  
Blue Prism Authentication Modes: Blue Prism Native / Single Sign-on  
Requires server-side certificate: No  
Transport: SOAP over HTTP

Only the message content is encrypted. The SOAP and HTTP headers remain unencrypted which assists complex routing, load balancers, proxies etc. Client and server identity is validated via Windows / Active Directory.

Binding:

Host Name or IP Address: localhost

Port: 8199

Disable Scheduler

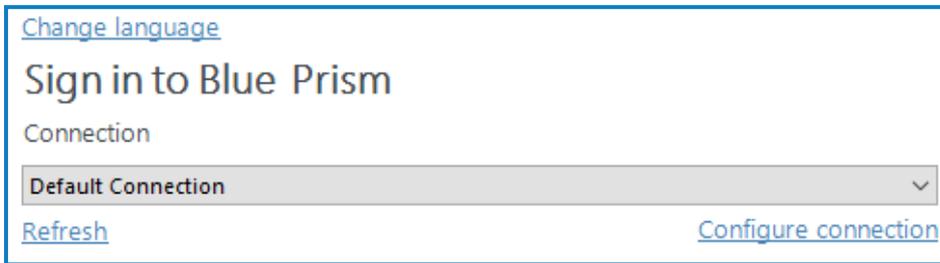
Save Cancel

 Please be aware that starting and running a runtime resource with elevated permissions might affect the interaction with the application that is being automated. Generally, the permissions of the runtime resource must match those of the user context of the target application.

### 1. Configure a Blue Prism connection to the Blue Prism application server

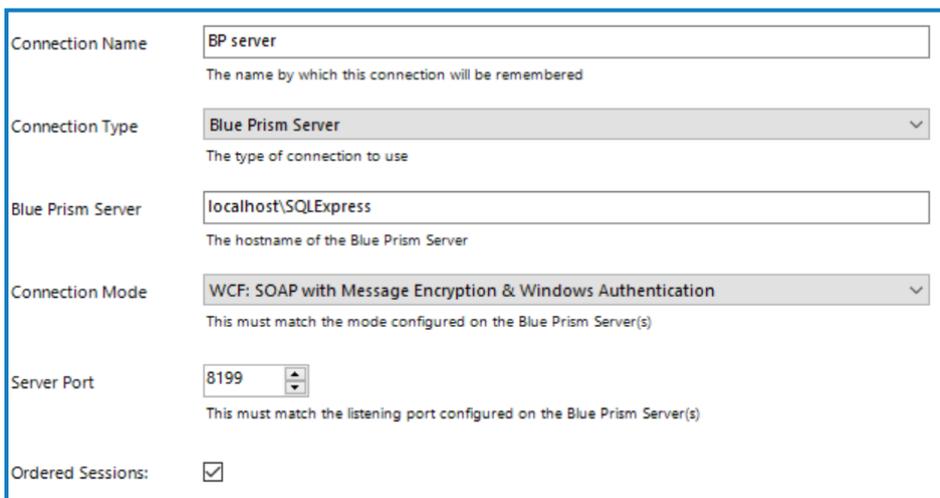
The server service can be tested locally by configuring an additional Blue Prism connection on the local device that is configured to connect via the newly configured server service.

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



2. This will open the Connection Configuration Dialog where you can provide the connection information:

- **Connection Name** - Friendly name for the connection.
- **Connection Type** - Select **Blue Prism Server** from the drop-down.
- **Blue Prism Server** - Hostname of the Blue Prism server. Must match the server binding, and be resolvable.
- **Connection Mode** - Connection mode to use. This must match the mode configured on the [Blue Prism Server](#).
- **Server Port** - The port that the server is listening on.
- **Ordered Sessions** - This is enabled by default and controls whether WCF connection sessions must be transmitted in order or not. Disabling this setting will reduce the amount of time a Blue Prism interactive client takes to connect to a large number of runtime resources.



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 see [Troubleshooting an installation](#) and [Troubleshooting the application server connection](#).

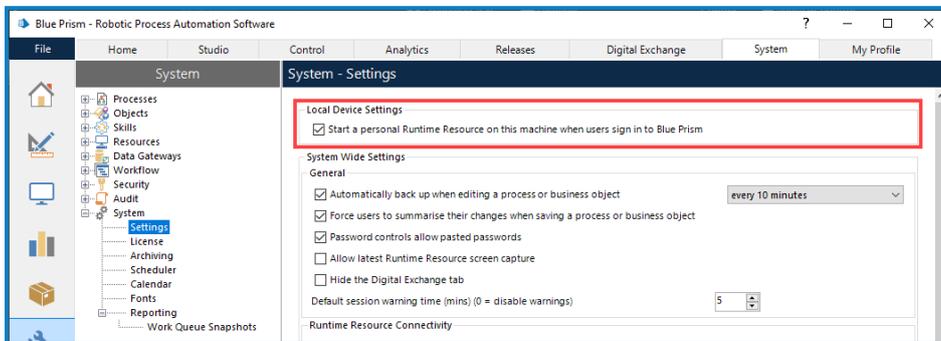
Administrators can now use the two connections configured in the local Blue Prism client to validate:

- Direct connections to the Blue Prism database.
- Connections to the environment via the application server.

## 2. 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 under System > System - Settings.



## 3. 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 [User profile settings](#). These include:

- Screensaver and auto-lock
- Power saver options
- Default remote access settings

## 4. 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](#).

## 5. 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
```

For example, 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` command line parameter to authenticate as the logged on user in a Blue Prism environment configured to use Active Directory authentication.

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

- Use the `/user [username] [password]` command line parameter to authenticate in a Blue Prism environment configured to use native authentication.

```
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 third-party systems (for example, 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` command line parameter 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` command line parameter 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` command line parameter 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"
```

## 6. Ensure there is a mechanism for runtime resources to log in 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 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.

For more details, see the [Login Agent user guide](#).

# Standalone deployment

 Prior to following this guidance, ensure that you have fully considered the information in [Preparation](#).

An overview of the steps typically required to complete a standalone 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.

**Install and configure the device**

3. Install Blue Prism
4. Configure a connection to the SQL Server instance
5. Create/Configure a Blue Prism SQL Server Database
6. Login for the first time
7. Install a Blue Prism License Key
8. Configure an Encryption Scheme
9. Verify the Blue Prism Deployment



Standalone  
Blue Prism Deployment

If problems are experienced whilst installing see [Troubleshooting an installation](#).

## 1. Install Blue Prism

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

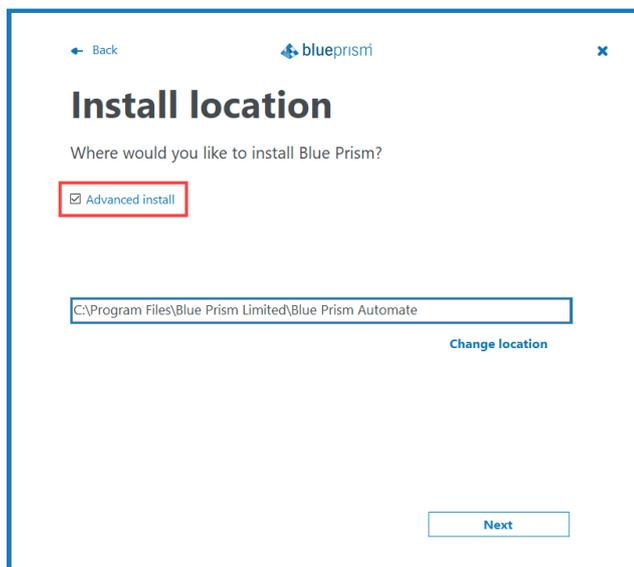
- 32-bit Installer: BluePrismx.x.nn\_x86.msi
- 64-bit Installer: BluePrismx.x.nn\_x64.msi

Installers are available from the [Blue Prism Portal](#).

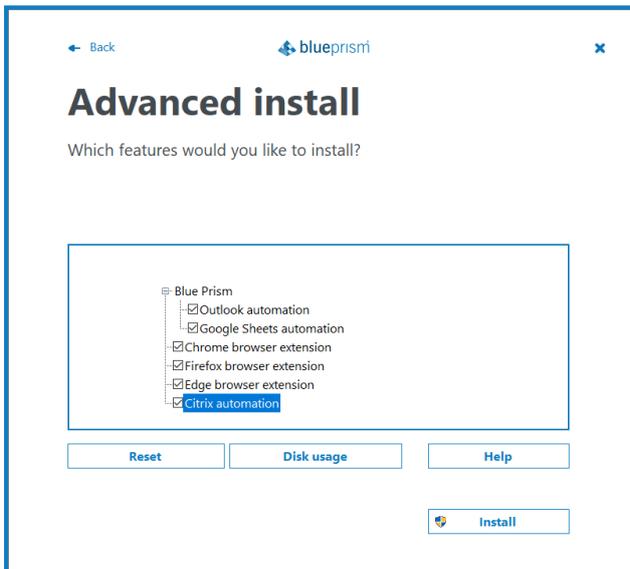
Click **Get started** to follow the steps in the installation wizard and complete the installation. If required, you can change the language in the wizard by clicking **Choose language** at the top of the first screen.

### Advanced install options

The following additional components are available during a Blue Prism installation if the **Advanced install** option is enabled on the Install location screen. Components selected by default that are not required must be deselected before proceeding with the installation.



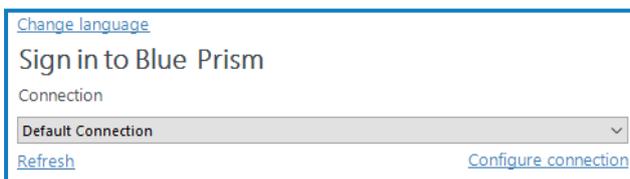
- **Outlook automation** - Required on devices where the Blue Prism MS Outlook Email VBO will be executed.
- **Google Sheets automation** - Required on devices where the Blue Prism Google Sheets VBO will be executed.
- **Chrome browser extension** - Required on devices that will be used to automate Chrome.
- **Firefox browser extension** - Required on devices that will be used to automate Firefox.
- **Edge browser extension** - Required on devices that will be used to automate Chromium-based Edge.
- **Citrix automation** - Required on devices that will be used to automate applications natively via a Citrix Virtual Desktop Environment (VDE). This option is only available for selection if Citrix Workspace has been installed. For more details, see [Citrix integration](#).



## 2. 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. On the Blue Prism login screen, click **Configure connection**.



2. In the Connection Configuration dialog, specify the connection details as outlined in the image below:

Connection Name	Default Connection	Friendly name for the connection
Connection Type	SQL Server (SQL Authentication)	Type of SQL authentication to use (e.g. SQL Authentication; or Windows Authentication*)
Database Server	localhost/sqlexpress	Network location of the SQL Server Instance
Database Name	BluePrism	The name of the database that will be created (or that already exists)
User ID	BluePrism_DBAdmin	SQL Authentication username used to interact with the database server*
Password	*****	SQL Authentication password
Additional SQL Connection Parameters	TrustServerCertificate=true;Encrypt=true	Optional connection parameters**

\*If the Connection type selected includes 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.

- **SQL Server (SQL Authentication)** - Connection Name (must be unique), Database Server, Database Name, User ID
- **SQL Server (Windows Authentication)** - Connection Name (must be unique), Database Server, Database Name
- **Availability Group (SQL Authentication)** - Connection Name (must be unique), Database Server, Database Name, User ID
- **Availability Group (Windows Authentication)** - Connection Name (must be unique), Database Server, Database Name
- **SQL Server (Custom Connection String)** - Connection String (the complete SQL connection string must 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:

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

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

As the database does not yet exist, one of the following messages will display:

**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 <b>OK</b> to clear the message and then click <b>Create Database</b> .		Click <b>OK</b> to clear the message and then click <b>Configure Database</b> .
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 <a href="#">Troubleshooting an installation</a> .

### 3. Create and configure a Blue Prism SQL Server database

There are threestages 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 by using the Create Database action.
- **Apply Blue Prism schema** - The database schema is applied to the configured database.

The 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 against a pre-existing database. The CreateScript.sql can be obtained via request from Blue Prism Customer Support or generated using the Blue Prism client - Click **Generate Script** at the bottom of the Create a new database or Upgrade the database screens.

- **Configure Blue Prism sign-on settings** - A number of configuration options are applied to the database. These are applied automatically when using the 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 is completed in a single step when using the Create Database functionality.

1. To create and configure a database, click **Create Database** or **Configure Database** in the Connection Configuration dialog.

2. In the Create a new database dialog, enable the **Drop any existing database with the specified name** option if you want to purge and recreate a database that already exists.

3. Select the preferred authentication method for users connecting to Blue Prism. You can choose between two types of environments:
  - **Multi-authentication environment** - This environment supports three types of authentication, where roles and permissions are mapped to individual users in Blue Prism. The authentication type is configured when a [user is created](#) and cannot be changed later.
    - **Blue Prism native authentication** - User accounts are individually created and maintained in Blue Prism and user login attempts are processed by verifying the supplied credentials configured in the Blue Prism database. For more details, see [Authentication in Blue Prism](#).
    - **Active Directory authentication** - If Active Directory authentication has been configured in Blue Prism, Active Directory user accounts can be created by retrieving users from the Active Directory and assigning them to Blue Prism user roles.
    - **Native authentication via Authentication Server** - An Authentication Server configuration is required when using the Blue Prism API and/or browser-based Control Room from version 7.0 onwards. Authentication Server user accounts can be created directly in Blue Prism Hub (version 4.3 and later), or by mapping users between the Authentication Server and Blue Prism databases, and assigning them to Blue Prism user roles. For more details, see [Authentication Server](#).
  - **Single-authentication environment** - referred to as *Active Directory Single Sign-On* prior to Blue Prism 6.8, this environment supports Active Directory authentication where users log in via Active Directory only and roles are mapped to Active Directory security groups. To set up a single-authentication environment, 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 select the security group within that domain whose members will be granted system administrator access to Blue Prism. For more details, see [Single sign-on](#).
4. Click **OK** to complete the database configuration.

### Support for contained databases

Blue Prism supports the use of contained databases, hosted on Microsoft SQL Server. To use a contained database, it is necessary to manually create the database and apply the Blue Prism CreateScript.sql.

For more information, see [Contained databases](#).

## 4. Log in for the first time

It is now possible to log in for the first time and carry out some system-wide configuration.

You will first need to log in using the default Blue Prism native credentials to configure the system for the required authentication methods.

Default credentials:

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

Follow the onscreen instructions to change the administrator password.

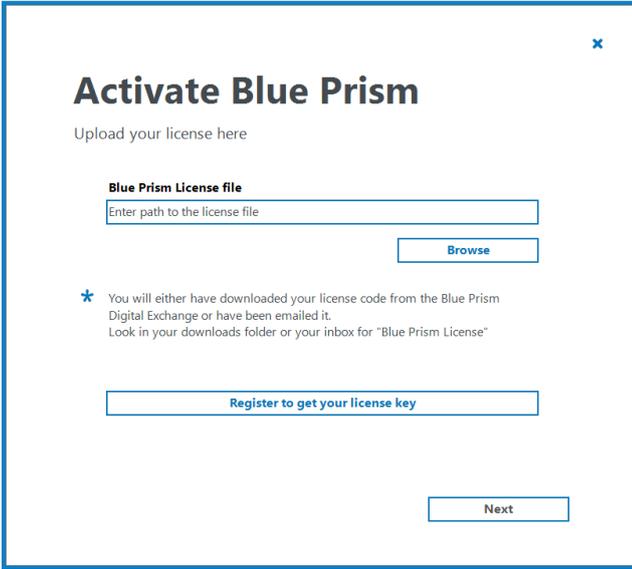
 This [video](#) shows you how to recover your admin password.

See [Authentication in Blue Prism](#) for more details.

## 5. Install a Blue Prism license key

A license file containing a valid license key is required to activate the software. License files can be obtained from a Blue Prism Account Manager. Your license and EULA are emailed to you from [digitalworker@blueprism.com](mailto:digitalworker@blueprism.com). Save the files to your hard-drive.

After logging into Blue Prism, if a license is not already installed, you will be prompted to enter your license key.



1. Click **Browse**, select the required License (.lic) file and click **Next** to start the license activation wizard.
2. Follow the steps in the wizard and save or copy the generated activation code.
3. When prompted, click to open the Blue Prism Portal.

You will be directed to [portal.blueprism.com/products/activation](https://portal.blueprism.com/products/activation).

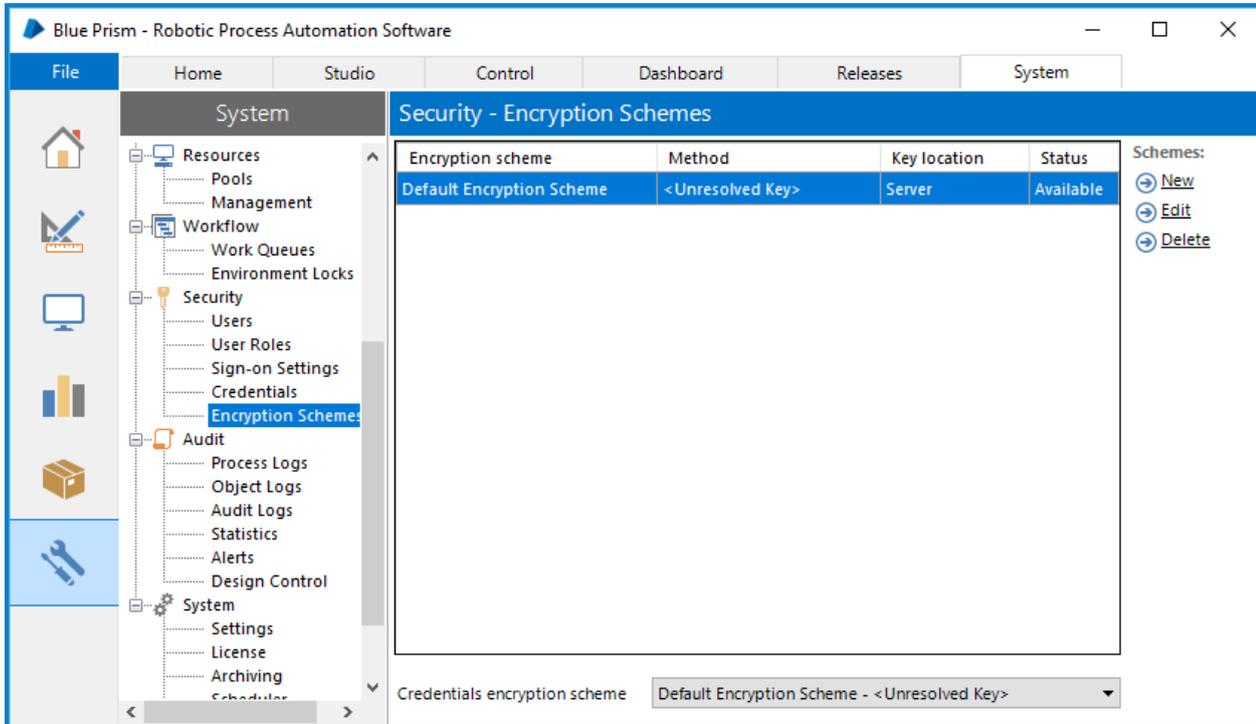
 If you are not already logged into the Blue Prism Portal, you will be prompted to log in.

4. Paste or import the generated activation code and click **Submit license activation**.
5. Copy the activation key, paste it back into the Blue Prism license activation wizard, and click **Next**.  
Your Blue Prism license is activated.

For information on how to manage your license after activation, see [Licensing](#).

## 6. Configure an encryption scheme

In order to support the use of Credential Manager (for securely storing credentials), you must 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:

 It is not recommended practice for enterprise customers operating at scale to store the encryption scheme keys in the database.

Standalone Deployment	Multiple Component (App Server) Deployment
<div style="border: 1px solid #0056b3; padding: 5px;"> <p>Name: <input type="text" value="Default Encryption Scheme"/> <input checked="" type="checkbox"/> Available</p> <p>Location: <input type="radio"/> Application Server (recommended) <input checked="" type="radio"/> Database</p> <p>Method: <input type="text" value="AES-256 AesCryptoService (256 bit)"/> <a href="#">Generate key</a></p> <p>Key: <input type="text" value="....."/></p> </div> <ol style="list-style-type: none"> <li>Select <b>Database</b>.</li> <li>Select <b>AES-256</b>.</li> <li>Click <b>Generate Key</b>.</li> <li>Click <b>OK</b>.</li> </ol>	<div style="border: 1px solid #0056b3; padding: 5px;"> <p>Name: <input type="text" value="Default Encryption Scheme"/> <input checked="" type="checkbox"/> Available</p> <p>Location: <input checked="" type="radio"/> Application Server (recommended) <input type="radio"/> Database</p> <p>The secret key for this scheme should be added to the Server Key Store using the Configuration utility on each Application Server.</p> </div> <ol style="list-style-type: none"> <li>Select <b>Application Server</b>.</li> <li>Click <b>OK</b>.</li> </ol>

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

## 7. Verify the installation

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

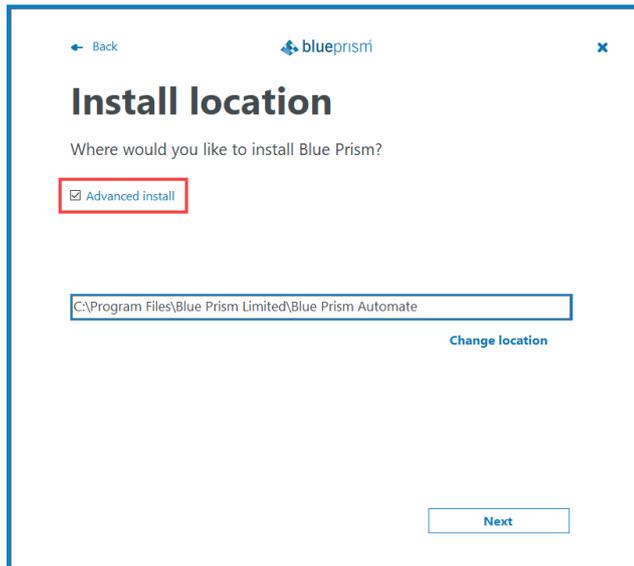
For step-by-step instructions, see [Verify an Installation](#).

## Advanced configuration

This section provides details about advanced configuration techniques for configuring Blue Prism Enterprise:

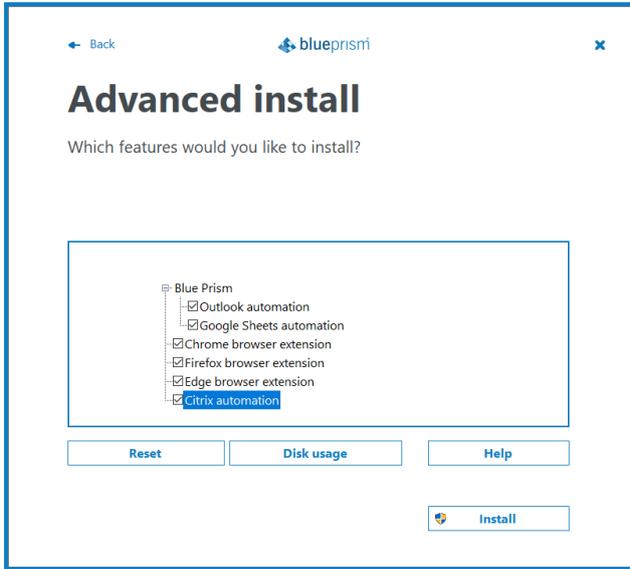
### Advanced installation options

The following additional components are available during a Blue Prism installation if the **Advanced install** option is enabled on the Install location screen. Components selected by default that are not required must be deselected before proceeding with the installation.



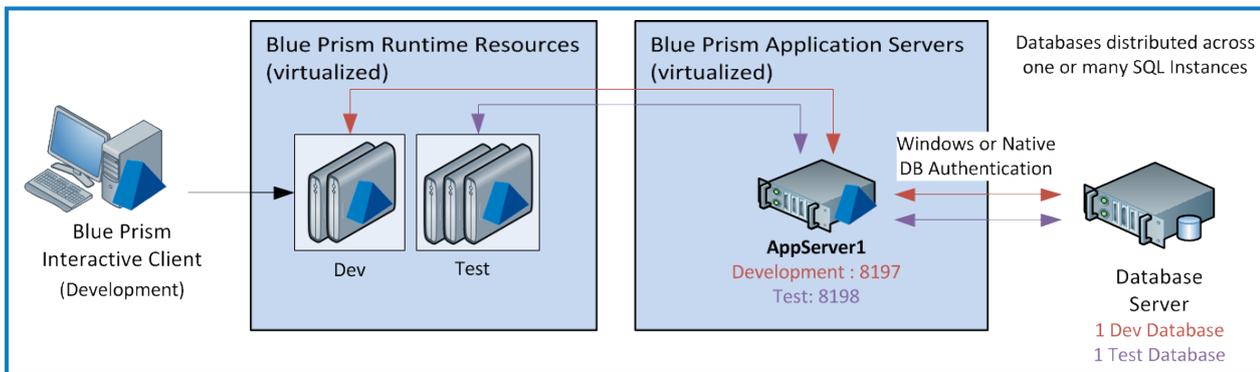
- **Outlook automation** - Required on devices where the Blue Prism MS Outlook Email VBO will be executed.
- **Google Sheets automation** - Required on devices where the Blue Prism Google Sheets VBO will be executed.
- **Chrome browser extension** - Required on devices that will be used to automate Chrome.
- **Firefox browser extension** - Required on devices that will be used to automate Firefox.
- **Edge browser extension** - Required on devices that will be used to automate Chromium-based Edge.

- **Citrix automation** - Required on devices that will be used to automate applications natively via a Citrix Virtual Desktop Environment (VDE). This option is only available for selection if Citrix Workspace has been installed. For more details, see [Citrix integration](#).

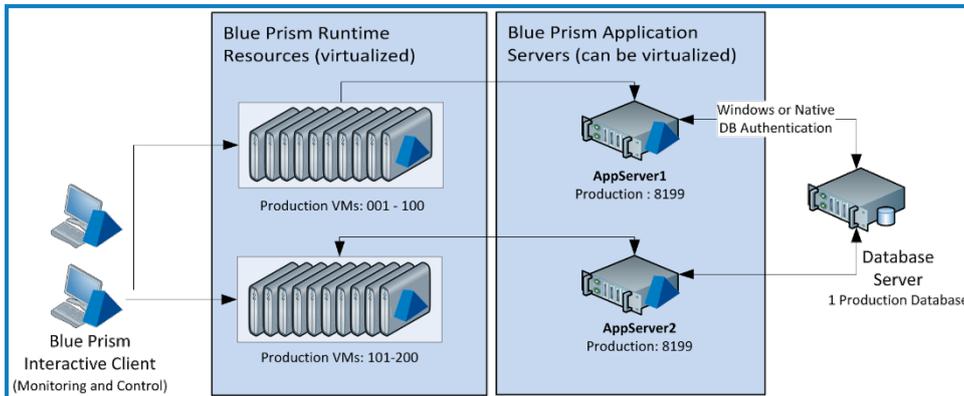


## Multiple and co-hosted application servers

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 encryption 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.

```

File Edit Format View Help
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost

10.188.15.3 AppServer001.mydomain.local
10.188.15.4 AppServer002.mydomain.local
10.188.16.1 resource001.mydomain.local
10.188.16.2 resource001.mydomain.local
10.188.16.3 resource001.mydomain.local
    
```

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 specialized techniques for interfacing with applications written in the Java Programming Language.

For more information, see [Java Access Bridge\(JAB\)](#).

## Active Directory configuration

Blue Prism supports single sign-on using Microsoft Active Directory Domain Services, which allows users who have been authenticated by the operating system, and who are members of appropriate domains and forests, to log into Blue Prism without resubmitting their credentials. Integration with Active Directory is configured for specified instances of Blue Prism allowing full segregation of roles across multiple environments such as Development, Test, and Production.

Blue Prism provides two types of environments for managing Active Directory authentication to the platform:

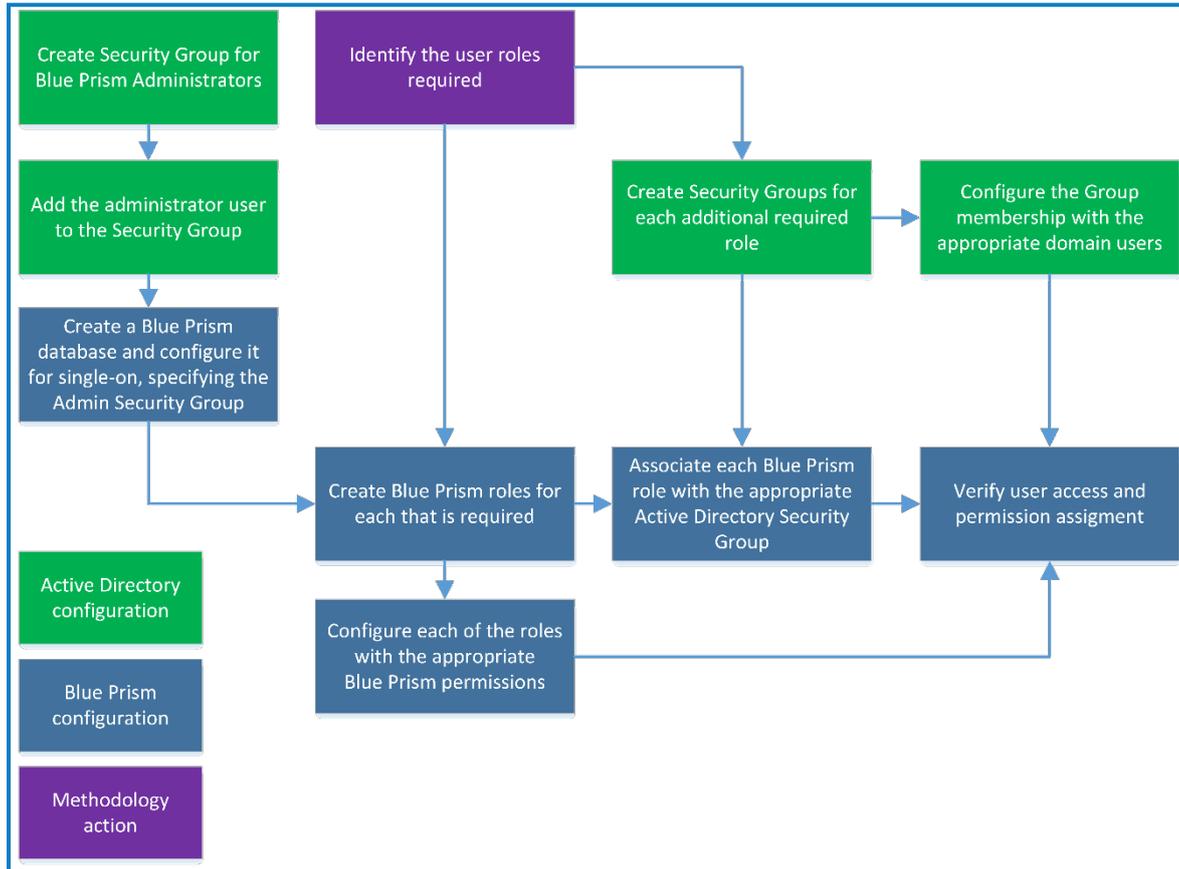
- **Multi-authentication environment** - supports Active Directory accounts where roles are mapped to individual users in Blue Prism. In multi-authentication environments, Active Directory users can be contained in multiple domains and multiple forests.
- **Single-authentication environment** - referred to as *Active Directory Single Sign-On* authentication in previous versions of Blue Prism, it supports Active Directory accounts where roles are mapped to Active Directory security groups. In single-authentication environments, Active Directory users can be contained within multiple domains but only a single forest.

The environment type is selected when the [database is created](#) and it can only be changed when [converting](#) a single-authentication Active Directory environment to a multi-authentication Active Directory environment.

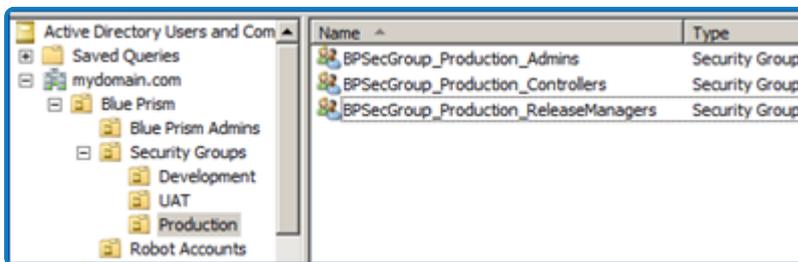
### Active Directory configuration in a single-authentication environment

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 role after which users will be granted access to the platform based on their Active Directory security group membership.

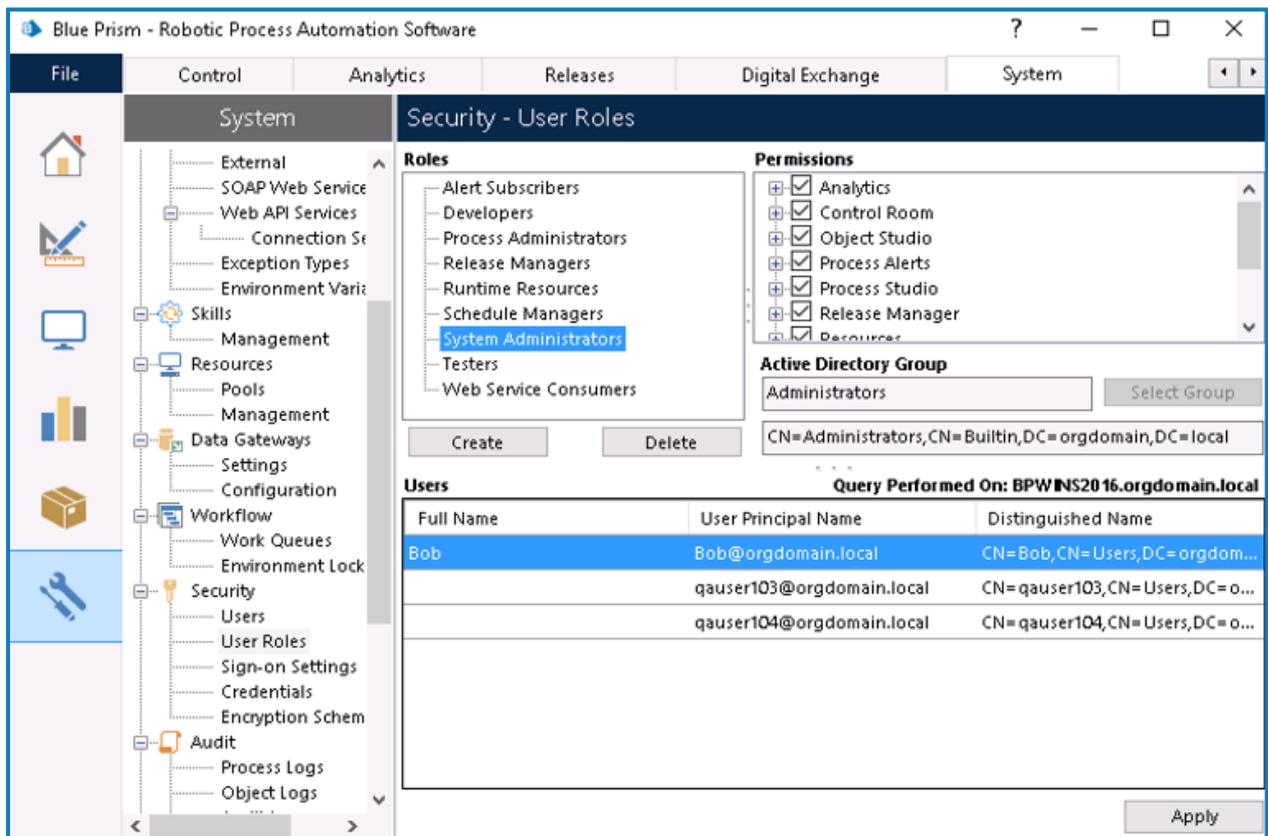
The steps required to configure Blue Prism integration with Active Directory for single sign-on in a single-authentication environment are illustrated in the diagram below:



1. **Configure Active Directory security groups** - Security groups should be set up in Active Directory to reflect each user role in a Blue Prism environment. The users within the domain should then be added to the relevant security group.



2. **Specify the domain that hosts the Active Directory security groups** - Blue Prism must be configured with the domain where the Active Directory security groups will reside. Only security groups in the specified domain can be associated with a Blue Prism user role, however, users from any domain within the common Active Directory forest can be assigned to these security groups. They can either be direct members of this group, or be granted membership via a nested group. As part of the configuration it is necessary to select which Active Directory security group users should be members of before granting them System Administrator rights.
3. **Configure and map the Blue Prism roles to Active Directory security groups** - The pre-configured Blue Prism user roles can be edited if required, and new roles can also be added. Each active role in a given Blue Prism environment must then be mapped to an existing Active Directory security group within the configured domain.



 Blue Prism 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.

Users who belong to the groups that have been configured should now be able to log into Blue Prism and perform the actions permitted by the corresponding Blue Prism role. Users may have to log out of Windows and log back in again for Active Directory changes to take effect.

## Active Directory configuration in a multi-authentication environment

The following steps are required for managing Active Directory user access to a multi-authentication environment:

1. **Enable Active Directory authentication in Blue Prism** - Blue Prism administrators who are members of an Active Directory domain must enable Active Directory authentication on the Security - Sign-on Settings - Sign-on Settings screen in Blue Prism before mapping Active Directory users to Blue Prism roles.

**Security - Sign-on Settings**

**Password Rules**

Passwords must contain:

- Upper case (A, B, C, ...)
- Lower case (a, b, c, ...)
- Digits (1, 2, 3, ...)
- Special (!, \$, %, &, ...)
- Brackets ([, ], {, }, (, ), <, >)

Must contain additional characters:

Minimum password length:

Passwords cannot match:

- Number of previous passwords:
- Password used in a number of preceding days:

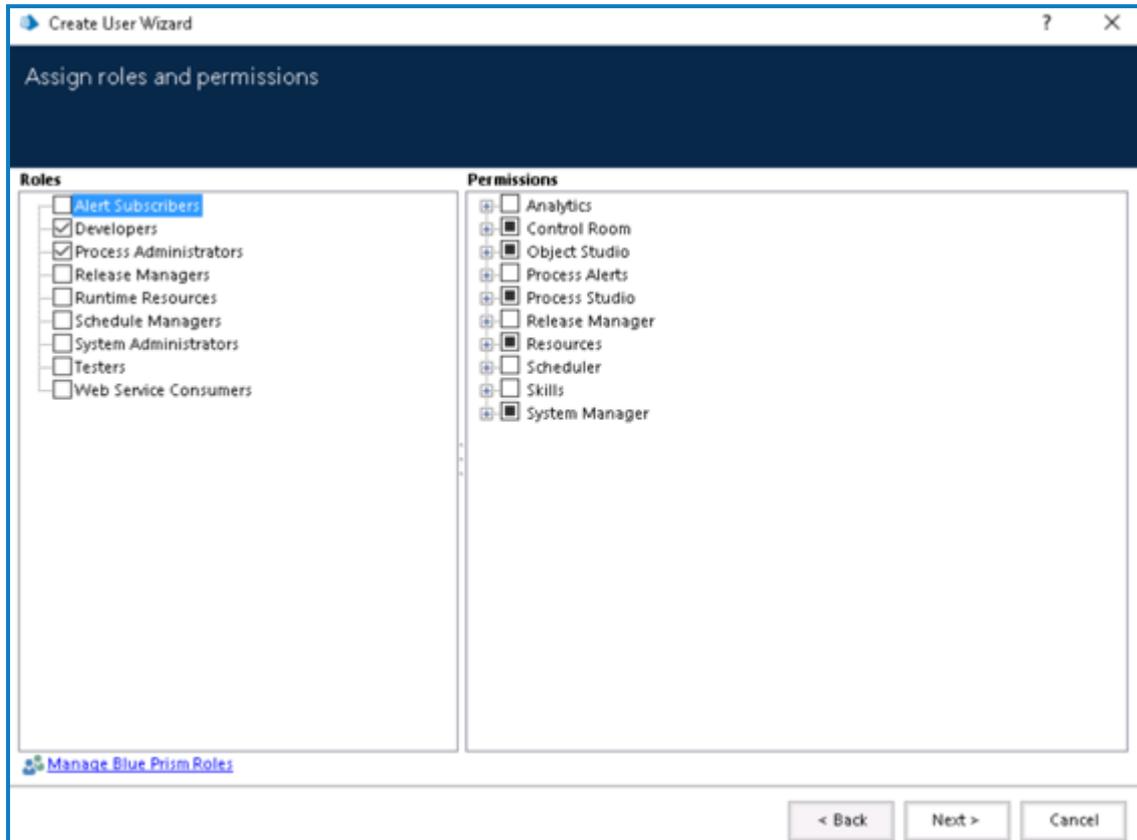
**Login Options**

- Show a list of users on the login screen
- Start with a default log in name:
- User is locked after failed login attempts:
- Warn when password or account is due to expire:

**Active Directory Authentication**

- Enable Active Directory authentication

2. **Map Active Directory users to Blue Prism roles** - Active Directory users are retrieved from the Active Directory domains and forests and mapped individually to Blue Prism roles via the [Create User Wizard](#) in Blue Prism.



## Database conversion

Blue Prism administrators can convert a single-authentication Active Directory database to a multi-authentication Active Directory environment. This is a one-way irreversible operation which converts all single-authentication accounts in a Blue Prism environment to multi-authentication accounts, automatically mapping roles to individual users based on their Active Directory security group membership (after which group membership is no longer relevant).

This feature is available in the [single sign-on settings](#) for administrators using the single-authentication environment.

Before starting the conversion please ensure:

- you are using one of the [supported connections](#) for Active Directory authentication.
- you have backed up your database.
- you have stopped all processes.
- all users and runtime resources are logged out of the environment.

After closing down any runtime resources the administrator will need to wait two minutes before they are able to perform the conversion, otherwise they will be reminded that all users must be logged out before they can proceed with the conversion.



Please be aware that depending on the number of users you are converting and any potential latency, the database conversion might take a few minutes.

When converting a single-authentication Active Directory environment to a multi-authentication Active Directory environment, administrators are prompted to create a recovery administrator user that uses Blue Prism native authentication. A native user with a secure password is required during the conversion process as Active Directory users in a multi-authentication environment cannot update an expired license using Active Directory credentials, since a Blue Prism server cannot be started with an expired license and Active Directory users cannot sign in to this environment using a direct SQL server database connection.

 This user can be removed once the database conversion has completed, however it is recommended to retain it for troubleshooting purposes, particularly in environments where all administrator accounts use multi-authentication Active Directory.

For more information on managing multi-authentication user accounts, see [Manage users](#).

## Runtime resource authentication

Runtime resources can authenticate via Active Directory either in a multi-authentication or single-authentication environment by passing the `/sso` switch in the command line at resource start-up. The `/sso` switch supports only the client/server [connection modes](#) mentioned above.

Authentication occurs using the currently logged-in Windows user's credentials. In a multi-authentication environment, the runtime resource inherits the Blue Prism user roles mapped to the currently logged-in Windows user. In a single-authentication environment, the runtime resource inherits the Blue Prism roles mapped to the Active Directory security groups to which the currently logged-in Windows user has been assigned.

## Supported connection modes

Only the following client/server connection modes are supported for Active Directory authentication:

- WCF: SOAP with Message Encryption and Windows Authentication,
- WCF: SOAP with Transport Encryption and Windows Authentication
- .NET Remoting: Secure.

## Silent installation

 Downloading and installing any of the SS&C | Blue Prism® Enterprise components, including by silent installation via command line, means that you accept the [End User License Terms](#).

The Blue Prism Enterprise components can be installed via the command line using the commands in the sections below.

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 from the command line, see the following [Microsoft article](#).

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

### Blue Prism

 If you use scripts to install Blue Prism, you must ensure that you enter the exact installer name into the script, which is specific to the Blue Prism software version. The examples below use `BluePrism7.0.0_x64.msi`. If you are installing on to 32-bit systems, you will need to use `BluePrism7.0.0_x86.msi`.

The example scripts use the switches `/QB` (basic UI during the installation process) or `/QN` (no UI during the installation process). For more information on the switches, see the [Microsoft documentation on Windows Installer command-line options](#).

Elevated permissions may be required to run a silent installation (`/qn`) of Blue Prism. If you do not have the required permissions (for example, permissions to install to the specified folder), the silent installation may fail.

### Core application

To install Blue Prism use the command:

```
msiexec /i BluePrism7.0.0_x64.msi /QB- ALLUSERS=1
```

This command installs Blue Prism including the default optional components, such as the Chrome browser extension.

 By default, Blue Prism is installed in C:\Program Files. If you want to install Blue Prism to a different drive or folder, you can use the `INSTALLFOLDER` parameter. For example, to install Blue Prism Enterprise in E:\Program Files\Blue Prism Limited\Blue Prism Automate, use the following command line:

```
msiexec /i BluePrism7.0.0_x64.msi /QB INSTALLFOLDER="E:\Program Files\Blue Prism Limited\Blue Prism Automate" ALLUSERS=1
```

You cannot install a 64-bit application into the Program Files (x86) folder, nor a 32-bit application into the 64-bit folder.

### Custom install options

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

```
msiexec /i BluePrism7.0.0_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
<code>OutlookAutomation</code>	Installs the DLLs required on all devices on which the Blue Prism MS Outlook Email VBO will be executed.
<code>GoogleSheets</code>	Installs the DLLs required on all devices on which the Google Sheets VBO will be executed.
<code>ChromePlugin</code>	Installs the Blue Prism Chrome browser extension required on devices that will use this mechanism to automate Chrome.
<code>EdgePlugin</code>	Installs the Blue Prism Edge browser extension required on devices that will use this mechanism to automate Microsoft Edge.
<code>FirefoxPlugin</code>	Installs the Blue Prism Firefox browser extension required on devices that will use this mechanism to automate Firefox.
<code>CitrixDriver</code>	Installs the Blue Prism virtual driver and supporting DLLs on an interactive client or digital worker.

To install Blue Prism with the Chrome, Edge, and Firefox browser extensions, use the command:

```
msiexec /i BluePrism7.0.0_x64  
ADDLOCAL=BluePrism,BPServer,ChromePlugin,EdgePlugin,FirefoxPlugin /qn
```

To install Blue Prism and the components required to interact with Microsoft Outlook:

```
msiexec /i BluePrism7.0.0_x64 ADDLOCAL=BluePrism,BPServer,OutlookAutomation /qn
```

To install Blue Prism with Google sheets:

```
msiexec /i BluePrism7.0.0_x64 ADDLOCAL=BluePrism,BPServer,GoogleSheets /qn
```

To install Blue Prism and the Citrix virtual driver on an interactive client or digital worker:

```
msiexec /i BluePrism7.0.0_x64 ADDLOCAL=BluePrism,BPServer,CitrixDriver /qn
```

## Configure the database connection

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

For the SQL Server (SQL Authentication) mode, use this format:

```
Automate.exe /dbconname <Friendly name for the connection> /setdbname <Database name>  
/setdbserver <Database server> /setdbusername <Database user> /setdbpassword <User's  
password>
```

For example:

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

For the SQL Server (Windows Authentication) mode use this format:

```
Automate.exe /dbconname <Friendly name for the connection> /setdbname <Database name>  
/setdbserver <Database server>
```

For example:

```
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 authentication, or Single Sign-on Active Directory authentication will be used to secure access to Blue Prism.

### Configure 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 ""
```

### Configure a database for an environment to be secured using Active Directory Single Sign-on authentication

Database secured using SQL Authentication

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

Database secured using Windows Authentication

```
AutomateC.exe /createdb "" /setadomain "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 the license file>
```

For example:

```
AutomateC.exe /license "c:\temp\MyBluePrismLicense.lic"
```

The /license switch needs to be used in conjunction with either /sso or /user <user> <password>.

## Create the server service profile

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

```
AutomateC.exe /serverconfig <Profile name> <Connection name> <Port number>
```

For example:

```
AutomateC.exe /serverconfig "Default" "Connection friendly name" "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, using the format below.

```
Automate.exe /dbconname <Default connection> /setbpserver <Server name> <Port number>
```

For example:

```
Automate.exe /dbconname "Default connection" /setbpserver "Server1" "8181"
```

### Import processes

If there are business objects or processes to be imported the XML files can be imported individually using a command in the following format:

```
AutomateC.exe /import <Path to XML file> /user <User name> <User's password>
```

For example:

```
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.

### Publish processes

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

```
AutomateC.exe /publish <Process name> /user <User name> <User's password>
```

For example:

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

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

### Script references

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

Topic	Help Reference	Download Location
Msiexec	<a href="http://technet.microsoft.com/en-us/library/cc759262%28WS.10%29.aspx">http://technet.microsoft.com/en-us/library/cc759262%28WS.10%29.aspx</a>	N/A
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 > <Name of script>
```

For example:

```
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 <Enter the script number> > <Name of script>
```

When upgrading from a patch release, use the script number of the base minor version for the /fromrev switch to make sure all the relevant updates are included. For example, if you are upgrading from 6.10.6, use the script number of version 6.10.0. For example:

```
Automatec.exe /getdbscript /fromrev 395 > "c:\temp\UpgradeScript.sql"
```

Blue Prism version	Script number
6.3	255
6.4	275
6.5	318
6.6	332
6.7	360
6.8	373
6.9	381
6.10	395
7.0	444

## Advanced scripted techniques

### Set up 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 <Service name> binPath= "[Blue Prism Install Location]\BPServerService.exe <Configuration Name>"
```

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\""
```

### Configure 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 set up 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 using message encryption with no server binding specified on the server profile

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

#### WCF mode using message encryption with a server binding specified on the server profile

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

#### WCF mode using transport encryption with no server binding specified on the server profile

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

#### WCF mode using transport encryption with a server binding specified on the server profile

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

### Associate 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:

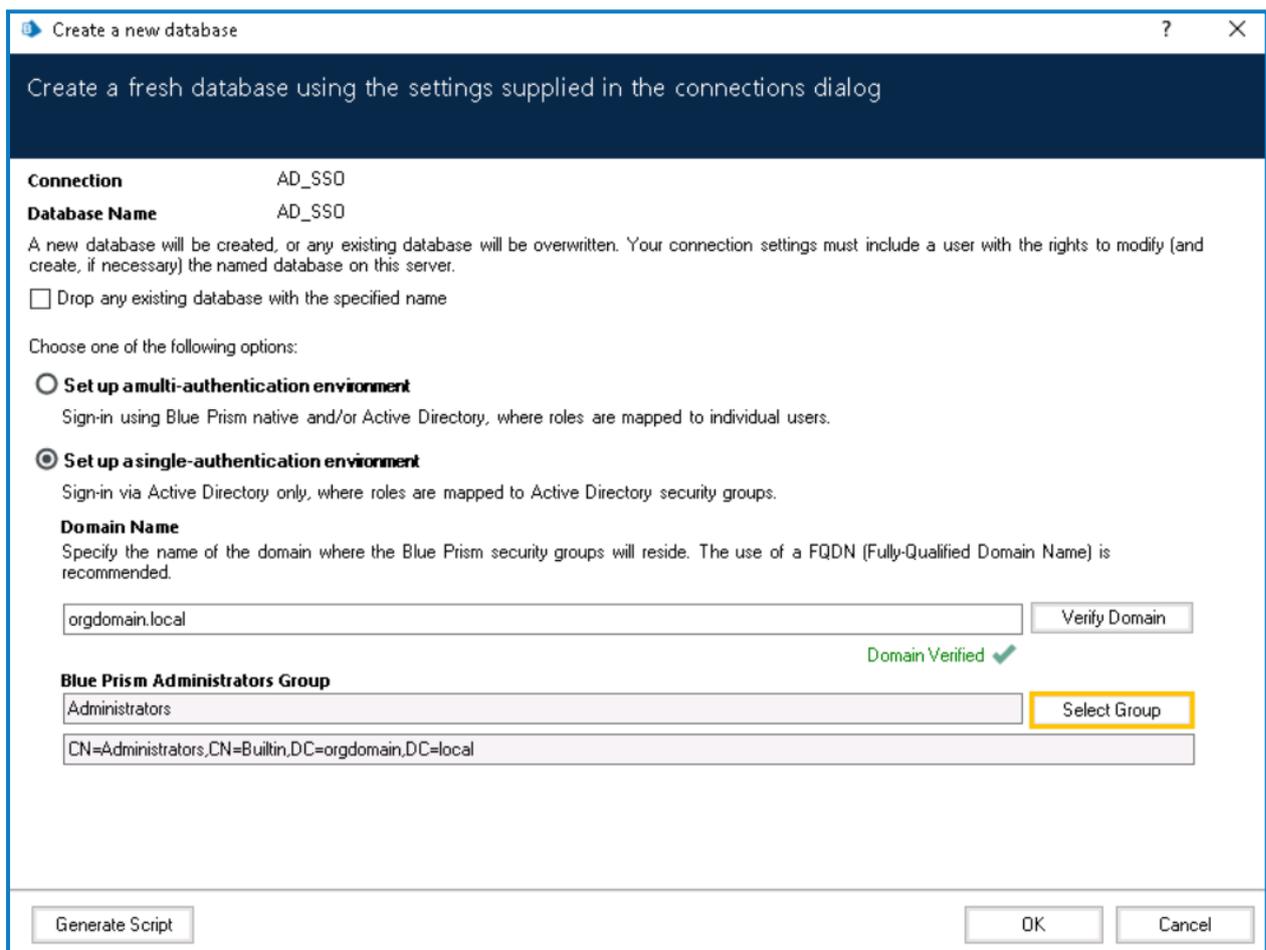
```
netsh http add sslcert ipport=10.0.2.15:8199 certhash=bac31cc4094793d275167cf02b31bbac2718f3c7 appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

## Contained databases

Blue Prism supports the use of contained databases, hosted on Microsoft SQL Server. To use a contained database, it is necessary to manually create the database and apply the Blue Prism CreateScript.sql.

The CreateScript.sql script can be obtained in the following ways:

- Via a request to Blue Prism Customer Support
- Generated using AutomateC. To generate the script, use the following command:  
`AutomateC.exe /getdbscript > CreateScript.sql`
- Generated using the Blue Prism client: Click **Generate Script** at the bottom of the Create a new database or Upgrade the database screens.



## Create and configure contained databases

1. Create a SQL Server database using Microsoft SQL Server Management Studio or by using an alternative method if required.
2. Run the script to create the required Blue Prism tables, views, and other required objects in the database.
3. Configure a connection to the database as described in [Create and configure a Blue Prism SQL database](#).

## Deploying to a virtualized or cloud environment

For some smaller implementations where there is less demand for scalability or where virtualization is not feasible, Blue Prism can be deployed to a wholly physical environment and can largely make use of existing desktops - albeit in a secured environment.

Virtualization however, is commonly the recommend approach as it more easily provides benefits which include physical security and scalability. Many virtualization technologies also simplify the roll-out of software updates and the implementation of disaster recover capabilities.

The core Blue Prism components can be deployed to persistent virtualized Windows devices and there are two main approaches:

### Use of an existing virtualization technology

Where organizations already have access to virtualization technologies such as VMWare or Citrix XenDesktop, there may be the capability to utilize these to provide the virtual machines which will host the required Blue Prism components. Further details on virtualization patterns are provided within the Virtualization Guide (available on request).

### Provision a dedicated virtualization host

Virtualization can be provided by provisioning a new dedicated server (or set of servers) on which new virtual machines are configured and used to host the required Blue Prism components. These typically use technologies such as Microsoft Hyper-V or Aware ESX although others are available.

When deploying to this type of host machine it is important to ensure that the specification of the host machine is sufficient to not only cater for the underlying operating system, but also provide the appropriate resources and performance for each of the virtual machines that will be configured.

#### Dedicated Virtual Host (example)

- 10-15 Blue Prism runtime resources
- Dual Socket Virtualization hosts:
- Quad Intel Xeon Quad Core Processors
- 32GB RAM (minimum)
- 450GB available space after applying RAID to arrayed disks
- 2 physical 1000Mbit NIC
- Operating System appropriate to technology (e.g. Hyper-V, ESX)

### Cloud-based deployment patterns

Blue Prism may be deployed on a cloud environment such as Microsoft Azure or Amazon AWS. This may be appropriate if the organization has an existing cloud strategy. Further details may be found in:

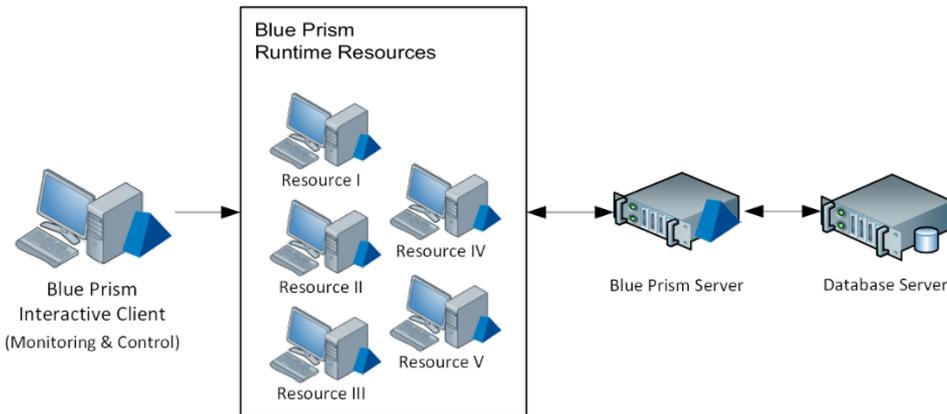
- Blue Prism Data Sheet - Cloud Deployments
- Blue Prism Data Sheet - Azure Reference Architecture
- Blue Prism Data Sheet - AWS Reference Architecture

## Deployment options

The following examples provide sample architectures based on the scale, or key features of the environment. Factors such as security, resilience, scalability and cloverleaf should also be considered. The example deployment options below include:

### Deployment example 1: Proof of Concept / Pilot / Pre-Production Up to 5 resources

For deployments with up to 5 Blue Prism runtime resources, a configuration using physical machines can be used. The machines should be appropriately secured and can be used either with or without the Blue Prism Server component (depending on requirements for scheduling and encryption).

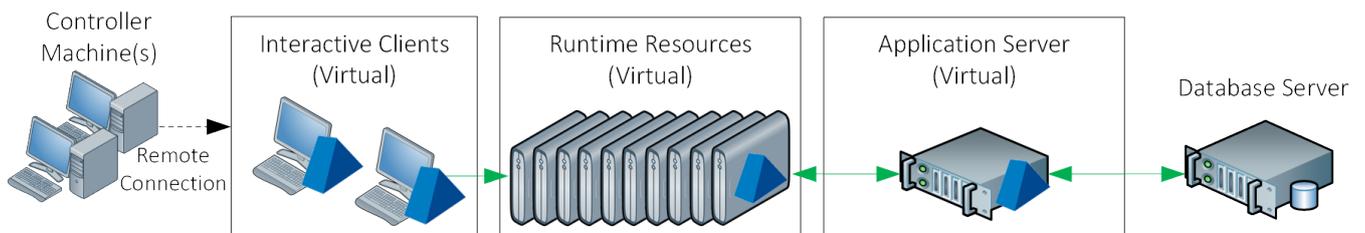


The Blue Prism server and database can be hosted on the same physical or virtual machine for pre-production scenarios

### Deployment example 2: Up to 100 resources

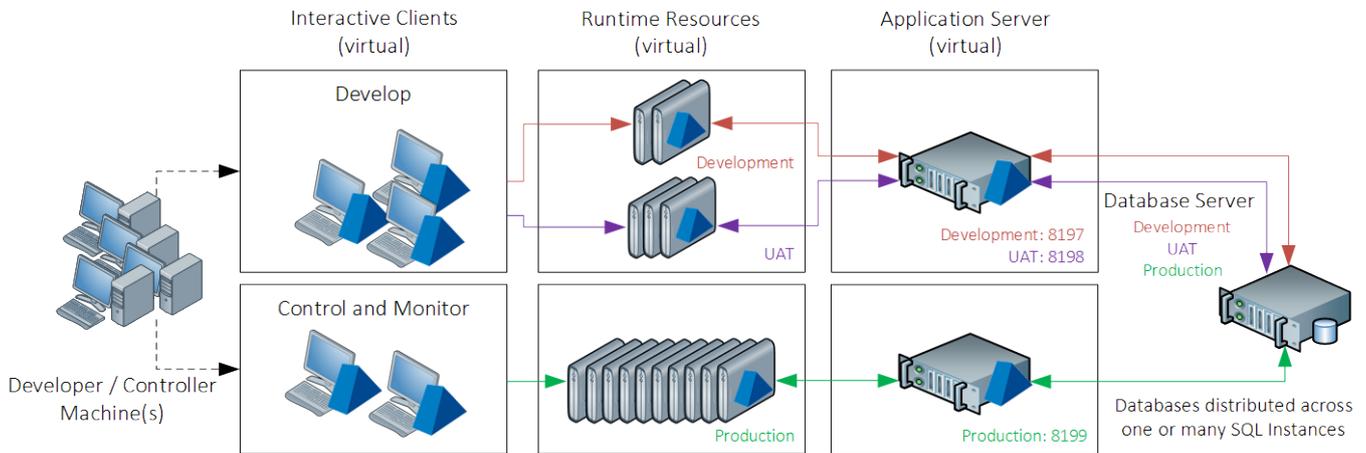
For deployments above 5 physical runtime resources, Blue Prism recommends installing on Windows desktops provided by a virtualized environment such as VMWare ESX or Citrix XenDesktop.

Blue Prism is installed on each virtual instance and becomes more easily secured and scaled up according to the size and capacity of the host server(s).



### Deployment example 3: Environments for Development, Test and Production

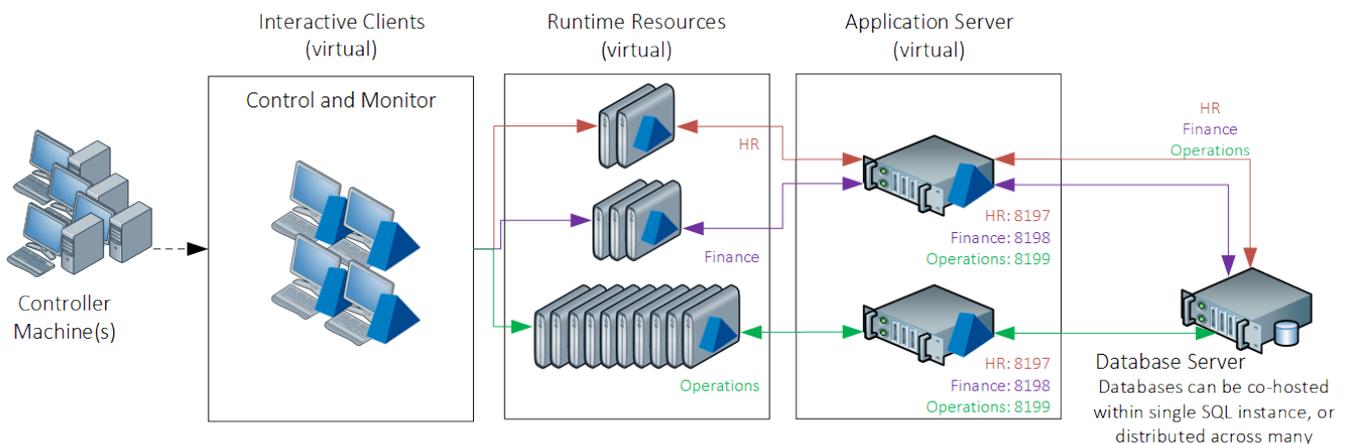
When deploying a number of environments such as for Dev, Test and Production purposes, each environment will require a dedicated database, however it is possible for some of the Blue Prism components to be shared. In the example below a single virtual server is used to host the Blue Prism Server service for the separate Dev and Test environments. Likewise a single interactive client can be configured to access any number of environments.



### Deployment example 4: Environments for Independent Business Areas

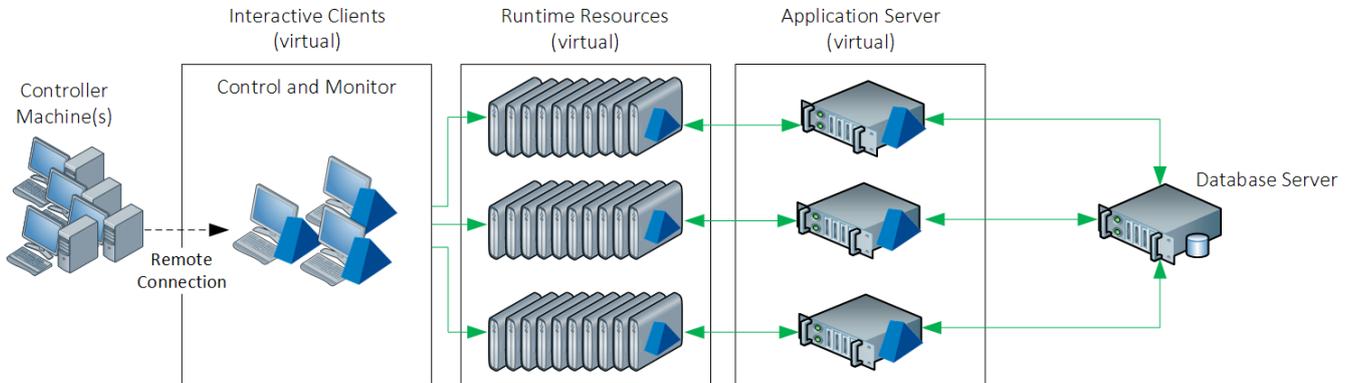
In larger or more complex scenarios it is possible to configure separate environments, such as for purposes of data or process segregation, whilst still sharing certain central features.

The example below demonstrates how three environments, each specifically purposed for supporting a defined business area can be configured. In this example, each business area has a series of dedicated runtime resources, and has a dedicated Blue Prism Server service, but the Server services are co-hosted on shared hardware.



### Deployment example 5: Up to 300 resources

For larger scale environments, the Blue Prism runtime resources are replicated and scaled, and each is paired with a dedicated application server for database communication. For cloverleaf and DR the hosts can be co-located at different physical sites. It is possible to deploy large numbers of runtime resources by following this approach.

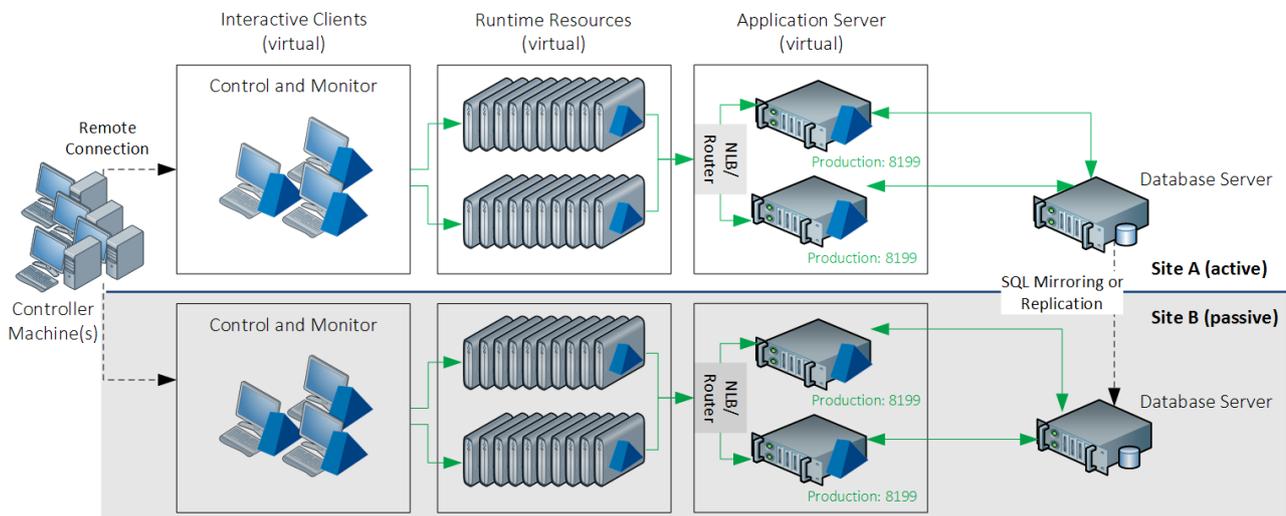


In the above example, each application server can marshal the connectivity for up to 100 Blue Prism runtime resources.

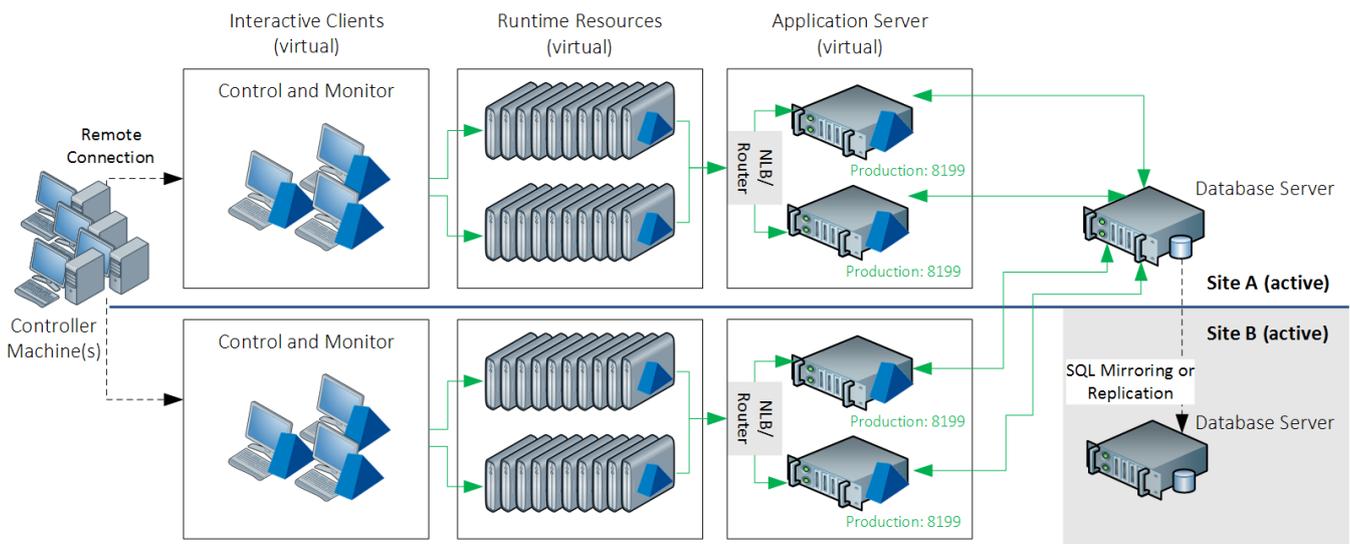
### Deployment Example 6: Multi-site - Abstractive or Active Passive

Where there is a requirement to deploy across multiple sites, Blue Prism can accommodate either an Addictiveness or Abstractive scenario depending on considerations such as network performance and security.

#### Active/passive



Active/active



## Service Principal Name (SPN) configuration for Kerberos authentication

If using the following connection modes with a Blue Prism Server connection, a Service Principal Name (SPN) must be configured against the Active Directory (AD) account under which each Blue Prism Server service instance is running:

- WCF: SOAP with Message Encryption & Windows Authentication
- WCF: SOAP with Transport Encryption & Windows Authentication
- .NET Remoting Secure

This is because when a Blue Prism interactive client or a runtime resource connects to an application server using one of the connection modes above, the Microsoft Negotiate Security Package is used to select the best Security Support Provider (SSP) to authenticate the connection. The internal code of the Blue Prism interactive client provides the expected SPN to the Microsoft Negotiation Security Package, which prompts Microsoft Negotiation to select the Kerberos SSP over New Technology LAN Manager (NTLM) SSP, provided the SPN is present in Active Directory. If the SPN is not present in Active Directory, Kerberos authentication will fail. See [this Knowledge Base article](#) for more details on the Windows security update for CVE-2022-21920 which affects this behavior. From Blue Prism 7.0.2, if the SPN is not present in Active Directory, and if the `/forcentlm <flag>` is set in Automate C, the NTLM SSP will be used.

It is recommended to contact your organization's IT team for assistance with this configuration, and that you first test the configuration in a non-production environment.

This configuration applies to all Blue Prism environments, however, if the Active Directory account under which your BP Server instances are running resides in a different domain to the Active Directory account used for the Blue Prism interactive client and runtime resource, we recommend you do not install the Windows security update for CVE-2022-21920. If you have already installed it, we recommend that you uninstall it. From Blue Prism 7.0.2, the additional configuration in Automate C outlined [below](#) is required.

To configure the SPN, follow the steps below on each Blue Prism Server Service instance:

1. Log into the Blue Prism Server using a Privileged Windows User Account that is a member of the Domain Admins or Enterprise Admins group.

See [the Microsoft documentation](#) in this topic for further details including required permissions. This is an essential step to review with your organization's IT team to ensure that the `Setspn` command does not fail to execute due to missing account permissions.

2. Open Command Prompt as an administrator on the application server and run the command below.

If the Blue Prism Server is running as a Local System account:

```
Setspn -S HTTP/SERVER_FQDN:SERVER_PORT/BPServer COMPUTER_HOSTNAME
```

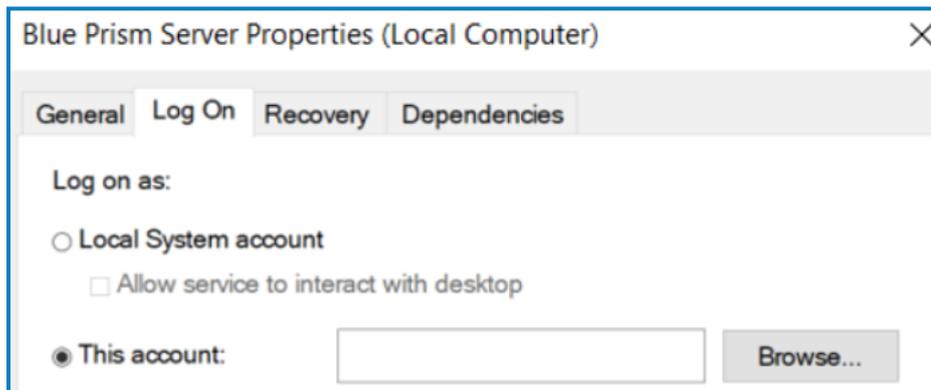
If the Blue Prism Server is running as a user account:

```
Setspn -S HTTP/SERVER_FQDN:SERVER_PORT/BPServer DOMAIN\Username
```

Where:

- HTTP accounts for both HTTP and HTTPS. Do not change the command to include HTTPS specifically as the configuration will fail.
- SERVER\_FQDN:SERVER\_PORT must be the Fully Qualified Domain Name (FQDN) of the Blue Prism application server.
- COMPUTER\_HOSTNAME is the hostname of the computer if BP Server Service is running as a Local System account.
- DOMAIN\Username is the domain username if BP Server Service is running as a user account.

This should match the **Log on as** setting in the Blue Prism Server Properties (Local Computer) window.



Example with local system:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>setspn -S HTTP/BPWINS2016.orgdomain.local:8199/BPServer BPWINS2016
```

Example with DOMAIN\Username:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1466]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>setspn -S HTTP/BPWINS2016.orgdomain.local:8199/BPServer orgdomain\mmb-adm
```

- After setting the SPN you will need to wait for the Kerberos ticket cache to renew (the default setting is 15 minutes, but it can be changed via Group policy). For more details, see the [Kerberos authentication documentation](#).

Alternatively, you can either:

- Restart the Blue Prism interactive client or runtime resource; or
- On the machine running the interactive client or runtime resource, open Command Prompt and run `Klist purge` to refresh the Kerberos tickets.

This command should not be performed within an elevated Command Prompt as it will not purge all the user Kerberos tickets.

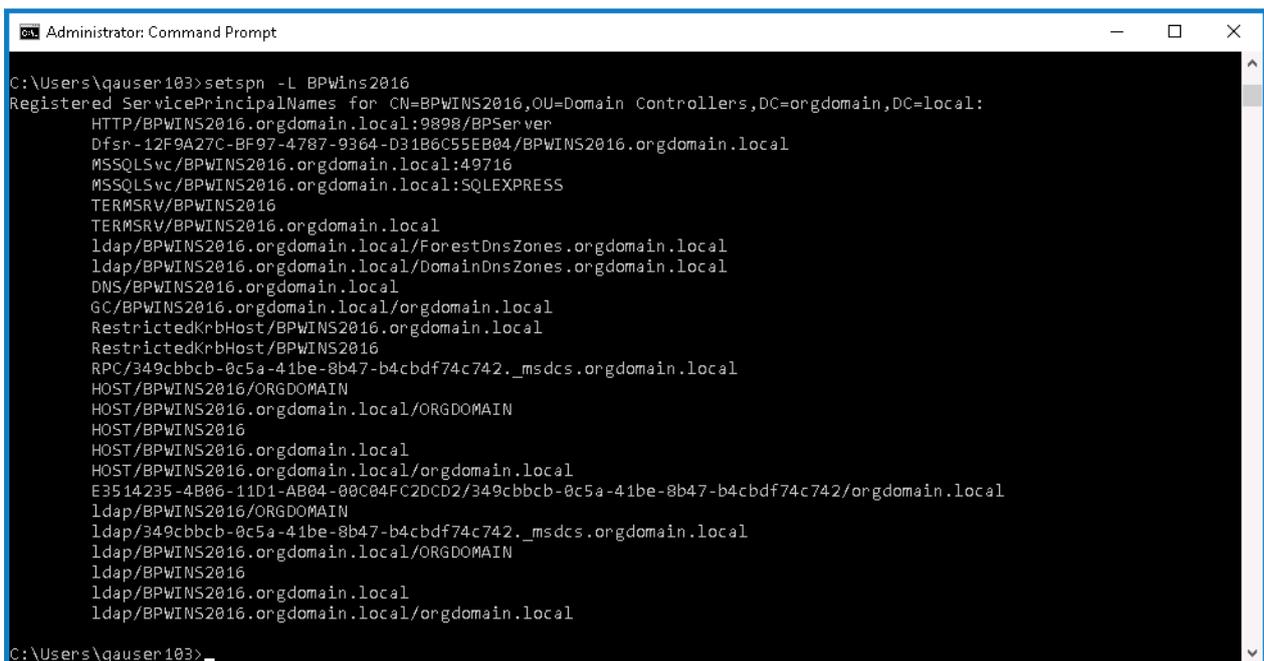
- Check that this is working as expected by connecting to the Blue Prism Server from a Blue Prism interactive client running on another machine.
- Repeat the steps above on each instance of the Blue Prism Server Service running on every Blue Prism Server.

### Check SPN entries and remove an incorrect SPN

- To check SPN entries for troubleshooting purposes, you can see a list of the added SPNs on the application server using the following command:

```
Setspn -L ACCOUNTNAME
```

Example of SPN list:



- Check the entries for the SPNs you added for the BP Server Service. You can remove the one added in error using the command listed below:

```
Setspn -D SPN_NAME ACCOUNTNAME
```

Where SPN\_NAME is the name displayed in the SPN entries list, for example, HTTP/SERVER\_FQDN:SERVER\_PORT/BPServer.

### Additional configuration for Blue Prism application servers in load balanced environments

It is essential that all instances of the Blue Prism Server Service in the same load balancer pool are running under the same service account and the SPN is registered to this account.

Additionally, it is recommended to register SPNs for the application server's FQDNs to the same service account, as this will allow for testing of a direct connection to the application servers. For more information, see [SPN troubleshooting](#).

### Additional configuration for Active Directory authentication in multi-forest environments

 This functionality is only available from Blue Prism 7.0.2 onwards.

To support Kerberos authentication in Blue Prism environments configured to use Active Directory authentication in multiple forests, the following settings must be configured in Automate C:

- `/setkerberosrealm` - For example, `/setkerberosrealm mycompany.com`. This must be configured for each BP Server connection in the interactive client where the user's Kerberos realm is different to that of the user account configured to run BP Server.

 The Kerberos realm is usually the same as the domain name, however, please check with your IT team for the correct value. This should be the realm of the service account running the Blue Prism Server service. In some environments, it may be necessary to apply the same configuration where the service account exists in another domain within the same forest. You can verify whether the Kerberos realm must be specified by running a `klist get` command against an SPN. For more information, see [SPN troubleshooting](#).

- `/forcentlm <flag>` - For example, `/forcentlm true`. Forces Microsoft Negotiate Security Package to select New Technology LAN Manager (NTLM) as the Security Support Provider (SSP) for the last used or specified connection (using the `/dbconname` switch) when authenticating the Blue Prism server connection. This option is provided so that NTLM can be used when Kerberos is unavailable or not configured.

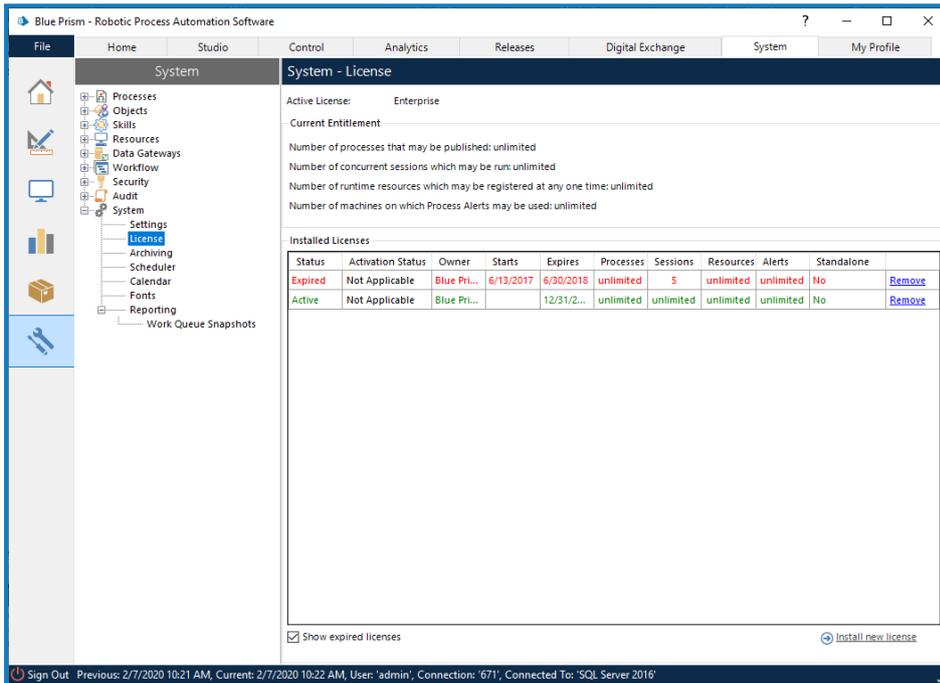
 Please consult with your security team before enabling this option as NTLM is considered a less secure protocol.

## Update a 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 Enterprise license file, follow the steps below:

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



The Blue Prism application server must be restarted for the changes to be fully recognized. After that, the changes are applied automatically to Blue Prism components on each interactive client and runtime resource. You should plan the scheduled maintenance window to restart the Blue Prism application server between the license update and the license expiry date.

 If you typically log into the interactive client through an application server, and the application server is not running, it will not start if you do not have a valid license deployed for the environment. The workaround is log into the interactive client using a direct database connection and update the license. You can do this on a client computer or typically on the application server computer.

## 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](#).

### 1. Import the Microsoft Word object

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

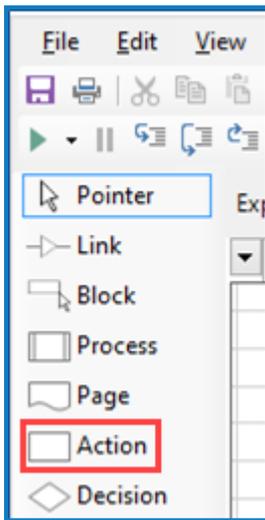
1. Launch Blue Prism and sign in using the *admin* username.
2. Select **File > Import**.
3. Select the *BPA Object - MS Word.xml* file. For the default install location, this is in C:\Program Files\Blue Prism Limited\Blue Prism Automate\VBO.
4. Complete the wizard to import the object.

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

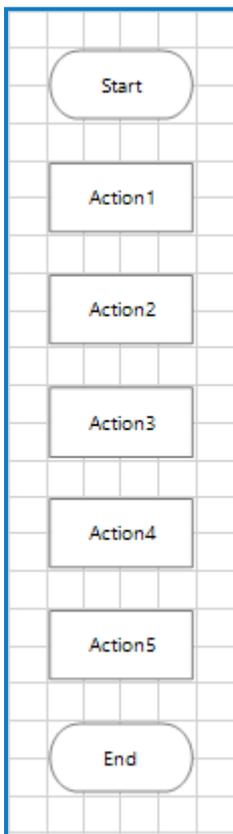
### 2. Create a new process

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.

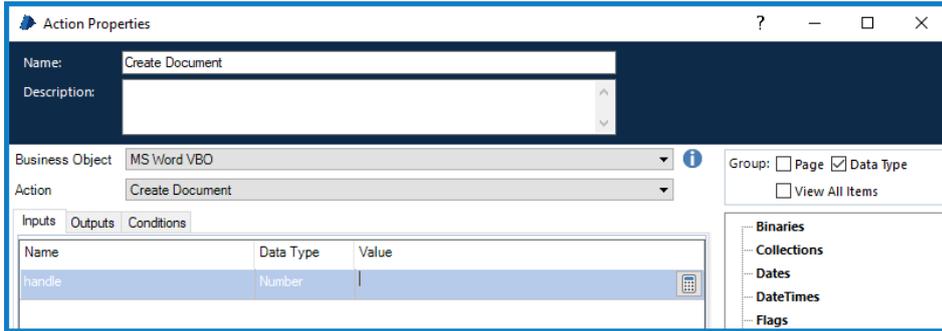


7. Place the action stages between the Start and End stages.



8. Double click the first action stage to open the Action Properties dialog.

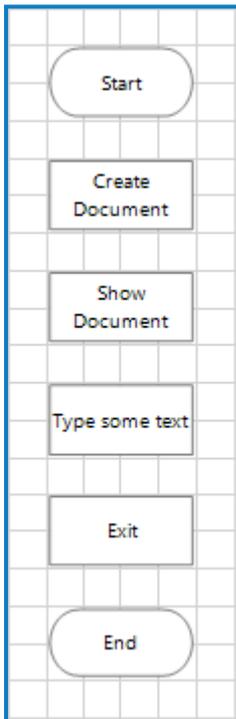
- Enter *Create Document* as the action name and select **MS Word VBO** and **Create Document** as the Business Object and Action.



Leave the input blank.

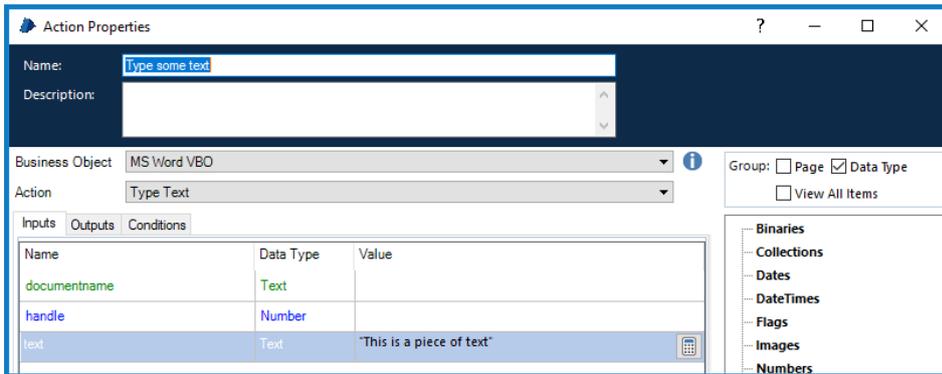
- Click **OK** to save the changes.
- Repeat these steps for each for the remaining three stages using the following details.

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

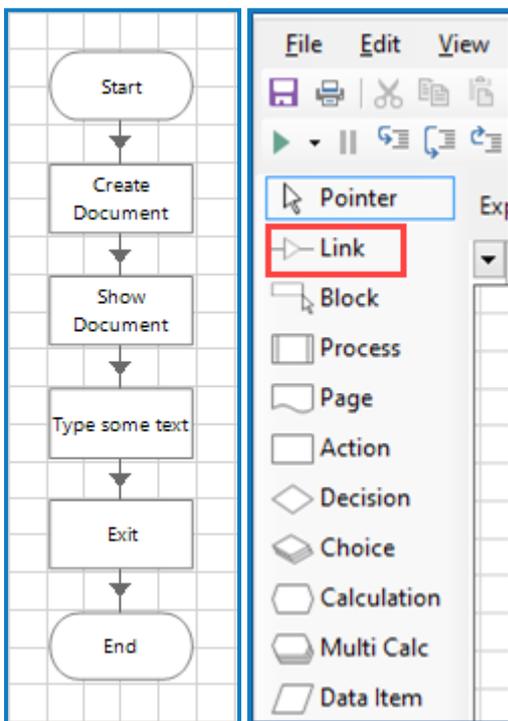


- Double click **Type some text** stage.
- Select the **Inputs** tab.

- 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.



- Click **OK** to return to Process Studio.
- From the toolbar select the Link tool and connect each of the stages in turn by dragging from one stage to the next.



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

### 3. 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.

## Verify software versions

### Verify the Blue Prism Enterprise version

The Blue Prism Enterprise version information displays in the application under **Help > About**.

### 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: [How to: Determine which .NET Framework versions are installed](#).

## Troubleshoot an installation

The following sections 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.

### 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*

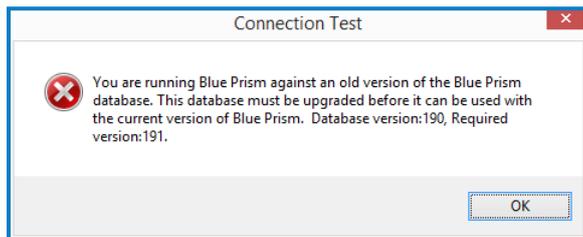
### *Provider, error: 40 - Could not open a connection to SQL Server)*

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 databases 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

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.

## Application server

### Application server configuration

#### The Windows Service cannot start

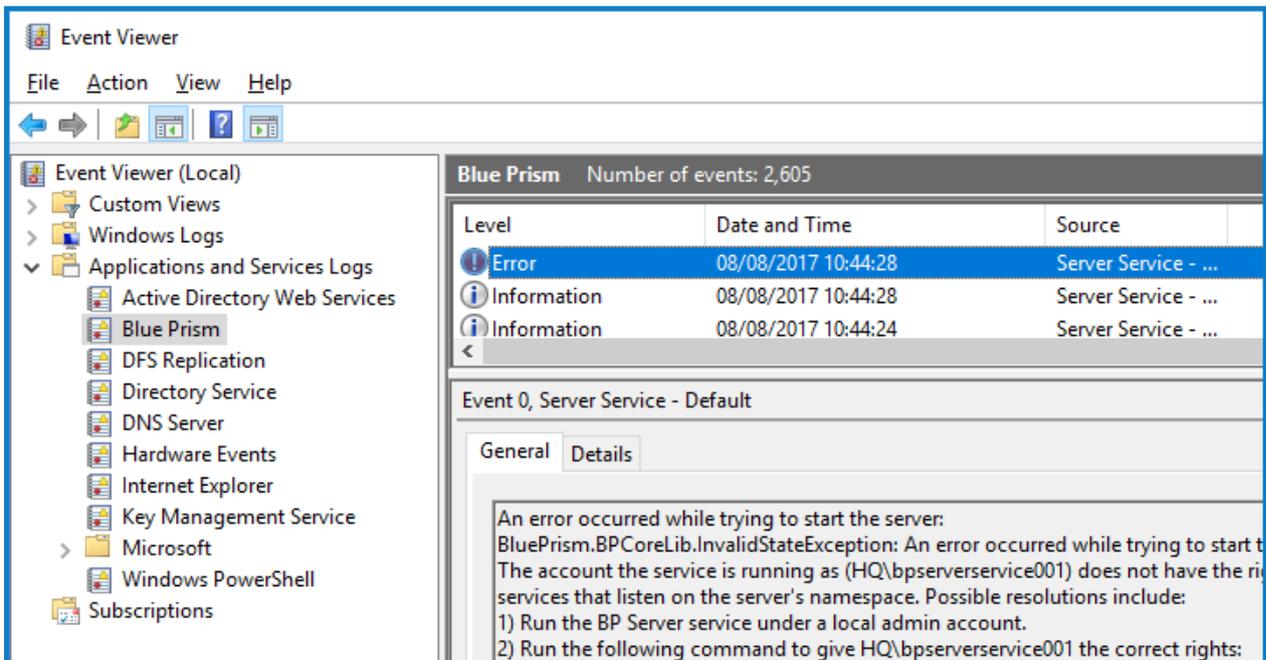
If the Windows service will not start or starts and immediately stops, this indicates that there is a problem with the configuration of the server.

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 behavior seen here can differ in comparison 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.

### 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.

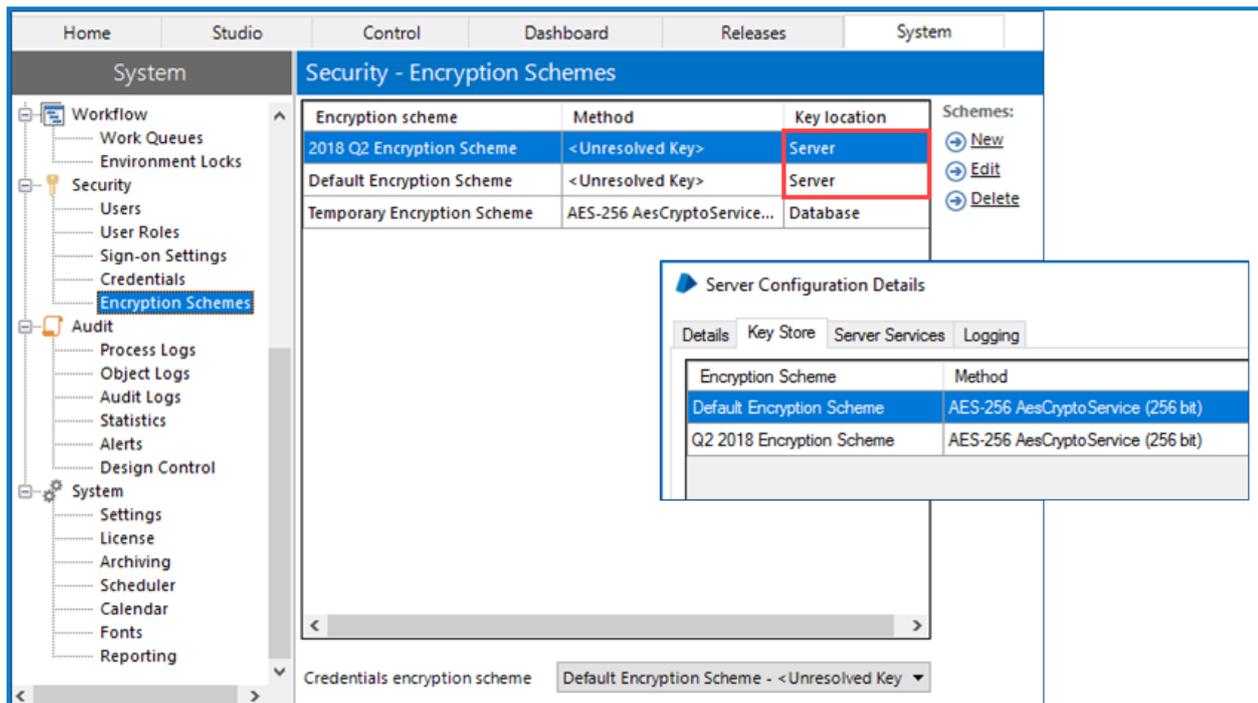
A new license key can be installed via the Blue Prism user interface. It may be necessary to use a client that has a direct database connection to carry out this action.

### 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\bpserver-service001) 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.

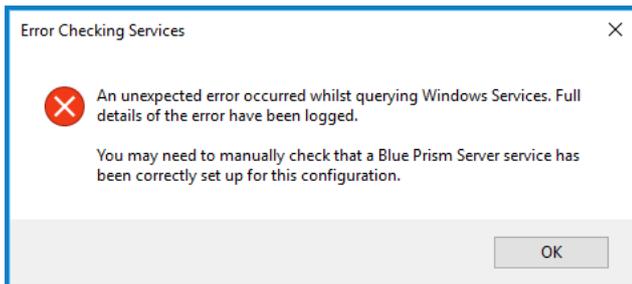
To resolve the issue either:

- Use the Blue Prism Server configuration utility to set up 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.

### Encryption certificate cannot be found

If the certificate used for encryption cannot be accessed or restored the following message displays: *The certificate used for encryption of the server configuration cannot be found. Please add the certificate with the correct thumbprint to the certificate store.*

In this situation, the user configuring the Blue Prism server will need to recreate the server configuration profiles. To do this, delete the Automate.config file, which is located in: ProgramData\Blue Prism Limited\Automate V3. A new Automate.config file will be automatically created when the BPServer.exe is launched. An encryption scheme and new certificate can then be applied to the new server configuration file.

### Service Principal Name (SPN) configuration for Kerberos authentication

#### Verify that DNS lookup is working

1. Check the hostname of the configured Blue Prism Server on the Connection Configuration screen in the Blue Prism interactive client.
2. Perform a forward DNS lookup from the Blue Prism interactive client: `nslookup <BP Server hostname>`

This will return the FQDN to use in the SPN registration.

If this is not working, please contact your internal IT Team to troubleshoot further.

#### Verify that the SPN has been registered correctly

1. Open Command Prompt as an administrator and run the command `setspn -L ACCOUNT_NAME .`  
This will list the SPNs registered for the account that you specified during the [SPN registration](#).
2. Confirm that the returned SPN is the same as the one registered, which should be in the following format: `<service class>/<host>:<port>/<service name>`

Where:

- `service class` is HTTP. This should NOT be changed to HTTPS.
- `host` is the FQDN of Blue Prism application server, for example `appserver.bpdomain.local`
- `port` is the port the Blue Prism Application server is running on. The Default = 8199
- `service name` is the BP Server

It is important that the SPN is configured exactly as outlined in [SPN configuration](#) to function correctly. SPNs should be unique in the Active Directory forest but under some circumstances duplicates may exist. To check for duplicate entries you can use `setspn -F -Q */BPserver`. This will list all SPN entries in the forest that contain 'BPserver'. If there is more than one entry, this can be removed by running the command `setspn -D SPN_NAME ACCOUNT_NAME`.

## Verify Kerberos service tickets

If the SPN is registered to the correct account it should be possible to use `klist` from a non-elevated command line to check that a Kerberos service ticket can be obtained.

This can be done by:

- Purging the Kerberos tickets using `klist purge`.
- Running `klist get SPN_NAME`, for example, `klist get HTTP/appserver.bpdomain.local:8199/BPServer` on the client machine to obtain the output below. If the SPN is in a different realm from your user, you can test by running `klist get SPN_NAME@KERBEROS_REALM`.

Example Kerberos service ticket:

```
Client: testuser @ BPDMAIN.LOCAL
Server: HTTP/appserver.bpdomain.local:8199/BPServer @ BPDMAIN.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent ok_as_delegate
name_canonicalize
Start Time: 1/11/2022 12:00:00 (local)
End Time: 1/12/2022 22:00:00 (local)
Renew Time: 1/18/2022 12:00:00 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x200 -> DISABLE-TGT-DELEGATION
Kdc Called: dc1.bpdomain.local
```

The Kerberos service ticket can be identified by checking the "Server:" section in the above example. If a Kerberos service ticket for the registered SPN is NOT returned, please check that the previous steps have been followed correctly.

If you have followed the steps above, and are still unable to return a Kerberos ticket for the registered SPN, you will need to contact your internal IT Team to investigate further, as Windows Kerberos authentication is not functioning as expected.

If you can successfully return a Kerberos service ticket for the registered SPN, but the issue is not resolved, please see the section [below](#).

## RC4 Encryption

In the example above, the Kerberos service ticket has a base Encryption type of RC4 which is considered to be a vulnerable cipher and is not recommended for use.

In some environments, RC4 tickets may be generated, but rules preventing the client from accepting and using such a Kerberos ticket may have been enabled.

If you see RC4 tickets being generated like in the example above, please contact your Internal IT Teams to ensure that the service account's Kerberos authentication mechanism is able to use RC4, or has AES encryption enabled. The Kerberos authentication type can be identified by checking the KerbTicket Encryption Type section in the example above.

## Application server connection

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 resolvable (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.

## Connecting to the database

Review the [Database Connectivity](#) troubleshooting section 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.

## Runtime resources

### 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 log into 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.

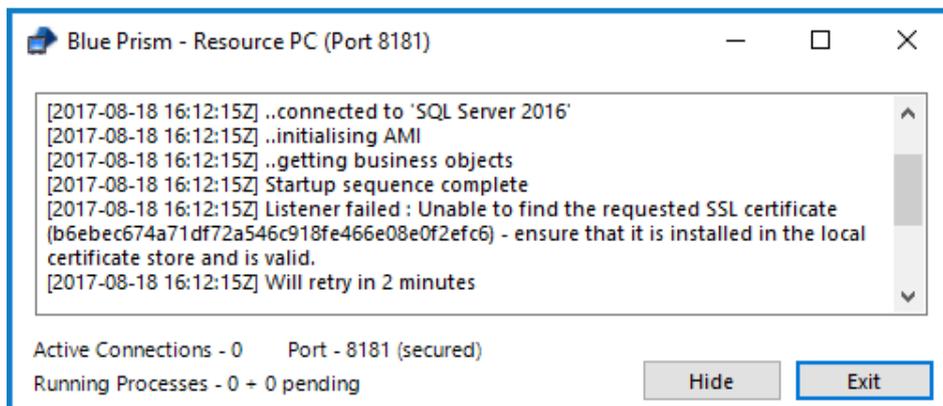
Blue Prism may also forcibly prevent a connection if the runtime is connected to one environment (such as Production: Finance), but the Control Room is connected to a different environment (such as Production: Ops)

### 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*



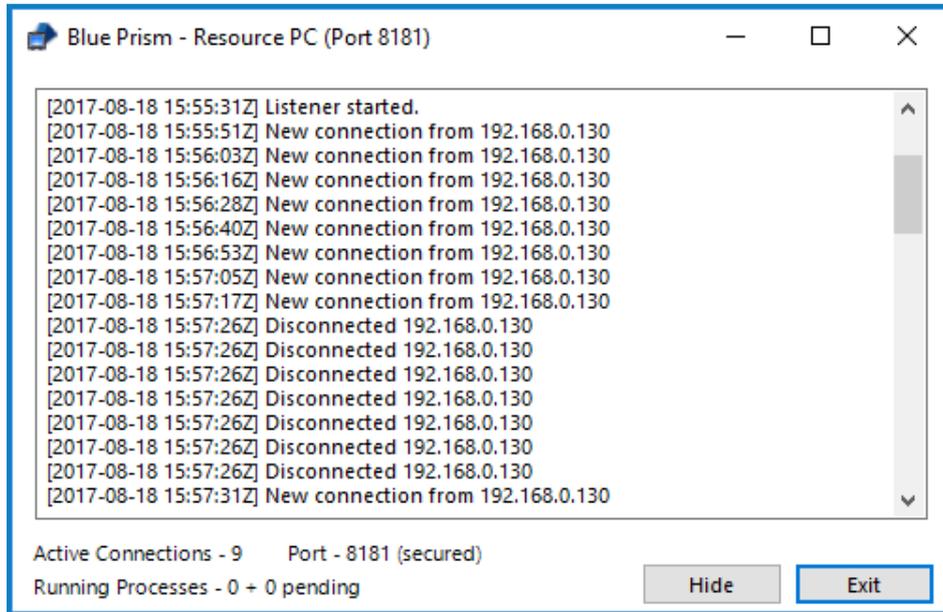
In order to address errors that state that the certificate cannot be found, it is necessary to ensure that the certificate has been installed on the local machine (within the computer account) and that the thumbprint has been set correctly.

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



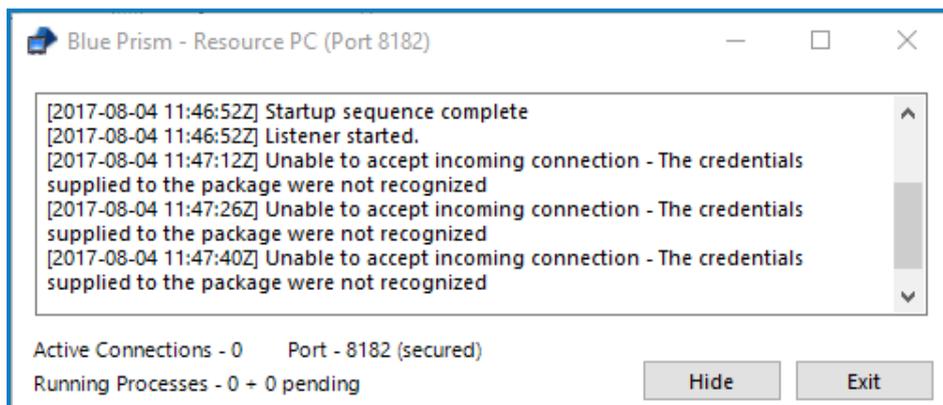
To address this type of issue is necessary to ensure that:

- 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.

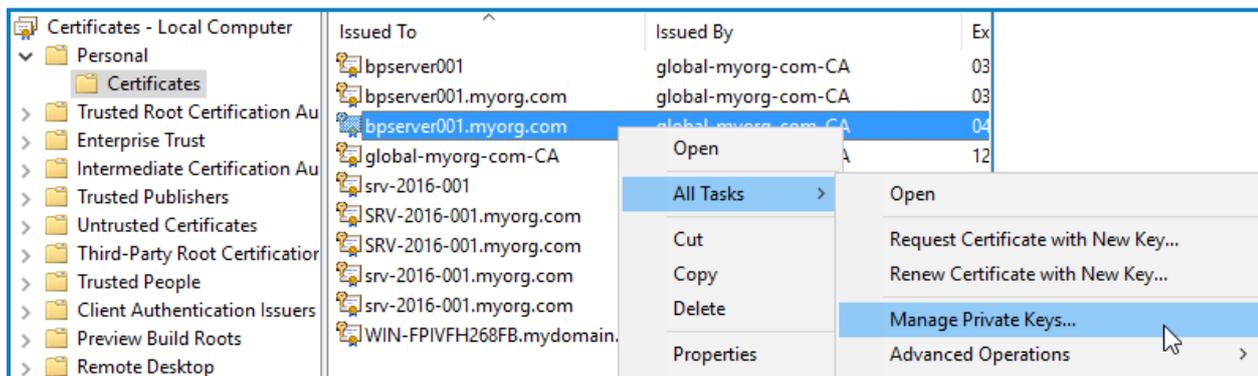
To diagnose and resolve this issue, start the runtime resource from an elevated command prompt. For example: start command prompt as an administrator and use it to launch a runtime resource using the same switch configuration.

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).