blueprism®

Robotic Process Automation Software

Installing v5.0 Enterprise Edition

USER GUIDE

Version: 5.0.30

For more information please contact:

info@blueprism.com | UK: +44 (0) 870 879 3000 | US: +1 888 757 7476

www.blueprism.com

Contents

1. Introduction

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

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

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

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

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

1.1. Related Documents

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

Document Title	Description
Blue Prism Infrastructure Reference Guide	A detailed overview of Blue Prism infrastructure templates, including architectures, failover and DR strategies, communication methods and virtualization requirements
Blue Prism User Guide - Setting up the Java Access Bridge	A detailed overview of the steps required to install the Access Bridge using the installer and manually, along with methods for verifying the installation.
Blue Prism Data Sheet - Active Directory Integration	A guide to integrating Blue Prism with Active Directory for user authentication

2. Quick Start Guide

This chapter provides the steps to be followed to carry out a simple install of Blue Prism.

It is strongly recommended that the **Blue Prism Infrastructure Reference Guide** be reviewed prior to starting the deployment as it contains detailed guidance and considerations on a range of topics in relation to the environment. Additionally it details each of the Blue Prism components and provides a series of architectural options and it is important that the scale and type of the deployment is identified prior to continuing.

As a minimum it is recommended that the following questions have been answered prior to commencing with the installation:

- How many of each type of Blue Prism component are required?
  (Is a standalone PC deployment appropriate for the environment)
- Is this environment for Dev/Test or Prod?
- Will the Blue Prism components be installed into an Active Directory Domain?
- Will the environment be integrated with Active Directory for Single Sign-on?
- Where will the database be hosted?
- Which components, if any, will be virtualized?
- What type of authentication will be used to log the Blue Prism Runtime Resources on to the network, and will this log on action be automated?

Administrative access will be required for each machine or device that will be configured (physical or virtual). Additionally each must be pre-configured with:

- An appropriate operating system.
- A supported Microsoft .NET Framework version.

Review the **Supported Software** chapter within the **Appendix** for details of the supported operating systems and .NET Framework versions.

Guidance on **Verifying the .NET Framework Version(s)** can be found within the **Appendix**.

2.1. Deployment Overview

This chapter provides an overview of the steps required to carry out two different types of installation:

- Standalone Deployment
- Typical Deployment

2.1.1. Standalone Deployment

Suitable only for non-production, short-term use, the minimum required Blue Prism components are deployed to a single machine.

For non-production environments, a minimum of one device is required as components can be co-hosted, although it is typically recommended that a minimum of two resources are deployed:

- **Target Machine:** On which to install Blue Prism
- **SQL Server:** Where the Blue Prism database will be located.
  A SQL Server instance must be pre-configured prior to the installation of Blue Prism. For short-term use, it is often common for a local install of SQL Server Express to be used to host the database.

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

Preparation

1. Ensure a SQL Server instance is available that is supported by Blue Prism
2. Ensure the machine where Blue Prism will be installed meets the collective minimum specification for the Interactive Client, Application Server and Database Server
3. If using Microsoft SQL Azure, ensure an Azure database is available and that it is configured to accept connections from this platform.

Standalone
Blue Prism Deployment

Install and configure the first Blue Prism component

4. Install Blue Prism
5. Configure a Blue Prism connection to the SQL Server Instance
6. Create a Blue Prism SQL Server Database
7. Login and Set the Admin Password
8. Install the Blue Prism License Key
9. Configure an Encryption Scheme
10. Verify the Blue Prism Deployment

Further information on each of the steps above can be found within the **Step-by-step Installation** chapter.

If problems are experienced whilst installing, review **Troubleshooting an Installation**.

2.1.2. Typical Deployment

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

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.

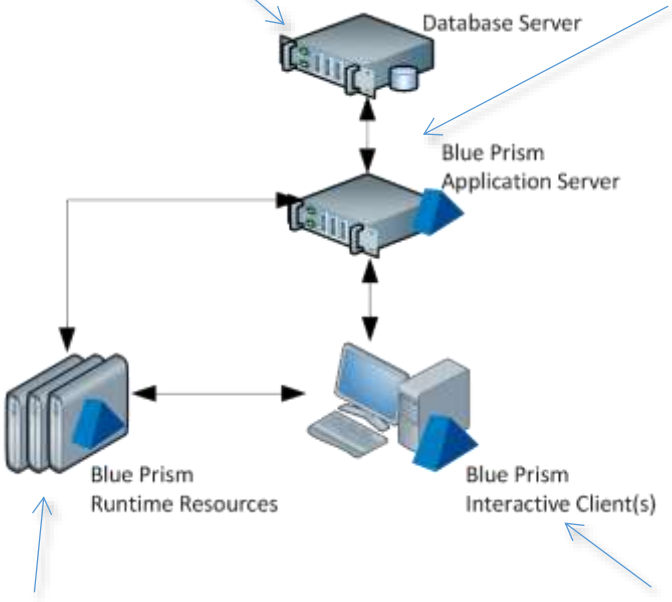
Most deployments will feature various numbers of each type of component. Factors to consider include:

- The type of environment (e.g. a Development environment may have a small number of Runtime Resources (robots) and an Interactive Client per developer; whilst a Production environment is likely to have a higher number of Runtime Resources (robots) and only a few Interactive Clients – one per controller).
- The number of Runtime Resources (robots) being deployed
- Application Servers and SQL Servers are commonly shared between environments (e.g. a single Application Server may host a service for Development and Test environments and be responsible for providing connectivity to the appropriate database).
  The Blue Prism Application Server chapter provides detailed information on how to achieve this.

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

Preparation

1. Ensure a SQL Server instance is available that is supported by Blue Prism
2. Ensure the machine where Blue Prism will be installed meets the collective minimum specification for the Interactive Client, Application Server and Database Server
3. 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 first Blue Prism component

4. Install Blue Prism
5. Configure a Blue Prism connection to the SQL Server Instance
6. Create a Blue Prism SQL Server Database
7. Login and Set the Admin Password
8. Install the Blue Prism License Key
9. Configure an Encryption Scheme
10. Verify the Blue Prism Deployment

Blue Prism Application Server

11. Configure the Server Profile
    Create a Blue Prism Server Profile which uses the configured SQL connection
12. Register and Configure a Windows Service (including defining the logon and start-up properties of the Blue Prism Server Profile)
13. Optionally disable the setting to "Start the process engine on this machine automatically"

Blue Prism Interactive Client (for each)

14. Install Blue Prism
15. Configure a Blue Prism Connection to the Blue Prism Application Server
16. Optionally disable the setting to "Start the process engine on this machine automatically"
17. If used to develop and configure processes, access will also be required from this device to all appropriate third-party applications that will be automated.

Blue Prism Runtime Resource (for each)

18. Install Blue Prism
19. Configure a Blue Prism Connection to the Blue Prism Application Server
20. Assign a user account to the device and configure the user profile
    (including configuring remote access settings).
21. Verify connectivity to line of business applications.
22. Configure the Runtime Resource to start automatically when the device is logged in.

Further information on each of the steps above can be found within the **Step-by-step Installation** chapter.

If problems are experienced whilst installing, review **Troubleshooting an Installation**.

3. Step-by-step Installation

The chapters within this section provide guidance on installing and configuration various Blue Prism components.

Irrespective of the component being installed, it is important that before component specific configuration takes place within an environment, that the first instruction for **Installing and configuring the first Blue Prism component** takes place.

The **Quick Start Guide** section provides an overview of the steps required to configure Blue Prism and references the various chapters within this section including:

- Installing and configuration of the first Blue Prism component
- Blue Prism Application Server
- Blue Prism Interactive Client
- Blue Prism Runtime Resource

3.1. Install and configure the first Blue Prism component

For standalone deployments, this will be the only component, however for a typical Blue Prism deployment, this will typically be the Blue Prism Application Server component.

The same installer is used irrespective of the type of Blue Prism component being deployed.

3.1.1.1. Install Blue Prism

Locate and run the appropriate installer depending on whether you wish to install a 32-bit or 64-bit version. Review the **Supported Software** chapter within the **Appendix** for details of which versions are supported for the operating system and whether you intend to set up an Interactive Client, Resource or Server.

- 32-bit Installer: BluePrism5.0.nn_x86.msi
- 64-bit Installer: BluePrism5.0.nn_x64.msi

When the installation is complete, start the Blue Prism application.

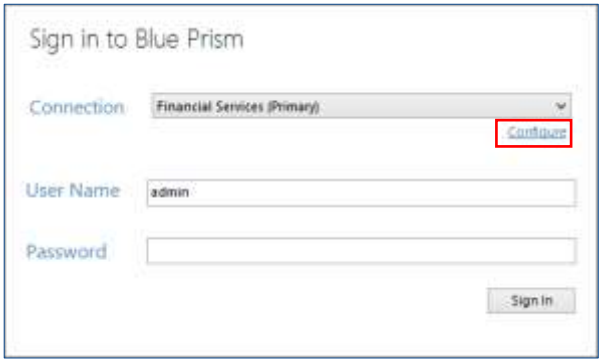
3.1.1.2. Configure a Connection to the Database

When Blue Prism is launched for the first time it is necessary to specify the database connection details. The connection details describe how Blue Prism will connect to the database.

Typically the Blue Prism Application Server component(s) will have a connection which connects directly to the SQL Server and database, whereas subsequent components (Interactive Clients, Runtime Resources etc.), will connect to the Application Server.

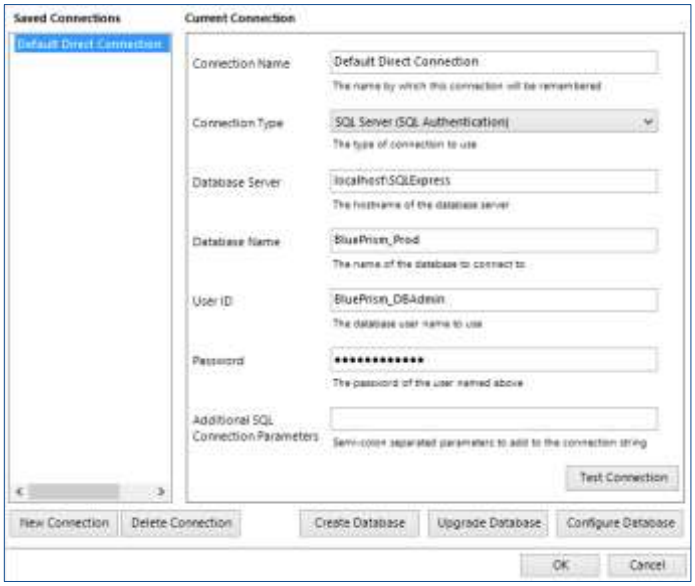
These instructions provide guidance on creating a **direct connection** to the SQL database server.

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



a. The Connection Configuration window is now displayed.

Enter the connection details for the database that will be used.
If the database does not exist, and permissions allow, Blue Prism can create it.



Enter the details as below:

Connection Name:	**Default Direct Connection**
Connection Type:	**SQL Server (SQL Authentication)** - Select the appropriate connection type based on the security settings of the SQL Instance (further guidance is provided within the **SQL Database Guide**).
Database Server:	**localhost\SQLExpress*** - The path specified is the default path when SQL 2008 Express is co-located on the same machine as Blue Prism. A different path may be required if a default install of SQL 2008 Express is not being used or if it is installed in a different location.
Database Name:	**BluePrism** - this is the name of the database that will be created later – this can be set to a custom name if required.
User ID:	**BluePrism_DBAdmin** - The username configured in SQL for authenticating with the database (only required for connection types of SQL Authentication).
Password:	******* - The password for authenticating with the database (only required for connection types of SQL Authentication).
Additional SQL Connection Parameters	[Blank] – this field can be populated 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.

See the details overleaf for example information to use when connecting to **Microsoft SQL Azure**.

If using Microsoft SQL Azure, the connection details provided within the Azure database configuration area should be used. Example settings (ADO.NET) are provided below:

Connection Name:	Default Direct Connection
Connection Type:	SQL Server (SQL Authentication)
Database Server:	e12n3456.database.windows.net,1433 - The path of the database server can be obtained from within the SQL Azure portal.
Database Name:	BluePrism
User ID:	authUser@e12n3456
Password:	*******

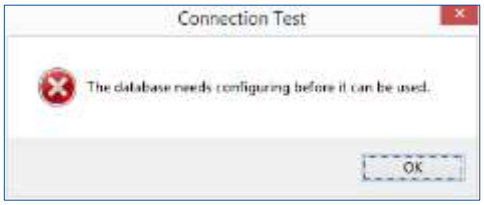
2. Click **Test Connection**.
If a connection can be established with the SQL Server, commonly one of the following messages will be presented.

   a. **Database does not exist**
   This indicates that the database has not yet been created.

   Press **OK** to clear the message, and press **Create Database**. Follow the **Creation** actions within the following section: **Create or Configure a Database**

   b. **Not a valid Blue Prism Database**
   This indicates that the database exists, 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.

   Press **OK** to clear the message, and press **Create Database**. Follow the **Creation** actions within the following section: **Create or Configure a Database**



   c. **Database needs configuring**
   This indicates that the database exists and that the schema has been applied but that there is some further in-product configuration that is required. This would typically be the case where the database has been manually created and has had the Blue Prism schema applied via a manually executed script.

   Press **OK** to clear the message, and press **Configure Database**. Follow the **Configuration** actions within the following section: **Create or Configure a Database**

   d. **Other Messages**
   If alternative messages are presented please refer to the section on Troubleshooting an Installation in this guide.

A detailed version of the step by step guide to configuring a connection to the database can be found in the **Appendix** under **Configuring a Connection to the Database**.

3.1.1.3. Create or Configure a Blue Prism Database

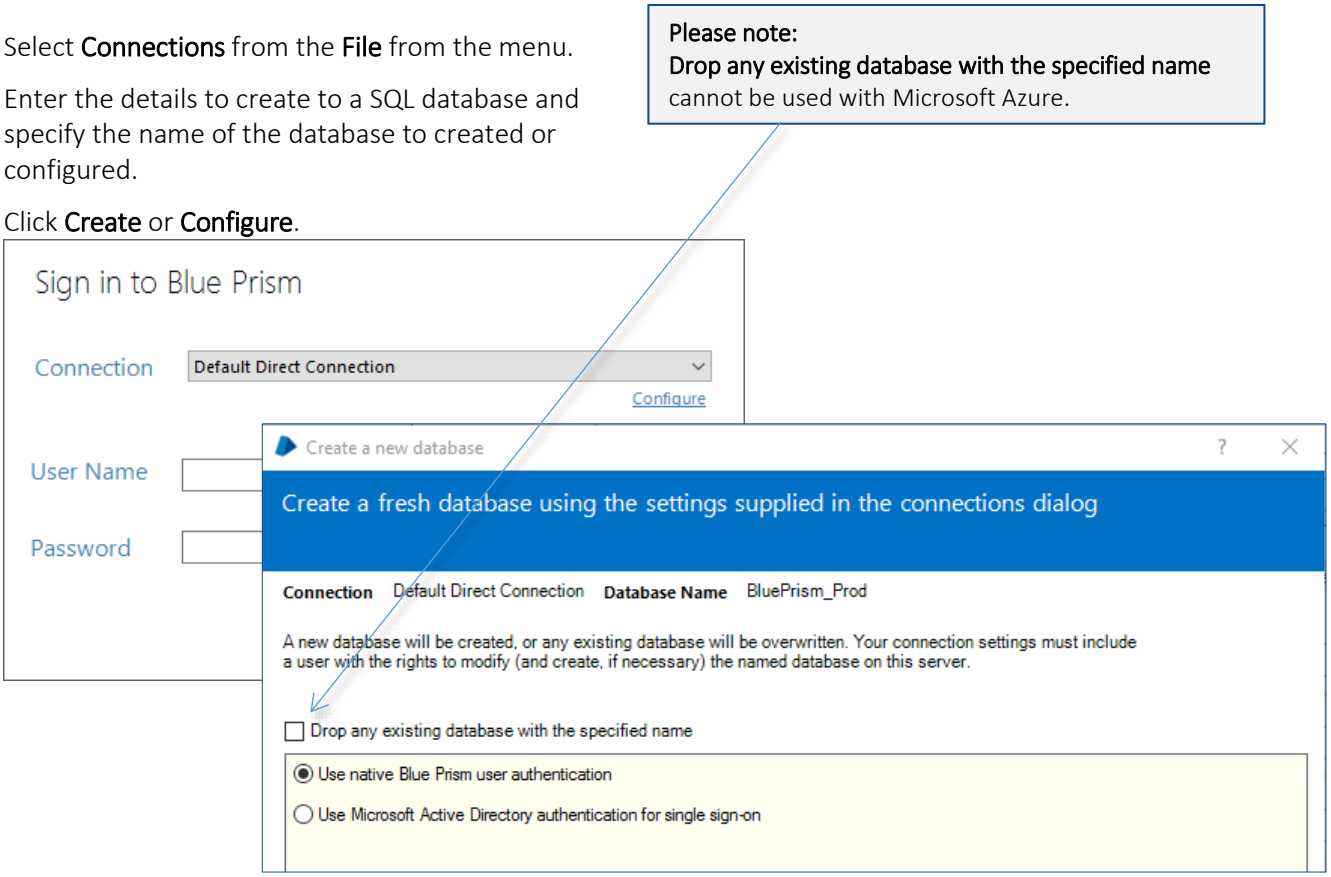
Once the connection has been created, the Blue Prism database will need to be configured. There are three stages:

1. **Database Creation**: A SQL Server database must be created. This can either be achieved manually or through use of the in-product **Create Database** action.
2. **Application of the Database Schema**: The database schema must be applied to the created database. This is best achieved through use of the in-product **Create Database** action, or manually by applying the CreateScript.sql. By default, if the database already exists, the schema will be applied to the pre-existing database.
3. **Configuration Options within the Database**: A number of configuration options are applied to the database. These are applied automatically when using the in-product **Create Database** action. If the database has been created and had the schema applied manually the **Configure Database** action must be used.

Where the database has not yet been created, or where the database exists but has not had the schema applied the **Create Database** feature should be used.

Where the database has been created and had the schema applied, the **Configure Database** features should be used.

1. Select **Connections** from the **File** from the menu.
2. Enter the details to create to a SQL database and specify the name of the database to created or configured.
3. Click **Create** or **Configure**.



4. Complete the default settings.
5. Click **OK** to create and configure the database.

If the implementation is to be integrated with Active Directory, this must be configured now by selecting the option to **Use Microsoft Active Directory for single sign-on**.
A detailed step by step guide can be found in the section entitled: **SQL Database Guide**

3.1.1.4. Set the Admin Password

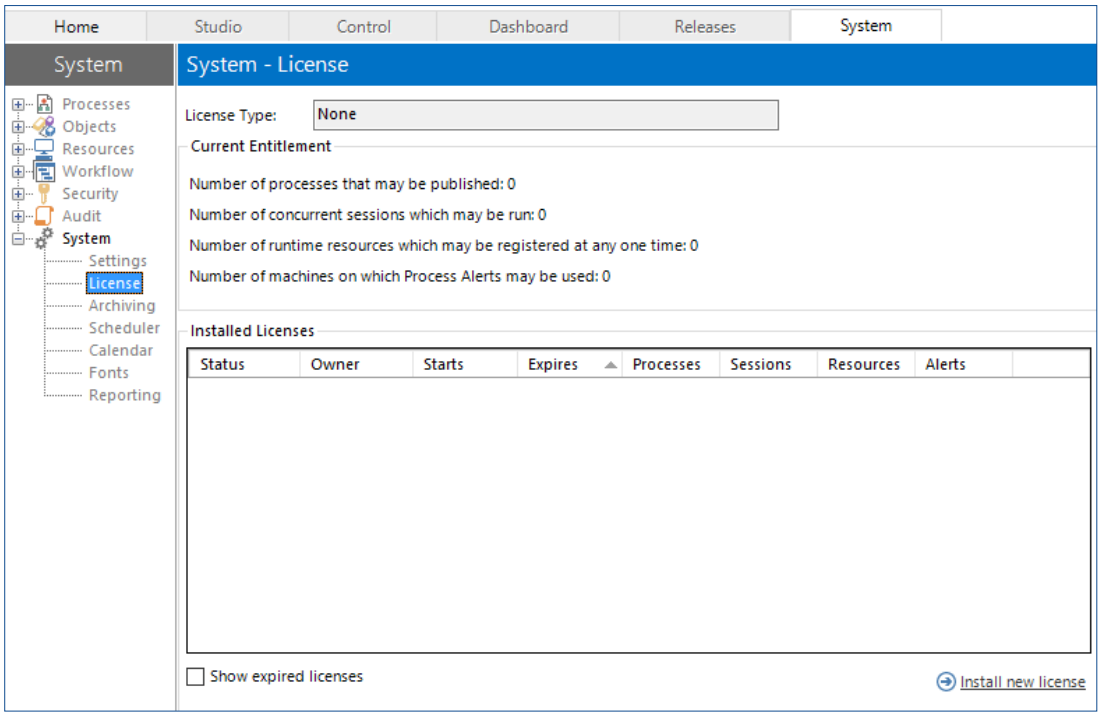
When a new Blue Prism database is created, a single user is created with the credentials:
Username: admin
Password: admin

Launch Blue Prism and log in using the above credentials. You will be prompted to change the admin password – enter a secure password and make a note of it.

3.1.1.5. Install the License

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

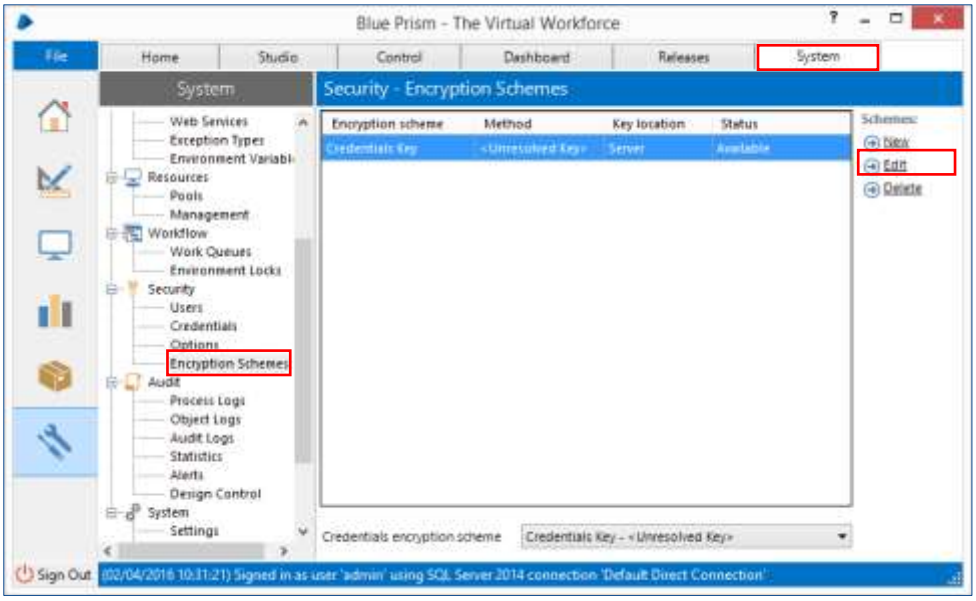
1. Launch Blue Prism.
2. Click System Manager.
3. Click the **System** menu item.
4. Click the **License** tab.
5. Select **Install new licence.**
6. Select the License file and click **OK.**



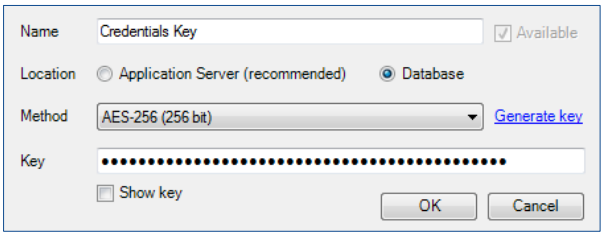
3.1.1.6. Configure an Encryption Scheme

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

1. Click **System**.
2. Under Security, click **Encryption Schemes.**
3. Click the scheme named **Credentials Key** and click **Edit.**
4. Follow the steps below as appropriate.

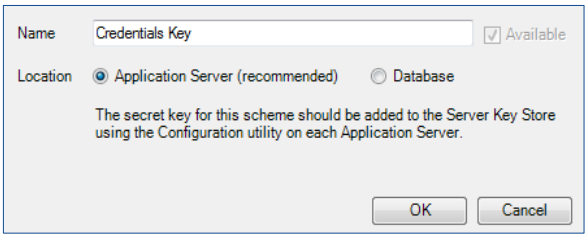


Standalone Blue Prism Deployment



1. Select Database
2. Select **AES-256**
3. Click Generate Key
4. Click **OK**

Multiple Component (App Server) Deployment



1. Select **Application Server**
2. Click **OK**

> 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.

3.1.2. 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.

A step by step guide to **Verify an Installation** can be found within the **Appendix.**

3.1.3. Setup role specific configuration

Finally it is necessary to configure the device to have the appropriate settings and configuration for its specific within the deployment.

- If this installation is for a **standalone Blue Prism deployment** without an Application Server – the installation is now complete.
- If a multiple component deployment is being configured, the configuration for the component being setup must now be followed. Typically the first component to be configured will be a **Blue Prism Application Server**.
  See the chapter on **Blue Prism Application Server** for more information.

Instructions on provisioning additional Blue Prism Components are also provided within the subsequent chapters.

3.2. Blue Prism Application Server

There are a number of steps to configure the installation to take on the role of a Blue Prism Application Server.

Whilst it is typical for a single Blue Prism Application Server instance to be configured, there is the option to co-host multiple Application Server instances on a given server. (E.g. a separate Application Server instance could be configured and co-hosted for the development environment and the test environment within a single install of Windows Server).

The following key steps are required to provision each Blue Prism Application Server service:

1. Verify that the database settings have been configured for the environment and that Blue Prism has been installed on the device.
2. Configure the service using the BPServer.exe tool.
3. Register a **Windows Service** that references the above service configuration.
4. Configure the start-up and logon settings for the Windows Service.

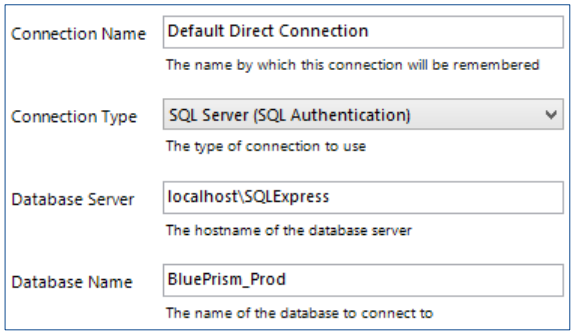
Administrator access will typically be required to complete these steps.

> The Blue Prism Server window service which is installed by default **should not** be removed however it can be disabled if it is no longer required.

3.2.1. Verify that the database settings and that Blue Prism has been installed

Prior to configuring a Blue Prism Application Server it is necessary to first ensure that Blue Prism has been installed on the device being configured and that a Blue Prism database connection has been configured on this machine for the environment. Also ensure that for this environment the Create Database action has been completed.

On the device hosting the Blue Prism Application Server the Blue Prism connection is typically direct to the database.

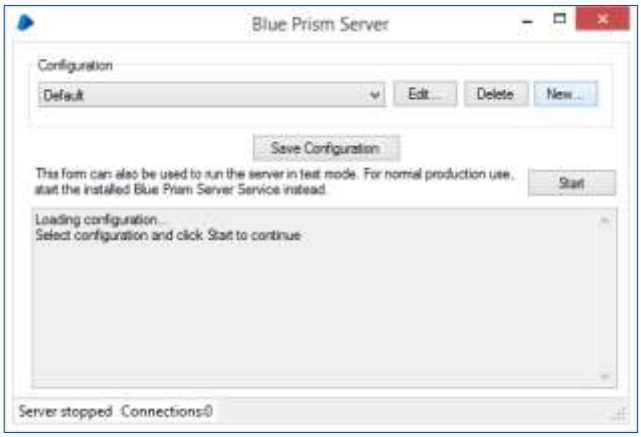


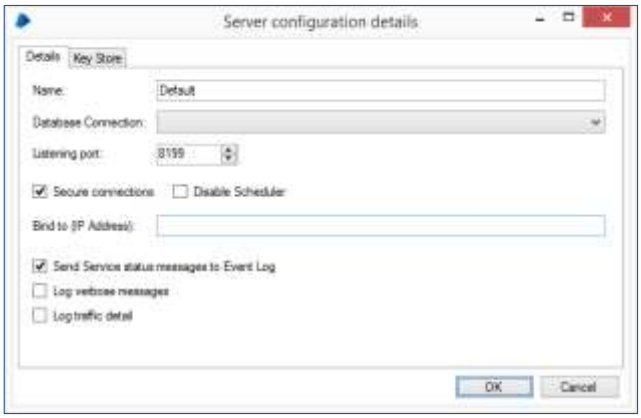
3.2.2. Configure the Server Service Profile(s)

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 service configuration includes:

- Defining the port on which it will operate.
- Specifying database connection information.
- Configuring a credentials key which is used for all data encryption in that environment.

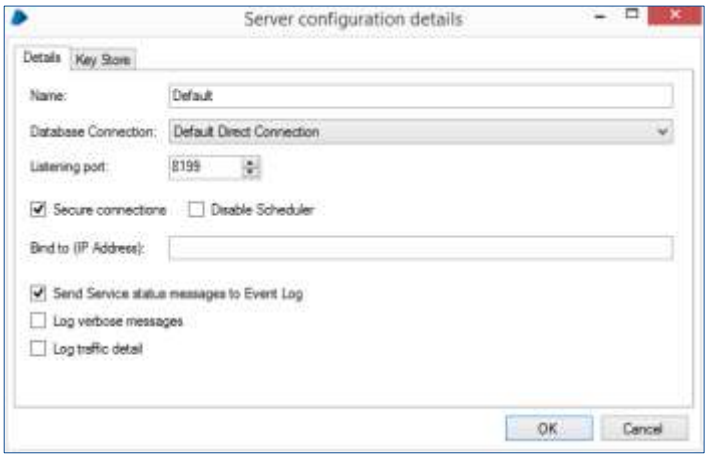
1. Navigate to the Blue Prism installation directory, typically C:\Program Files\Blue Prism Limited\Blue Prism Automate and launch **BPServer.exe**.
   Click **New** to create a server configuration.



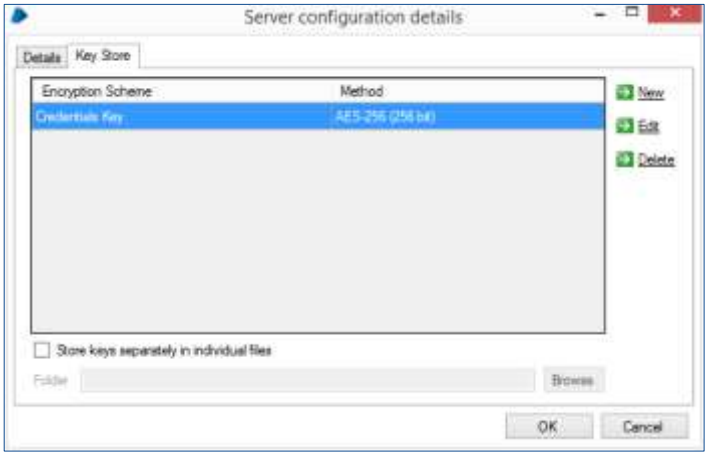


2. Enter the **name** to be used for the configuration.
   If configuring a single Blue Prism Application Server service on a given server, it is recommended that the server configuration should be named: **Default**.

3. Select the database connection that the server should use. The port can usually be left as the default for a single server, but can be altered if necessary here.



4. Select the **Key Store** tab and click **New**. Enter **Credentials Key** as the scheme name (to match the one configured under **Encryption Schemes** within the Blue Prism client).
If this is the first Application Server that is being configured for the environment, select **AES-256** as the encryption method and click **Generate Key** followed by OK.



If an Application Server instance has already been setup for this environment enter the Credentials Key used for the other Application Server - this key is used to encrypt credentials in the Blue Prism Credentials handling so it is important that all servers servicing the same database and environment use the same key.

> 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.

Note: If setting up a failover or replacement Blue Prism Server for an existing database environment then you should specify the same key being used on the existing Blue Prism Server.

5. **Use secure connections** can ONLY be ticked if all Blue Prism components will be installed within a single Active Directory network infrastructure. E.g. within a single domain, or within a series of trusted domains. If the components are to be deployed within segregated domains, or within a workgroup, **Use Secure Connections** must be un-ticked.
   Secure connections **MUST** be ticked if using Active Directory integrated authenticated for Blue Prism – using AD integrated authentication over an unsecure connection will mean that the platform will not be able to correctly apply the users permissions.

6. If the server is running on a machine with multiple IP addresses, enter the address which the server should listen on for Blue Prism Resource / Client connections.

   Where multiple Application Server services are to be co-hosted on a single operating system, create multiple profiles ensuring that the **Listening port** and **Bind to (IP Address)** combination is unique for each environment.

   To enable status messages to be sent to the Windows Event Log, tick the checkbox at the bottom of the form. When expecting to run the BP Server as a service, this is the only way that diagnostic messages will be recorded, so it is advisable to set it.

   When configuration for the individual service is complete, click **OK**, then click the **Save Configuration** to save all server configurations to a local location.

3.2.3. Register and Configure a Windows Service

As part of the Blue Prism installation, a **Blue Prism Server** Windows Service is automatically registered for a server configuration named **Default**. Therefore if this corresponds to the name chosen for the configuration above, no further action is required to register the service.

If the server has been configured with a name other than **Default**, it is necessary it manually register a Windows Service for each configuration.

3.2.3.1. Setup the Windows Services

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

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

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

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

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

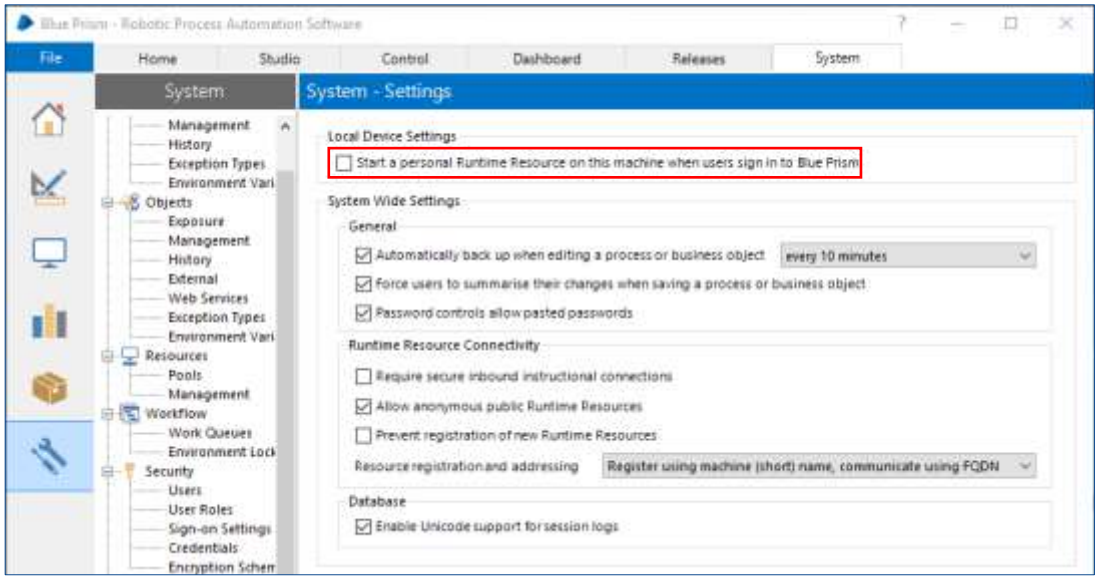
Where the server configuration name contains spaces, it is necessary to use a backspace as an escape character. The example below shows the setup where the server configuration name is “Development Environment”

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

3.2.4. Optionally disable the automatic initiation of a Runtime Resource

It is not very common for a user to log into Blue Prism directly on the Application Server, however if they do it is unlikely that they will want to be able to run processes directly on the Blue Prism Application Server however there is a default setting that will automatically start a Runtime Resource on this machine if a user does log in.

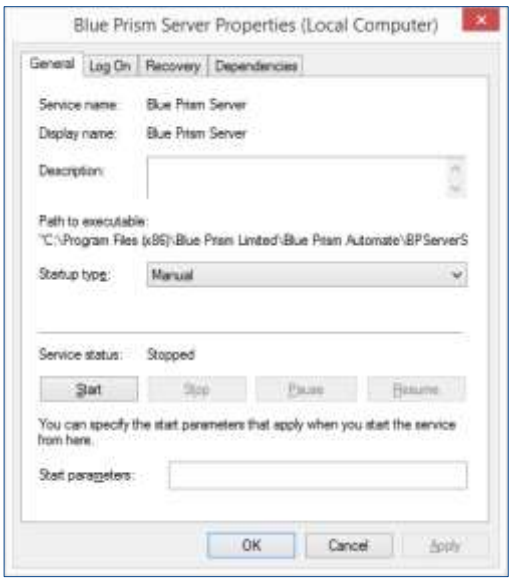
This setting can be disabled within the System tab.



3.2.4.1. Configure the Windows Service

Once created, the Windows Service(s) can be configured as appropriate for the environment. 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 if required. Where Windows Authentication is used for database communication, it is the account specified here that will be used by the service when connecting to the database.



When starting the service, if it won't start or if it stops immediately, it can indicate a configuration problem - there should be a message in Windows Event Viewer, in the Application log which provides additional information about the problem.

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 is likely to be required.

3.3. Blue Prism Interactive Client

The following key steps are required to provision each Blue Prism Interactive Client:

1. Verify that the database settings have been configured for the environment and that Blue Prism has been installed on the device.
2. Ensure the Blue Prism Connection on this machine is to the Application Server (and that the option for Use Secure Connections is appropriate to the deployment).

   Secure connections **MUST** be ticked if using Active Directory integrated authenticated for Blue Prism – using AD integrated authentication over an unsecure connection will mean that the platform will not be able to correctly apply the users permissions.
3. Optionally disable the automatic initiation of a Runtime Resource on this device.

3.3.1. Verify that the database settings and that Blue Prism has been installed

Prior to configuring an Interactive Client it is necessary to first ensure that Blue Prism has been installed on the device being configured and that for the environment the component is being added to, that a Create Database action has been completed.

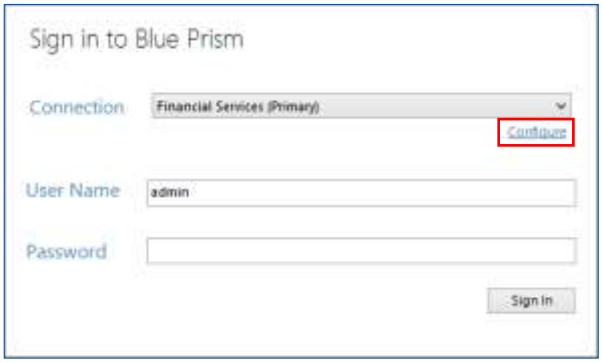
3.3.2. Create a Blue Prism connection via the Application Server

Where a Blue Prism Application Server is being deployed as part of the environment, Blue Prism installations for Runtime Resources and Interactive Clients are typically configured to connect via the Blue Prism Server (rather than directly to the database).

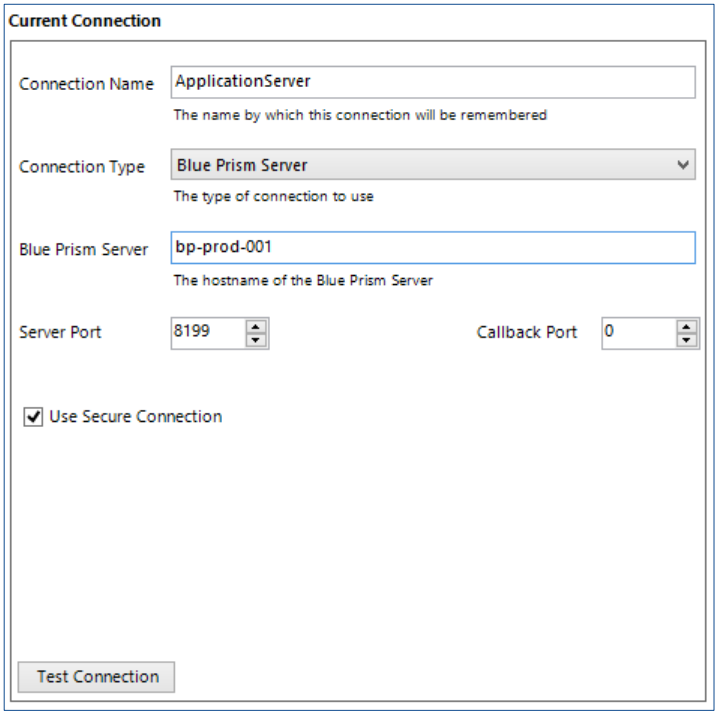
If a Blue Prism Application Server **is not** deployed in the environment the connection will need to be direct to the database.

These instructions provide guidance on creating a **Connection to the Application Server**.

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



2. The Connection Configuration window should now be displayed.



Enter the details as below:

Connection Name:	ApplicationServer
Connection Type:	Blue Prism Server
Blue Prism Server:	[server name of the Application Server]
Server Port	[port that the Application Server is configured to listen on (Default: 8199)
Callback Port	0 (zero is the default and indicates that dynamic ports will be used)
Use Secure Connection	**Use secure connection** can ONLY be ticked if all Blue Prism components will be installed within a single Active Directory domain, or within a series of trusted domains. If the components are to be deployed within segregated domains, or within a workgroup, **Use Secure Connection** must be un-ticked. Secure connections **MUST** be ticked if using Active Directory integrated authenticated for Blue Prism – using AD integrated authentication over an unsecure connection will mean that the platform will not be able to correctly apply the users permissions.

3. Press **Test Connection** to verify the settings are correct.
4. Press **OK** to save the data and return to the Blue Prism client.

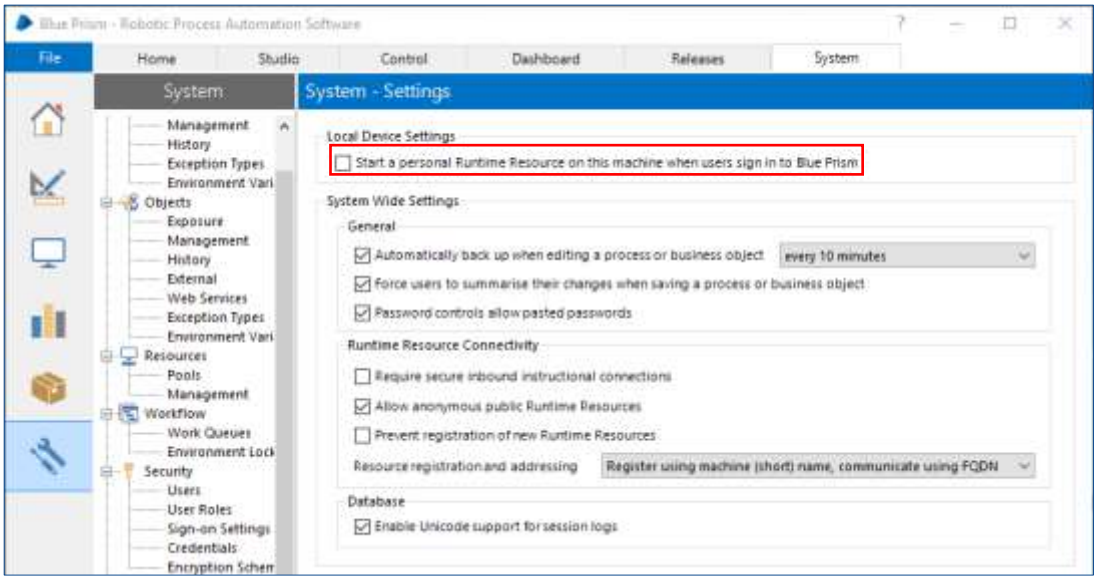
3.3.3. Optionally disable the automatic initiation of a Runtime Resource

Blue Prism Interactive Clients are typically configured differently depending on whether the client will be used for development and/or test purposes.

- Non-Production Environments
  Where an Interactive Client is used for developing processes it will be necessary to ensure that the device has connectivity to the business applications that will be automated as part of a Blue Prism process.
- Production Environments
  Where Interactive Clients are using only for developing and controlling, there may not be a requirement for direct connectivity to the business applications.

  There is a default setting within Blue Prism that will automatically start a Runtime Resource on the same machine as the Interactive Client when the user logs in however this isn't typically appropriate for production environments as processes should only be executed on dedicated Runtime Resources.

  This setting can be disabled within the System tab.



3.4. Blue Prism Runtime Resource

> Before proceeding ensure that the first component for this Blue Prism deployment has already been configured with a connection to a database, and that Blue Prism has been installed onto the device being configured.
> Each Blue Prism component is installed using the same installer.

The following steps are typically required to configure a Blue Prism installation to take on the role of a Runtime Resource:

1. Verify that the database settings have been configured for the environment and that Blue Prism has been installed on the device.
2. Ensure the Blue Prism Connection on this machine is to the Application Server (and that the option for Use Secure Connections is appropriate to the deployment).

   Secure connections **MUST** be ticked if using Active Directory integrated authenticated for Blue Prism – using AD integrated authentication over an unsecure connection will mean that the platform will not be able to correctly apply the users permissions.
3. Assign a user account to the device and configure the user profile (including configuring remote access settings).
4. Verify connectivity to line of business applications.
5. Implement start-up configuration (incl. login and auto-start).

3.4.1. Verify that the database settings and that Blue Prism has been installed

Prior to configuring a Runtime Resource it is necessary to first ensure that Blue Prism has been installed on the device being configured and that for the environment the component is being added to, that a Create Database action has been completed.

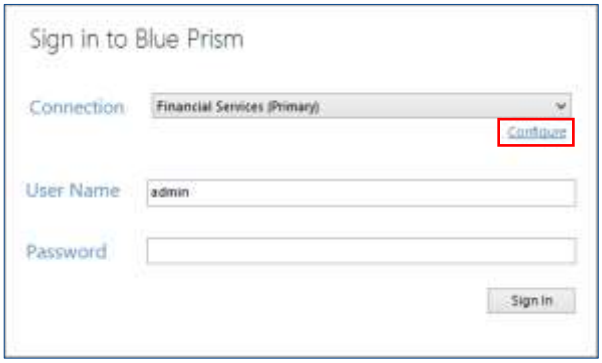
3.4.2. Create a Blue Prism connection via the Application Server

Where a Blue Prism Application Server is being deployed as part of the environment, Blue Prism installations for Runtime Resources and Interactive Clients are typically configured to connect via the Blue Prism Server (rather than directly to the database).

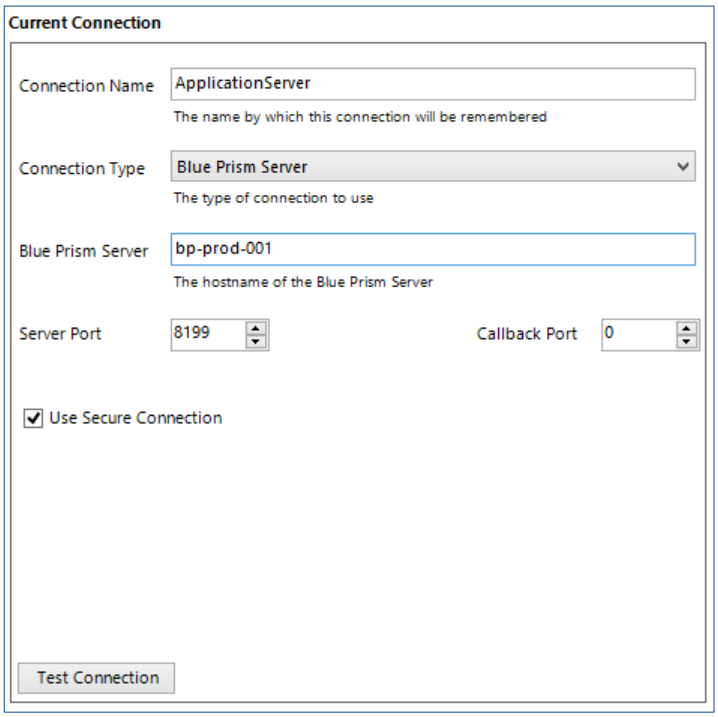
If a Blue Prism Application Server **is not** deployed in the environment the connection will need to be direct to the database.

These instructions provide guidance on creating a **Connection to the Application Server**.

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



2. The Connection Configuration window should now be displayed.



Enter the details as below:

Connection Name:	ApplicationServer
Connection Type:	Blue Prism Server
Blue Prism Server:	[server name of the Application Server]
Server Port	[port that the Application Server is configured to listen on (Default: 8199)
Callback Port	0 (zero is the default and indicates that dynamic ports will be used)
Use Secure Connection	**Use secure connection** can ONLY be ticked if all Blue Prism components will be installed within a single Active Directory domain, or within a series of trusted domains. If the components are to be deployed within segregated domains, or within a workgroup, **Use Secure Connection** must be un-ticked. Secure connections **MUST** be ticked if using Active Directory integrated authenticated for Blue Prism – using AD integrated authentication over an unsecure connection will mean that the platform will not be able to correctly apply the users permissions.

3. Press **Test Connection** to verify the settings are correct.
4. Press **OK** to save the data and return to the Blue Prism client.

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

It is recommended that a user account should be assigned to each Blue Prism Runtime Resource (although it is possible for many devices to share a single network login).

The **Blue Prism Infrastructure Guide** provides a wealth of information in relation to selecting the appropriate type of login account to use and the implications of each.

Once selected, the user profile should be configured to address the considerations referenced within the **Blue Prism Infrastructure Guide**. These include:

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

3.4.4. Verify connectivity to line of business applications

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

Following the install, the **Advanced Topics** should be reviewed for additional information such as the requirement for Blue Prism to interact with Java based applications.

3.4.5. Implement start-up configuration

There are two main actions that are required when a Blue Prism Runtime Resource is started up (such as following a restart):

1. Log on
   A Blue Prism Runtime Resource must be logged in to allow a Blue Prism process to be run. Options may include manually logging into these resources following a reboot, using auto-login, or using Blue Prism Login Agent. Further information is provided within the **Blue Prism Infrastructure Guide**.

2. Start-up Blue Prism
   In order to run Blue Prism in Runtime Resource mode a command line method is used to launch the application to allow it to accept and run processes received from Control Room and the Scheduler. Placing the command(s) in a bat file allows a simple manual start up procedure and also provides the flexibility to trigger the start-up automatically. Further information is provided within the **Blue Prism Infrastructure Guide**.

   The command line method is:

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

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

Multiple Runtime Resources on a single device

Where there is a requirement to configure multiple Blue Prism Runtime Resources on a single device, the start-up configuration can be modified to start up a number of different runtime instances - each configured to operate on a different port.
Further information about this configuration is provided in the **Blue Prism Infrastructure Guide**.

```
automate.exe /resourcepc /public /port 8001
```

```
automate.exe /resourcepc /public /port 8002
```

```
automate.exe /resourcepc /public /port 8003
```

Configure encrypted inbound connections

If an appropriate certificate has been deployed locally on the Resource the /sslcert switch can be used to apply certificate-based encryption to all communication received on the nominated port:

```
automate.exe /resourcepc /public /port 8181 /sslcert [Certificate Thumprint]
```

```
automate.exe /resourcepc /public /port 8181 /sslcert 33a4d8aa6a3d57b04c10eb32278d8a8612ffae9d
```

Configure robot authentication

The Runtime Resource can be configured to authenticate with the environment which is necessary where anonymous public Runtime Resources are prevented.
Use the /SSO switch to authenticate as the logged on user against a single sign-on Blue Prism environment.
Use the /user [usernme] [password] switch to authenticate against a native Blue Prism environment.

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

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

Override the selected connection

If there is a requirement for the Resource to use a specific named connection to the database or application server (such as where callback ports are defined statically), the /dbconname switch can be used:

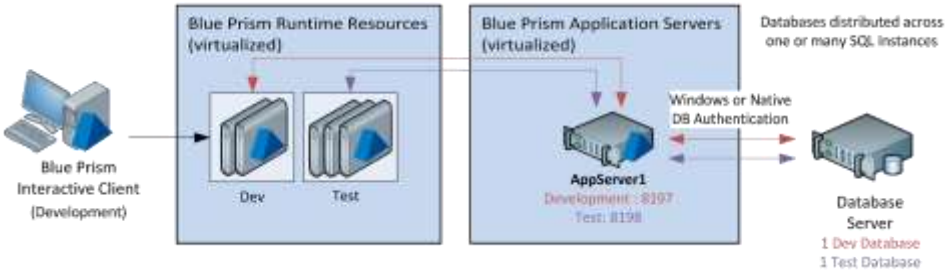
```
automate.exe /resourcepc /public /port [port] /dbconname [Connection Name]
```

```
automate.exe /resourcepc /public /port 8001 /dbconname "Production 001"
```

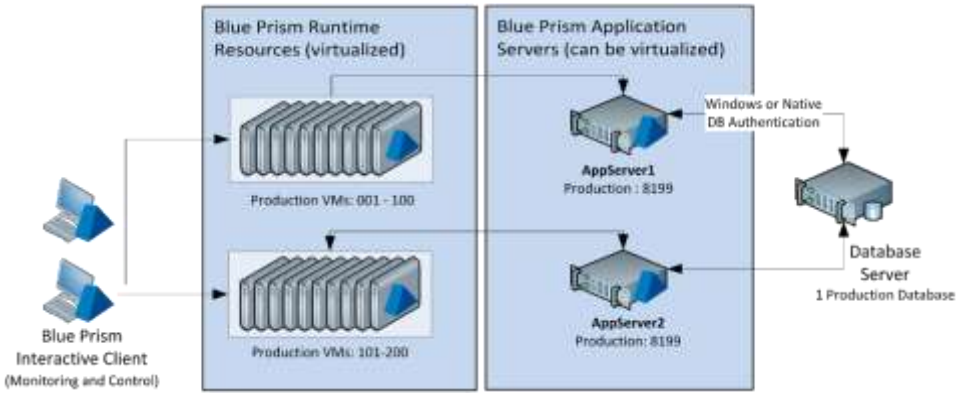
4. Advanced Topics

4.1. Multiple and Co-hosted Application Servers

Information is provided within the Blue Prism Application Server chapter on the steps required to configure multiple Blue Prism Application Servers for various environments on a single device and includes instructions on how to set up an independent service connected through to a dedicated database.



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



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

4.2. DNS Resolution

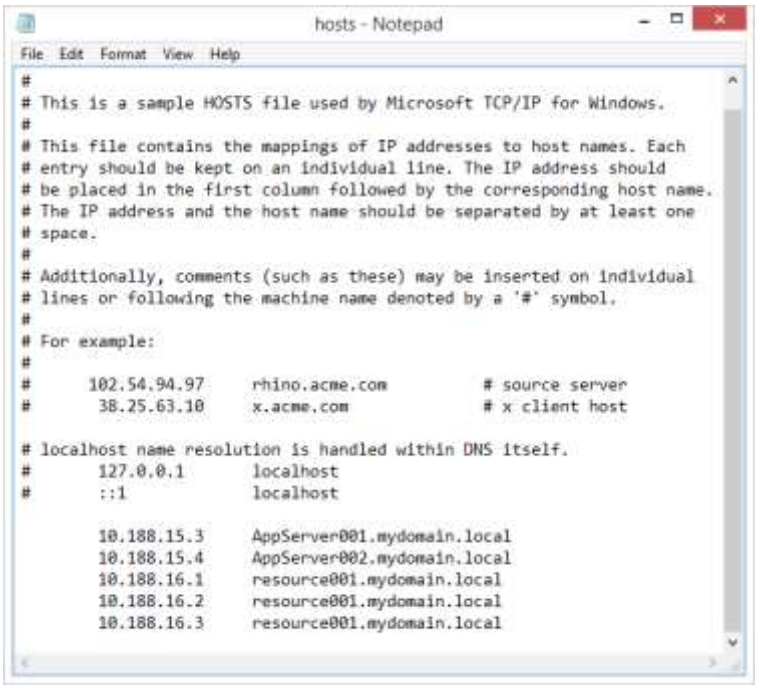
Blue Prism installations communicate with each other using their respective machine names - it is therefore necessary to ensure that these can be resolved successfully.

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

4.2.1. Local Host Files

To configure DNS records using a local host file follow the steps below:

1. Open the host file on the local machine using a text editor such as Notepad (administrator level access is required)
   C:\Windows\System32\drivers\etc\hosts
2. Enter the IP addresses and host names that are relevant to the deployment



3. **Save** and **Exit** Notepad

4.3. Java Access Bridge

If any of the target applications are deployed using the Java Runtime Environment (including browser plug-ins), then the Java Access Bridge is required to be installed on each Blue Prism client desktop. Information on obtaining the appropriate installers can be provided by your Account Manager to the Blue Prism Support Team.

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

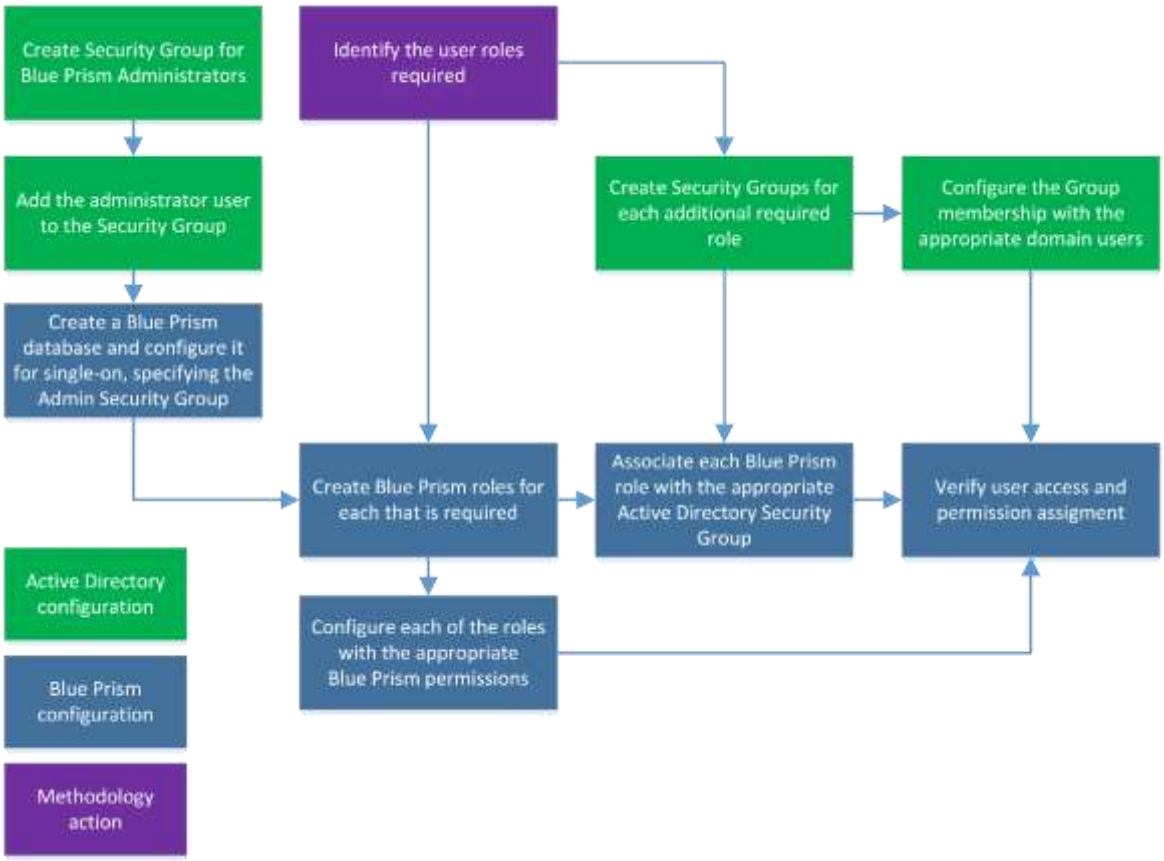
For information about the supported versions of the Java Access Bridge and Java Runtime Environment see the chapter on **Supported Software** within the **Appendix.**

Refer to the **Java Access Bridge - Setup Guide**, available from Blue Prism Support, for details.

4.4. Active Directory Configuration

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

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

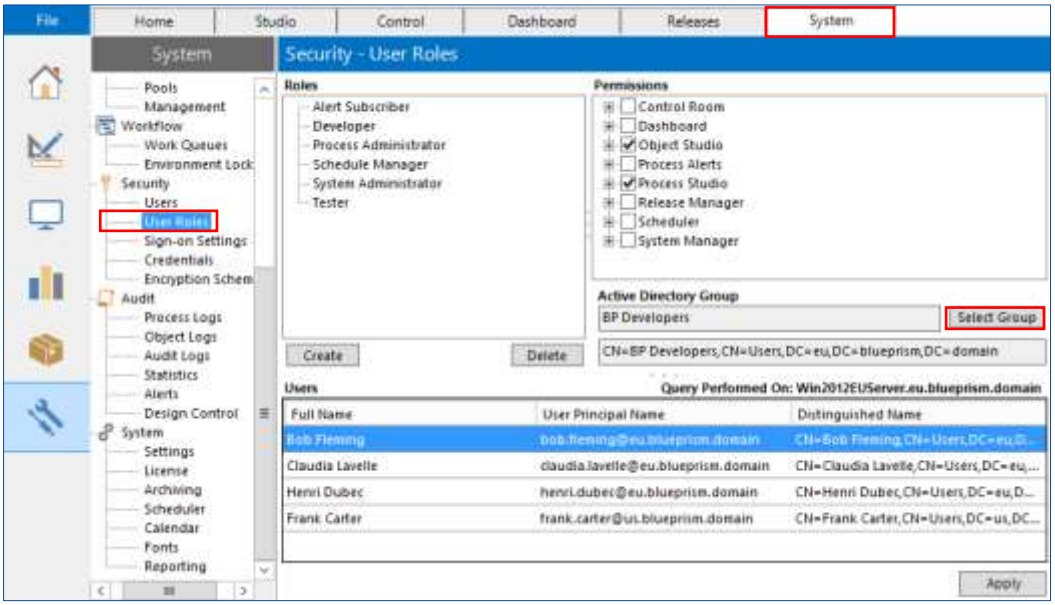


When configuring Blue Prism to use Active Directory for authentication, the database must be configured at the time of creation to use Microsoft Active Directory Authentication of single sign on. Information on this topic is provided within the section entitled **Creating or Configuring a Database** section within the **Appendix.**

4.4.1. Configure Active Directory Users and Roles

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

1. Click System Manager.
2. Click **Security** and select the **User Roles**.
3. From the right hand menu select **User Roles.**
   For each Role, configure the permissions that should be granted and select the Active Directory Security Group whose members should be assigned to this role



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

4. Once complete, click **OK**.
   Users who belong to the groups that have been configured should now be able to log in to Blue Prism and perform the actions permitted by the corresponding Blue Prism role (as indicated by the tree on the right). Users may have to log out of windows and log back in again for Active Directory changes to take effect.

4.5. Scripted Installation

It is possible to script the installation of the pre-requisite, supplementary and Blue Prism software. This section provides examples and reference indicators that should help with this.

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

4.5.1. Pre-requisite and Supplementary Software

4.5.1.1. .NET Framework

To install the .NET Framework, the following commands can be used:

```
WindowsInstaller-v2-x86.exe /passive

dotNetFx40_Full_x86_x64.exe /passive
```

The above commands should be verified to ensure that they are suitable for the target operating system and that the switches in use are appropriate.

4.5.1.2. SQL Server

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

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

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

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

4.5.2. Blue Prism

4.5.2.1. Core Application

To install Blue Prism use the command:

```
MSIEXEC.EXE /I "Automate5.0.5_x86.msi" /QB- ALLUSERS=1
```

4.5.2.2. Configure the Database Connection

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

For **SQL native authentication** mode, use:

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

For **SQL windows authentication** mode use:

```
Automate.exe /setdbname "DB Name" /setdbserver "DB Server"
```

4.5.2.3. Create a Blue Prism Database

Once a database connection has been defined a Blue Prism Database can then be created.

Native Blue Prism Authentication

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

The password is only required if SQL Authentication is being used to connect to the database server. In the above example the AutomateC.exe executable is being used rather than Automate.exe.

Active Directory Authentication

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

The password specified after **/createdb** only needs to be supplied if **SQL Authentication** is being used to connect to the database server.

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

It is also necessary for a manual step to be carried out: you must sign in and configure the **Single Sign-on Groups.** Instructions are provided within the **SQL Database Guide** in the **Appendix** which contains a chapter on **Creating or Configuring a Database**.

4.5.2.4. Register the License

The license is contained within a file and can be set using the command:

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

4.5.2.5. Import Processes

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

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

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

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

4.5.2.6. Publishing Processes

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

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

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

4.5.2.7. Scripting References

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

Topic	Help Reference	Download Location
.NET Framework Redistributable	https://www.microsoft.com/en-gb/download/details.aspx?id=17718	https://www.microsoft.com/en-gb/download/details.aspx?id=17718
Msiexec	http://technet.microsoft.com/en-us/library/cc759262%28WS.10%29.aspx	N/A
SQL 2012	https://technet.microsoft.com/en-us/library/ms144259(v=sql.110).aspx	https://www.microsoft.com/en-gb/download/details.aspx?id=29062
Blue Prism	AutomateC.exe /help or Contact your Account Manager or the Technical Support Team	N/A

5. Appendix

5.1. Supported Software

The following technologies are supported for use with the software.

5.1.1. Operating System

Version	Blue Prism Client	Blue Prism Server
Windows XP (SP2+)	✓	✓
Windows Vista (32-bit / 64-bit*)	✓	✓
Windows 7 (32-bit / 64-bit*)	✓	✓
Windows 8.1 (32-bit / 64-bit*)	✓	✓
Windows 10 (32-bit / 64-bit*)	✓	✓
Windows Server 2000 (SP4)	✓	✓
Windows Server 2003 (SP1) (32-bit / 64-bit*) (inc. R2)	✓	✓
Windows Server 2008 (32-bit / 64-bit*) (inc. R2)	✓	✓
Windows Server 2012 x64* (32-bit / 64-bit*) (inc. R2)	✓	✓

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

✓ = Supported ✓ = Supported but still undergoing testing

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

5.1.2. Microsoft SQL Server

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

	Express	Standard	Enterprise
SQL 2005	✓	✓	✓
SQL 2008 (32-bit / 64-bit) (inc. R2)	✓	✓	✓
SQL 2012 (32-bit / 64-bit) (inc. R2)	✓	✓	✓
SQL 2014 (32-bit / 64-bit) (inc. R2)	✓	✓	✓
SQL 2016 (64-bit)	✓	✓	✓

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

SQL Azure is also supported.

5.1.3. Microsoft .NET Framework

To install Blue Prism, **Microsoft .NET Framework 4** is required.

Microsoft .NET applications built on the following .NET Framework Versions can be automated by Blue Prism:

- 2.0
- 3.0
- 3.5
- 4.0

See the chapter on **Verifying the .NET Framework Version(s) Installed** for additional guidance.

5.1.4. Web Browser

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

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

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

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

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

5.2. Verifying Software Versions

5.2.1. Verifying the Blue Prism Version

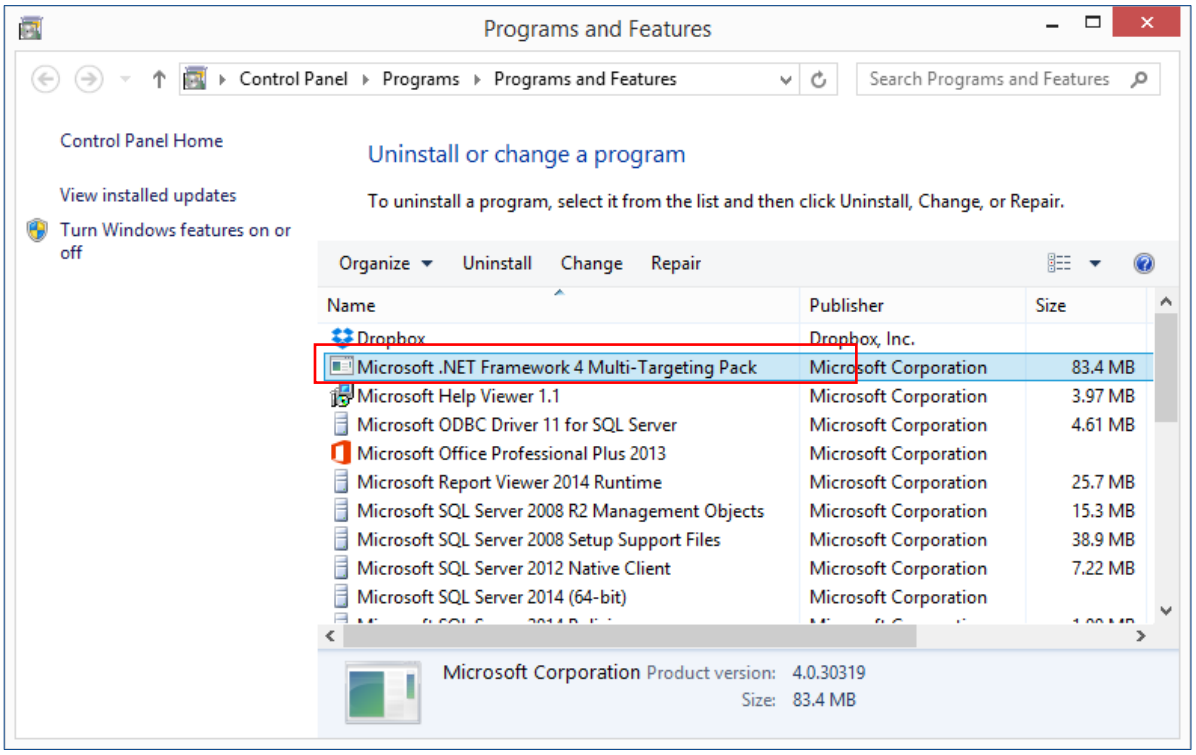
The Blue Prism version information can be found within the application under **Help** -> **About**.

5.2.2. Verifying the .NET Framework Version(s)

It is possible that more than one .NET Framework version may be installed as some versions do not necessarily supersede earlier releases.

The installed version(s) can typically be viewed from within the Programs list accessed via Control Panel.

If you are using Windows 7, the Programs list is called **Programs and Features**.



5.3. SQL Database Guide

The following sections provide step by step guides to help carry out common database related tasks for Blue Prism.

In addition it is strongly recommended that the Blue Prism data sheets in relation to Provisioning and Maintaining a Blue Prism Database Server are reviewed as these contain a wealth of information about the settings and common maintenance activities that are required.

5.3.1. Configuring SQL Server to accept Remote Connections

Where the SQL Server is installed on a separate server to the Blue Prism installation, it is important to ensure that the SQL Server is able to accept Remote Connections. In many default installs of SQL 2008 R2 or later, **Remote Connectivity** is disabled by default.

Typically enabling **Remote Connectivity** is done for a given SQL Server Instance and therefore affects all databases within that Instance.

The links below are to articles published by Microsoft on this topic.

Enable the TCP/IP Protocol for a Database Instance (2005, 2008)

Enable the TCIP/IP Network Protocol for SQL Server (2012)

Additionally it is important that the **SQL Browser Server** is started on the applicable **SQL Servers**. This is particularly important for **SQL Server Express** editions where the service is disabled by default.

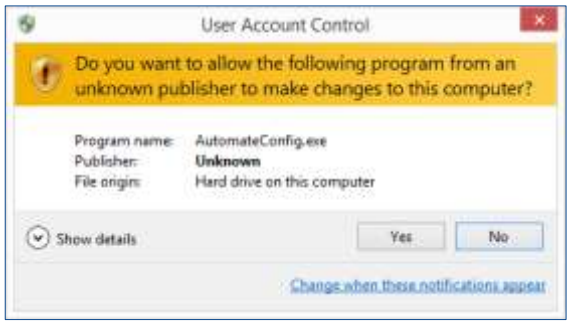
5.3.2. Configuring a Connection to the Database

This guide provides step by step instructions to set up the database connection information for the SQL Server within Blue Prism.

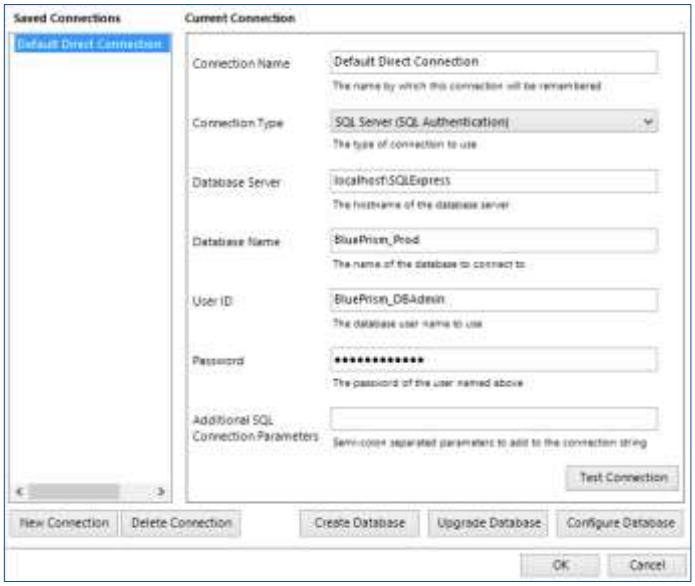
If any issues are experienced whilst following these instructions please refer to the section on **Troubleshooting an Installation** in this guide.

1. Start Blue Prism from the Windows start menu or desktop.
2. When you open Blue Prism on a computer for the first time, a message appears indicating that **you must specify a database connection before Blue Prism can function**.
3. Click **Configure**. This will launch the wizard that can be used to provide the connection information.

   a. If you are using Windows Vista or later and User Account Control is enabled it may be necessary to enter elevation mode and additional device or network credentials may be required.



4. The Connection Configuration window is now displayed.



The connection information for the database server and target database should be entered here.

Connection Types

The following definitions provide more information on each of the options for Connection Types:

a. **SQL Server (SQL Authentication)**
Connect to a named SQL Server instance which has been configured with SQL Authentication (i.e. using a saved User ID and password).

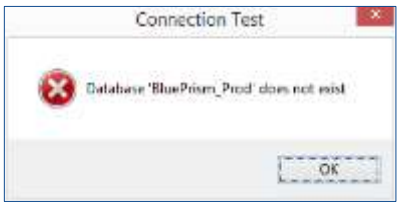
b. **SQL Server (Windows Authentication)**
Connect to a named SQL Server instance using Windows Authentication. Note that database rules governing security must be implemented on the database for the currently logged in user or user's group.

c. **Blue Prism Server**
Connect to a named host and port which is running a Blue Prism Server instance. Further guidance regarding Blue Prism Server is given later in this document and in the Help file distributed with the product.
Select this option to link the Blue Prism installation to a database via a configured Blue Prism Server.

d. **Availability Group (SQL Authentication)**
Connect to a SQL Availability Group listener using SQL Authentication. Includes the option to specify the port number and whether MultiSubnetFailover will be set as part of the connection string.

e. **Availability Group (Windows Authentication)**
Connect to a SQL Availability Group listener using Windows Authentication. Includes the option to specify the port number and whether MultiSubnetFailover will be set as part of the connection string.

1. Click **Test Connection**.
   If a connection can be established with the SQL Server, commonly one of the following messages will be presented.

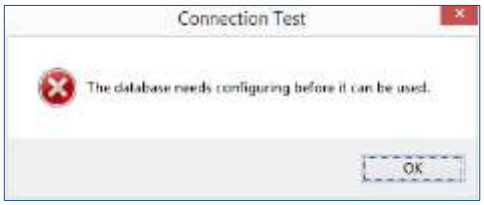


   a. **Database does not exist**
      This indicates that the database has not yet been created.

      Press **OK** to clear the message, and press **Create Database**. Follow the **Creation** actions within the following section: **Create or Configure a Database**

   b. **Not a valid Blue Prism Database**
      This indicates that the database exists, 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.

      Press **OK** to clear the message, and press **Create Database**. Follow the **Creation** actions within the following section: **Create or Configure a Database**



   c. **Database needs configuring**
      This indicates that the database exists and that the schema has been applied but that there is some further in-product configuration that is required. This would typically be the case where the database has been manually created and has had the Blue Prism schema applied via a manually executed script.

      Press **OK** to clear the message, and press **Configure Database**. Follow the **Configuration** actions within the following section: **Create or Configure a Database**

   d. **Other Messages**
      If alternative messages are presented please refer to the section on Troubleshooting an Installation in this guide.

A detailed version of the step by step guide to configuring a connection to the database can be found in the **Appendix** under **Configuring a Connection to the Database**.

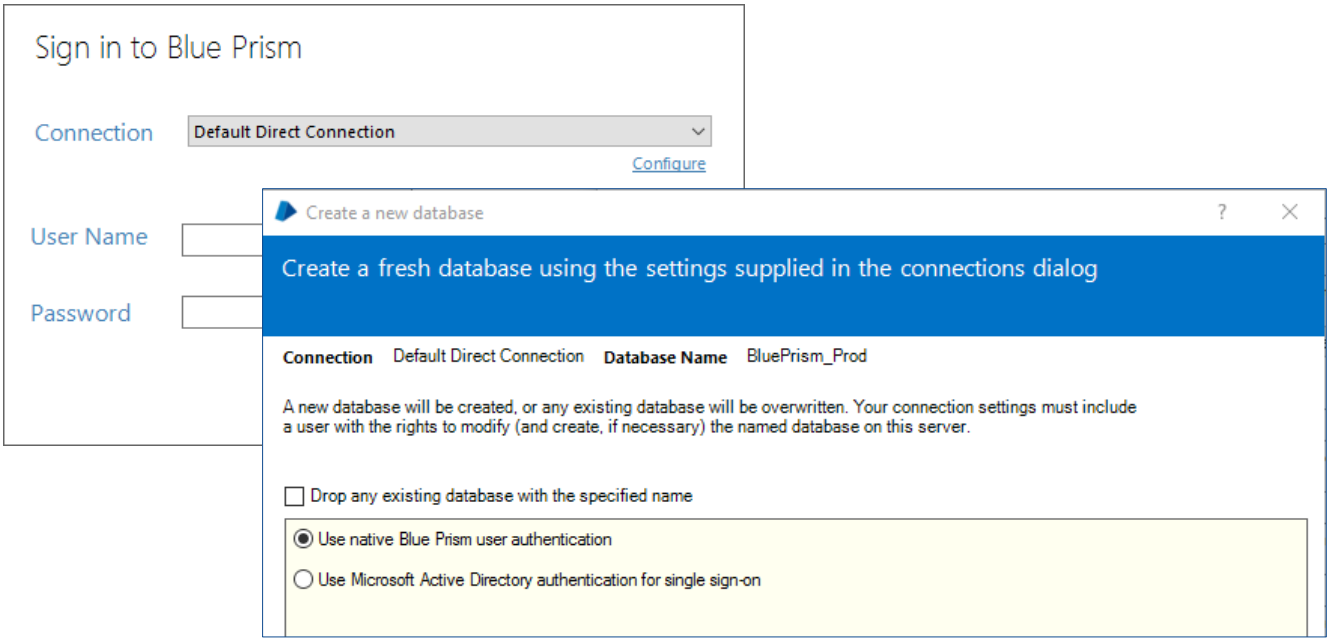
5.3.3. Creating or Configuring a Database

The instructions below cater for the scenarios whereby the information specified on the selected Blue Prism connection is:

- Used to **create a new database** and configure it for Blue Prism; or
- Used to **configure an existing database and configure it for Blue Prism**
  This option is commonly used when the database has been created manually such as when created by a DBA or when working with Microsoft SQL Azure.

If required scripts can be provided separately which will allow a Database Administrator to configure the databases manually. The scripts can be obtained by contacting Blue Prism Technical Support.

Within the Blue Prism application, click the **Configure** option on the Sign in screen, enter the details for a SQL Server, provide the name of the database that should be created and click **Create Database**.



There are two options for Blue Prism user authentication and this **cannot be changed** once the database has been created.

- **Native Authentication**
  Preferred for simple or small-scale installations. User accounts are stored and managed in the Blue Prism database. User accounts must be created individually for users (or shared as a generic login) within Blue Prism. There is no relationship with the current operating system user and, beyond a database / BP Server instance, there are no further external dependencies for this option.
- **Microsoft Active Directory authentication for single sign-on**
  Designed for large organizations with centralized control over users and resources. There is no need for user management within Blue Prism: this is all handled centrally in Active Directory. Users are authenticated to use Blue Prism according to their operating system user credentials (provided they belong to the relevant groups), and enjoy the convenience of automatic sign-in as a result.

5.3.3.1. Native Authentication

If **Native** user authentication is selected it is necessary to enter the database credentials to allow the database to be created.

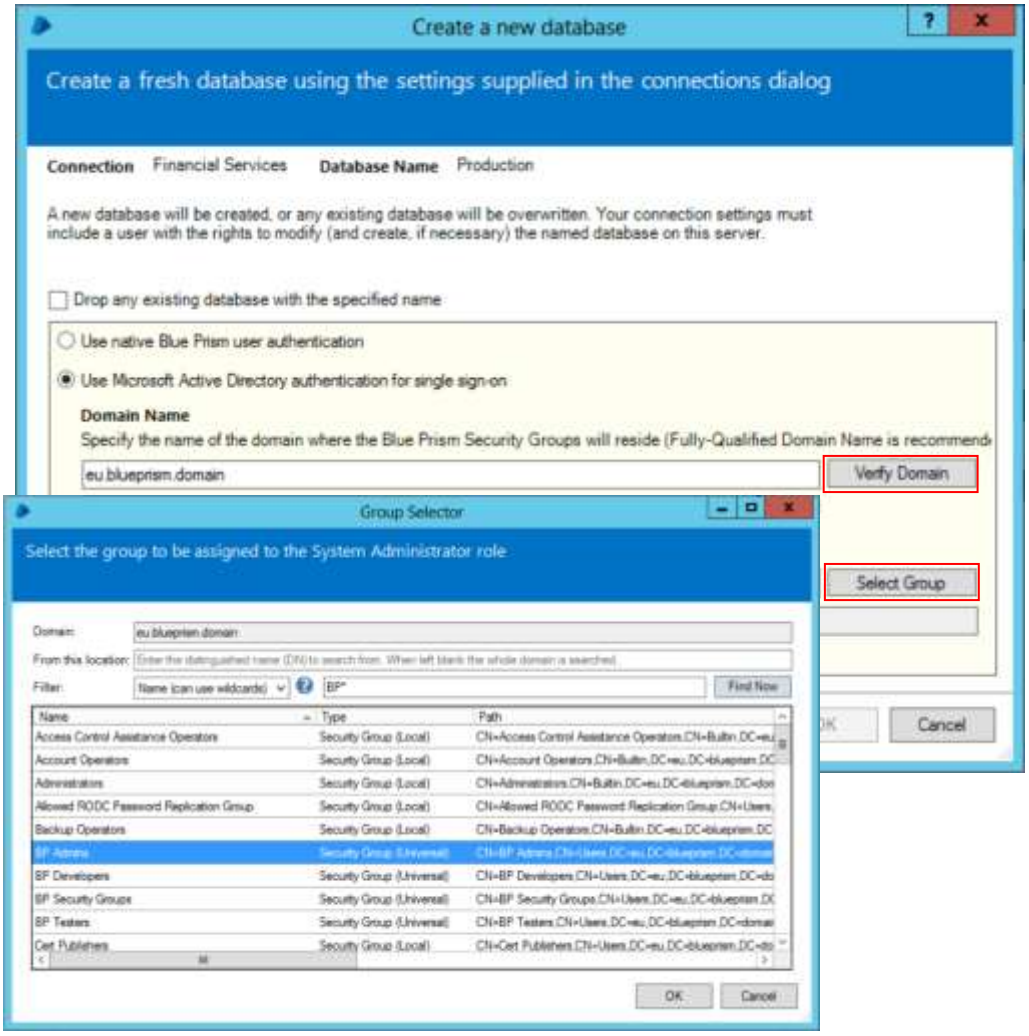
Once the credentials are provided, clicking **OK** will create the database.

5.3.3.2. Active Directory Authentication

When selecting to use **Active Directory** authentication for Blue Prism, it is necessary to provide the name of the domain that will contain the Security Groups which can be associated to Blue Prism security roles, and also to select a pre-existing security group that will be used to represent the users that will be granted Blue Prism System Administrator privileges.

To use Microsoft's Active Directory for Blue Prism user authentication:

- Select the Use Microsoft Active Directory authentication for single sign-on radio button
- Enter the name of the domain which contains the Security Groups that will later be associated with Blue Prism Security Roles and click **Verify Domain**
- Click **Select Group** to search the specified domain for the Security Group whose members will be granted System Administrator access within Blue Prism.



Once logged into Blue Prism further Blue Prism Security Role can be defined and these can individually be mapped to Active Directory Security Groups to grant users within those groups with the appropriate Blue Prism permissions.

5.3.4. Minimum SQL Permissions

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

- Datareader
- Datawriter
- [All roles prefixed with bpa_] E.g.
    - bpa_ExecuteSP_DataSource_bpSystem
    - bpa_ExecuteSP_DataSource_custom
    - bpa_ExecuteSP_System

The minimum SQL permissions do not provide appropriate privileges to carry out Create, Configure or Upgrade database actions, therefore an appropriate administrator account (e.g. dbowner) will need to be used when any of these actions are required.

5.4. Updating the License

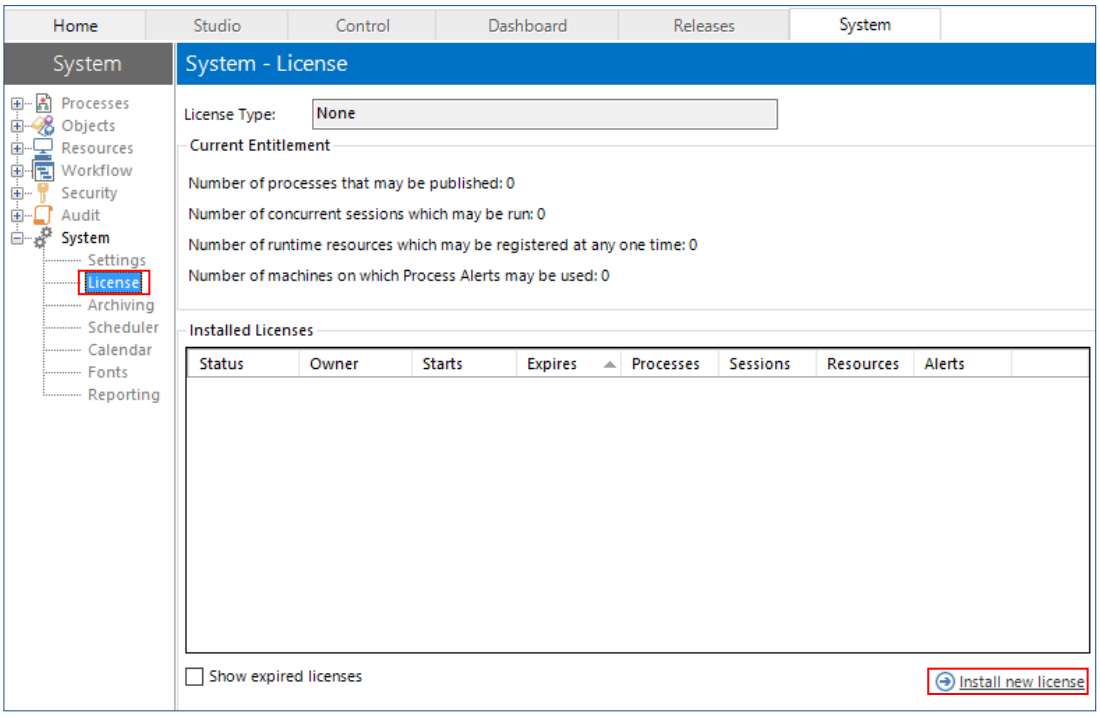
Apply the license using the instructions below based on the version of the software that is installed.

The changes will be effective immediately after the license has been successfully updated.

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

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

1. Launch Blue Prism.
2. Click System Manager.
3. Click the **System** menu item.
4. Click the **License** tab.
5. Select **Install new licence.**
6. Select the License file and click **OK.**



5.5. Verify an Installation

This section provides a simple automation scenario in order to test that the installation was successful. It should be noted that successfully completing this verification confirms 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.
  To verify an installation using this section the Microsoft Word Object must be installed
- Test the Process.

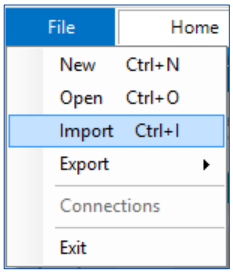
These instructions assume that the Blue Prism database is empty and that Microsoft Word has been installed on the device. If that is not the case, any process names which conflict with existing processes will need to be changed.

If problems are experienced whilst verifying the installation, in the first instance the section on **Troubleshooting an Installation** should be reviewed.

5.5.1. Import the Microsoft Word Object

A Microsoft Word automation object is included with the release package, and it is recommended that this is imported into the Blue Prism database (if it hasn't been previously imported in the environment).

1. Launch Blue Prism
2. Sign in using the username admin
3. From the File menu select Import.

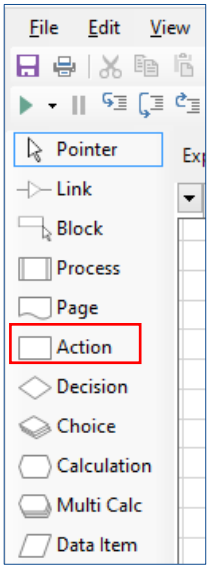


4. Browse for a file called **BPA Object – MS Word.xml** this is typically found within C:\Program Files\Blue Prism Limited\Blue Prism Automate\VBO.
5. Complete the wizard to import the object.

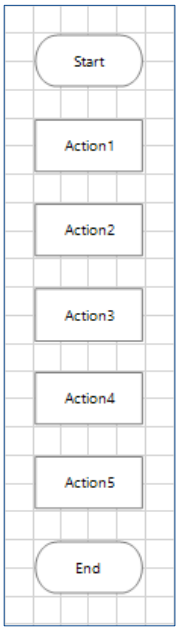
Optionally the above steps can be repeated to import the Microsoft Excel Object.
BPA Object – MS Excel.xml

5.5.2. Create a new Process

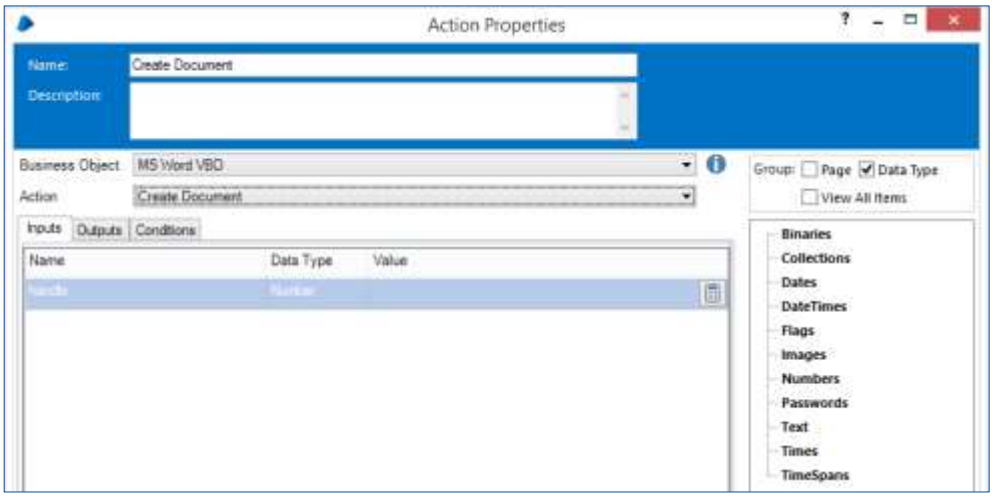
1. Click **Process Studio** from the left-hand navigation menu.
2. Click **Create a new Process** on the resulting screen. A wizard will pop up.
3. Enter the name **Letter Writing Test** for the new process.
4. Enter the description **Evaluation test**.
5. **Process Studio** will now appear.
6. From the toolbar at the top chose the **Action stage** tool as illustrated.



7. Place four action stages vertically on the diagram, equally spaced between the **start** and **end** stages.



8. Double click the first stage (or right-click and choose “properties”). A properties form will appear. Enter the name **Create new Document** at the top, and from the combo boxes below, choose the combination **MS Word VBO** and **Create Document**.

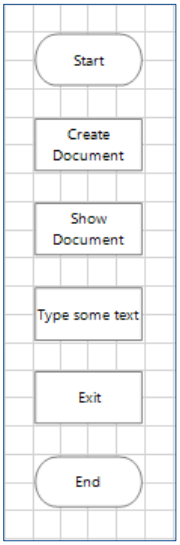


The inputs may be left blank.

9. Click **OK** to save your changes and exit the form.

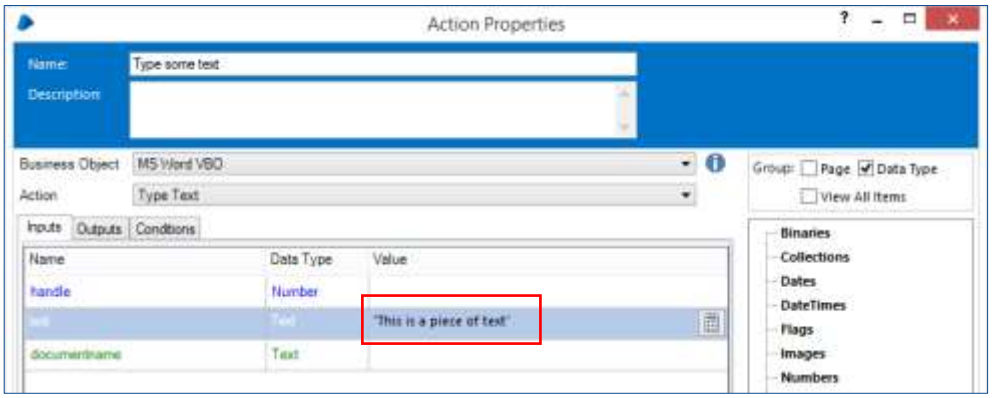
10. Repeat the same steps for each for the remaining three stages using the **names** and **actions** as identified in the table below.

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



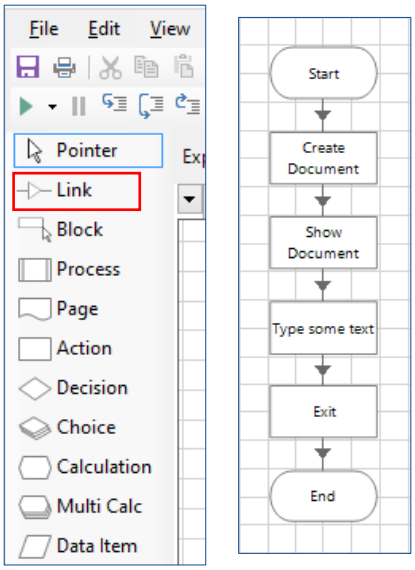
11. **Double click** the stage named **Type some text** to edit the properties.

12. Within the Value column of the Input parameter called **text,** enter a short sentence which will be entered into the word document when the process runs.
    The sentence will need to be within double quotation marks.
    E.g. “This is a piece of text”



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

14. From the toolbar select the **Link** tool and use the mouse to link each of the stages in turn by dragging from one stage to the next.

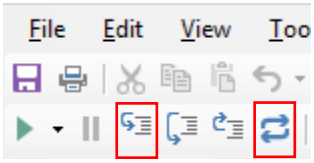


15. Save the process from the **File** menu – a confirmation message should be displayed in the status bar at the bottom of the window.

5.5.3. Test the Process

To test the process we will need two buttons from within the toolbar of 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 in the toolbar. This should cause the first stage in the process diagram to be highlighted in orange and indicates that this is the next stage to be run. Next time **Step** is pressed the actions within that stage will be performed.
3. Click **Step** again and this will cause the actions in the first stage to be performed (e.g. a new Microsoft Word document will be created although at this time it is not yet visible to the user).
4. Continue to click **Step** to progress from the stage to stage.
   Verify that the expected action takes place with each step (i.e. the new Microsoft Word document is shown, the correct text is typed into the document, and the document disappears on “Exit”).
5. If you wish to run the process again, click the “reset” button and repeat.

5.6. Troubleshooting an Installation

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

5.6.1. Cannot connect to [SQL Server]

There are a number of things to check where a connection cannot be made to a SQL Server over the LAN.

1. **Verify Network Connectivity**
   Ensure that all relevant devices are connected to the same network and able to communicate.
2. **SQL Credentials**
   Verify the SQL Credentials and that the user has appropriate permissions on the SQL Server.
3. **Firewall**
   Firewalls on the servers themselves or within the network may be preventing communication.
4. **SQL Browser Service**
   The SQL Browser Service on the SQL Server will need to be 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 to SQL, **TCP/IP** connectivity will need to be enabled for the SQL Instance. For guidance on enabling this connectivity see the chapter on **Configuring SQL Server to accept Remote** Connections within the **SQL Database Guide.**
It may also be necessary to also enable support for **Named Pipes** connectivity.

5.6.2. 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.

For guidance on enabling this connectivity see the chapter on **Configuring SQL Server to accept Remote** Connections within the **SQL Database Guide** in this document.

5.6.3. Failed to create Database – A network-related…

When creating a SQL database through Blue Prism an error message is displayed:

```
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.

For guidance on enabling this connectivity see the chapter on **Configuring SQL Server to accept Remote** Connections within the **SQL Database Guide** in this document.

5.6.4. Error Message 2869 on installation

If, when installing over an earlier version of Blue Prism, an error message is displayed with an **Error Code 2869**, the earlier version should be uninstalled first. If, when attempting to do this, an empty error message box is displayed and the uninstall fails, the earlier version may have been corrupted by the aborted installation.

To fix this, enter the **Add/Remove Programs** applet in Control Panel, and Repair the Blue Prism installation. Attempting to uninstall Blue Prism should now work correctly, and the new version can be installed normally.

5.6.5. Insufficient Permissions error message is displayed

A message is displayed:

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

This indicates that the SQL user does not have permission to create a new database. This typically happens with Windows Authentication, but may occur with a SQL authenticated user with restricted power. A number of options are available for working around this issue:

Giving the user the **CREATE DATABASE** permission in the SQL Server instance

Configuring the connection to use a different login with the **CREATE DATABASE** permission

Running Blue Prism as administrator may be enough to fix it. This only works if the Administrators group is given the **dbcreate** role in the SQL Server instance - something which occurs by default in SQL Server Express 2005, but not in later versions. To do this, find the Blue Prism executable, right-click it and choose **Run as administrator**. The executable is typically found at:

C:\Program Files\Blue Prism Limited\Blue Prism Automate\Automate.exe

Asking a DBA to create the database. The database can be populated by the Blue Prism client using the **Create Database** command which will fill in the database with the Blue Prism tables.

5.6.6. Unhandled Exception entering System Manager in Windows Server

After installing on Windows Server, entering System Manager generates the exception:

```
System.TypeInitializationException: The type initializer for
'BluePrism.AutomateLicensing.clsLicensingRuntime' threw an exception. --->
System.InvalidOperationException: This implementation is not part of the Windows
Platform FIPS validated cryptographic algorithms.
at System.Security.Cryptography.MD5CryptoServiceProvider..ctor()
at BluePrism.AutomateLicensing.AuthorisationDetails.GetCheckSum()
at BluePrism.AutomateLicensing.AuthorisationDetails.FromLicenseKey(String A)
at BluePrism.AutomateLicensing.clsLicensingRuntime..cctor()
```

In order for the encryption used in the Blue Prism license to work correctly, the **Enforce FIPS** policy within Windows may need to be disabled. This can be done by disabling the setting within the local/group policy:

System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithms

If this is not possible, a workaround is available to fix this within Blue Prism only. Create an XML file with the contents as below and copy it into the Blue Prism installation directory. It will need to be copied several times to affect all of the Blue Prism executable files. It should be saved with the following filenames:

- Automate.exe.config
- AutomateC.exe.config
- BPServer.exe.config
- BPServerService.exe.config

On running the application, System Manager should be available once more.

XML File Contents

```
<configuration>
    <runtime>
        <enforceFIPSPolicy enabled="false"/>
    </runtime>
</configuration>
```

5.6.7. Unable to Connect to the Blue Prism Server Service

```
Not connection could be made because the target machine actively refused it.
```

On running the application, System Manager should be available once more. This message typically means that either the Blue Prism Server Service is not available on the defined server and port or that the Use Secure Connection option is not valid.

Verify that the server name and port are correct and that the Blue Prism Server service is started on the target machine.

5.6.8. Error Starting the Blue Prism Server Service

Bad Configuration Name

```
Service cannot be started. System.ApplicationException: Invalid arguments
```

Might suggest that the {CONFIGURATIONNAME} has spaces in it - this is not advisable.

Missing Configuration Name or Invalid Profile)

```
The Blue Prism Server service on Local Computer started and then stopped.  Some
services stop automatically if they are not in use by other services or programs.
```

If the above message is received when trying to start the Blue Prism Server service, check the event logs on the server for additional information. It commonly relates to situations where either the configuration profile cannot be found, or where there are errors within the profile.

- When the Blue Prism server windows service was created, it is directed to use a specifically named configuration file that aligns to one created using BPServer.exe. The Blue Prism server service installed natively by Blue Prism uses a configuration within BPServer.exe called **Default**.
  If the configuration file of the appropriate name cannot be found an error similar to the below will be displayed within the event logs. To resolve the error, use BPServer.exe to ensure a saved profile of the appopriate name exists.
  ```
  BluePrism.BPCoreLib.InvalidValueException: Server configuration 'Default' is not
  defined
  ```
- The Blue Prism server service requires access to authenticate with the Blue Prism database. If an error similar to the below is presented in the event logs, it suggests that the logon account for the Blue Prism server service does no thave access to the database.
  ```
  BluePrism.BPCoreLib.InvalidStateException: Connection not valid: Connection failed -
  Cannot open database "DemoFS_v5" requested by the login. The login failed.
  Login failed for user 'NT AUTHORITY\SYSTEM'.
  ```
- As part of the startup procedure, the Blue Prism server service evaluates whether the encryption schemes configured in the database indicates that there should be local encryption schemes configured on the server. If the database encryptoin scheme records indicate that there should be local schemes on the server, but they can't be found, the service will fail to start. In the example below, the server could not locate a local encryption scheme within the BPServe.exe configuration named **Credentials Key**.
  ```
  Failed to start server - The following encryption keys could not be resolved:
  Credentials Key
  ```

Name Mismatch

```
Service cannot be started. System.ApplicationException: Server configuration 'Dev' is
not defined.
```

Indicates a name mismatch or a missing configuration file - check the server configuration to ensure the configuration name matches up to that which is defined in the windows service, and ensure that the configuration file is in the correct location:

For Windows Vista / 7 / Server 2008

```
%PROGRAMDATA%\Blue Prism Limited\Automate V3\Automate.config
```

For Windows 2000, XP, Server 2003

```
%ALLUSERSPROFILE%\Application Data\Blue Prism Limited\Automate V3\Automate.config
```

Other Errors

```
Service cannot be started. System.ApplicationException: Failed to start server
```

Further information with a more detailed description can be found in the **Blue Prism** event log.

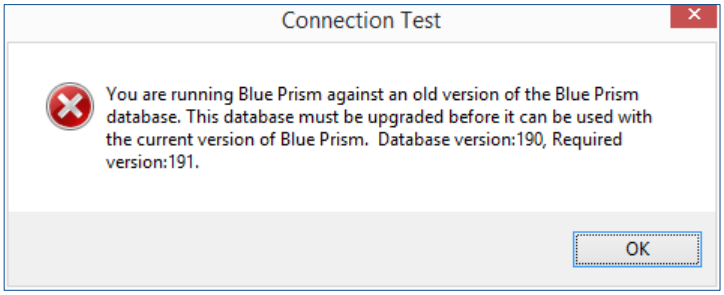
Unauthorised Access to the Database

If the error **Failed to start server** message is presented and the following message is in the Blue Prism event log:

```
Connection failed - Unable to determine whether database exists - Login failed for user
'{DOMAIN}\{HOSTNAME}$'
```

This may indicate that windows authentication is being used to log into the database, and the local user (i.e. the user which the service runs as) does not have access permissions on the database. To solve this, the username described in the error message (i.e. "**{HOSTNAME}**$" where **{HOSTNAME}** is the name of the computer) must be given the appropriate permissions to the Blue Prism database.

5.6.9. 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. Commonly the database version will be a lower number than the required version – the ability to **Upgrade Database** to the appropriate version is provided within the **Connections** menu. 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 will be required.