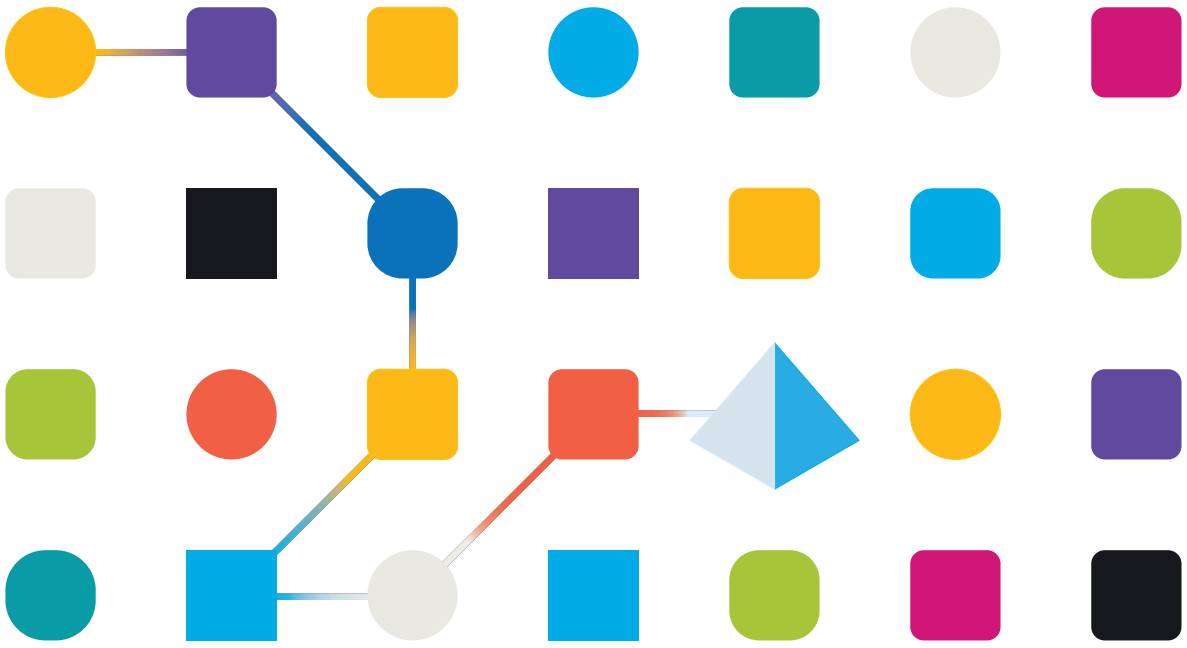
SS&C | blueprism®

Interact 4.4

Install Guide

Document Revision: 3.0



Trademarks and Copyright

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

Contents

Introduction

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

Blue Prism Interact is only supported in a Multi-device Deployment. This is where the Blue Prism components are deployed across a number of devices. The reasons for this are:

- It provides an extensible deployment of Blue Prism components suitable for a broad range of scenarios.
- Advanced techniques relating to deploying additional services or securing and hardening the environment will commonly require this type of deployment.

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. For more information, see Contact us.

This information relates only to the version 4.4 of Blue Prism Interact.

Blue Prism Hub must be installed before attempting to install Interact.

Upgrading Interact

If upgrading from an earlier version of Interact 4, Blue Prism supplies an upgrader. For more information, see Upgrading Hub and Interact.

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.

Videos

In addition to this install guide, you can watch our videos demonstrating the install process. Click here to see the Interact installation videos.

Related documents

The following documents provide further information on specific aspects of the implementation of Hub and Interact.

Document Title	Description
Hub user guide	A detailed document explaining how to get the best out of Hub, including user access, licensing plugins and customization of Hub.
Interact plugin user guide	A detailed document explaining how to get the best out of Interact, including creating Forms and assigning them to Roles.
Interact user guide	A detailed document explaining how to use Interact to submit and approve forms.

Document Title	Description
Interact Web API Service user guide	A document providing detailed information on how to use the Interact Web API Service and related Blue Prism Object.

Preparation

Prior to undertaking an installation of Blue Prism Interact it is important to ensure that the architecture is configured to support the installation. Multiple systems are required to support the installation of Interact.

Planning

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

- A SQL Server must be available to host the Blue Prism component databases, such as, Authentication Server , Hub, Audit, Interact, InteractCache and so on. Administrator-level access is required during the installation process. See Minimum SQL permissions for more details.
- A Message Broker server must be available hosting RabbitMQ Message Broker.
- A Web Server for the co-existing Hub (see Prerequisites on the next page) and Interact installations
- Administrator access to the devices where Blue Prism Interact 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 local network, including communication with your Blue Prism Database.
- The account performing the installation must have access to the hosts file. This is typically stored in C:\Windows\System32\drivers\etc\hosts or %SYSTEMROOT%\System32\drivers\etc\hosts.

When planning your deployment, the following points should be considered:

- Will the database be added to an existing database server or will a new one be commissioned?

  Blue Prism recommend that databases are kept on separate database servers.
- Is there sufficient space and resources to host the added databases?

  You should check and ensure that sufficient disk space and compute resources can cope with the additional load.
- What authentication mode is required for the SQL database (SQL Native or Windows Authentication)?

  This is your IT organizations decision.
- Has the Message Broker server been setup and configured to support the installation of Hub?

  A Message Broker server is required to complete the installation of Hub.
- Do all devices where Blue Prism Hub is to be installed meet the minimum requirements (including version 4.7.2 of the .NET Framework)?

  See Software requirements and permissions for details.

Prerequisites

See Software requirements and permissions for details of software requirements and minimum SQL permissions.

Installing Interact requires the following prerequisites:

- Blue Prism Hub requires a Message Broker server to be installed and configured.
- The Message Broker server build is a generic setup and base install of a RabbitMQ Message Broker service. It is recommended that the default passwords are changed and any security requirements such as applying SSL certifications are completed by your IT department.

  To complete the Message Broker build, the following need to be downloaded:

  - Erlang/OTP – the version of Erlang/OTP is dependent on the version of RabbitMQ.

    To check the Erlang/OTP version against the RabbitMQ version, see https://www.rabbitmq.com/which-erlang.html.

    To download Erlang/OTP, go to https://www.erlang.org/downloads and select the appropriate version.

  - RabbitMQ Server, available here: https://github.com/rabbitmq/rabbitmq-server/releases/

  > Installation guidance is provided here: https://www.rabbitmq.com/install-windows-manual.html

- Blue Prism Hub is installed on the web server and therefore requires Internet Information Services Manager (IIS) and the .NET Core components installed. These need to be pre-installed to enable a successful installation of Blue Prism Hub. See Install and configure the web server on page 25 for more information.
- The Interact system is a Web Server and therefore requires IIS Web Server and the .NET Core components installed. These are all installed as part of a successful installation of Blue Prism Interact using the Blue Prism Hub and the Blue Prism Interact installation media.
- You will be creating the following websites with the Interact installer – you should define the URLs based on your organizations domain:

Website in IIS	Default URL
Websites with a UI for use by end-users	
Blue Prism – Interact	https://interact.local
Websites for use by the application only (services)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

> The default URLs shown above are suitable for a standalone environment, such as a test environment. Your organization's DNS and Domain structures must be considered when choosing host names for your installation.

These are in addition to the websites created by the Hub installer, see Configure SSL certificates on page 26 for a list.

- Certificates – During the installation process you will be asked for the SSL certificates for the websites being setup. Depending on your infrastructure and IT organization security requirements this could be an internally created SSL certificates or purchased certificates to protect the websites. The installer can be run without the certificates being present, though for the sites to operate, the bindings in the IIS websites will need to have valid SSL certificates present. See Configure SSL certificatesfor details.
- By default, IIS Application Pools are used. Application pools must have access to the application files and certificates that are created during installation for data protection and authorization. These certificates are BluePrismCloud_Data_Protection and BluePrismCloud_IMS_JWT which are located within the default Windows certificate folder. If using Windows Authorization for access to SQL server, this will need to be configured manually. For more information, see Default application information on page 14.
- By default, the 'Local System' account is used for services. This account must have access to application files. If using Windows Authorization for access to SQL server, this will need to be configured manually.

Software download list

Blue Prism Hub

This lists all the downloads that are required to install Hub. These are all referenced later in the install guide:

Software and reference link	Related guidance
RabbitMQ 3.8.16 or 3.8.17 For more information, see Downloading and Installing RabbitMQ.	Install the Message Broker server on page 20
Erlang/OTP 24.x The version of Erlang that you require is dependent on the RabbitMQ version you intend to use. For more information, see RabbitMQ Erlang Version Requirements.	
IIS 10.0 Included with Windows Server 2016 and Windows Server 2019.	Install and configure the web server on page 25
.NET Core 3.1.11 Windows Server Hosting https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-aspnetcore-3.1.11-windows-hosting-bundle-installer	
.NET Core 3.1.11 Windows Desktop Runtime https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-desktop-3.1.11-windows-x64-installer	
Visual C++ Redistributable 2012 (x64) https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe	
.NET Framework 4.7.2 https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer This is installed by default on Windows Server 2019. You only need to install the .NET Framework if you are using Windows Server 2016.	
Blue Prism Hub 4.4 Download from the Blue Prism Portal.	

Blue Prism Interact

Blue Prism Interact is a license-controlled plugin in Hub and an additional website for end-users. If your organization intends to use Interact, you will need to download the following in addition to the downloads listed in Blue Prism Hub on the previous page.

Software and reference link	Related guidance
Blue Prism Interact 4.4 Download from the Blue Prism Portal.	Install Blue Prism Interact
Blue Prism Interact Remote API.bprelease file Download from the Blue Prism Portal.	Install and configure the Interact Web API service

Minimum hardware requirements

The information below details the minimum hardware requirements recommended for effectively installing and running Hub and Interact 4.4. For software requirements, see Software requirements and permissions on the next page.

Runtime Resource

Please refer to the minimum requirements in the installation guide for the version of Blue Prism that you have installed. Visit the Blue Prism help for more information.

Database server

- Intel Quad Xeon Processor
- 8 GB RAM
- SQL Server:
  - 2016, 2017 or 2019 (64-bit) – Express, Standard or Enterprise editions

    SQL Express editions are only appropriate for non-production environments, such as for the purposes of proof of concept exercises.
  - Azure SQL Database
  - SQL Server on Azure Virtual Machines
  - Azure SQL Managed Instance
- For appropriate operating system support, see:
  - SQL Server 2016 or 2017: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver15
  - SQL Server 2019: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

Message Broker server

- Intel Dual Xeon Processor
- 8 GB RAM
- Windows Server 2016 Datacenter or 2019

Web server

- Intel Dual Xeon Processor
- 8 GB RAM
- Windows Server 2016 Datacenter or 2019
- Prerequisites as detailed in Preparation on page 7

Software requirements and permissions

Software requirements

The following technologies are supported for use with the software:

Operating system

Version	Web Server	Message Broker
Windows Server 2016 Datacenter	✓	✓
Windows Server 2019	✓	✓

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

Microsoft SQL Server

The following Microsoft SQL Server versions are supported for locating the Blue Prism component databases:

Version	Express	Standard	Enterprise
SQL Server 2016	✓	✓	✓
SQL Server 2017	✓	✓	✓
SQL Server 2019 (64-bit)	✓	✓	✓

SQL Express is only appropriate for non-production environments, such as for the purposes of proof of concept exercises.

The following are also supported:

- Azure SQL Database.
- SQL Server on Azure Virtual Machines.
- Azure SQL Managed Instance, however, the databases must be created before the installation.

Message Broker server

The following software is required on the Message Broker server:

- RabbitMQ 3.8.16 or 3.8.17
- Erlang/OTP 24.x – The version of Erlang that you require is dependent on the RabbitMQ version you intend to use.

  For appropriate Erlang/OTP support, see RabbitMQ Erlang Version Requirements.

  For appropriate operating system support, see https://www.rabbitmq.com/platforms.html.

See Install the Message Broker server on page 20 for more information.

Web server

The following software is required on the Web server:

- .NET Framework 4.7.2 – Installed by default on Windows Server 2019.
- IIS 10.0
- .NET Core Windows Server Hosting 3.1.11
- .NET Core Windows Desktop Runtime 3.1.11
- Visual C++ Redistributable 2012 (x64)

See Install and configure the web server on page 25 for more information.

Blue Prism

Blue Prism 6.4.0 or later is required for use with Interact.

Minimum SQL permissions

The minimum SQL permissions for the user required to connect to the database during the installation process must have the appropriate privileges to Create or Configure database from within the product, therefore an appropriate administrator account will need to be used when running the installation process:

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

The database user required to connect to the databases during normal operation must have the minimum SQL permissions to access the Interact and Interact Cache databases. The required permissions are:

- db_datareader
- db_datawriter

A user with db_owner access to the database should be used during the installation process and on the first application run. Once completed, database access for this user can be changed to db_datareader and db_datawriter.

For more information, see Default application information below.

Default application information

The information below shows the applications that are created by the Interact installation, using the default values. All applications should have full access to the BluePrismCloud_Data_Protection certificate located in the certificate store on the local machine. IIS APPPOOL\ Blue Prism – IADA will also require access to the BPC_SQL_CERTIFICATE certificate.

For information on the Hub applications, see Hub software requirements and permissions.

Interact websites

Application name	Example service account name for SQL Windows Authentication	SQL Server permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - Interact	IIS APPPOOL\ Blue Prism – Interact	dbcreator / sysadmin	db_datawriter / db_datareader	InteractDB, InteractCacheDB
Blue Prism - Interact Remote API	IIS APPPOOL\ Blue Prism – Interact Remote API	dbcreator / sysadmin	db_datawriter / db_datareader	AuthenticationServerDB, InteractDB
Blue Prism - IADA	IIS APPPOOL\ Blue Prism – IADA	dbcreator / sysadmin	db_datawriter / db_datareader	IadaDB

Interact services

Application name	Example service account name for SQL Windows Authentication	SQL Server permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - Submit Form Manager	NT AUTHORITY\ SYSTEM	N/A	db_datawriter / db_datareader	InteractDB

Multi-device deployment considerations

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

Area	Environmental concerns (Development / Test / Pre-Production / Production)
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.
Message Broker Server	This is a single device focused on providing Message Broking services between Blue Prism components. A device per environment is recommended.
Web Server	A single device which can host multiple Blue Prism components. It is not recommended that environments are shared on this device and that a separate device is used per environment.
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. (For example, Production environments are likely to be most business critical). It is recommended that different types of environments, such as Development, UAT and Production environments, have their own dedicated SQL Server instance. However, you could run multiple Development environments on the same SQL Server instance.
Digital Worker Certificates	Decide if there is an additional requirement to apply certificate-based security to the instructional communications from the Interactive Clients and Application Servers to each Digital Worker; and to inbound communications received by the Digital Workers if they are hosting web services. If a certificate is required, this must be manually generated and installed on each applicable Digital Worker. The common name on the certificate must align with the address that the Blue Prism components will be configured to use when communicating with the devices (for example, FQDN or machine short name). Additionally, all devices that will connect to the Digital Workers must trust the Certification Authority that issued the manually generated certificate(s).

Network ports

To ensure Network connectivity between devices within the architecture the Windows Firewall on the applicable servers will need to allow the following traffic flows:

Database server	Port 1433 to allow SQL Server Connectivity from the Web Server. If the SQL Server instance is a named instance, it will also require: • The TCP Port for the named instance (this is dynamic by default from the ephemeral range) or the defined port if a static one to allow SQL Server Connectivity from the Web Server. • UDP Port 1434 for the SQL Server Browser Service to allow SQL Server Connectivity from the Web Server.
Message Broker server	Port 5672 to allow RabbitMQ Messaging connectivity. Port 15672 to allow RabbitMQ Management Console connectivity.
Web server	Port 443 to allow HTTPS connectivity.
Digital Workers	Port 443 to allow HTTPS connectivity.

It is recommended that your organization's network infrastructure expert is consulted when configuring the ports. There may be other ports that need to be configured to ensure connectivity in your organization.

Typical deployment

Suitable for production and non-production use, a typical deployment contains all components of Blue Prism Interact deployed to separate machines.

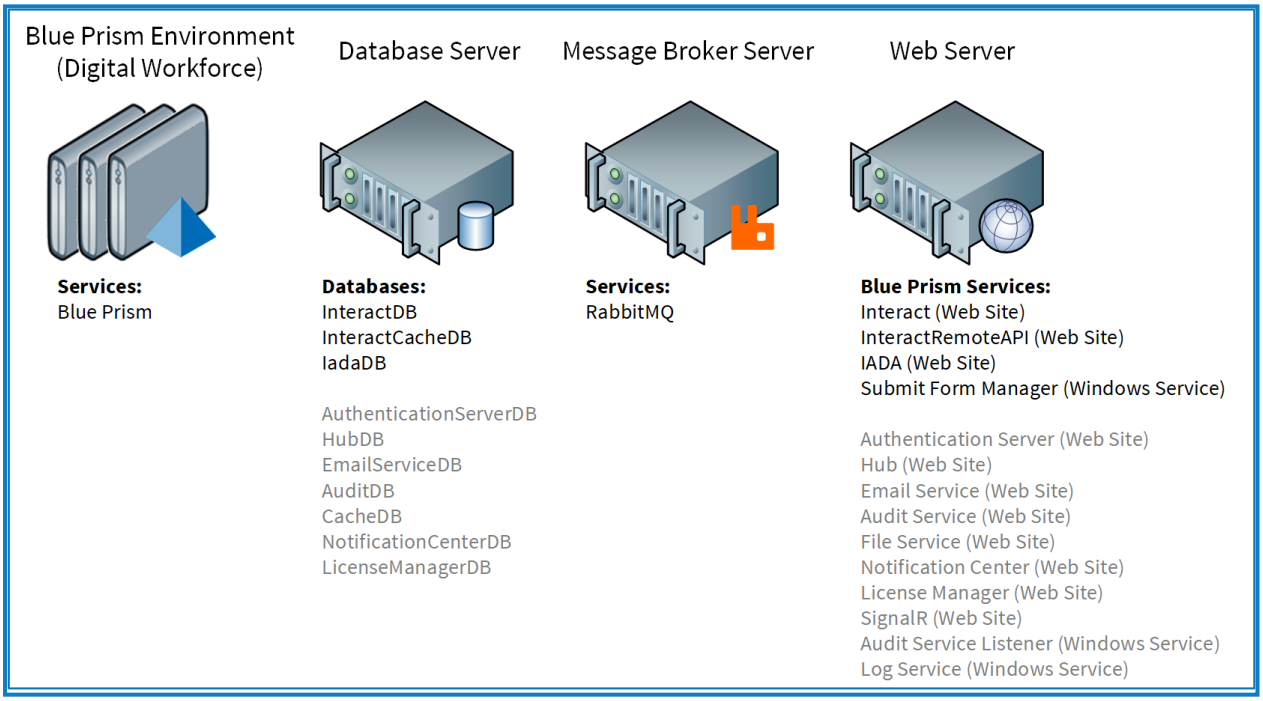
Prior to following this guidance, ensure that you have fully considered the information in Preparation.

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

- Web Server
- Message Broker Server
- Digital Workers
- SQL Server

The Message Broker Server and SQL Server instances must be pre-configured prior to the installation of Blue Prism Interact.

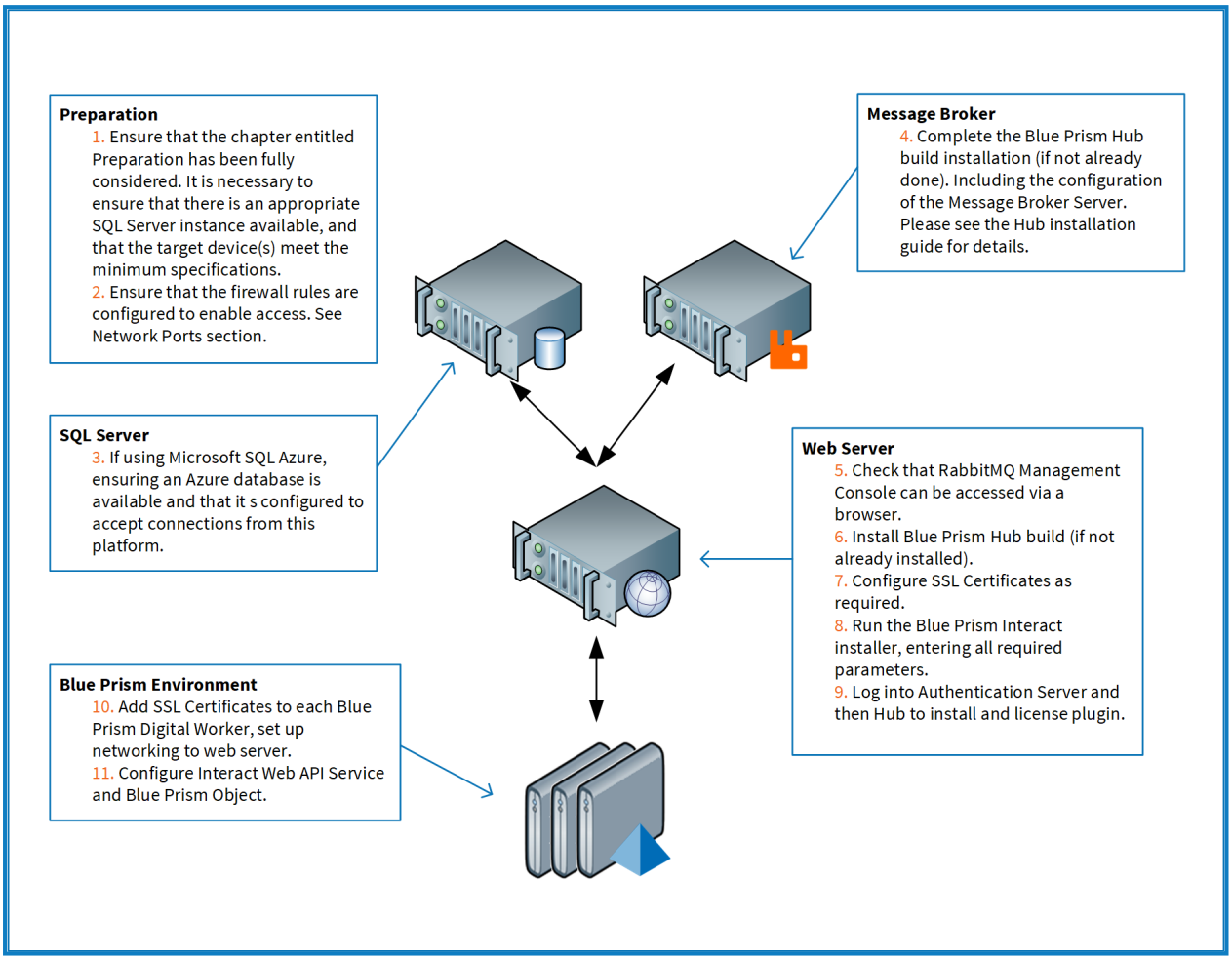
The diagram below illustrates the typical architecture for an environment.



Items in gray are deployed as part of the Blue Prism Hub installation.

Overview of typical installation steps

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



If you experience problems whilst installing, see Troubleshooting an installation.

Install the Message Broker server

Install and configure the Message Broker server, including configuring the Windows Firewall to enable network connectivity and the RabbitMQ management console.

Instructional videos on how to install the software for the Message Broker server are available from: https://bpdocs.blueprism.com/en-us/video/installation.htm.

If the Message Broker is not already installed and configured, then follow the steps below:

1. Download and install Erlang, accepting the default settings in the installation wizard.

   The version of Erlang that you require is dependent on the RabbitMQ version you intend to use. For:

   - Erlang/OTP version and support, see RabbitMQ Erlang Version Requirements.
   - Installation information, see the Erlang/OTP installation guide.
   - Downloads, see Download Erlang/OTP.

   To watch this installation step, see our Erlang installation video.

2. Download and install RabbitMQ and accept the default settings.

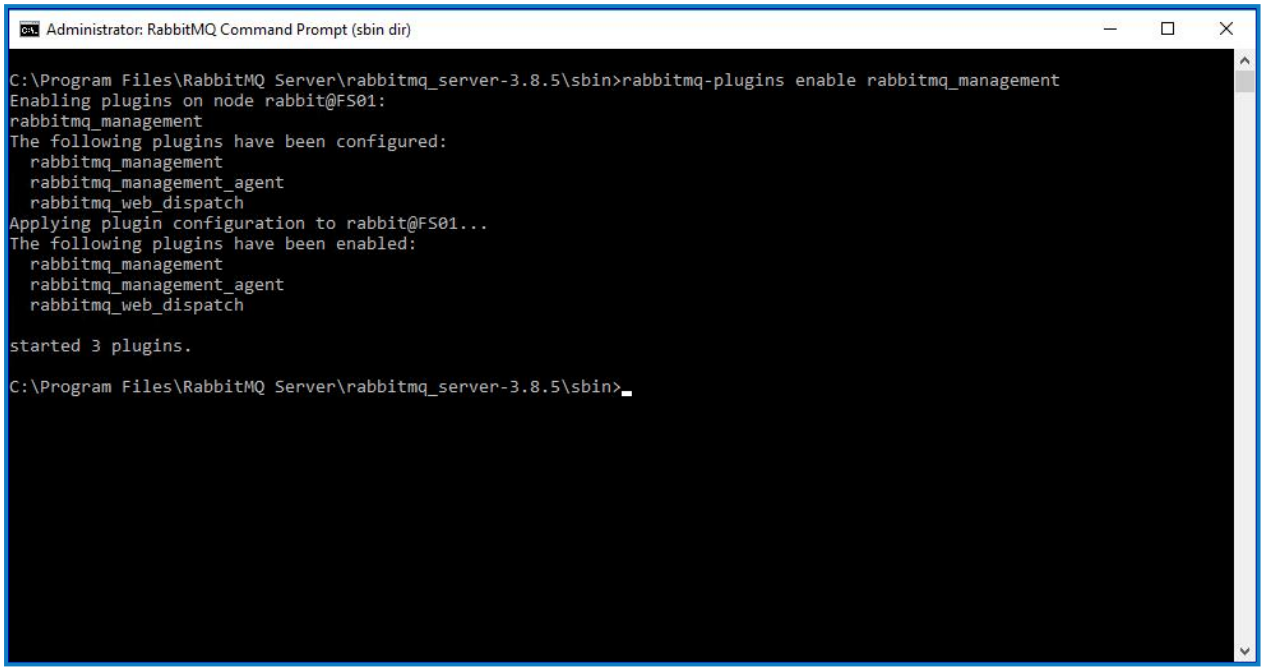
   For more information, see Downloading and Installing RabbitMQ.

   To watch this installation step, see our RabbitMQ installation video.

3. Configure Windows Firewall to enable inbound traffic to Ports 5672 and 15672.
4. From the Start menu, under the RabbitMQ Server folder, select the RabbitMQ Command Prompt (sbin dir).

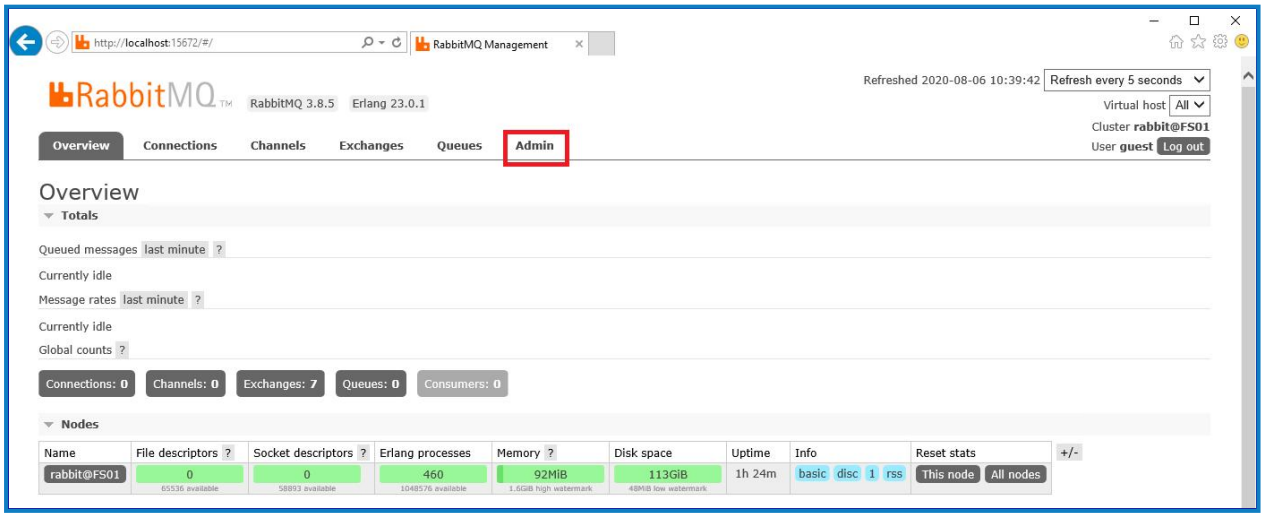
5. In the RabbitMQ Command Prompt window, type the following command:

```
rabbitmq-plugins enable rabbitmq_management
```

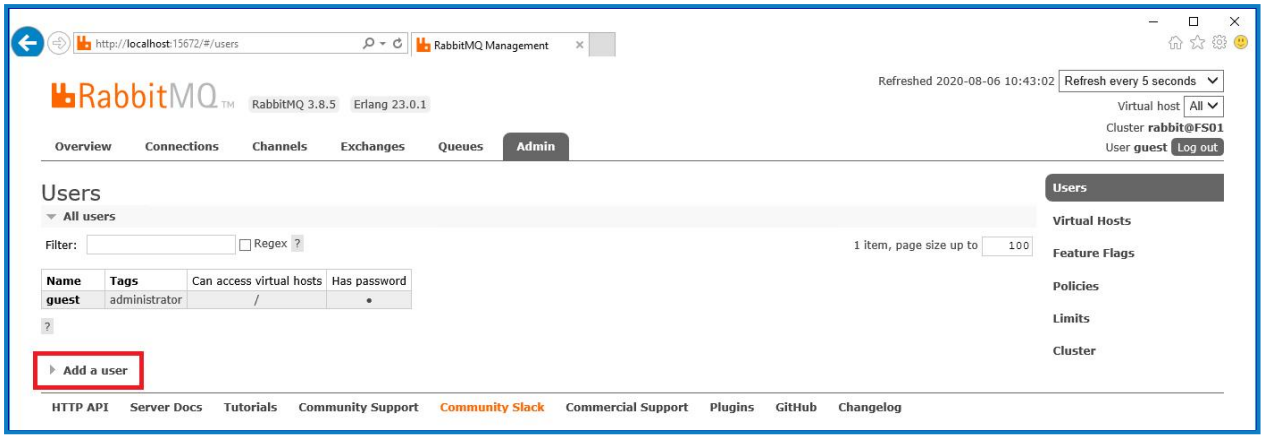


6. Launch a browser and navigate to the following URL: http://localhost:15672
7. In the RabbitMQ console, log on with the default credentials of guest/guest.

8. In the console, click **Admin**.



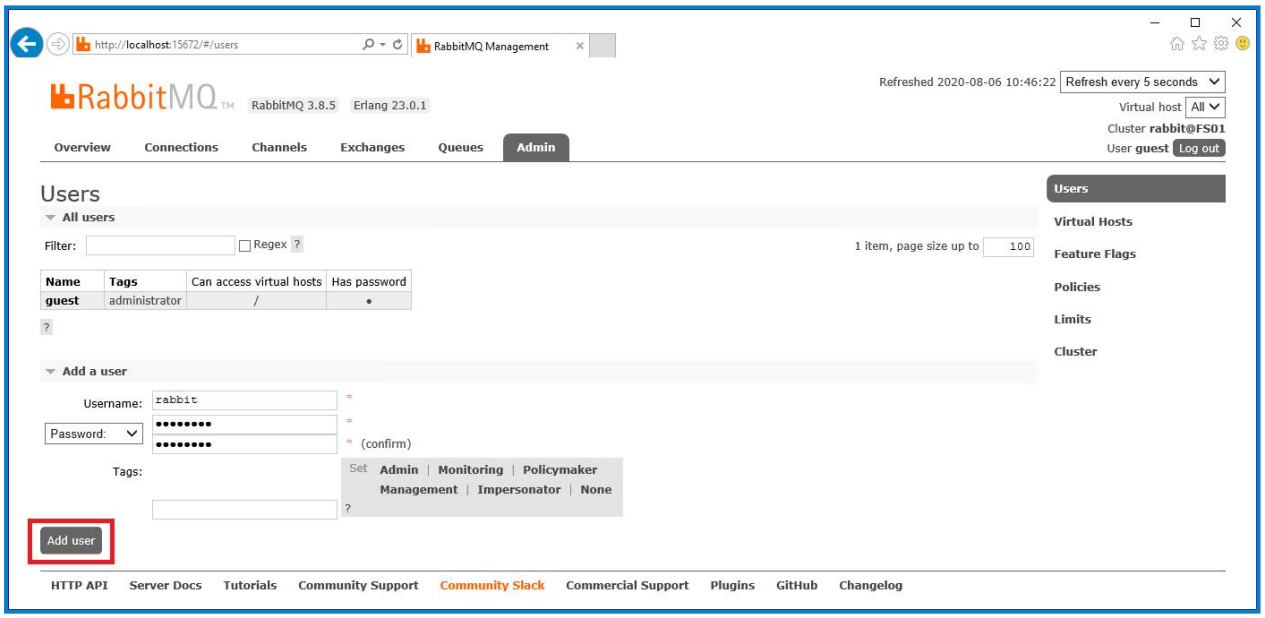
9. Click **Add a user**.



10. Enter the details for a new user, providing the username and password. The user does not require any special permissions and can be left at None.

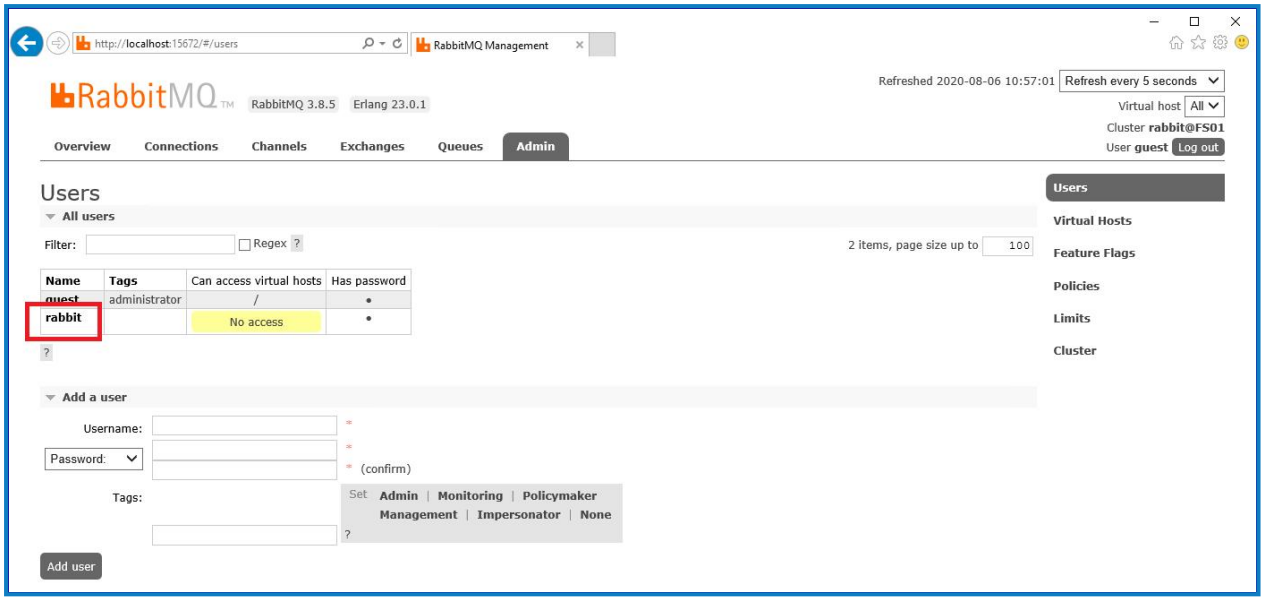
> The following characters must not be used for the password when creating the RabbitMQ user **# / : ? @ \ ` " $ '**.

11. Click **Add User**.

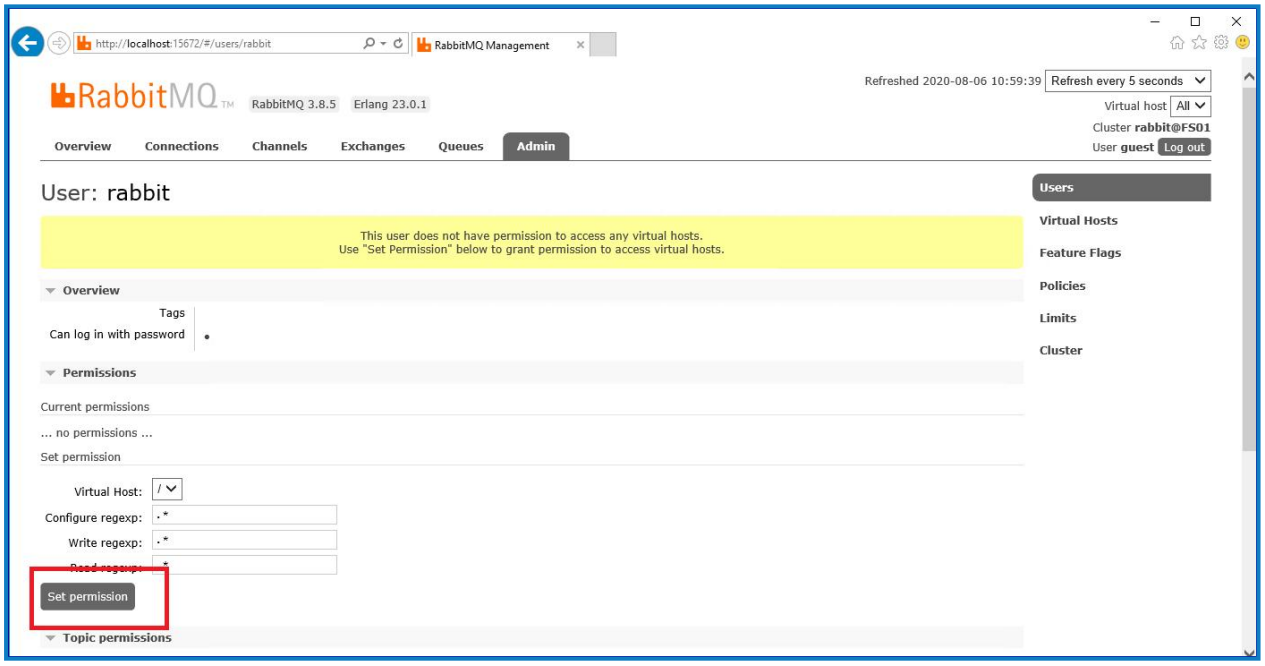


The next step is to set the permissions for the user.

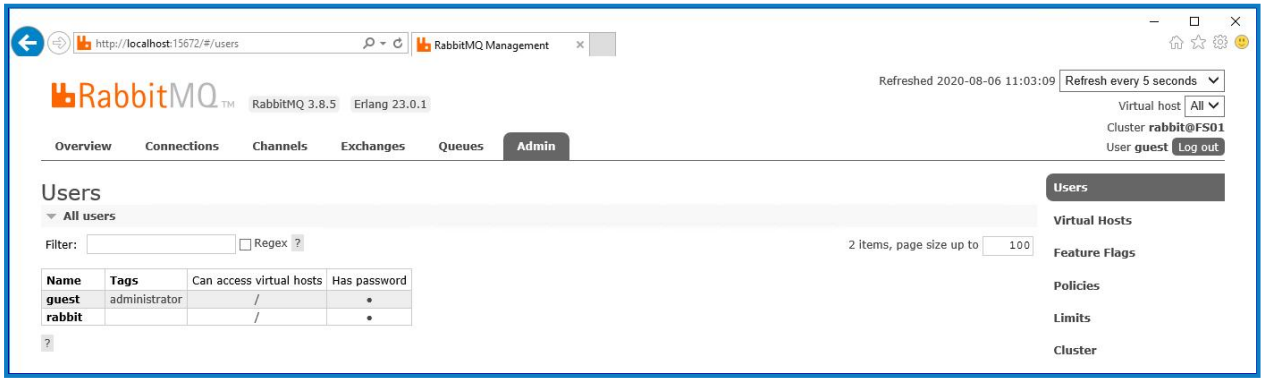
12. Click on the username of the user that you just created.



13. Click **Set Permission** to allocate the default permissions.



14. Select the **Admin** tab at the top and check that the permissions have been set properly as shown below.



This account has no Management Console access, so using the credentials you have just created will not enable any access.

This is a generic setup and base install of a RabbitMQ Message Broker service. It is recommended that the default passwords are changed and any security requirements such as applying SSL Certificates are completed by your IT department.

It is recommended that you create a new administrator account and remove the default guest account. Leaving the default guest account available may present a security risk.

Check RabbitMQ Message Broker connectivity

Launch a browser and type the following URL: http://<Message Broker Hostname>:15672

The login page for RabbitMQ Management Console should display.

You will not be able to log into the Management Console as the guest account is restricted to local access only and the account you created is not authorized to access the management console.

If the console does not appear, restart the RabbitMQ service. If the console still does not appear, see Troubleshoot a Hub installation on page 86.

Install and configure the web server

Before installing the Hub web server, ensure you have read the information in Preparation on page 7.

Install and configure the web server ensuring that the system can communicate with the RabbitMQ Message Broker.

The process consists of the following steps:

1. Install IIS
2. Configure SSL Certificates
3. Install the .NET Core components
4. Install Blue Prism Hub
5. Configure application pool recycling

The default host names provided in the procedures below are only suitable for a standalone environment, such as a test environment. Your organization's DNS and Domain structures must be considered when choosing host names in your installation.

Instructional videos on how to install the prerequisite software and Blue Prism Hub are available from: https://bpdocs.blueprism.com/en-us/video/installation.htm.

Install IIS

The system requires IIS Web Server and the .NET Core components to be installed.

It is important that IIS is installed prior to installing the .NET Core components and Blue Prism Hub. The IIS features and roles are automatically installed as part of the Blue Prism Hub installation.

Scripted installation

Run the command below using the PowerShell command prompt:

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

To watch this installation step, see our IIS installation video.

By default, IIS is installed with the **Anonymous Authentication** setting enabled. This setting is required by Hub and its associated sites. If you have disabled **Anonymous Authentication**, you must enable it before running the Hub installer. For more information about Anonymous authentication, see Microsoft's Anonymous Authentication page.

Configure SSL certificates

During the installation process you will be asked for the SSL certificates for the websites that are being set up. Depending on your infrastructure and IT organization security requirements, this could be an internally created SSL certificate or a purchased certificate to protect the websites.

The installer can be run without the certificates being present, though for the sites to operate, the bindings in the IIS websites will need to have valid SSL certificates present.

The tables below details the required SSL certificates.

Hub websites:

Website in IIS	Default URL (example only)
Websites with a user interface for use by end-users	
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – Hub	https://hub.local
Websites for use by the application only (services)	
Blue Prism – Email Service	https://email.local
Blue Prism – Audit Service	https://audit.local
Blue Prism – File Service	https://file.local
Blue Prism – Notification Center	https://notification.local
Blue Prism – License Manager	https://license.local
Blue Prism – SignalR	https://signalr.local

Interact websites:

Website in IIS	Default URL
Websites with a UI for use by end-users	
Blue Prism – Interact	https://interact.local
Websites for use by the application only (services)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

⚠ The default URLs shown above are suitable for a standalone environment, such as a test environment. Your organization's DNS and Domain structures must be considered when choosing host names for your installation.

Self-signed certificates

Self-signed certificates can be used but are only recommended for Proof of Concept (POC), Proof of Value (POV) and Development environments. For production environments, use certificates from your organization's approved certificate authority. It is recommended that you contact your IT Security team to check what their requirements are.

To generate a self-signed certificate:

1. Run PowerShell as an administrator and use the following command, replacing `[Website]` and `[ExpiryYears]` with appropriate values:

   ```
   New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "
   [Website].local" -FriendlyName "MySiteCert[Website]" -NotAfter (Get-Date).AddYears
   ([ExpiryYears])
   ```

   For example:

   ```
   New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
   "authentication.local" -FriendlyName "MySiteCertAuthentication" -NotAfter (Get-
   Date).AddYears(10)
   ```

   This example creates a self-signed certificate called *MySiteCertAuthentication* in the Personal Certificates store, with the Subject *authentication.local* and is valid for 10 years from the point of creation.
2. Open the Manage Computer Certificates application on your web server (type **manage computer** into the search bar).
3. Copy and paste the certificate from Personal > Certificates to Trusted Root Certification > Certificates.
4. Repeat this process for each website.

Scripted creation of self-signed certificates

> This process is not recommended for production environments. This process will create a single certificate which can be applied to each website.

Run the following PowerShell command:

```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
XXXXXXXXXX,authentication.local,hub.local,email.local,audit.local,file.local,signalr.local,notifi
cation.local,license.local,interact.local,iada.local,interactremoteapi.local -FriendlyName
"TheOneCert" -NotAfter (Get-Date).AddYears(10)
```

> XXXXXXXXXX should be replaced with the host server name.

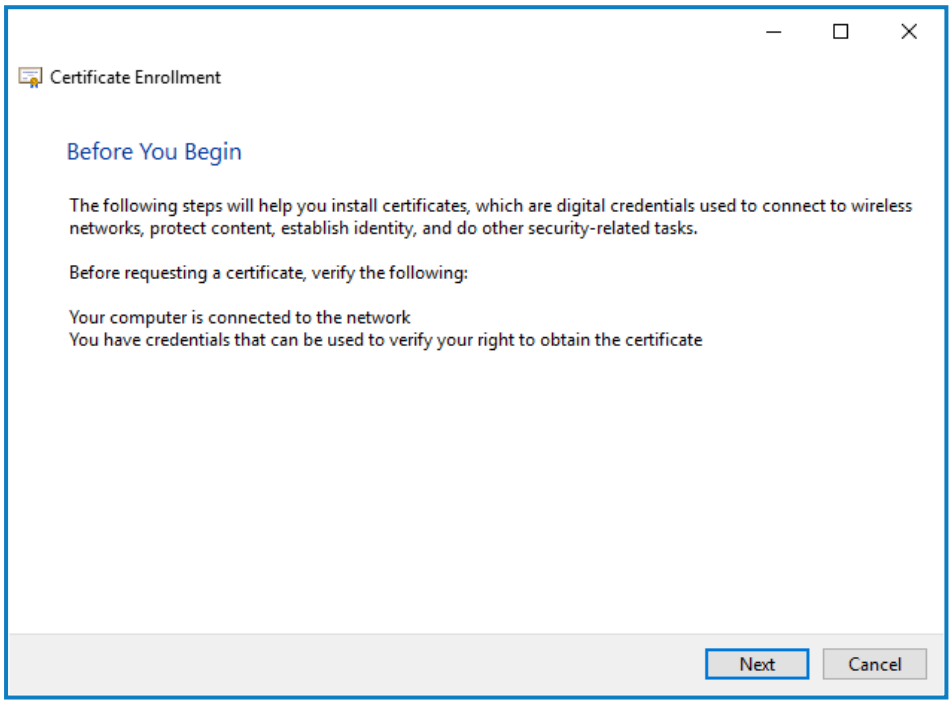
Once created, open the Local Machine certificate manager (certlm) and copy and paste the certificate into the trusted root certificate store.

Create an offline certificate request

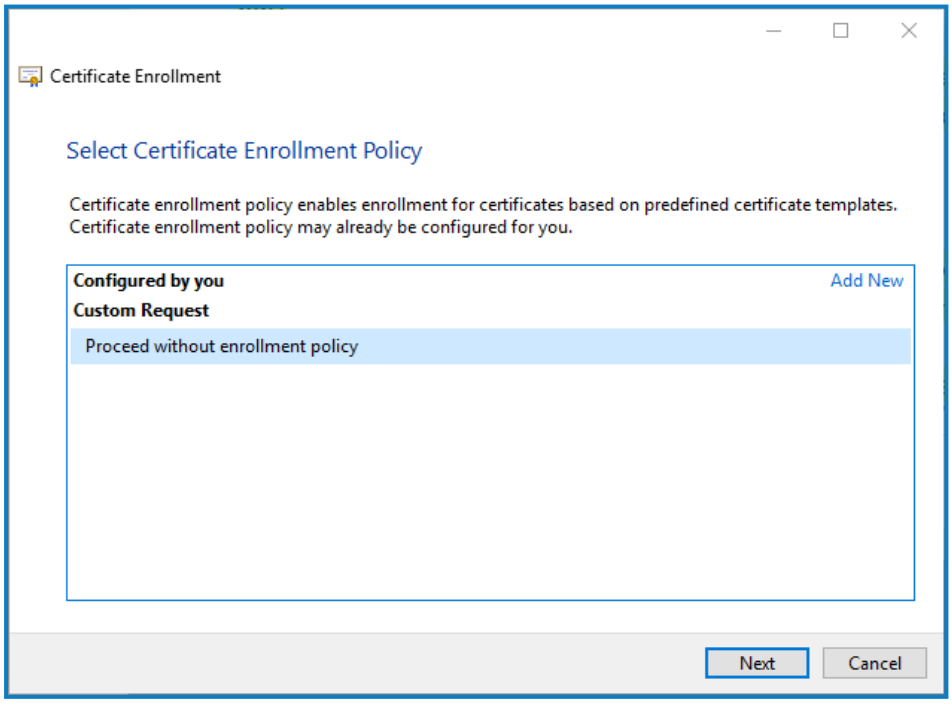
To create an offline certificate request, for each certificate follow this procedure:

1. Open the Manage Computer Certificates application on your web server (type **managed computer** into the search bar).
2. Right-click **Personal** > **Certificates** and select **All Tasks** > **Advanced Operations** > **Create Custom Request** from the shortcut menu.

   The Certificate Enrollment wizard displays.

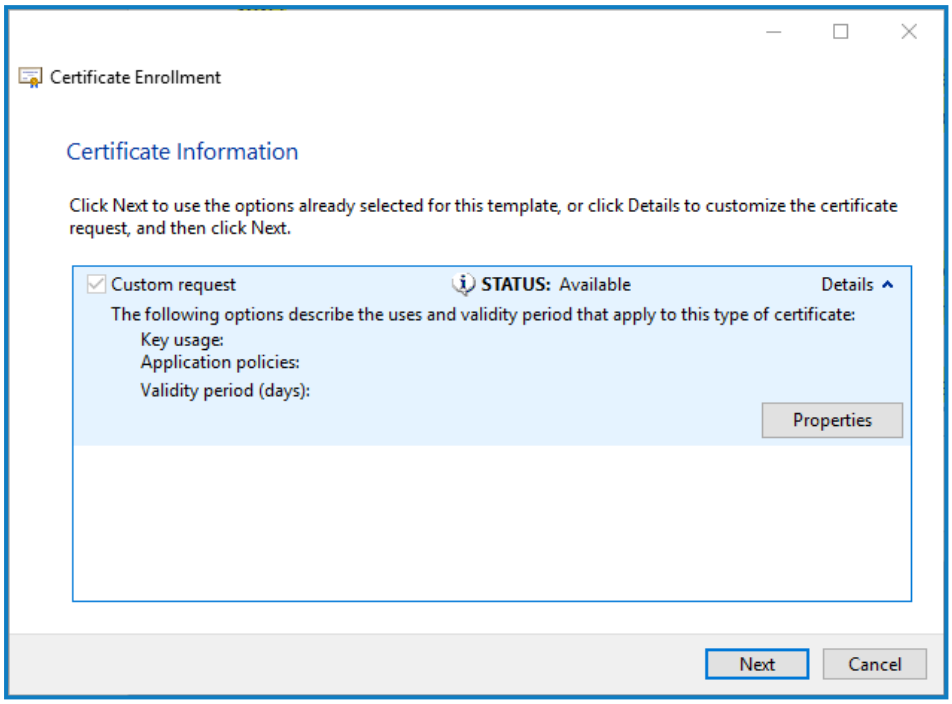


3. Click **Next**.



4. Select **Proceed without enrollment policy** and click **Next**.

5. On the Custom request screen, click **Next**.
6. On the Certificate Information screen, click the **Details** drop-down and click **Properties**.



7. On the General tab in the Certificate Properties dialog, enter a friendly name and description based on the website this certificate will be applied to.
8. On the Subject tab change the subject name type to **Common name**, enter the website URL in the **Value** field and click **Add**.

   The CN (common name) will display in the right-hand panel.
9. On the Extensions tab, click **Extended Key Usage**, select **Server Authentication** and click **Add**.
10. On the Private Key tab, click **Key options**, select a key size of your choice and select **Make private key exportable**.
11. Still on the Private Key tab, click **Hash Algorithm** and select a suitable Hash (optional).
12. Click **OK**.

    You are returned to the Certificate Enrollment screen.
13. Click **Next**.
14. Add a file name and path and click **Finish**.

After creating your certificate request, you will need to submit it to a Certificate Authority so they can process your request and issue a certificate. The certificate request is a text file. Usually, you are required to copy the text from the file and enter it into an online submission form on the Certificate Authority website. You will need to contact your Certificate Authority directly for instructions on the process for submitting your certificate request.

Install .NET Core Components

The .NET Core components must be downloaded and installed.

Step	Details
1	Download the following components and store them in a temporary location, for example, C:\temp: • .NET Core 3.1.11 Windows Server Hosting https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-aspnetcore-3.1.11-windows-hosting-bundle-installer • .NET Core 3.1.11 Windows Desktop Runtime https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-desktop-3.1.11-windows-x64-installer • Visual C++ Redistributable 2012 (x64) https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe • .NET Framework 4.7.2 https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer This is installed by default on Windows Server 2019. You only need to install the .NET Framework if you are using Windows Server 2016.

2	To install the .NET dependencies, run each of the following commands using the PowerShell command prompt, waiting until each completes, before running the next command:
	For Windows Server 2016:
	`start-process "C:\temp\dotnet-hosting-3.1.11-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-3.1.11-win-x64.exe" /q -wait`
	`start-process "C:\temp\vcredist_x64.exe" /q -wait`
	`start-process "C:\temp\NDP472-KB4054531-Web.exe" /q -wait`
	For Windows Server 2019:
	`start-process "C:\temp\dotnet-hosting-3.1.11-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-3.1.11-win-x64.exe" /q -wait`
	`start-process "C:\temp\vcredist_x64.exe" /q -wait`
	Ensure the file path matches the location where the files were stored in step 1.

3	Restart your server before installing Blue Prism Hub to ensure the components are fully installed and registered.

To watch this installation step, see our .NET installation video.

Install Blue Prism Hub

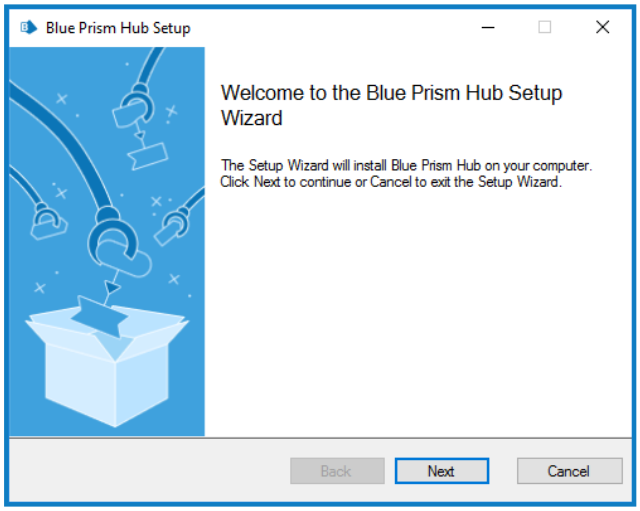
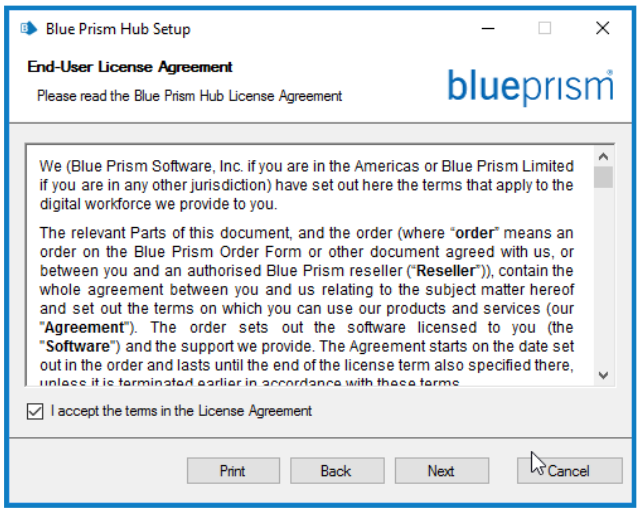
Before you install Blue Prism Hub:

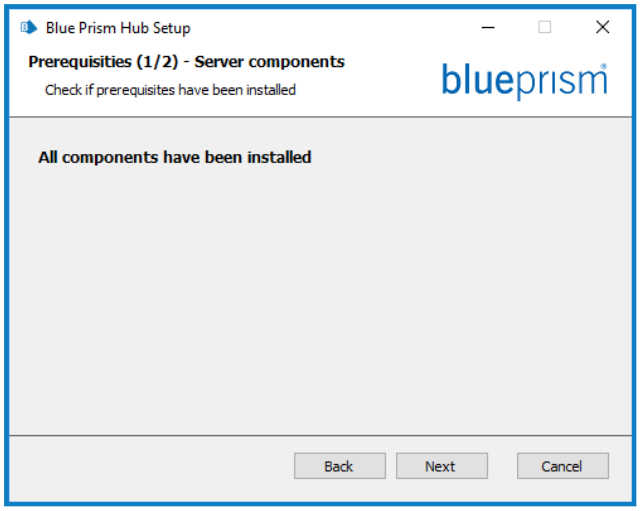
- If you have purchased ALM or Interact, you will need your Customer ID during this Hub installation. This can be found in the email that was sent to you when you purchased ALM or Interact.
- If you are reinstalling Blue Prism Hub after previously using and removing it, and the same database names are to be used, it is recommended that the databases should be cleared of any old data before re-installing.

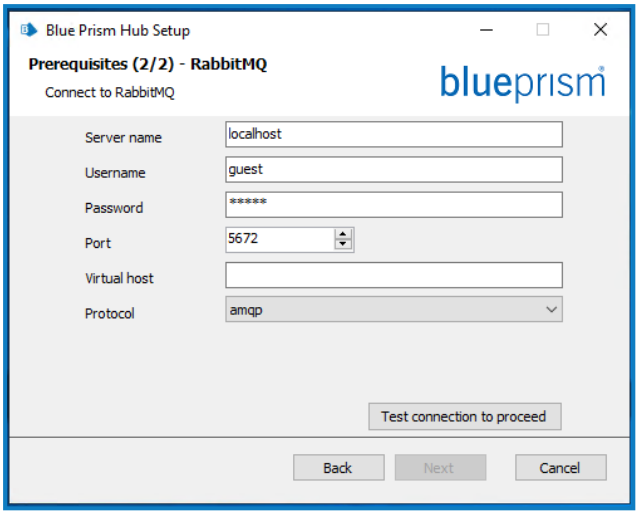
To watch the Hub installation and configuration process, see our Blue Prism Hub installation video.

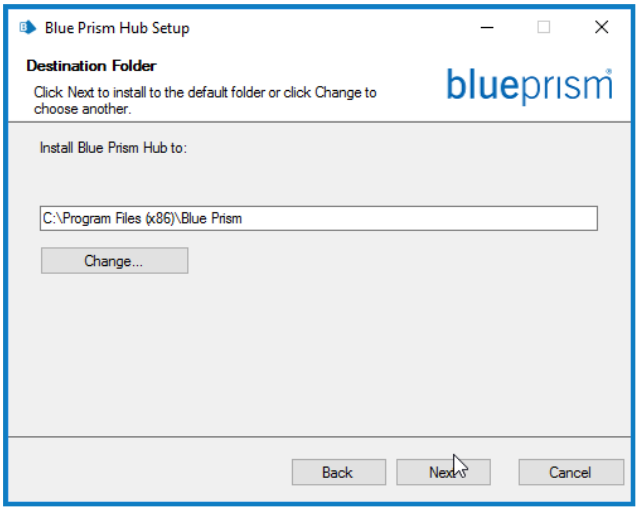
The steps below detail the process for installing the Blue Prism Hub software. This includes the Authentication Server, Hub, and other associated services. The installation process will create any new databases that are required.

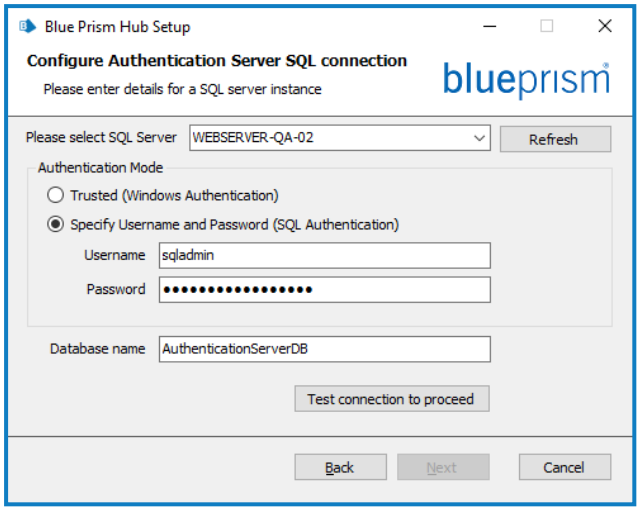
Download and run the Blue Prism Hub installer, available from the Blue Prism Portal, and progress through the installer as shown below. The installer must be run with administrator rights.

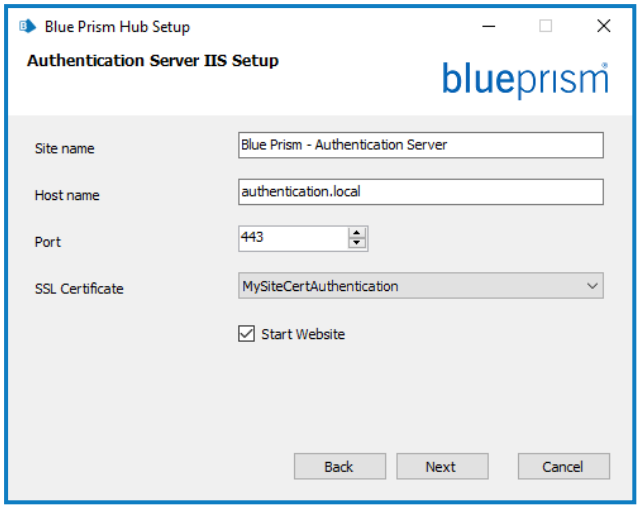
Step	Installer page	Details
1		**Welcome** Click **Next**.
2		**License agreement** Read the End-User License Agreement and if you agree to the terms, select the check box.

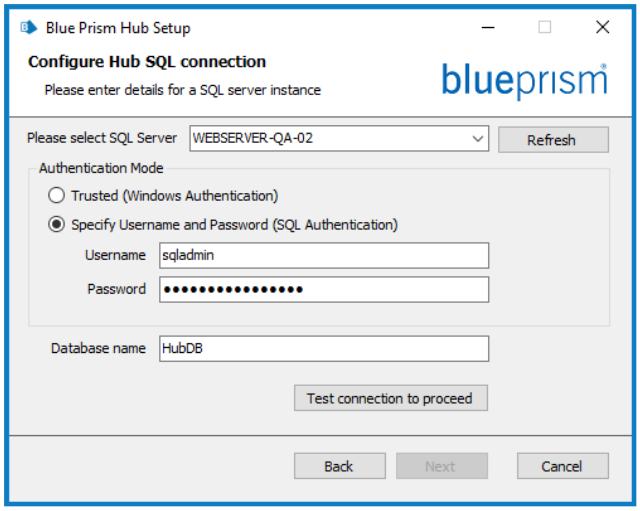
Step	Installer page	Details
3		**Prerequisites 1 – Server components** The installer checks that the prerequisites have been installed. Those that are not installed are identified. You cannot proceed until all the prerequisites are installed. If there are uninstalled prerequisites, cancel the installer and install the missing components before restarting the installer. Otherwise, proceed with the installation.

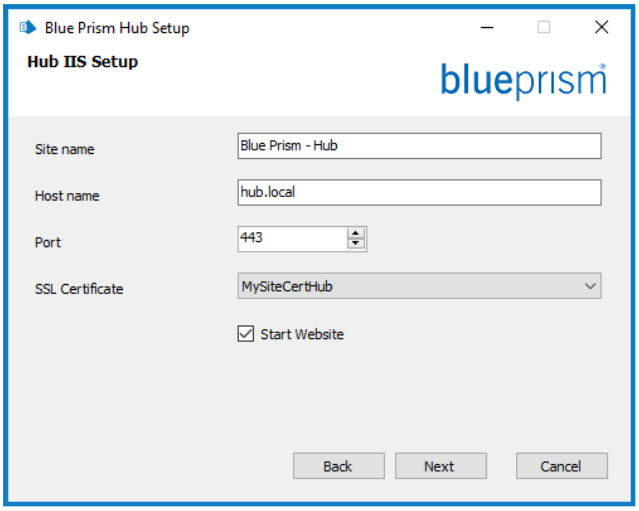
Step	Installer page	Details
4		**Prerequisites 2 – RabbitMQ** Enter the server name or IP address of the Message Broker server and the credentials of the user you created. The default message queuing port is 5672. This should only be changed if the default ports have been changed by your IT support organization. By default, the **Virtual host** field is blank. You can leave this as blank and the connection will be made to the RabbitMQ root. Alternatively, if you have virtual hosts set up in RabbitMQ, you can connect to a specific host. In **Virtual host**, enter the name of the virtual host on RabbitMQ that you want to connect to. The virtual host must already exist on RabbitMQ, you cannot enter a new name as this installer will not create a new virtual host. Further information about virtual hosts can be found on the RabbitMQ website - Virtual Hosts. From the **Protocol** drop-down list, select the protocol you want to use. You can select either AMQP or AMQPS. If you select AMQPS, an additional field displays for you to enter the certificate that should be used for the connection. Further information about TLS configuration and certificates can be found on the RabbitMQ website - TLS Support. If you are using AMQPS, you will need to give the Blue Prism IIS application pools full control of the RabbitMQ certificate. For more information, see Troubleshoot a Hub installation on page 86. Click **Test connection** to verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see

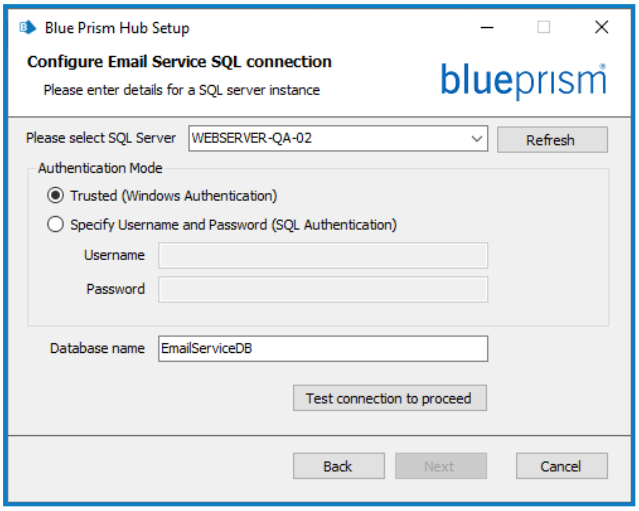
Step	Installer page	Details
		Troubleshoot a Hub installation on page 86 for further details.
5		**Destination folder** Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the **Change** button.

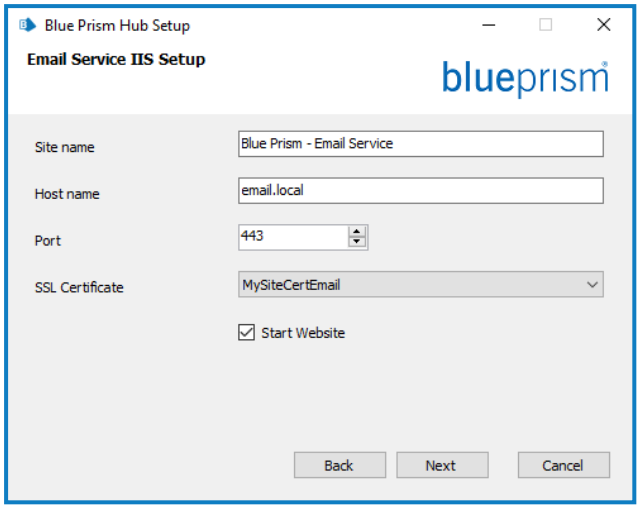
Step	Installer page	Details
6		**Authentication Server SQL connection** Configure the settings for the Authentication Server database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

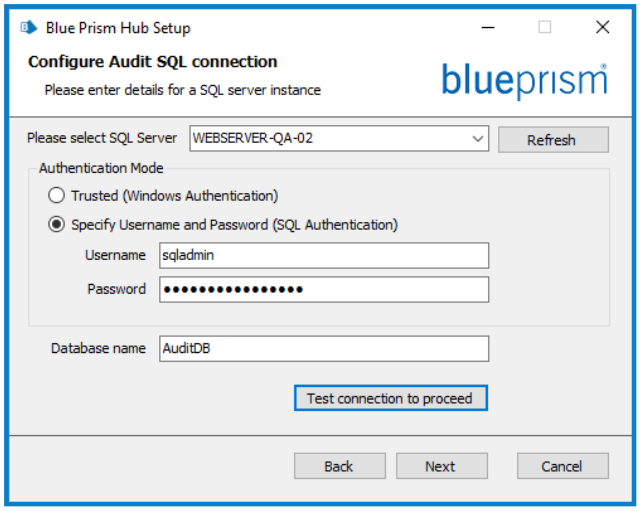
Step	Installer page	Details
7		**Authentication Server IIS setup** Configure IIS for the Authentication Server website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

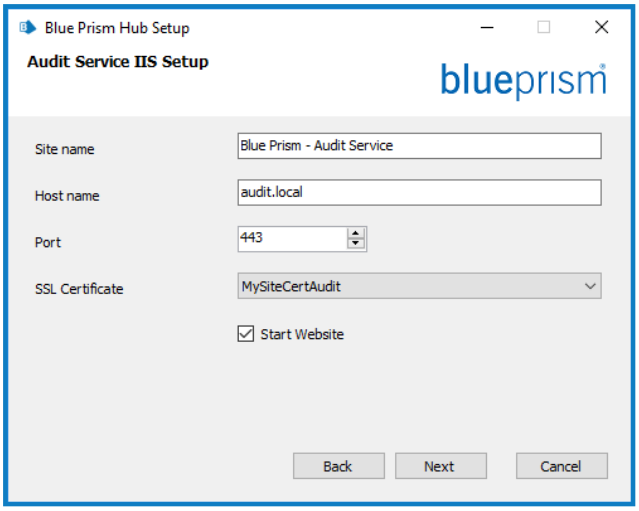
Step	Installer page	Details
8		**Hub SQL connection** Configure the settings for the Hub database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

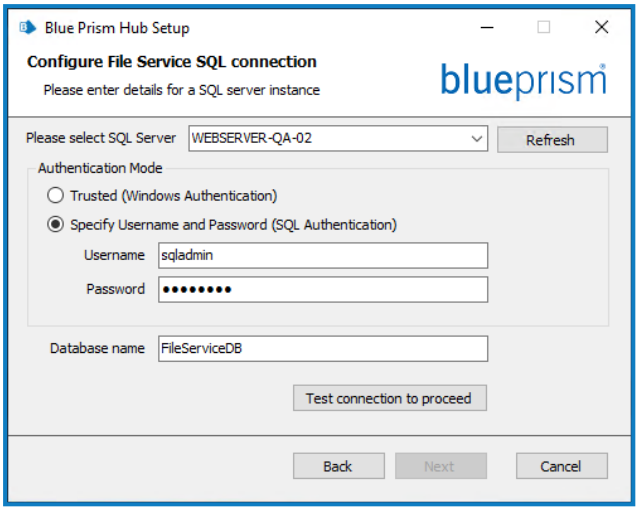
Step	Installer page	Details
9		**Hub IIS setup** Configure the Hub website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

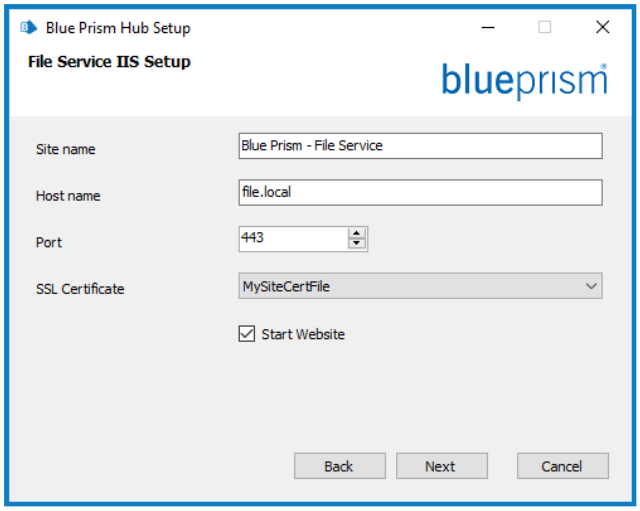
Step	Installer page	Details
10		**Email Service SQL connection** Configure the settings for the Email Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

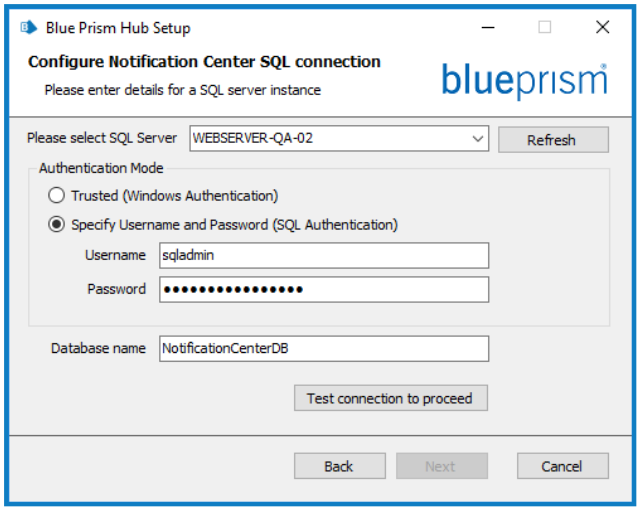
Step	Installer page	Details
11		**Email Service IIS setup** Configure the Email Service website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

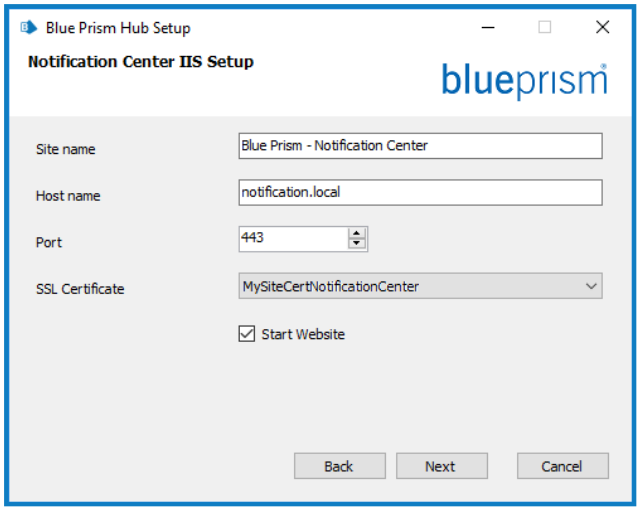
Step	Installer page	Details
12		**Audit SQL connection configuration** Configure the settings for the Audit database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

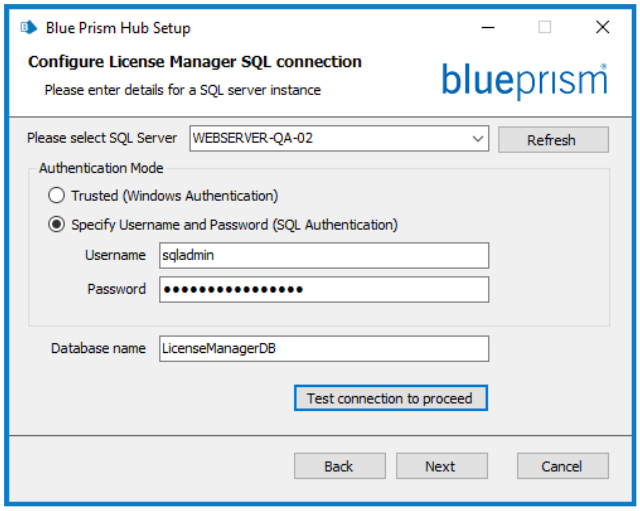
Step	Installer page	Details
13		**Audit Service IIS setup** Configure the Audit Service website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

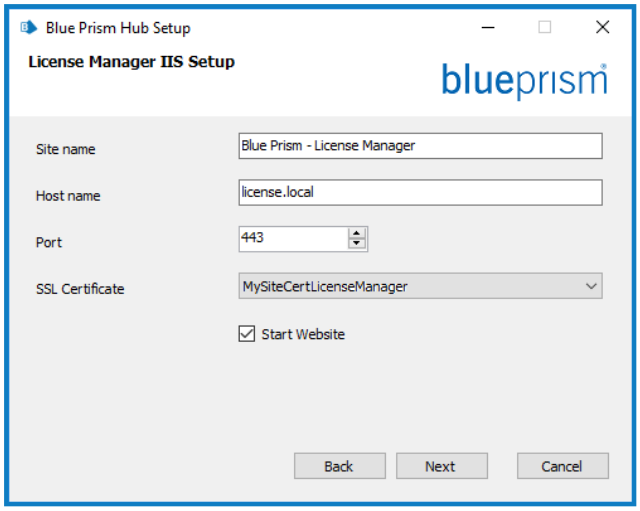
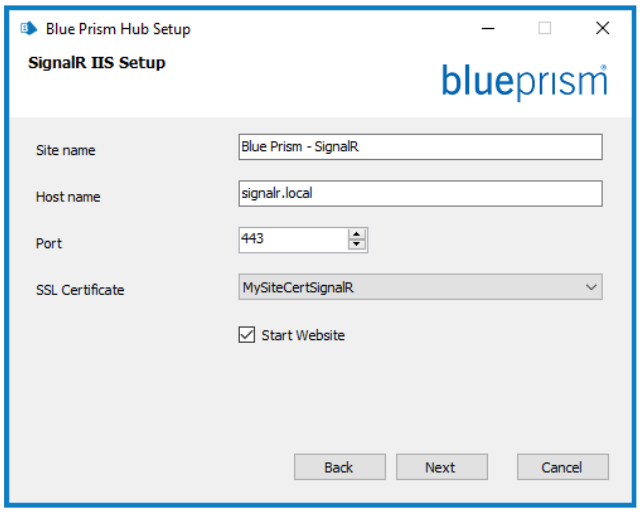
Step	Installer page	Details
14		**File Service SQL connection configuration** Configure the settings for the File Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

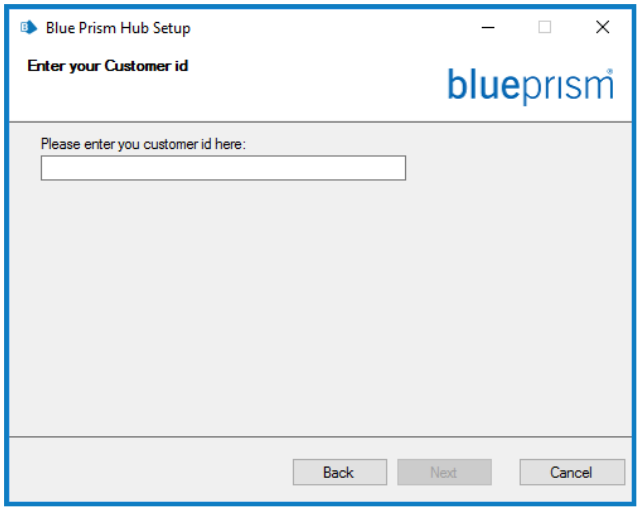
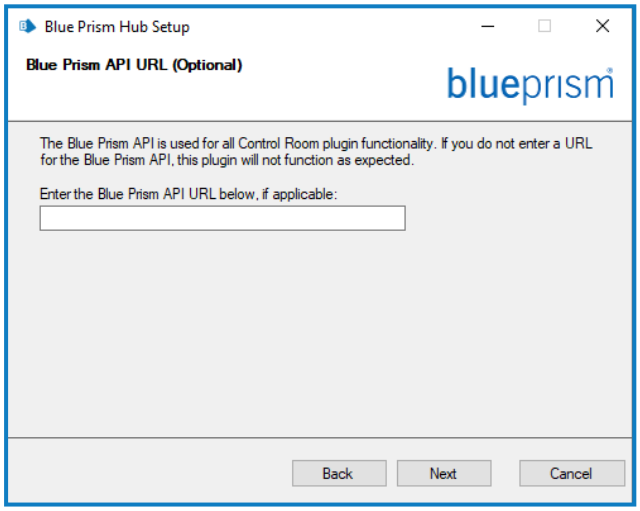
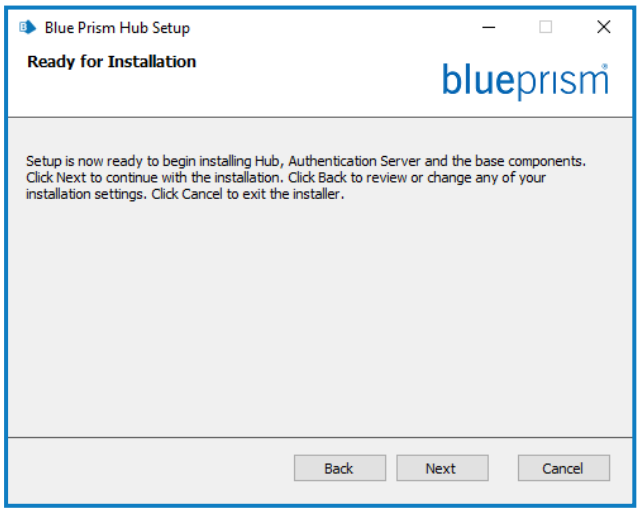
Step	Installer page	Details
15		**File Service IIS setup** Configure the File Service website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

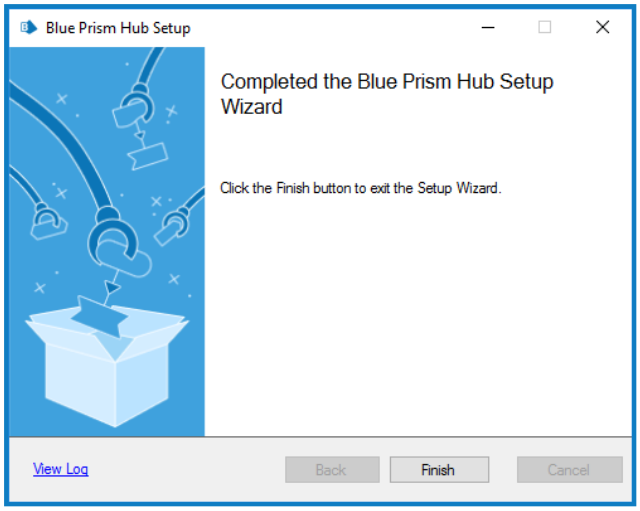
Step	Installer page	Details
16		**Notification Center SQL connection** Configure the settings for the Notification Center database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

Step	Installer page	Details
17		**Notification Center IIS setup** Configure the Notification Center website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

Step	Installer page	Details
18		**License Manager SQL connection** Configure the settings for the License Manager database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 86 for further details.

Step	Installer page	Details
19		**License Manager IIS setup** Configure the License Manager website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.
20		**SignalR IIS setup** Configure the SignalR website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

Step	Installer page	Details
21		**Enter your Customer Id** Enter your customer identifier. This identifier is supplied to you by Blue Prism when you receive your product license for ALM or Interact. If you have not purchased a licensed plugin, you can enter your own value. If you later purchase a licensed plug, your customer ID will need to be changed within the configuration file. For more information, see Troubleshoot a Hub installation on page 86.
22		**Blue Prism API URL (Optional)** If required, enter the URL for the Blue Prism API. This URL is essential if you want to use the Control Room plugin. The Control Room plugin is compatible with Blue Prism 7.0 or later. If you decide to use the Control Room plugin and you have not entered a URL at this point, you will need to update the configuration file. For more information, see Troubleshoot a Hub installation on page 86.
23		**Ready for Installation** Click **Next** to install Hub.

Step	Installer page	Details
24		**Installation complete** If the installation fails, the **View Log** option gives details of the error that was encountered. For more information, see Troubleshoot a Hub installation on page 86.

Configure application pool recycling

The application pools for Authentication Server and Hub should be set to recycle one after the other, with Authentication Server recycling first. You should configure the application pools to recycle at a specific time during non-working hours, or periods of low usage. The application pool for Authentication Server should be set to recycle at least 10 minutes before the Hub application pool.

There are several different methods you can use to set the recycling information. The steps below use the Internet Information Services (IIS) Manager:

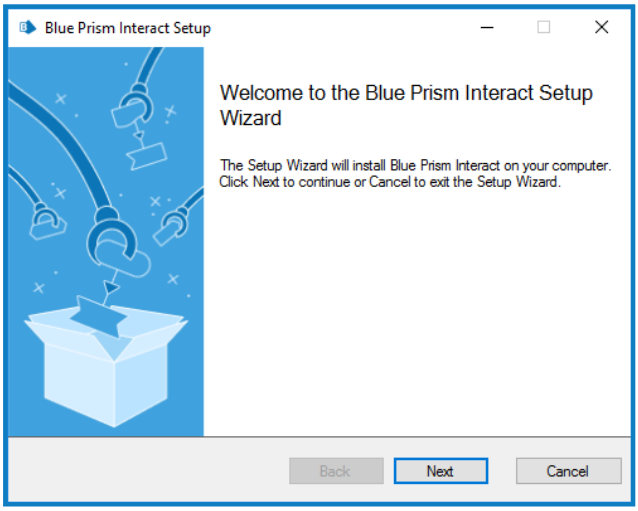
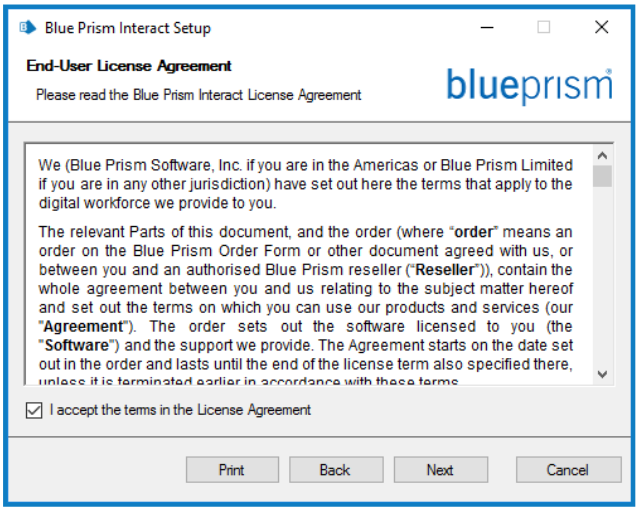
1. In the Internet Information Services (IIS) Manager, right-click the appropriate application pool and select **Recycling...**.
2. Clear the **Regular time intervals (in minutes)** option.
3. Select the **Specific time(s)** option and enter a time into the field:
   - For the Blue Prism - Hub application pool, set it to use a specific time during non-working hours, or periods of low usage.
   - For the Blue Prism - Authentication Server application pool, set it to use a specific time at least 10 minutes before the Hub application pool time.
4. Click **Next**, and then click **Finish**.

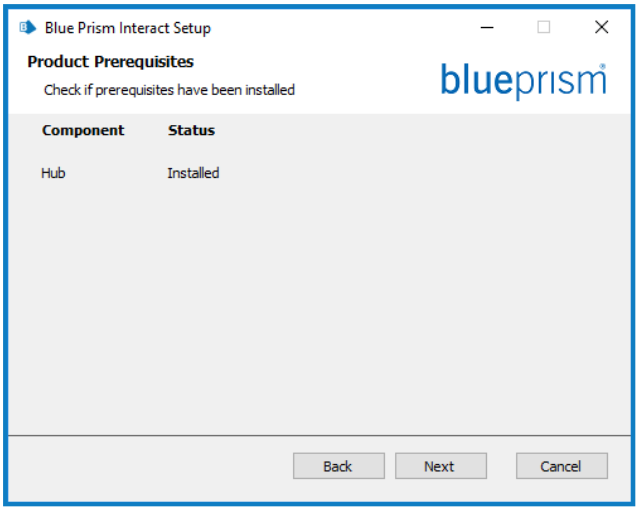
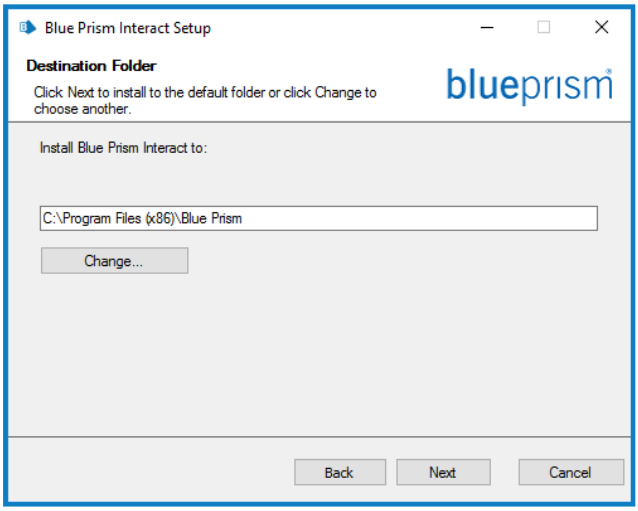
Install Blue Prism Interact

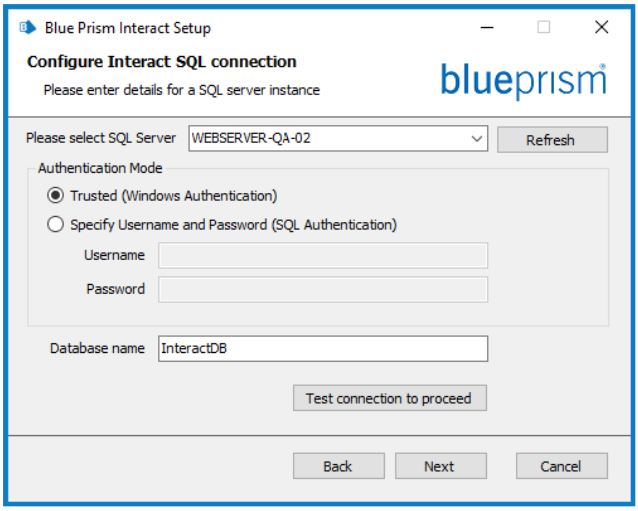
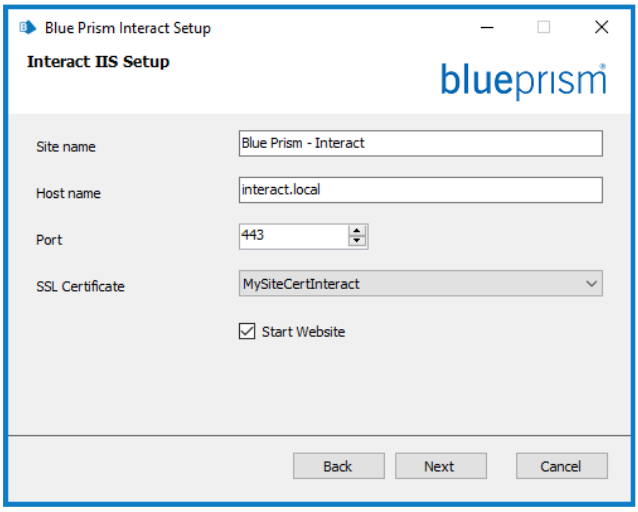
The steps below detail the process for installing the Blue Prism Interact software. This assumes that Blue Prism Hub has been installed which includes the Authentication Server, Hub, and other associated services.

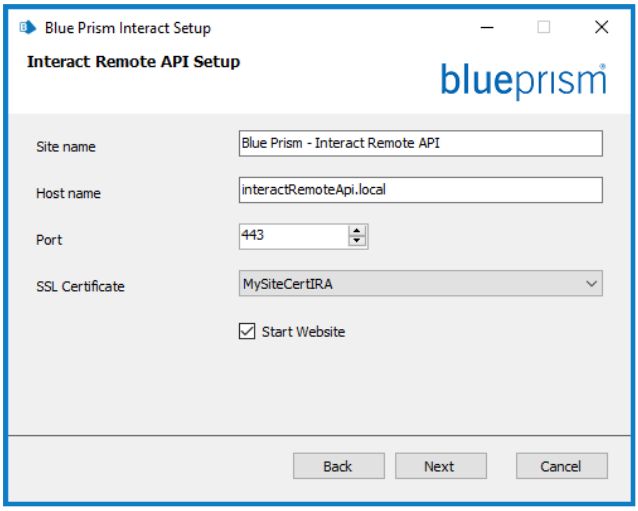
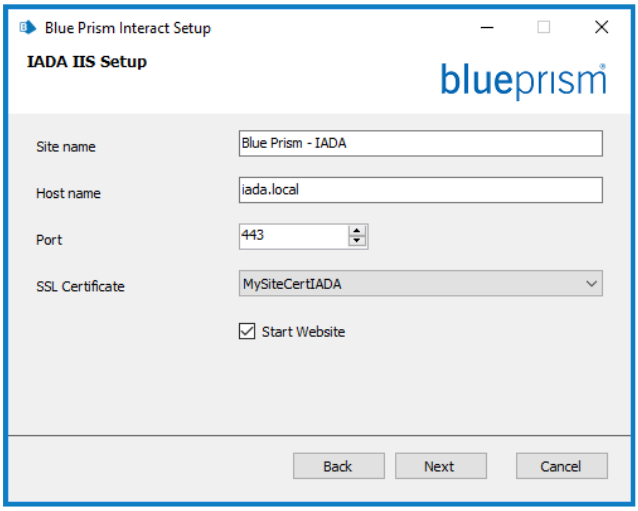
Download and run the Blue Prism Interact installer, available from the Blue Prism Portal, and progress through the installer as shown below. The installer must be run with administrator rights.

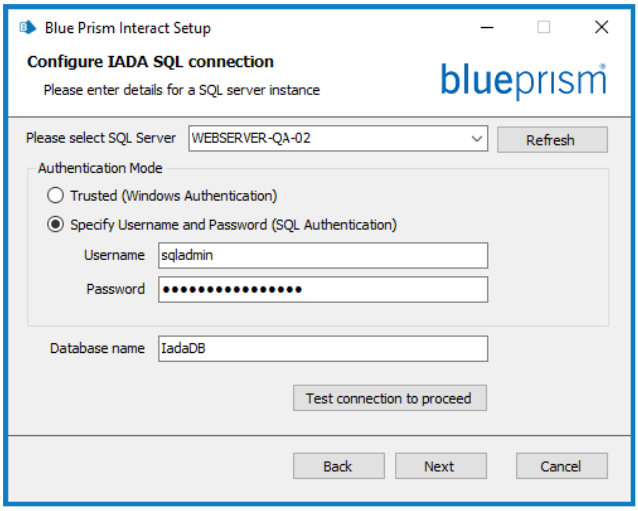
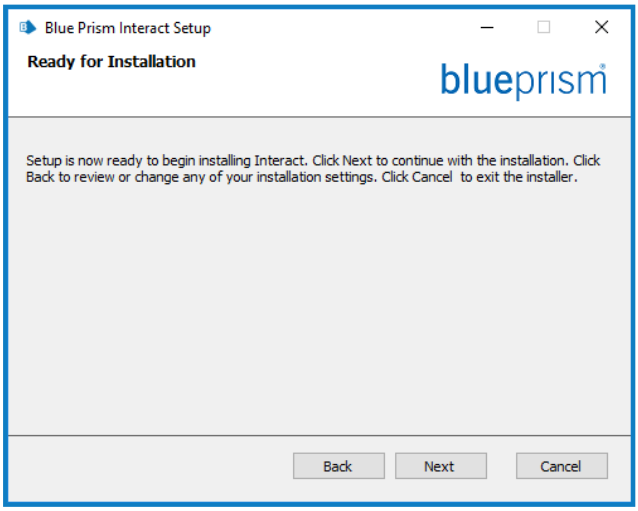
To watch the Interact installation and configuration process, see our Blue Prism Interact installation video.

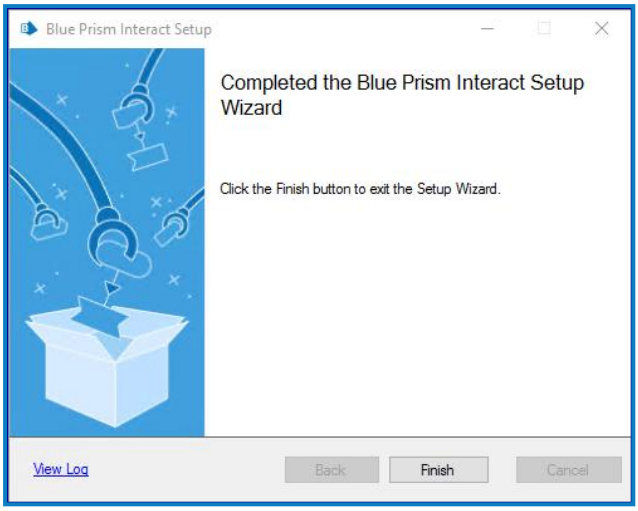
Step	Installer page	Details
1		**Welcome** Click **Next**.
2		**License agreement** Read the End-User License Agreement and if you agree to the terms, select the check box.

Step	Installer page	Details
3		**Product prerequisites** The installer checks that the prerequisites have been installed. If the installer finds any prerequisites missing these will be notified to you. Otherwise, continue with the installation. You cannot proceed unless all prerequisites have been installed.
4		**Destination folder** Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the **Change** button.

Step	Installer page	Details
5		**Configure Interact SQL configuration** Configure the settings for the Interact Database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 56 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot an Interact installation on page 80 for further details.
6		**Interact IIS setup** Configure the Interact website. You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

Step	Installer page	Details
7		**Interact Remote API setup** You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.
8		**IADA IIS setup** You need to: • Enter a site name. • Enter a host name – This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation.

Step	Installer page	Details
9		**Configure IADA SQL configuration** Configure the settings for IADA by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on the next page for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=) or a semi-colon (;). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot an Interact installation on page 80 for further details.
10		**Ready for Installation** Click **Next** to install Interact.

Step	Installer page	Details
11		**Installation complete** If the installation fails, the **View Log** option gives details of the error that was encountered. For more information, see Troubleshooting an installation. Click **Finish**.

Configure application pool recycling

The application pools for Authentication Server and Interact should be set to recycle one after the other, with Authentication Server recycling first. You should configure the application pools to recycle at a specific time during non-working hours, or periods of low usage. The application pool for Authentication Server should be set to recycle at least 10 minutes before the Interact application pool.

There are several different methods you can use to set the recycling information. The steps below use the Internet Information Services (IIS) Manager:

1. In the Internet Information Services (IIS) Manager, right-click the appropriate application pool and select **Recycling...**.
2. Clear the **Regular time intervals (in minutes)** option.
3. Select the **Specific time(s)** option and enter a time into the field:
   - For the Blue Prism - Interact application pool, set it to use a specific time during non-working hours, or periods of low usage.
   - For the Blue Prism - Authentication Server application pool, set it to use a specific time at least 10 minutes before the Interact application pool time.
4. Click **Next**, and then click **Finish**.

Installing using Windows Authentication

The account used when running the installation must have the relevant SQL Server permissions to carry out the installation, that is, membership in either the sysadmin or dbcreator fixed server roles.

If Windows Authentication is chosen during the installation process, a Windows service account must be used for the application pools and services that has the necessary permissions to execute the tasks and processes during normal operation. The Windows service account will need:

- The ability to perform the SQL database processes, see Minimum SQL permissions on page 14.
- Permissions for the required certificates.
- Ownership over the IIS Application Pool.
- Ownership over the Windows services installed by Hub and Interact.

Assigning the Windows service account as an owner on certificates

The Windows service account needs to be granted permissions to the BluePrismCloud certificates. To do this:

1. On the web server, open the Certificate Manager. To do this, type *Certificates* in the search box on the Windows taskbar, and then click **Manage Computer Certificates**.
2. In the navigation pane, expand **Personal** and click **Certificates**.
3. Follow the steps below for both the BluePrismCloud_Data_Protection and BluePrismCloud_IMS_JWT certificates:
    a. Right-click the certificate and select **All Tasks**, and click **Manage Private Keys...**.

    The Permissions dialog for the certificate displays.

    b. Click **Add**, then enter the service account and click **OK**.
    c. With the service account selected in the **Group or user name** list, ensure that **Full control** is selected in the **Permissions for {account name}** list.
    d. Click **OK**.

    The service account now has access to the certificate.

Assigning a Windows service account to the application pool

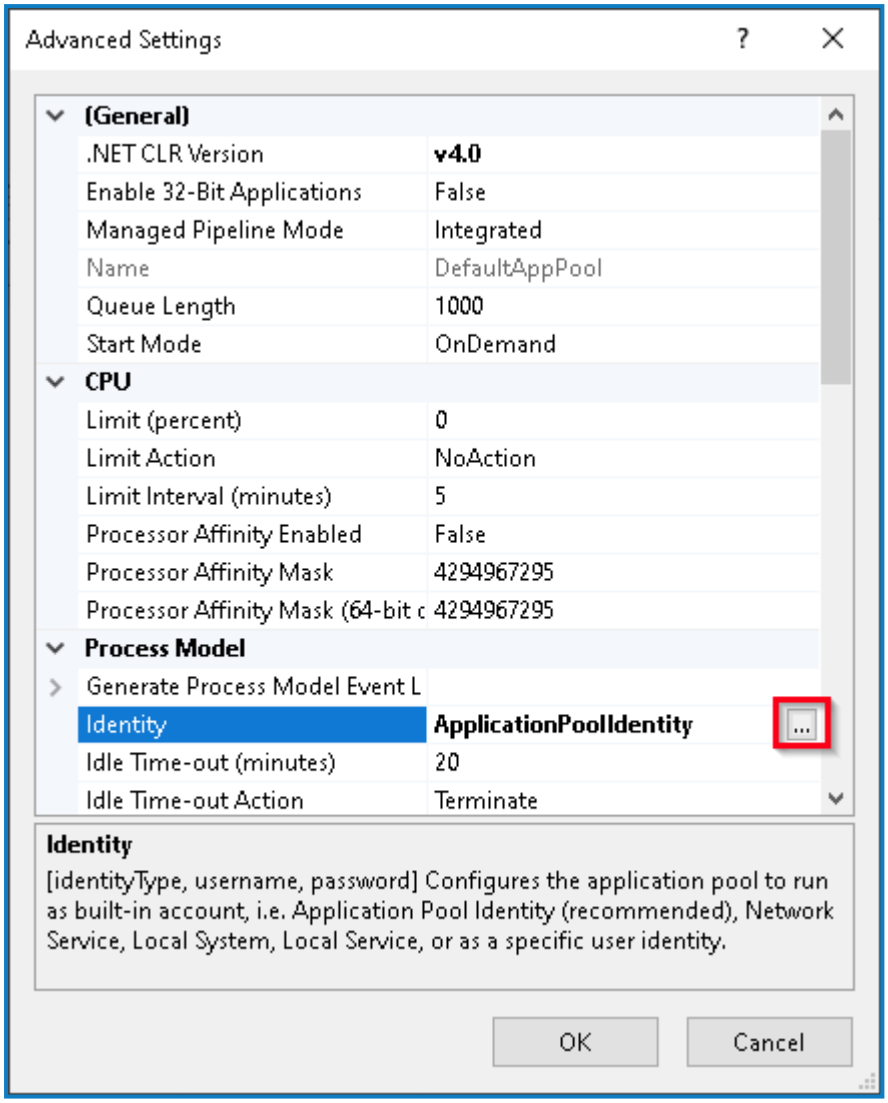
By default, the application pools are created with the identity 'ApplicationPoolIdentity'. After the installer has completed, the Windows service account will need to be allocated to manage the application pools. To do this:

1. On the web server, open Internet Information Services (IIS) Manager.
2. In the Connections panel, expand the host and select **Application Pools**.
3. Review the **Identity** column values.

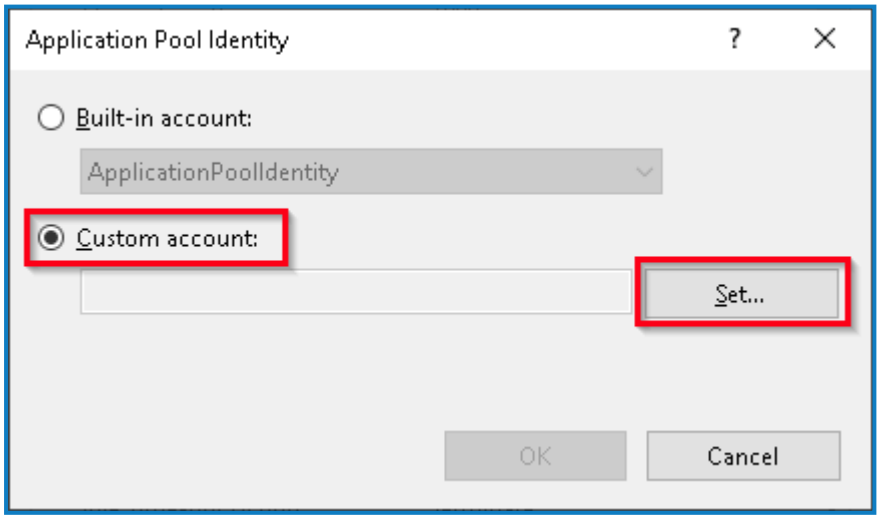
    The identity for an application pool should match the specific Windows service account.
4. For any application pools that have *ApplicationPoolIdentity* in the **Identity** column, right-click the row and select **Advanced Settings...**.

    The Advanced Settings dialog displays.

5. Select the **Identity** setting then click the **...** (ellipsis) button:



6. In the Application Pool Identity dialog, select **Custom account** and then click **Set...**.



The Set Credentials dialog displays.

7. Enter the credentials for the required Windows service account and click **OK**.
8. Repeat for any applications pools that need changing.

9. Restart the RabbitMQ Service.
10. Restart all application pools.
11. Restart IIS.

If there are issues with the Audit Service, make sure that the Windows service account has access to the Audit Service Listener as well as the Audit Database.

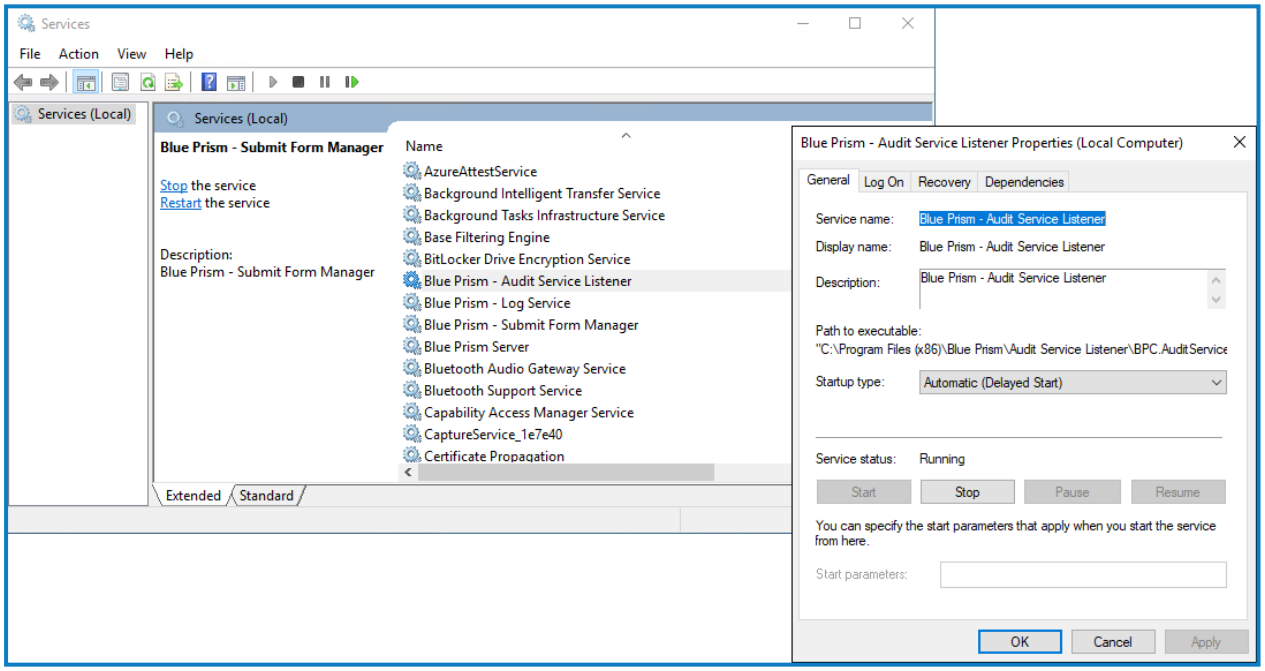
Assigning a Windows service account to a service

The Windows service account needs to be allocated to manage the following services:

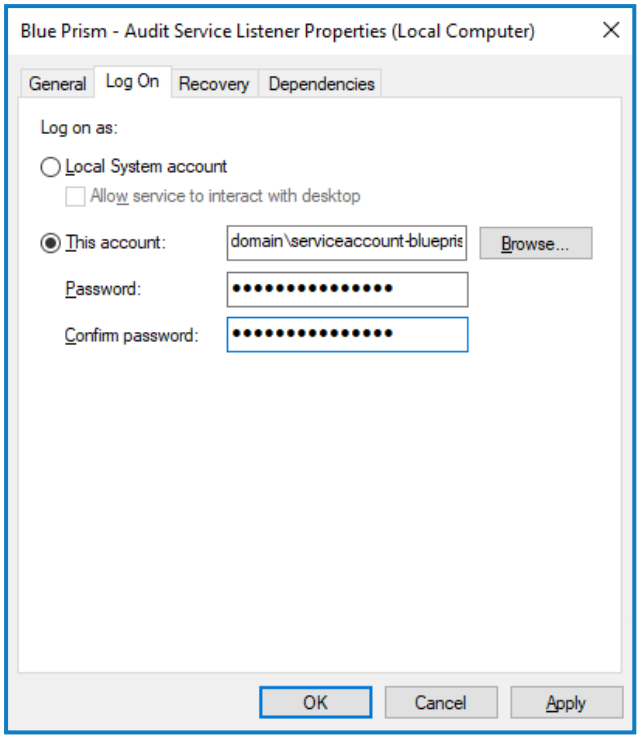
- Blue Prism - Audit Service Listener
- Blue Prism - Log Service
- Blue Prism - Submit Form Manager

To do this:

1. On the web server, open Services.
2. Right-click the service and click **Properties**.



3. On the Log on tab, select **This account** and then either enter the account name or click **Browse** to find the account you want to use.



4. Enter the password for the account and click **OK**.
5. In the Services window, right-click the service and click **Restart**.
6. Repeat for the other Blue Prism services.

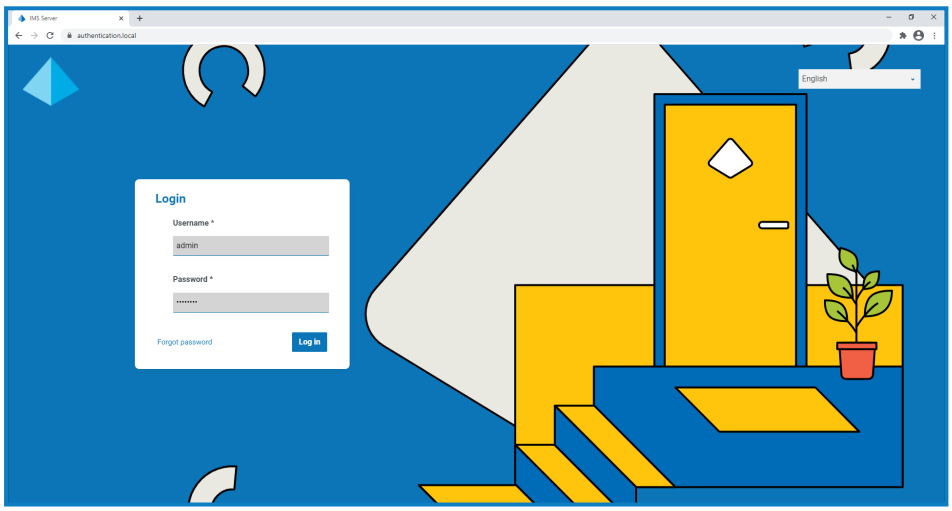
Initial Hub configuration

You can now log in for the first time and carry out some system-wide configuration.

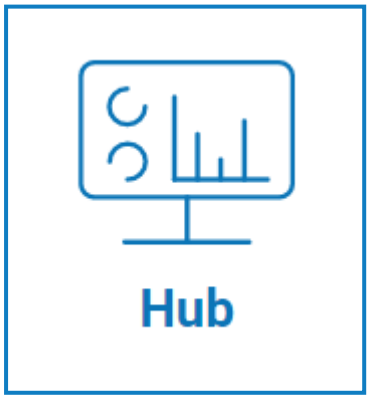
When you open the login page for Authentication Server, localization settings are automatically applied from your web browser. The login page and Hub display in the language most compatible with the language settings configured in the browser. If the language selected in your browser settings is not supported, English is used as the default. If required, you can manually change the language you want to use from the drop-down list on the login page.

To watch the Hub installation and configuration process, see our Blue Prism Hub installation video.

1. Launch a browser and go to the Authentication Server website, in our example: https://authentication.local



2. Log in using the default credentials.
   - **Username**: admin
   - **Password**: Qq1234!!
3. Click **Hub** to launch the Hub website.



4. Change the default password to a new secure password.
   a. In Hub, click the profile icon to open the Settings page, and then click **Profile**.
   b. Click **Update password**.

      The Update your password dialog displays.
   c. Enter the current admin password, then enter and repeat a new password.
   d. Click **Update**.

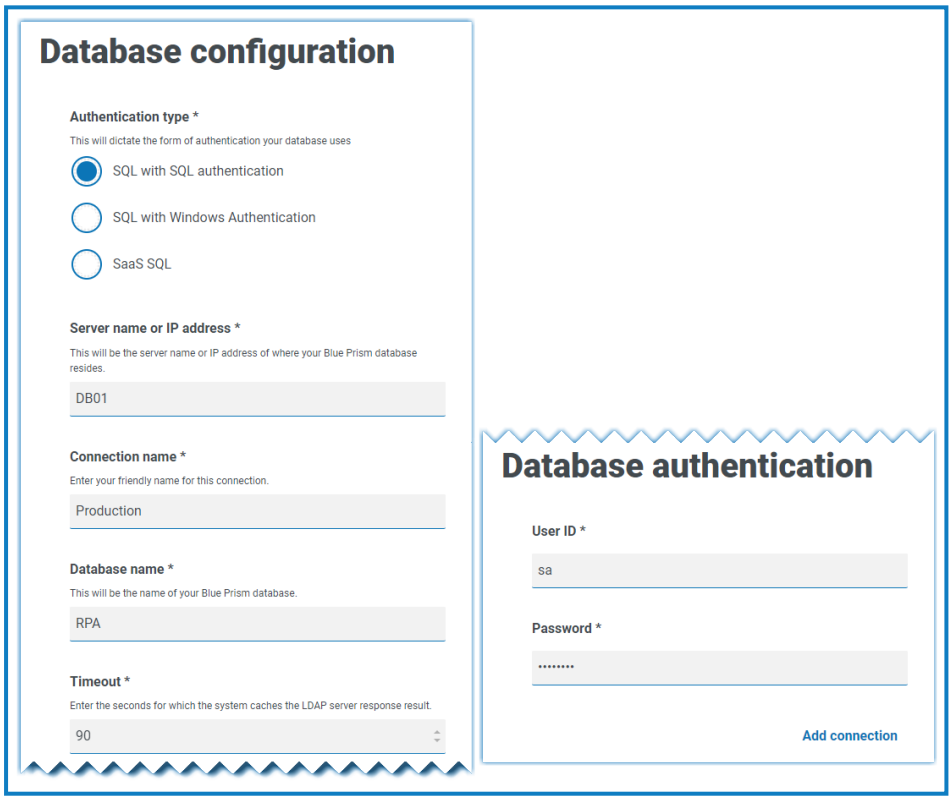
      The admin password is changed.

Database settings

To configure access to the Blue Prism database:

1. Click your profile icon to open the Settings page, and then click **Environment manager**.

   The Environment management page displays.
2. Click **Add connection** and enter the details of the Blue Prism database. An example is shown below:



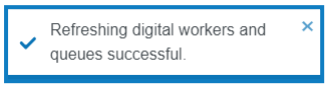
> The Timeout value is in seconds.

3. Click **Add connection** to save the details.

   The connection is created and displays in the Environment manager.

4. In the Environment manager, click the refresh icon on your new connection. This updates the information in Hub with the digital workforce and queues held in the database.

   If the connection is successful, the following message displays in the top right corner of the Hub user interface, which verifies the installation.

   If the message does not display, see Troubleshoot a Hub installation on page 86 for more information.

Create an administrator

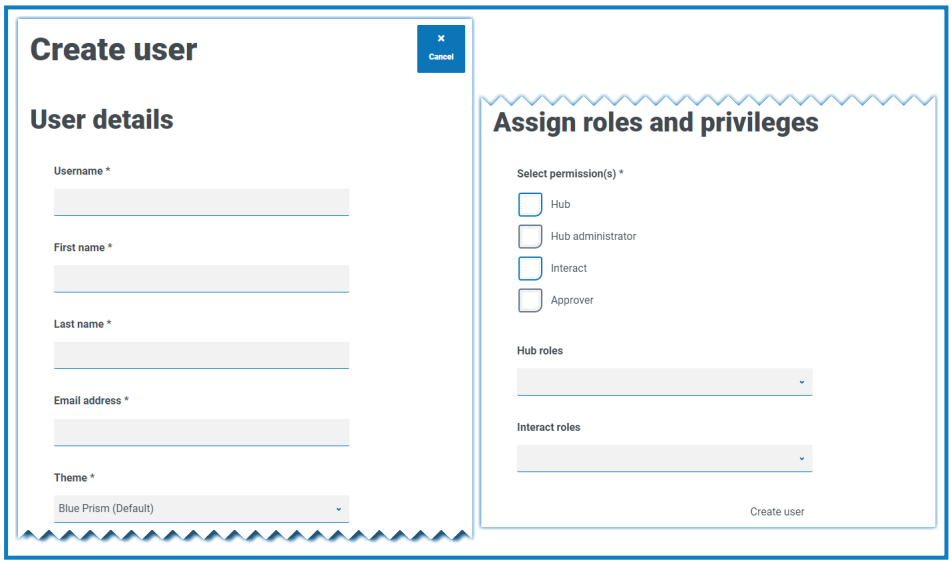
You will need to create an administrator account with valid information to finish the Hub configuration. You should not use the generic admin account to complete the configuration, this is because:

- A real email address is needed in order to test the email configuration.
- For a complete audit trail, a named user should be used to make configuration changes, rather than the generic account.

To create a new administrator:

1. Click your profile icon to open the Settings page, and then click **Users**.
2. On the Users page, click **Add user**.

   The Create user section displays.

3. Enter the following details:
   - Username
   - First name
   - Last name
   - Email address
4. Select the **Hub** and **Hub Administrator** permissions.
5. Click **Create user**.

   The Create password dialog displays.

6. Select **Manually update the user's password**.

   > Passwords must obey the restrictions within Hub.

7. Click **Continue** and follow the instructions on screen.
8. Finally, click **Create** to create the user.

   The new user displays in the list of users.
9. Log out of Hub and log back in using your new account.

Email settings

It is recommended that the SMTP setup is completed. This enables system emails to be sent, such as forgotten password emails.

The email address used to send emails is configured when setting up your profile.

> To configure the email settings, you must log in with the user you created in Create an administrator on the previous page. This is because the configuration process sends a test email, and therefore requires a user with an active email address.

You can configure your email settings using one of the following authentication methods:

- **Username and password** – This authentication method requires the following information:
  - **SMTP host** – The address of your SMTP host.
  - **Port number** – The port number used by the outgoing mail server.
  - **Sender email** – The email address that is used when sending emails. The email recipients will see this as the From address.
  - **Encryption** – The encryption method used by the email server to send the emails.
  - **Username** – The username for the SMTP authentication.
  - **Password** – The password for the account.
  - **Test email recipient** – The test email will be sent to this email address. This defaults to the email address of the user who is making the changes and cannot be changed.
- **Microsoft OAuth 2.0** – This authentication method requires the following information:
  - **Sender email** – The email address that is used when sending emails. The email recipients will see this as the From address.
  - **Application ID** – This information is the Application (client) ID defined in Azure AD and will be provided to you by your IT Support team.
  - **Directory ID** – This information is Directory (tenant) ID defined in Azure AD and the will be provided to you by your IT Support team.
  - **Client secret** – This is the client secret as generated by Azure AD and will be provided to you by your IT Support team and controls the authentication process

    > For information about finding these details in Azure AD, see the Microsoft documentation.

  - **Test email recipient** – The test email will be sent to this email address. This defaults to the email address of the user who is making the changes and cannot be changed.

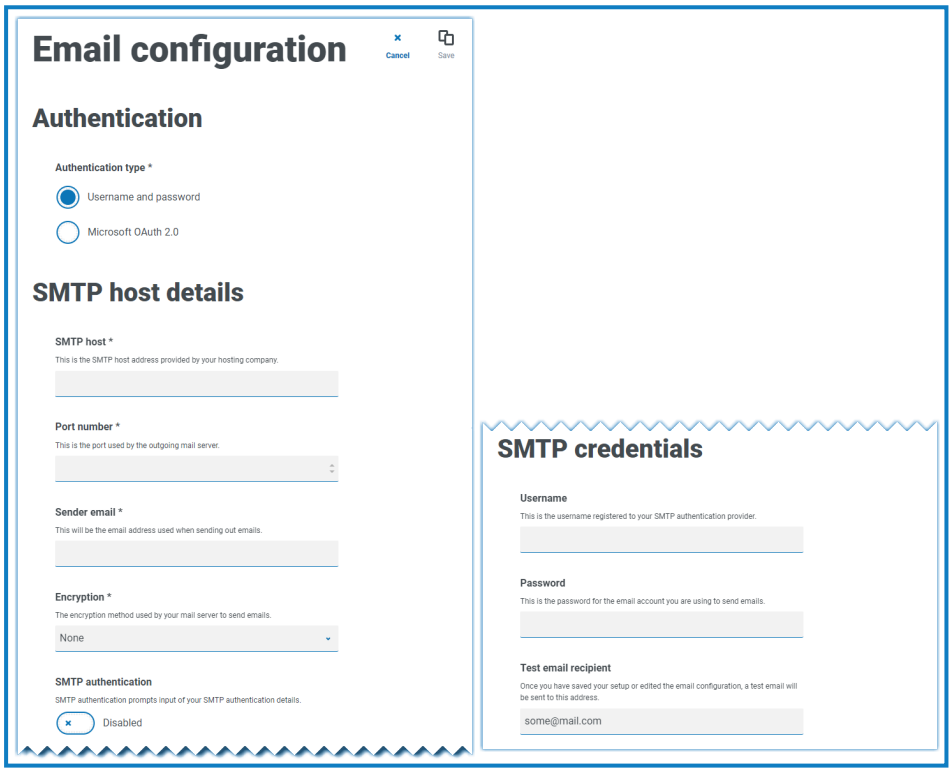
> If you are using Microsoft OAuth 2.0, the Mail.Send permission in Azure Active Directory must be enabled. This is found in the API Permission tab under the application properties in Azure Active Directory. For more information, see Troubleshoot a Hub installation on page 86.

To configure the email settings:

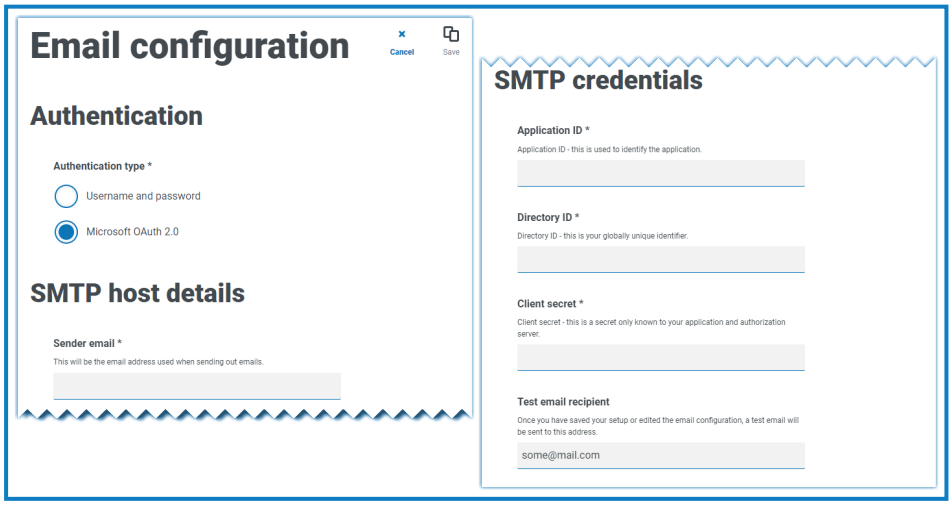
1. Click your profile icon to open the Settings page, and then click **Email configuration**.
2. Click **Edit**.
3. Select the authentication type you want to use.

   The fields on the page depend upon your selection as detailed above. If you select:

   - **Username and password**, the Email configuration page displays as follows:



   - **Microsoft OAuth 2.0**, the Email configuration page displays as follows:



4. Enter the required information.
5. Click **Save**.

If the email settings cannot be successfully configured, it is likely that the Message Broker server cannot be reached, see Troubleshoot a Hub installation on page 86 for more information.

For more information about configuring email settings, see Hub User Guide.

Configure Authentication Server

Authentication Server enables users to log into Blue Prism, Hub, and Interact using the same credentials. Authentication Server is compatible with Blue Prism 7.0 and later.

With Blue Prism 6

If your organization is using Blue Prism 6:

- Authentication Server cannot be used to authenticate users between Blue Prism and Hub. Users can log into Blue Prism and Authentication Server using independent accounts.
- You should configure the authentication settings in Hub. See Authentication settings below.

With Blue Prism 7

If your organization is using Blue Prism 7, you should consider whether your organization wants users to use the same account for the Blue Prism applications.

- If your organization wants to use the same user accounts:
  1. Configure Authentication Server, see the Authentication Server configuration guide.
  2. Configure the authentication settings in Hub. See Authentication settings below.
- If your organization does not want to use the same user accounts, only configure the authentication settings in Hub. See Authentication settings below.

To watch the configuration steps, see our Configure Authentication Server video.

Authentication settings

Blue Prism Hub comes with the ability to add Hub users and control their access. Additionally, if your organization wants to sync your users from Active Directory to enable them to use their existing credentials to log into Hub, you can do so using an LDAP connection configured using the Authentication settings page.

For more information about configuring an LDAP connection, see the Hub User Guide.

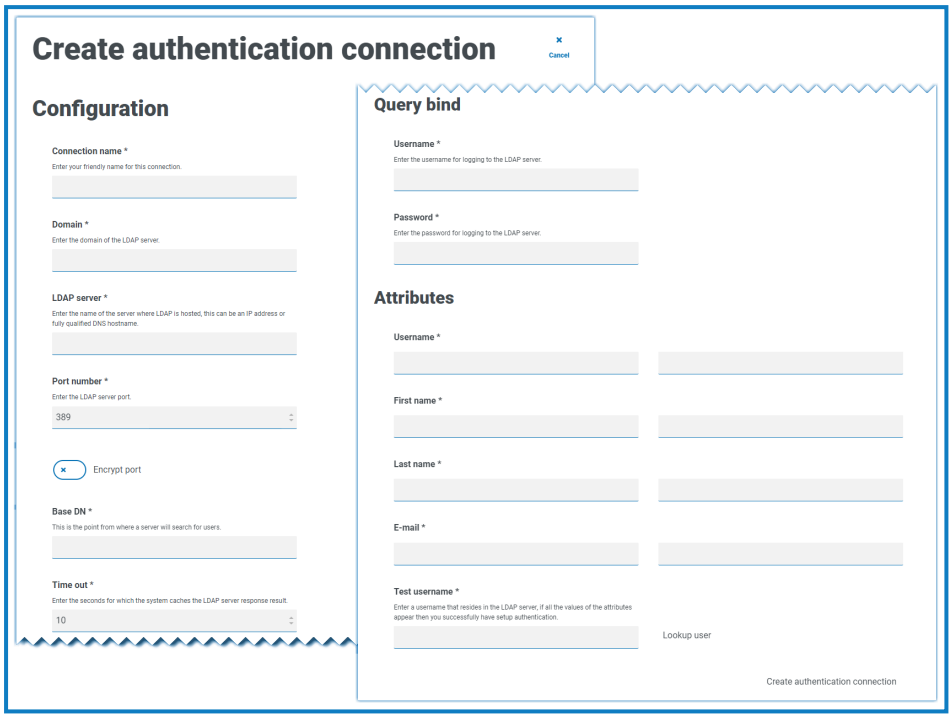
To configure the authentication settings:

1. Click your profile icon to open the Settings page, and then click **Authentication settings**.

   The Authentication settings page displays.

2. Click **Add new**.

   The Create authentication connection page displays.



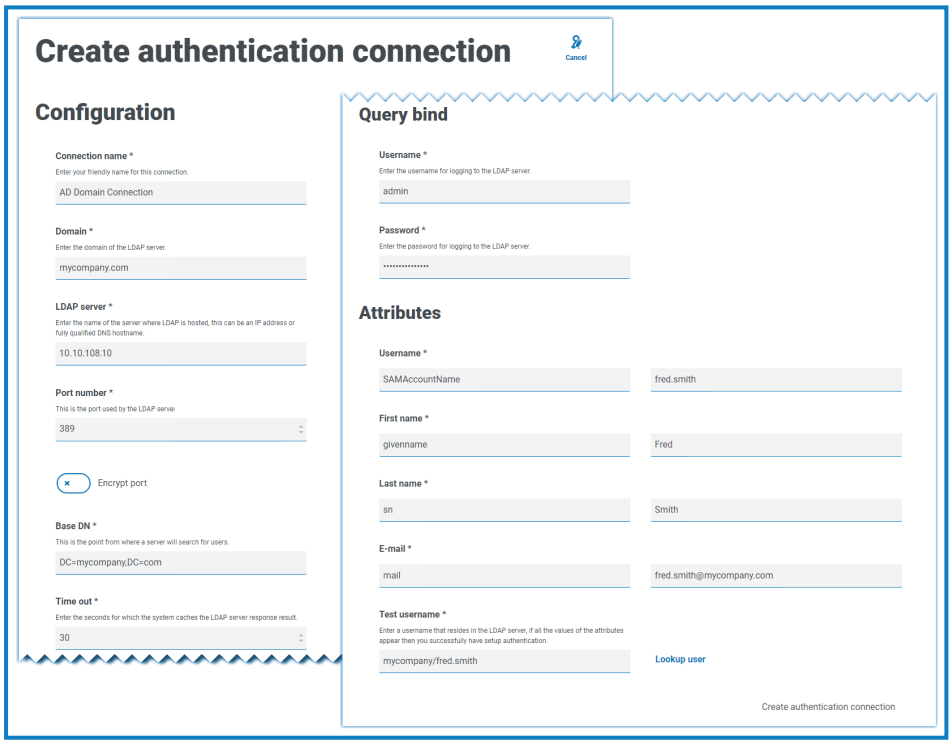
3. Complete the Configuration fields:
   - **Connection Name** – A name that you want the connection to be known as.
   - **Domain** – The name of the domain you are connecting to, for example “bp”.

     Do not use the fully qualified domain name (FQDN) of your domain. You must use the short name format.

   - **LDAP Server** – The hostname of the LDAP server, for example blueprism-srv1.local.
   - **Port Number** – The port number it operates on, by default this is port 389.
   - **Encrypt port** – Select this option if you want to encrypt the port. If you use port 636 (the LDAPS port), you should turn on this option.
   - **Base DN** – The starting point within the Active Directory where the system begins to look for users, for example dc=blueprism, dc=local.
4. Complete the Query Bind fields:
   - **Time Out** – The timeout period in seconds that the system will wait to get a response from the Active Directory server.
   - **Query Bind Username** – An Active Directory user that has access to the organization’s LDAP system.
   - **Query Bind Password** – The password for the Active Directory user.

5. Complete the Attributes fields. The purpose of this section it to map the Active Directory attributes to the Hub fields. The text entered in these fields must match named attributes within the user profile in Active Directory. You can use the Active Directory Users and Computers (ADUC) tool to find the user attributes by selecting a user and then clicking the **Attribute Editor** tab to view the mapping of attributes to values.
    - **Username** – The Active Directory attribute name for the username, for example, 'SAMAccountName'.
    - **First Name** – The Active Directory attribute name for the user's first name, for example, 'givenname'.
    - **Last Name** – The Active Directory attribute name for the user's last name, for example, 'sn'.
    - **E-mail** – The Active Directory attribute name for the user's email, for example, 'mail'.
6. To test that everything is set up correctly, enter the username in the **Test Username** field and click **Lookup User**. The text entered in the **Test Username** field must match the text format of the Active Directory Attribute. For example, if the username is set to:
    - 'SAMAccountName', then the test data is likely to be in the format *domain\user*.
    - 'name', then the test data is likely to be in the format *user*.

    The associated information will be retrieved and populated in the corresponding Attributes fields, for example:



7. Click **Create authentication connection**.

    A notification message displays confirming the connection is successful and you are prompted to import users.

8. Click **Yes** to synchronize now. Alternatively, you can select **No** and synchronize later.

   A message displays indicating the number of users found.

   > When importing a large number of users (for example, tens of thousands), the database transaction log files for the databases AuthenticationServerDB, HubDB and InteractDB will increase in size. If the size of the transaction log file of any of these three database is restricted by either a maximum file size that is too small or the file is not permitted to increase in size, the import may fail. It is therefore recommended that you enable the autogrow setting for the database transaction log files and set the growth setting to 1024 MB, whilst ensuring a sufficient maximum size is set to prevent the import from failing. For more information on autogrowth, see Microsoft's documentation.

9. Click **Proceed**.

   A list of users display. These have not yet been imported to Hub as you need to configure the permissions and roles for the required users.

10. Select a user to import and assign the appropriate Hub roles and/or any Interact responsibilities.

    > If you configure a user to have a Hub Administrator role, they will have access to all the plugins and features of Hub, including the ability to create new Database and LDAP connections and other security features so it is important to assign this role with care.

11. Repeat for all required users.
12. Click **Save access and roles**.

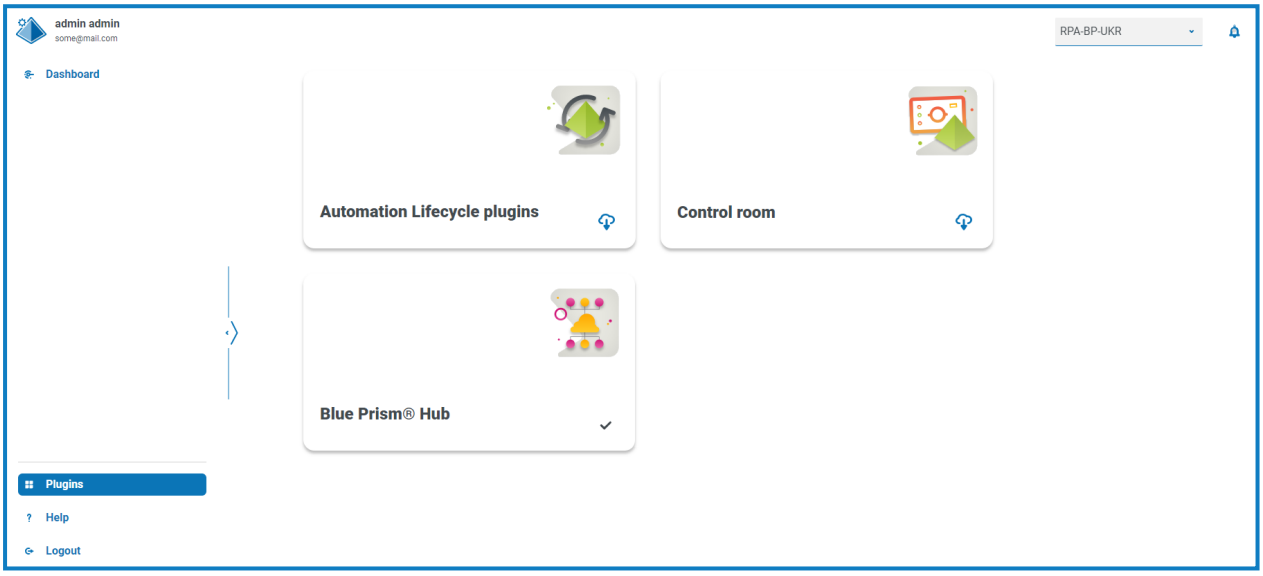
    Only the users that have had their roles and permissions defined are saved and the Users page displays with the new users shown.

Install Plugins

As part of the installation, Hub automatically installs the Hub plugins. However, if you want to use ALM or Interact, you will need to install the freely available Business processes plugin first.

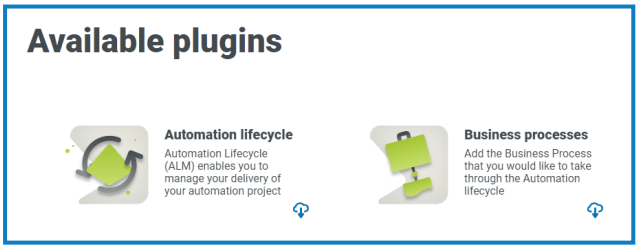
To watch this installation step, see our Business Processes plugin installation video.

1. Log in to Hub.
2. Click **Plugins** to open the plugin repository.



3. Click **Automation lifecycle**.

   The available plugin components display.



4. Click the download icon in the bottom corner of the **Business processes** tile to initiate the install.

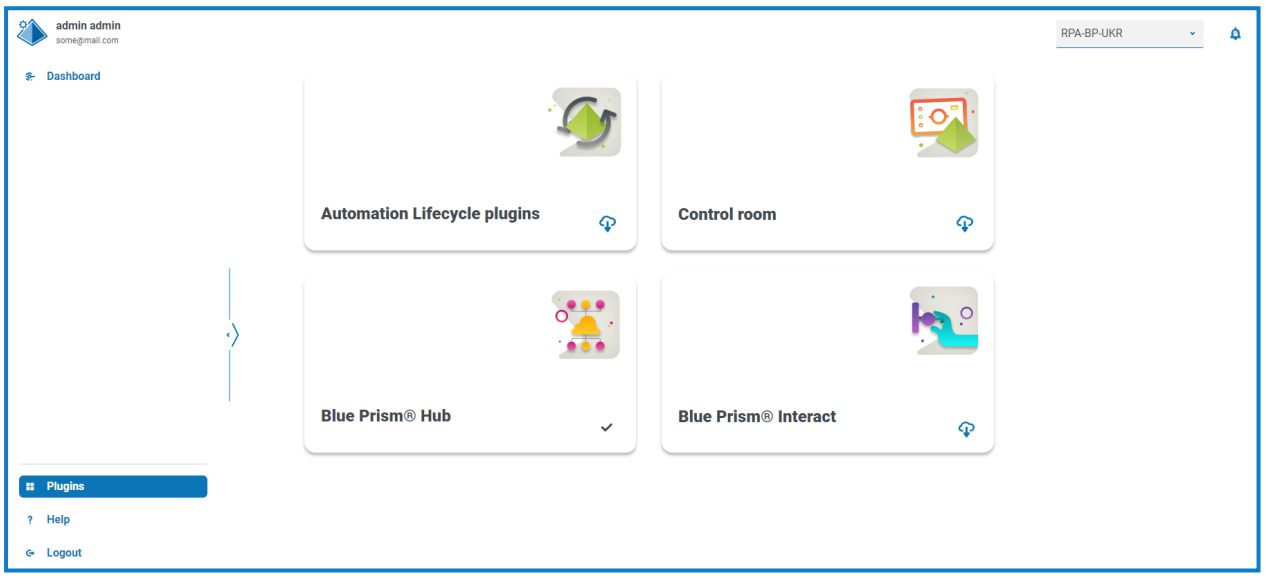
   The site restarts.

Install the Interact plugin

The Interact plugin is dependent on the Business processes plugin, as you can not create a form without a business process. The Business process plugin is provided free within the plugin repository and can be found under Automation Lifecycle Management (ALM). Ensure you have installed the Business processes plugin prior to installing Interact. For more information, see Install Plugins on the previous page.

The Interact plugin must be installed with the associated license.

1. Log in to Hub.
2. Click **Plugins** to open the plugin repository.



3. On the **Interact** tile, click the download icon in the bottom corner to initiate the install and apply the necessary license.

   The site restarts.

Configure Digital Workers

This section provides the steps that must be performed on each Digital Worker to enable it to connect to Interact.

The steps to be completed are:

- Install SSL certificates
- Configure the network
- Install and configure the Interact Web API Service

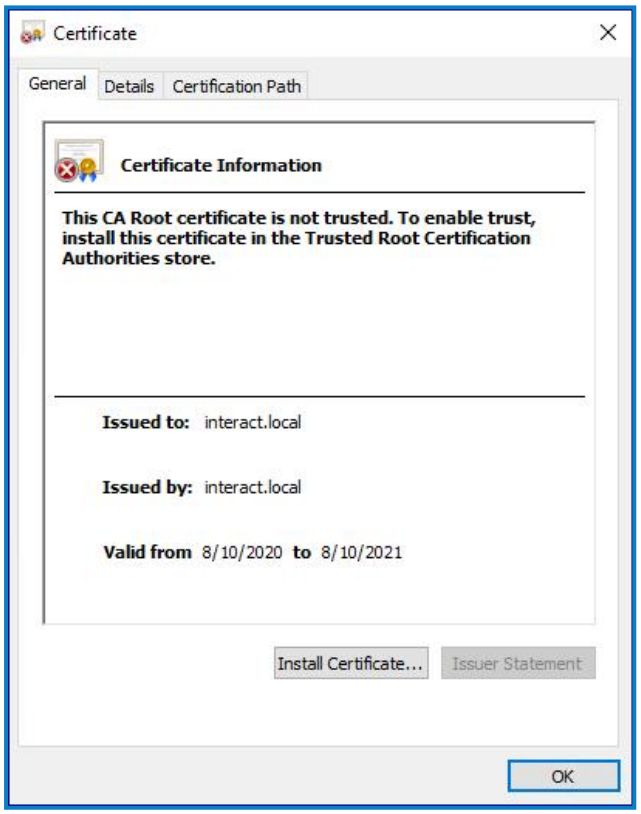
These instructions assume that the user is familiar with Blue Prism.

Install SSL certificates

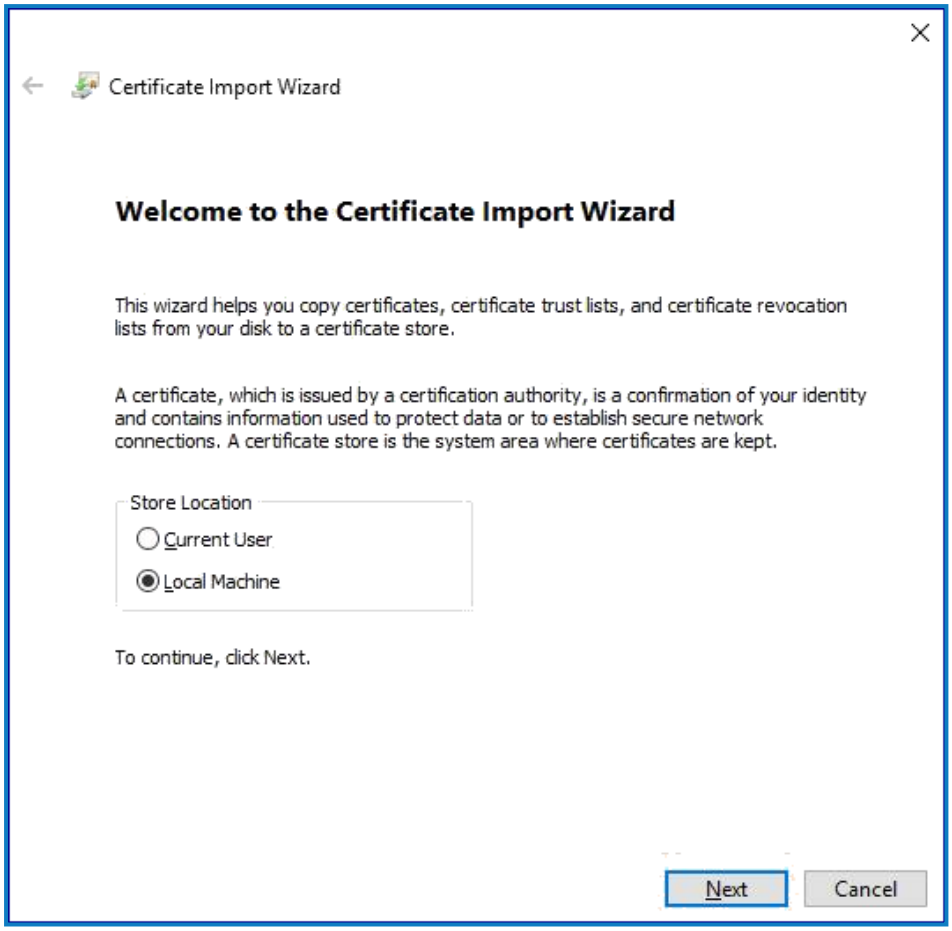
On each Digital Worker, log in and copy across the SSL Certificates for Interact, IADA, Interact Remote API, Authentication Server, and SignalR.

> As this needs to be performed on each Digital Worker the use of third-party tools or GPOs can be used to perform this task at scale.

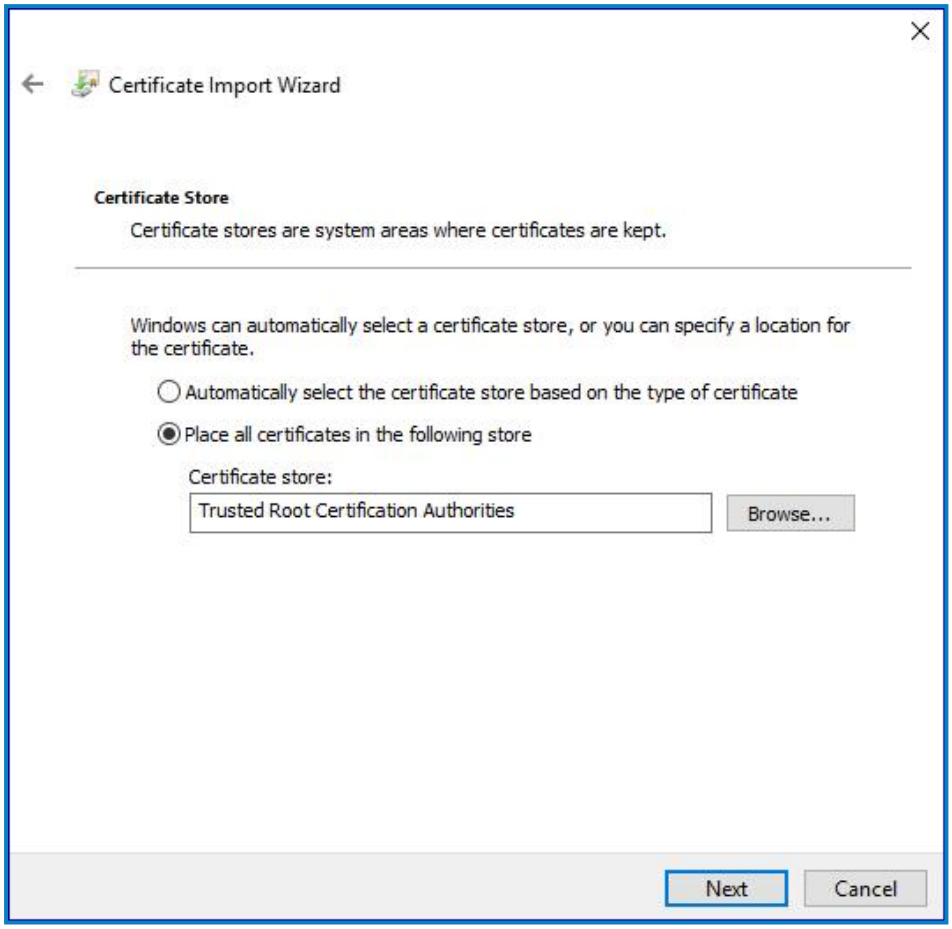
1. Double-click each SSL Certificate and select **Install Certificate**.



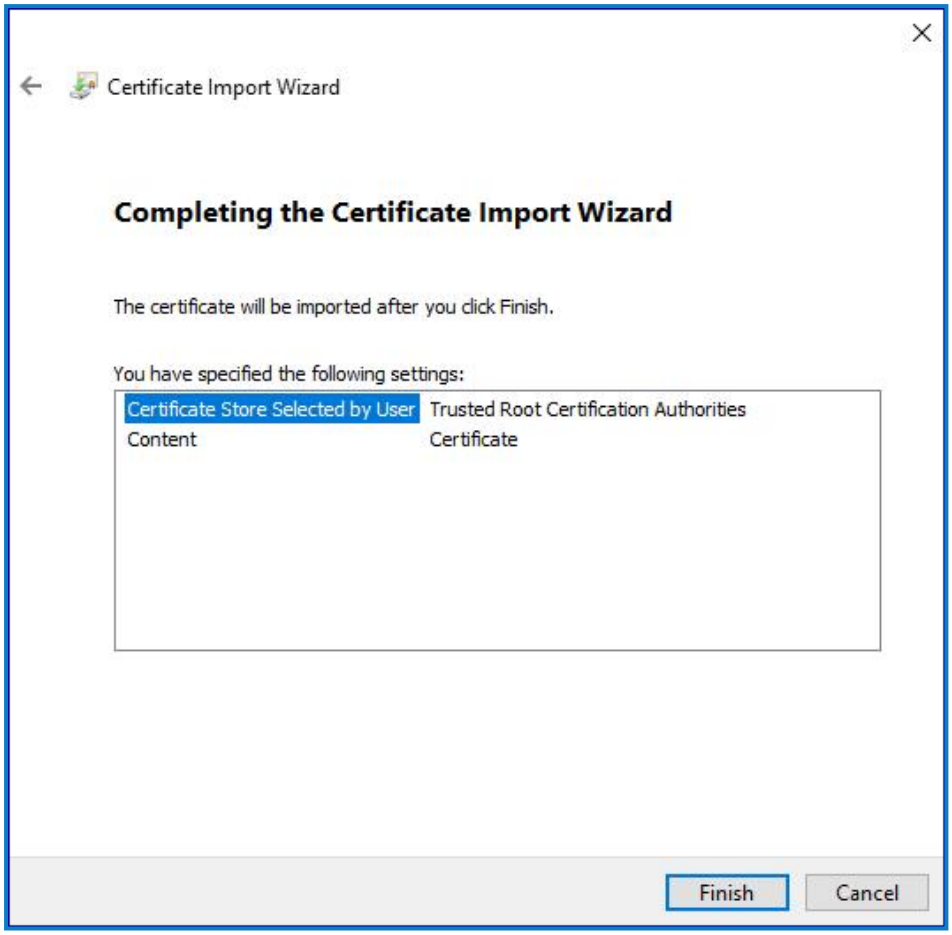
2. Change the Store location to **Local Machine**.



3. Select **Place all certificates in the following store**, click **Browse** and select **Trusted Root Certification Authorities store**.



4. Check that the SSL Certificate is allocated in the correct store, then click **Finish**.



5. Acknowledge the message confirming success.
6. Repeat the steps for all the SSL Certificates.

Configure the network

It is important that the Interact website and in particular the Interact Remote API site can be reached.

This is dependent on the architecture structure that was deployed, so this could already be established if the systems are domain joined and the IT organization has configured the servers. Alternatively the local hosts file may need to be adjusted to ensure that the sites can be reached.

The sites that need to be reachable from each Digital Worker are as follows:

Website in IIS	Default URL
Blue Prism – Interact	https://interact.local
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local
Blue Prism – SignalR	https://signalr.local

Authentication Server and SignalR are installed as part of the Hub installation.

Install and configure the Interact Web API service

Blue Prism and Interact communicate through the Blue Prism Interact Remote API. To use this API, the Interact API Service release file should be imported into Blue Prism, this includes a Web API Service and VBO. Once imported it will need to be updated with the appropriate base URL and authorization codes to enable secure communication.

In the web service there are a number of defined actions, see the Interact Web API Service user guide for more information.

To configure Blue Prism to use Interact, you need to:

1. Set up a service account in Hub and generate a secret key.
2. Set up the credentials for the Interact Web API service account in Blue Prism.
3. Import and configure the Interact API Service VBO to enable Blue Prism to communicate with Interact.

Set up a service account

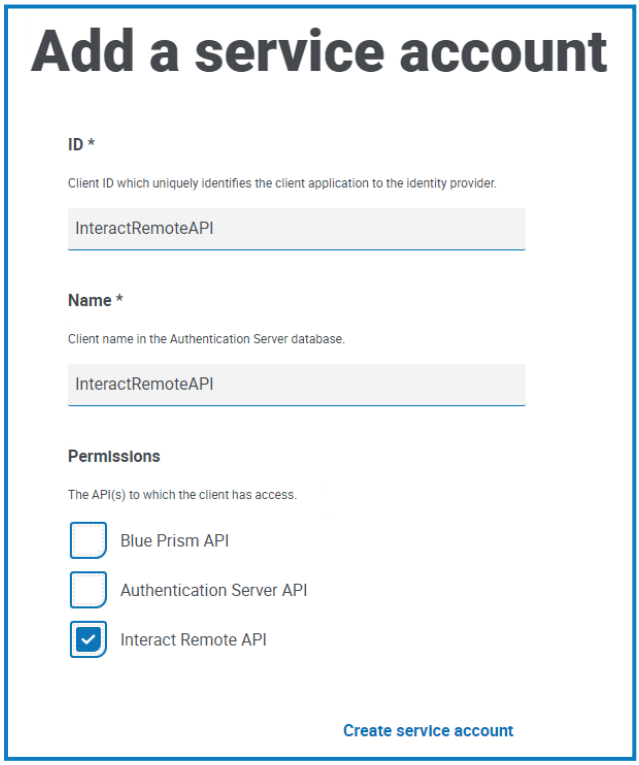
To set up the Interact Remote API credentials in Blue Prism, a secret key is required. This is generated from the associated service account in Hub for use with the Interact Remote API. If you lose the key, you can regenerate another key from the service account. For more information, see Service accounts.

To create a service account:

1. In Blue Prism Hub, on the Service accounts page, click **Add account**.
2. Enter a unique ID and a friendly name, for example, *InteractRemoteAPI*.

   Do not use *InteractRemoteClient*. This name is allocated internally in the system.

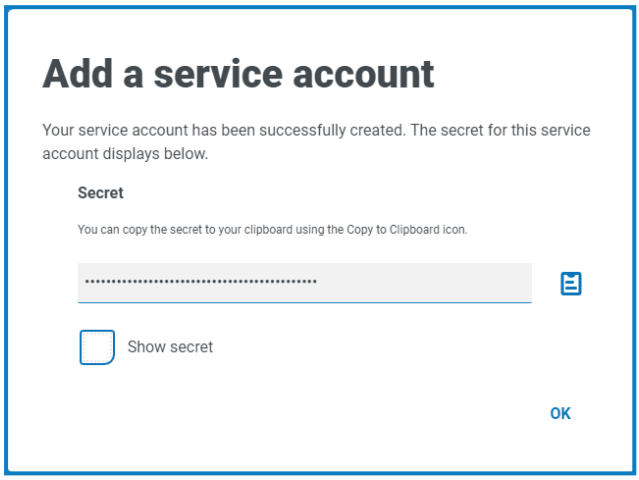
3. Under **Permissions**, select **Interact Remote API**.



4. Click **Create service account**.

   The Add a service account dialog displays with a generated secret key. You will need to enter this key into the Blue Prism interactive client when configuring the associated credential.

5. Copy the generated secret key to your clipboard ready to paste into the Blue Prism interactive client.



6. Click **OK** to close the dialog.

   The Service accounts page displays with the newly created account shown.

Set up credentials in Blue Prism

1. Log into the Blue Prism interactive client, select **System** and then click **Security** > **Credentials**. See Security > Credentials for additional information.
2. Click **New**.

   The Credential Details dialog displays.

3. On the Application Credentials tab of the Credential Details dialog:
   a. Enter a name.
   b. Change the **Type** to **OAuth 2.0 (Client Credentials)**.
   c. In **Client ID**, enter the ID that you used to create the service account above in Configure Digital Workers on page 72, for example, *InteractRemoteAPI*.
   d. In **Client Secret**, enter the secret key that was generated for the service account.
   e. In the **Additional Properties** section set the value for:
      - **grant_type** to *client_credentials*.
      - **scope** to *interact-remote-api*.

4. On the Access Rights tab of the Credential Details dialog, set up the required access permissions.
5. Click **OK**.

Import and configure the Interact API Service VBO

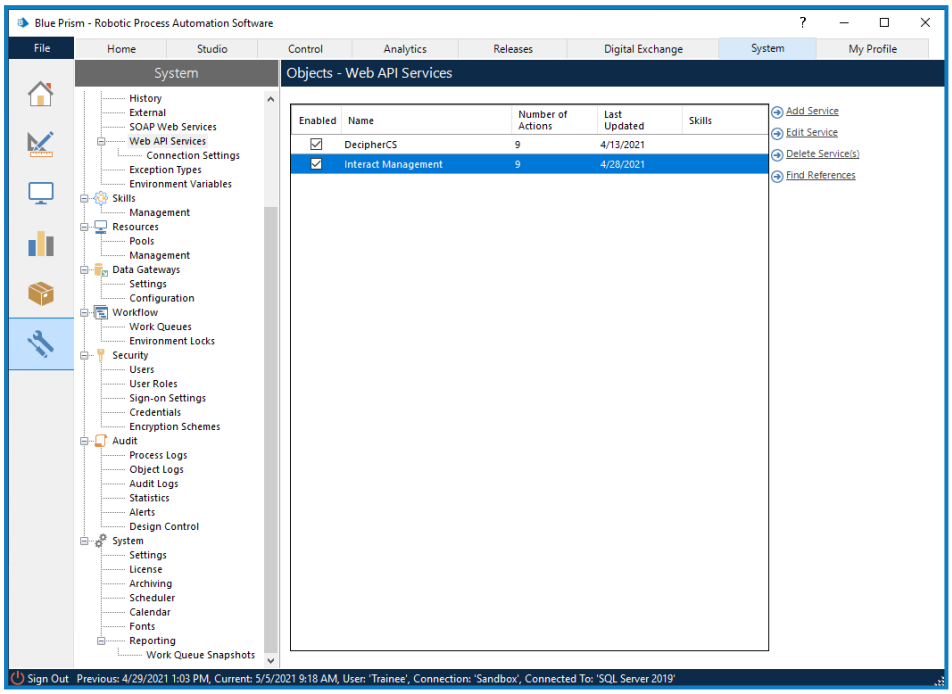
Import the VBO

1. Download the Interact API Service release file from the Blue Prism Portal.
2. In Blue Prism, select **File** and click **Import** > **Release / Skill** and follow the prompts to import the release file into Blue Prism. For more information, see Import a file.

Configure the web service

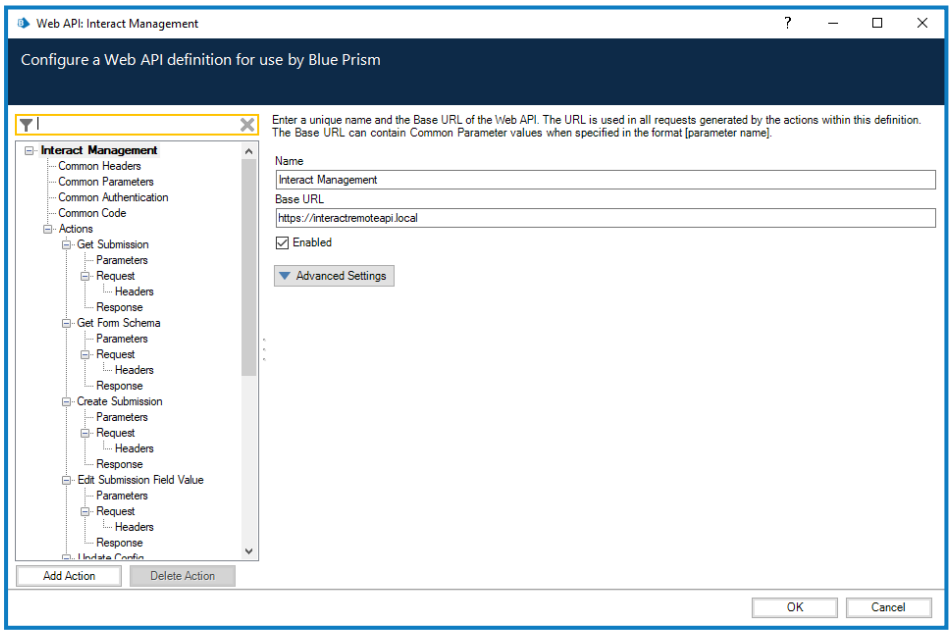
1. In Blue Prism, select **System** and then click **Objects** > **Web API Services**.

   The Objects - Web API Services screen displays. For example:



2. Select **Interact Management** and click **Edit Service**.

   The Web API: Interact Management screen displays.



3. On the Web API: Interact Management opening screen, in **Base URL**, enter the URL for your organization's Interact API service. This was defined during the installation of Interact.
4. Select **Common Authentication** in the navigation tree, then complete the following:

a. Ensure that **Authentication Type** is set to **OAuth 2.0 (Client Credentials)**

b. In **Authorization URI**, enter the Authentication Server URL in the format:

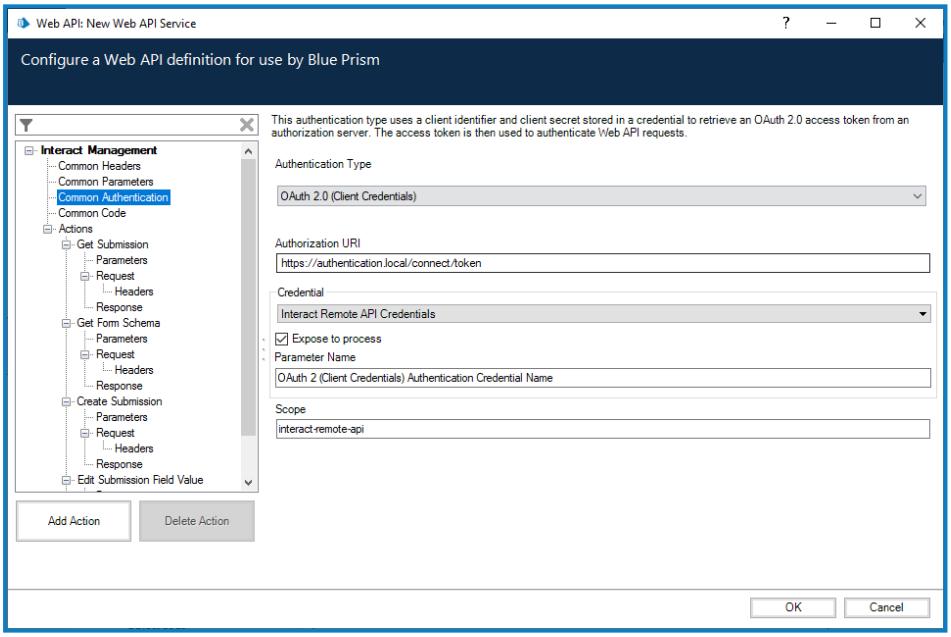
`<Authentication Server URL>:<port if specified during install>/connect/token`

For example, `https://authentication.blueprism.com:5000/connect/token`

Or, if the default port was used, `https://authentication.blueprism.com/connect/token`.

> If you have upgraded from a version earlier than 4.3, your system will still be using IMS. In this case, you should enter the information in the format:
>
> `<IMS URL>:<port if specified>/connect/token`
>
> For example, `https://ims.blueprism.com:5000/connect/token`.

c. In **Credential**, select the credential you created in Set up credentials in Blue Prism on page 77.



5. Click **OK** to save and complete the setup of the Web API Service.

Troubleshoot an Interact 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.

Database connectivity

The **Test connection to proceed** button within the installer checks the following:

- If the database exists:
  - That it can be connected to.
  - That the account has the rights to read, write and edit the database.
- If the database does not exist:
  - That the account has the right to create the database.

If these requirements cannot be met, the installation will stop.

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.

Another potential reason for failure is that the account used to create the databases within the installer has insufficient privileges to create the databases.

Web server

During the installation process the installer will check that all prerequisites are installed. It is recommended that if the prerequisites are not installed, that the installer is canceled, the prerequisites installed, and the installer process restarted.

Use RabbitMQ with AMQPS

If you are using RabbitMQ with AMQPS (Advanced Message Queuing Protocol - Secure), the application pools created as part of the Interact installation need to be granted permissions to the RabbitMQ certificate. To do this:

1. On the web server, open the Certificate Manager. To do this, type *Certificates* in the search box on the Windows taskbar, and then click **Manage Computer Certificates**.

2. Navigate to, and right-click the certificate that was identified for use with RabbitMQ AMQPS during Hub installation, and select **All Tasks**, and click **Manage Private Keys...**.

   The Permissions dialog for the certificate displays.

3. Click **Add**, then enter the following application pools into the **Enter the object names to select** field:

   ```
   iis apppool\Blue Prism - IADA;
   iis apppool\Blue Prism - Interact;
   iis apppool\Blue Prism - Interact Remote API;
   ```

   > These are the default application pool names. If you have entered different names during installation, ensure the list reflects the names you have used.

4. If you are using Windows Authentication, also add the name of the service account that is used for the following Windows services:
   - Blue Prism – Audit Service Listener
   - Blue Prism – Log Service
   - Blue Prism – Submit Form Manager
5. Click **Check Names**.

   The names should be validated. If they are not, check that the name matches the application pool or service account you are trying to use and correct as needed.

6. Click **OK**.
7. Select each application pool in turn in the **Group or user name** list, and ensure that **Full control** is selected in the **Permissions for {account name}** list.
8. Click **OK**.

   The application pools now have access to the certificate.

Windows Authentication

The account used when running the installation must have the relevant SQL Server permissions to carry out the installation, that is, membership in either the sysadmin or dbcreator fixed server roles. See Preparation for details.

If Windows Authentication is chosen during the installation process, it is recommended that a Windows service account is used that has the necessary permissions to execute the tasks and processes during normal operation. The Windows service account will need:

- The ability to perform the SQL database processes, see Minimum SQL permissions on page 14.
- Ownership over the IIS Application Pool.
- Permissions for the required certificates.

Assigning the Windows service account as an owner on certificates

The Windows service account needs to be granted permissions to the BluePrismCloud certificates. To do this:

1. On the web server, open the Certificate Manager. To do this, type *Certificates* in the search box on the Windows taskbar, and then click **Manage Computer Certificates**.

2. In the navigation pane, expand **Personal** and click **Certificates**.
3. Follow the steps below for both the BluePrismCloud_Data_Protection and BluePrismCloud_IMS_JWT certificates:
    a. Right-click the certificate and select **All Tasks**, and click **Manage Private Keys...**.

       The Permissions dialog for the certificate displays.
    b. Click **Add**, then enter the service account and click **OK**.
    c. With the service account selected in the **Group or user name** list, ensure that **Full control** is selected in the **Permissions for {account name}** list.
    d. Click **OK**.

       The service account now has access to the certificate.

Assigning a Windows service account to the application pool

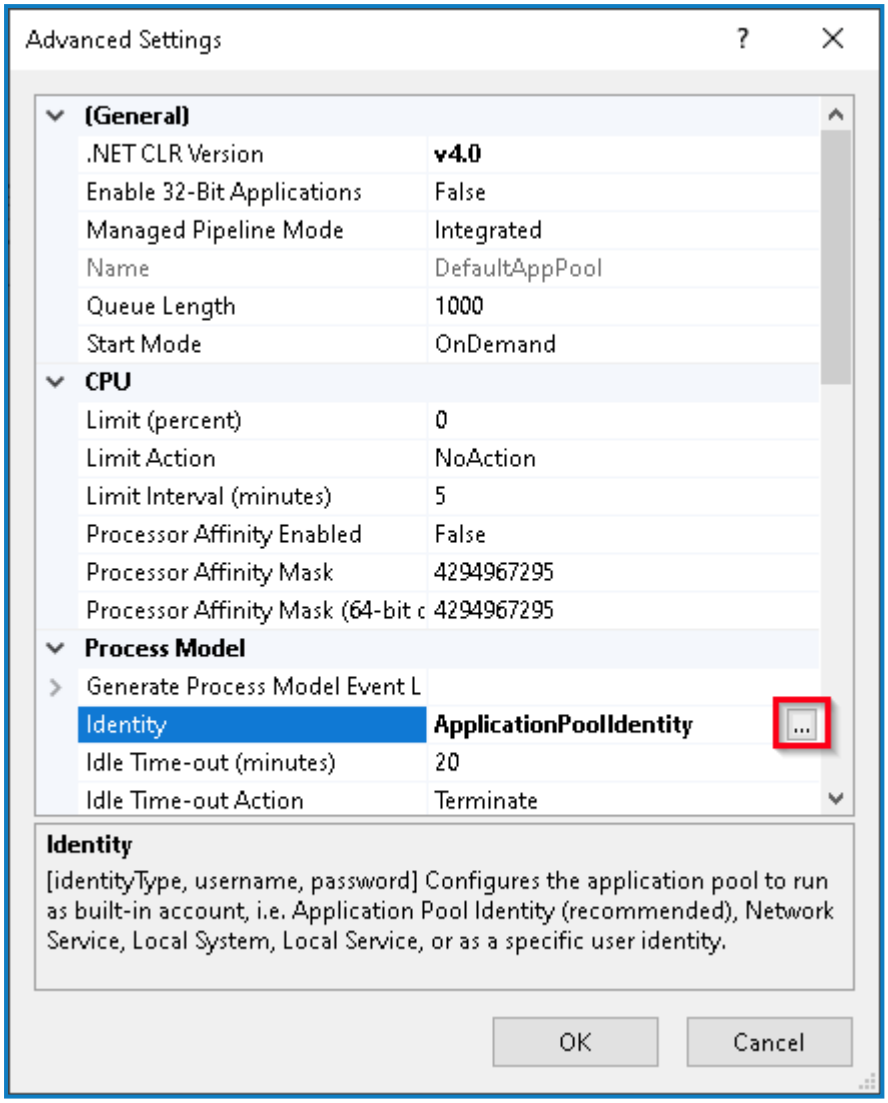
By default, the application pools are created with the identity 'ApplicationPoolIdentity'. After the installer has completed, the Windows service account will need to be allocated to manage the application pools. To do this:

1. On the web server, open Internet Information Services (IIS) Manager.
2. In the Connections panel, expand the host and select **Application Pools**.
3. Review the **Identity** column values.

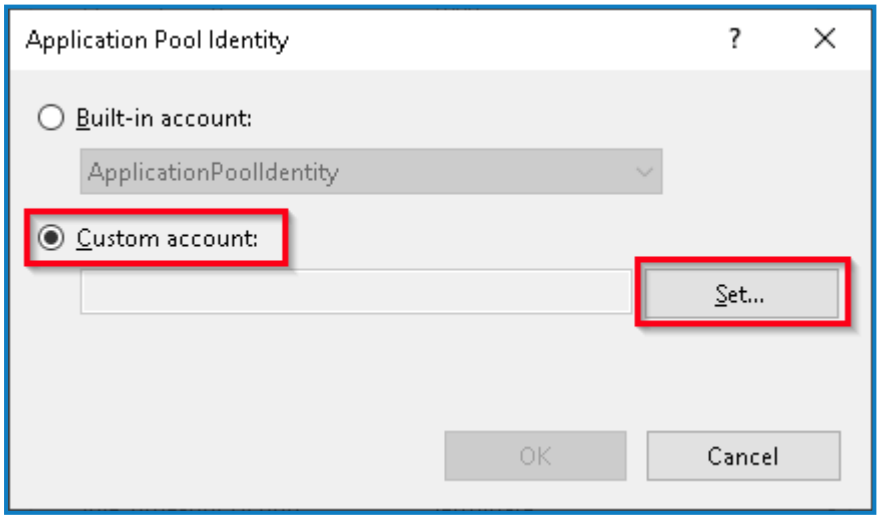
   The identity for an application pool should match the specific Windows service account.
4. For any application pools that have *ApplicationPoolIdentity* in the **Identity** column, right-click the row and select **Advanced Settings...**.

   The Advanced Settings dialog displays.

5. Select the **Identity** setting then click the **...** (ellipsis) button:



6. In the Application Pool Identity dialog, select **Custom account** and then click **Set...**.



The Set Credentials dialog displays.

7. Enter the credentials for the required Windows service account and click **OK**.
8. Repeat for any applications pools that need changing.

9. Restart the RabbitMQ Service.
10. Restart all application pools.
11. Restart IIS.

If there are issues with the Audit Service, make sure that the Windows service account has access to the Audit Service Listener as well as the Audit Database.

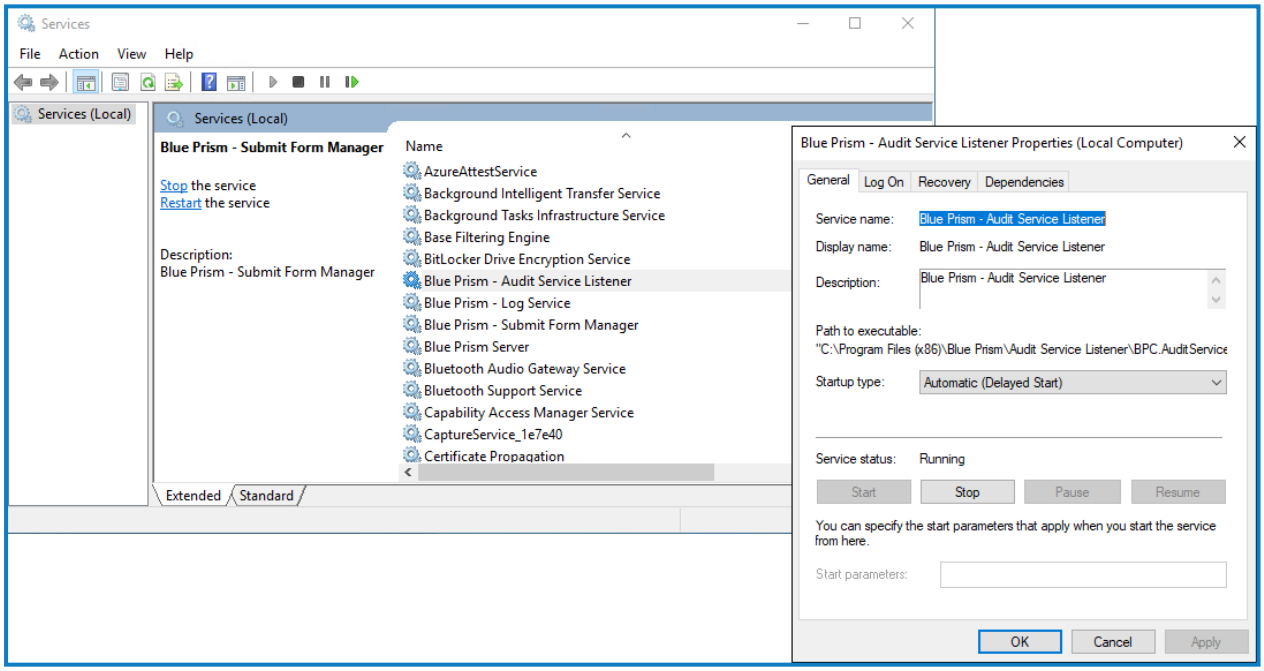
Assigning a Windows service account to a service

The Windows service account needs to be allocated to manage the following services:

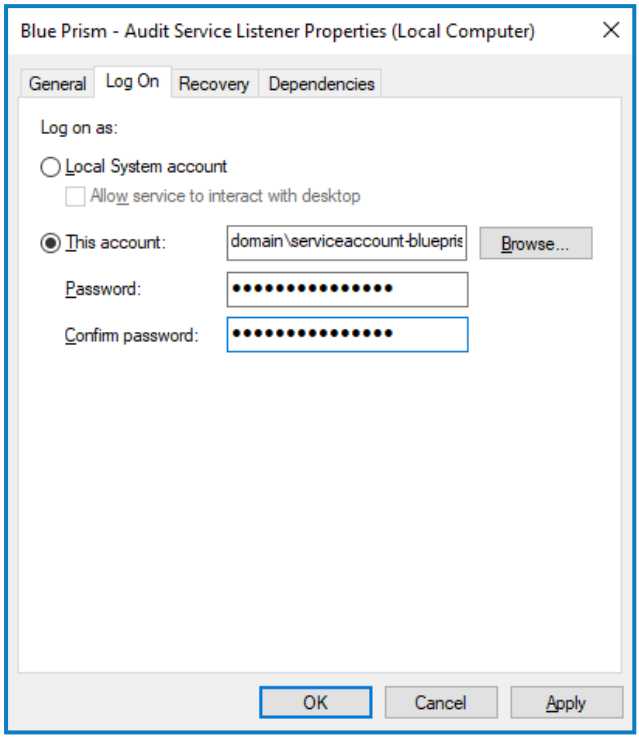
- Blue Prism - Audit Service Listener
- Blue Prism - Log Service
- Blue Prism - Submit Form Manager

To do this:

1. On the web server, open Services.
2. Right-click the service and click **Properties**.



3. On the Log on tab, select **This account** and then either enter the account name or click **Browse** to find the account you want to use.



4. Enter the password for the account and click **OK**.
5. In the Services window, right-click the service and click **Restart**.
6. Repeat for the other Blue Prism services.

Troubleshoot a Hub 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.

Message Broker connectivity

To verify the connectivity between the Web Server and the Message Broker check that the RabbitMQ Management Console is accessible through a web browser.

There could be several reasons that connectivity fails:

- Verify Network Connectivity – Ensure that all relevant devices are connected to the same network and are able to communicate.
- Firewall – Check that the firewalls on the servers themselves or within the network are not preventing communication.

> The RabbitMQ Management Console communicates, by default, on port 15672. The message broker queues use a different port, 5672, by default. The firewall should be checked for TCP access on all ports. This is especially true of the IT organization has specified non-default ports.

Database connectivity

The **Test connection to proceed** button within the installer checks the following:

- If the database exists:
  - That it can be connected to.
  - That the account has the rights to read, write and edit the database.
- If the database does not exist:
  - That the account has the right to create the database.

If these requirements cannot be met, the installation will stop.

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.

If when running the installer the installation process fails with database errors, see below, then test that the Web Server has a SQL connectivity to the database. This could be due to any of the reasons potentially listed above.

```
Error Number:53,State:0,Class:20
Info: CustomAction CreateDatabases returned actual error code 1603 (note this may not be 100% accurate if translation happened inside sandbox)
Info: Action ended 10:31:13: CreateDatabases. Return value 3.
```

Another potential reason for failure is that the account used to create the databases within the installer has insufficient privileges to create the databases.

Finally, if the installation is a re-installation after a removal of the software. Then if the same database names have been used, the original databases should be backed up and dropped before re-installing.

Web server

During the installation process the installer will check that all prerequisites are installed. It is recommended that if the prerequisites are not installed, that the installer is canceled, the prerequisites installed, and the installer process restarted.

For further information, see Prerequisites on page 8.

Use RabbitMQ with AMQPS

If you are using RabbitMQ with AMQPS (Advanced Message Queuing Protocol - Secure), the application pools created as part of the Hub installation need to be granted permissions to the RabbitMQ certificate. To do this:

1. On the web server, open the Certificate Manager. To do this, type *Certificates* in the search box on the Windows taskbar, and then click **Manage Computer Certificates**.
2. Navigate to, and right-click the certificate that was identified for use with RabbitMQ AMQPS during Hub installation, and select **All Tasks**, and click **Manage Private Keys...**.

   The Permissions dialog for the certificate displays.
3. Click **Add**, then enter the following application pools into the **Enter the object names to select** field:

   > These are the default application pool names. If you have entered different names during installation, ensure the list reflects the names you have used.
4. If you are using Windows Authentication, also add the name of the service account that is used for the following Windows services:
   - Blue Prism – Audit Service Listener
   - Blue Prism – Log Service
5. Click **Check Names**.

   The names should be validated. If they are not, check that the name matches the application pool or service account you are trying to use and correct as needed.
6. Click **OK**.
7. Select each application pool in turn in the **Group or user name** list, and ensure that **Full control** is selected in the **Permissions for {account name}** list.
8. Click **OK**.

   The application pools now have access to the certificate.

File service

If the File service fails to locate the imagery for Authentication Server and Hub then this is caused by an uninstallation and reinstallation of the Blue Prism products. This issue will not occur for first-time installations.

During the removal process, the databases are not removed and so if the reinstallation uses the same database names then the original paths to the file services and URLs will still be used.

To overcome this, after the removal process has been run, either delete or clean the databases so that any previous paths have been deleted or use alternatives database names during the reinstallation.

Hub shows an error on starting

If a user logs into the Authentication Server, selects Hub and the following message displays:

An error occurred while starting the application

This means that the IIS sites need to be restarted. This error affects systems that are installed on a single server and occurs if RabbitMQ starts up after the IIS sites. Therefore, it is recommended that the IIS sites have a startup delay set on them to allow RabbitMQ to start up first.

If this error occurs, it can be resolved in the following way:

1. On the server, open Internet Information Services (IIS) Manager and stop all the Blue Prism sites. For a list, see Hub websites.
2. Restart the RabbitMQ Service.
3. Restart all Blue Prism application pools.
4. Start the Blue Prism sites that were stopped in step 1.

To delay the IIS sites service startup:

1. On the server, open Services.
2. Right-click **World Wide Web Publishing Service** and select **Properties**.
3. On the General tab, set **Startup type** to **Automatic (Delayed Start)**.
4. Click **OK** and close the Services window.

Not able to configure SMTP settings in Hub

If you are unable to configure SMTP settings in Hub this is normally related to the startup order of the services.

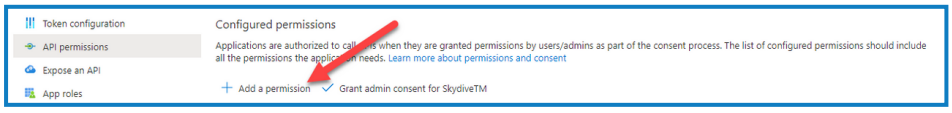
The web server must start up after the RabbitMQ services have all started. If the web server services start before the RabbitMQ service is ready, then going into the SMTP settings in Hub will result in a 'something went wrong' message.

Saving the SMTP setting returns an error when using OAuth 2.0

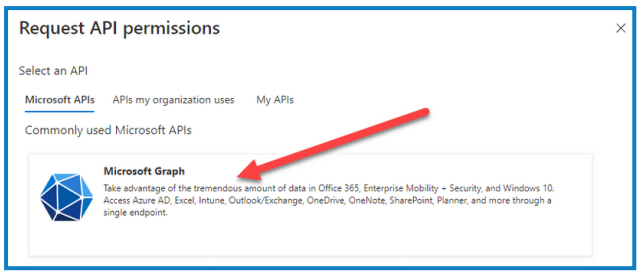
If you receive an error when saving a email configuration using OAuth 2.0, check that the Mail.Send permission is configured for the application in Azure Active Directory.

To add the Mail.Send permission:

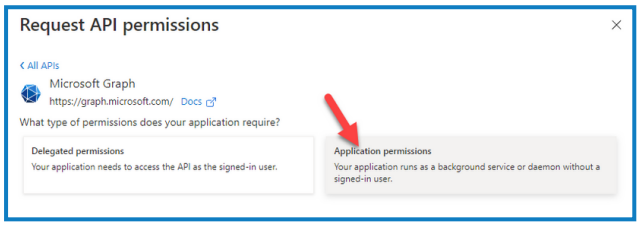
1. In Azure Active Directory, open the application properties for the application that you are linking Hub to.
2. Click **API permissions**.
3. Click **Add a permission**.



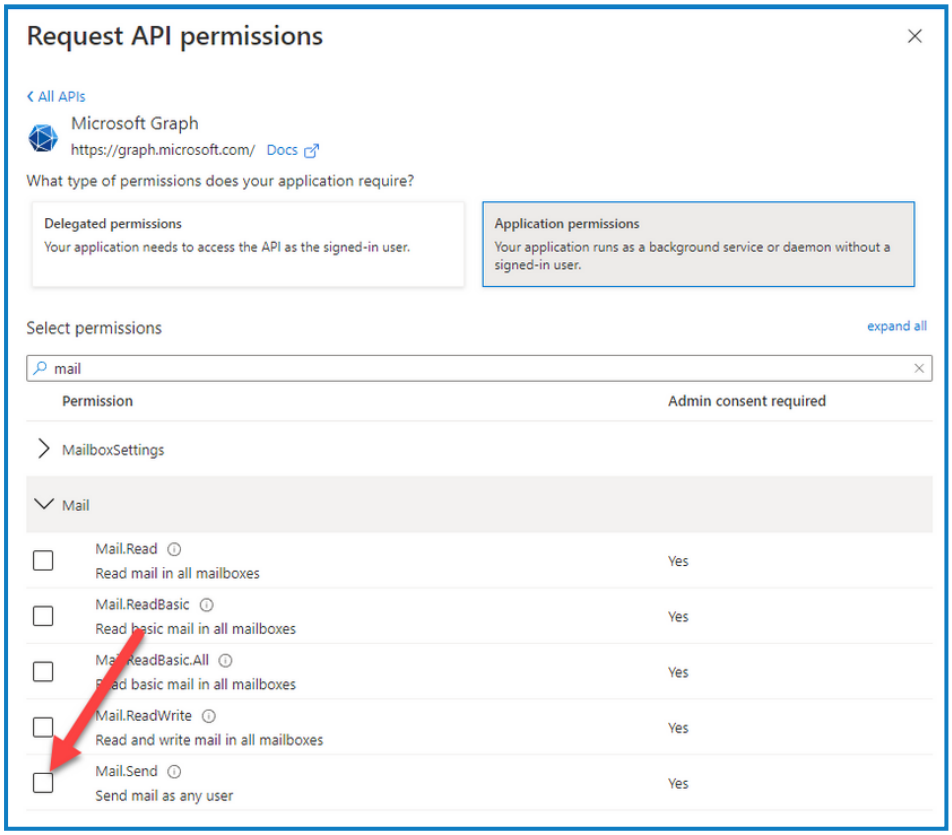
4. In Select an API, under Microsoft APIs, select **Microsoft Graph**.



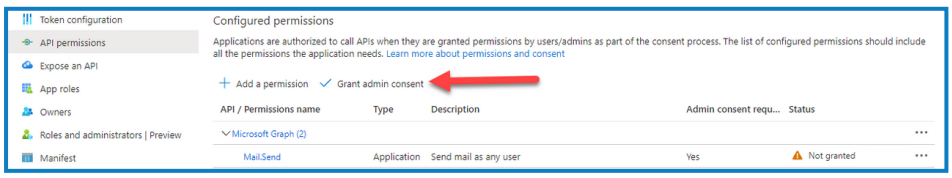
5. Under Microsoft Graph, click **Application permissions**.



6. Type *Mail* in the search field and press Enter.
7. Under the Mail list that is displayed, select **Mail.Send** and click **Add permissions**.



8. On the application permissions page, click **Grant admin consent**.



Updating the Customer ID after installation

If you need to enter or update your Customer ID after installation, you will need to update the License Manager appsettings.json configuration file. Once the configuration file has been updated, the License Manager must be restarted in Internet Information Services (IIS) Manager.

To update your Customer ID in the appsetting.json file:

1. Open Windows Explorer and navigate to `C:\Program Files (x86)\Blue Prism\LicenseManager\appsettings.json`.

   This is the default install location – adjust this if you have used a custom location.

2. Open the appsettings.json file in a text editor.
3. Locate the `License:CustomerId` section of the file and enter your new Customer ID, for example:

```
"License": {
    "CustomerId": "your-Customer-ID-here"
}
```

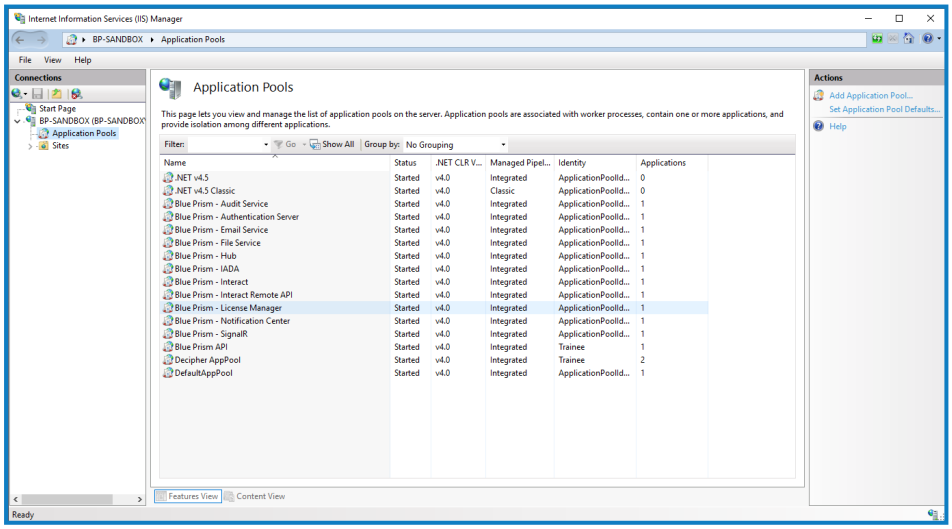
4. Save the file.

To restart License Manager:

1. Open Internet Information Services (IIS) Manager.
2. In the list of connections, select **Blue Prism - License Manager**.

   This is the default site name – if you have used a custom site name, select the appropriate connection.

3. Click **Restart** from the Manage Website controls.



The License Manager restarts.

Updating the Blue Prism API URL after installation

To use the Control Room plugin, connection to the the Blue Prism API is required. If have not enter the Blue Prism API URL during the installation, or you need to change the URL, you will need to update the appsettings.json configuration file. Once the configuration file has been updated, Hub must be restarted in Internet Information Services (IIS) Manager.

To update the API URL in the appsetting.json file:

1. Open Windows Explorer and navigate to `C:\Program Files (x86)\Blue Prism\Hub\appsettings.json`.

   This is the default install location – adjust this if you have used a custom location.

2. Open the appsettings.json file in a text editor.
3. Locate the `RemoteUrlConfiguration:BluePrismApiUrl` section of the file.
4. Change the `"BluePrismApiUrl"` element value to be the URL of your API installation. This example uses `"https://blueprism-api.com"`:

```
"RemoteURLConfiguration": {
    "BluePrismApiUrl": "https://blueprism-api.com"
}
```

5. Save the file.

To restart Hub:

1. Open Internet Information Services (IIS) Manager.
2. In the list of connections, select **Blue Prism - Hub**.

   This is the default site name – if you have used a custom site name, select the appropriate connection.

3. Click **Restart** from the Manage Website controls.

   The Hub application is restarted and configured to allow requests from the Control Room plugin to be sent to the API.

Uninstall Interact

You must be a system administrator to uninstall Blue Prism Interact.

To completely uninstall Interact 4.4, you need to:

1. Stop the Application Pools using IIS.
2. Remove Interact using the Programs and Features application.
3. Remove the databases.
4. Remove RabbitMQ data.
5. Remove the certificates.
6. Remove any remaining files.

Stop the Application Pools using IIS

1. Open the Internet Information Services (IIS) Manager. To do this, type *IIS* in the search box on the Windows taskbar, and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, click **Application Pools**.
3. Stop all the Application Pools associated with the Blue Prism sites – select each in turn and click **Stop**. For a list, see Interact websites on page 15.

Remove Interact using Programs and Features

1. Open Control Panel. To do this, type *control panel* in the search box on the Windows taskbar, and then click **Control Panel**.
2. Click **Programs** and then click **Programs and Features**.
3. Select Blue Prism Interact.
4. Click **Uninstall**.
5. Confirm that you want to continue with the uninstall.

Remove the databases

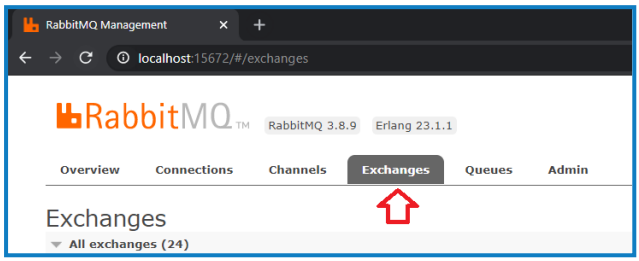
You should only remove databases for test systems. If you are contemplating removing a database for a system that had been in production, you should consider whether the data needs to be archived by your organization or used for audit purposes.

> Following the uninstall of Interact, if it is reinstalled at a later date using the same databases, then the databases should be cleared of any data prior to re-installation.

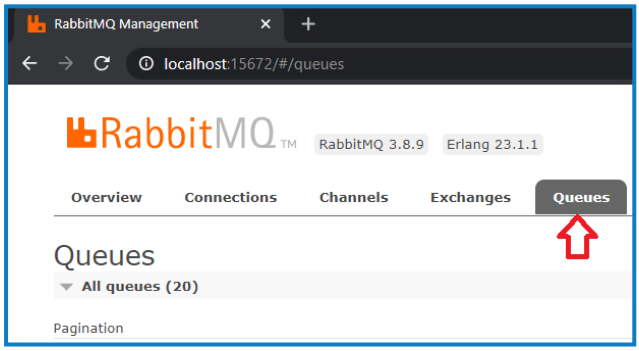
1. Delete, or archive, the database for the Interact application.

Remove RabbitMQ data

1. Open the RabbitMQ admin page. By default, the URL is http://localhost:15672/ on the local machine.
2. Click **Exchanges**.



3. Find and remove the following items:
   - Interact
4. Click **Queues**.



5. Find and remove the following items:
   - Interact

Remove the certificates

These certificates are also used by Hub. If Interact and Hub are installed on the same server, skip this section and remove them when you uninstall Hub. For more information, see the Hub Install Guide.

1. Open the Certificate Manager. To do this, type *Certificates* in the search box on the Windows taskbar, and then click **Manage Computer Certificates**.
2. In the navigation pane, expand **Trusted Root Certification** and click **Certificates**.
3. Select and delete any certificates that were created for the Blue Prism sites, as well as:
   - BluePrismCloud_Data_Protection
   - BluePrismCloud_IMS_JWT

Remove any remaining files

1. In Windows Explorer, open the parent folder for the Interact installation. By default, this is `C:\Program Files (x86)\Blue Prism` but it may have been changed during the Interact installation.

2. Delete the following folders and files:
    - IADA
    - Interact
    - Interact Remote API
    - Submit Form Manager