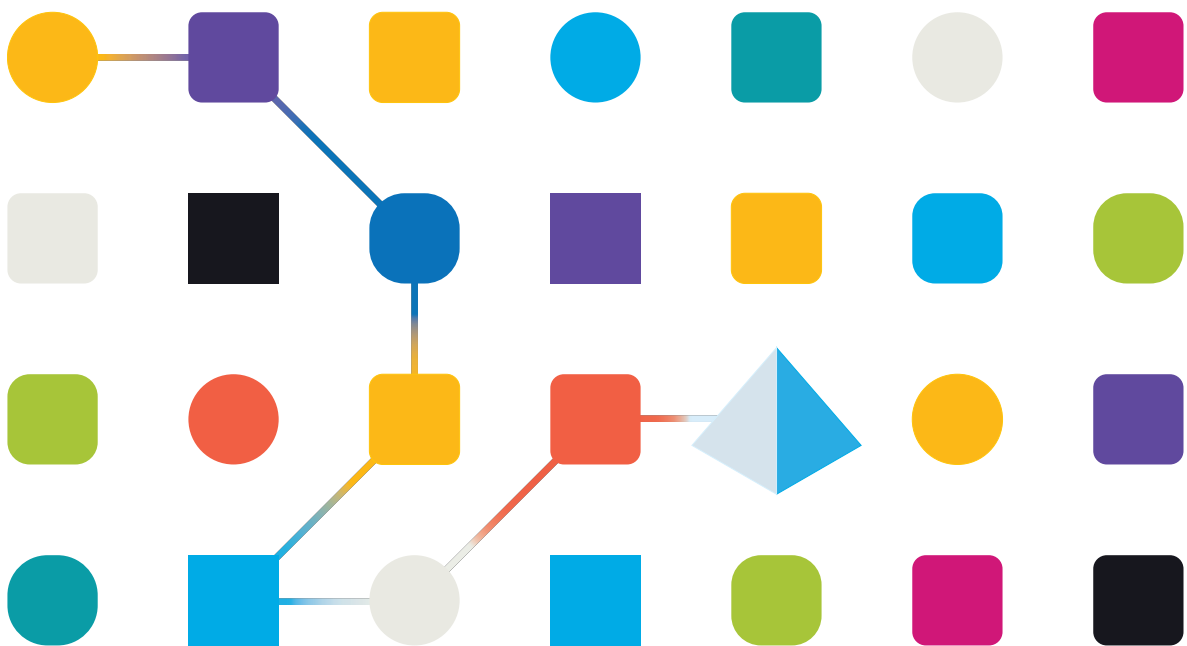




# Interact 4.7

## Install Guide

Document Revision: 9.1



## Trademarks and Copyright

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

© 2024 Blue Prism Limited

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

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

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

# Contents

<b>Introduction</b>	<b>5</b>
Upgrading Interact	5
Intended audience	5
Videos	5
Related documents	5
<b>Preparation</b>	<b>7</b>
Planning	7
Prerequisites	8
Software download list	10
<b>Minimum hardware requirements</b>	<b>12</b>
Runtime Resource	12
Database server	12
Message Broker server	12
Web server	12
<b>Software requirements and permissions</b>	<b>13</b>
Software requirements	13
Minimum SQL permissions	15
Default application information	15
<b>Multi-device deployment considerations</b>	<b>16</b>
<b>Network ports</b>	<b>17</b>
<b>Typical deployment</b>	<b>18</b>
Overview of typical installation steps	19
Install the Message Broker server	20
Install and configure the web server	25
Install Blue Prism Interact	54
Installing using Windows Authentication	60
Initial Hub configuration	65
Install the Interact plugin	74
Configure Digital Workers	75
Verify an installation	84
<b>Troubleshoot an Interact installation</b>	<b>89</b>
Database connectivity	89
Web server	89
Use RabbitMQ with AMQPS	89
Windows Authentication	90
Messages stuck in RabbitMQ	94
<b>Troubleshoot a Hub installation</b>	<b>96</b>
Message Broker connectivity	96
Database connectivity	96
Web server	97
Use RabbitMQ with AMQPS	97

File service .....	98
Configure browsers for Integrated Windows Authentication .....	98
Hub shows an error on starting .....	102
Not able to configure SMTP settings in Hub .....	102
Saving the SMTP setting returns an error when using OAuth 2.0 .....	103
Updating the Customer ID after installation .....	104
<b>Uninstall Interact .....</b>	<b>106</b>
Stop the Application Pools using IIS .....	106
Remove Interact using Programs and Features .....	106
Remove the databases .....	106
Remove RabbitMQ data .....	107
Remove the certificates .....	107
Remove any remaining files .....	107

## 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 4.7 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
<a href="#">Hub user guide</a>	A document aimed at Hub users explaining how to get the best out of Hub.
<a href="#">Hub administrator guide</a>	A detailed document aimed at Hub administrators explaining how to get the best out of Hub, including user access, licensing plugins and customization of Hub.
<a href="#">Interact plugin user guide</a>	A detailed document explaining how to get the best out of Interact, including creating Forms and assigning them to Roles.
<a href="#">Interact user guide</a>	A detailed document explaining how to use Interact to submit and approve forms.

Document Title	Description
<a href="#">Interact Web API Service user guide</a>	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?  
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:

- SQL Server must be configured to use SSL encryption. If your organization does not already use SSL encryption (you have been running your environment without certificates for your SQL Server, or you have been using a self-signed certificate), your organization should obtain a certificate from a trusted certificate authority and import it into SQL Server to enable this. For more information, see [Microsoft's documentation](#).

To import the certificate into SQL Server:

1. From the Windows task bar, open **SQL Server Configuration Manager**.
2. In the SQL Server Configuration Manager, expand **SQL Server Network Configuration** and right-click **Protocols for <SqlServerInstanceName>**, and then click **Properties**.
3. In the Protocols for <SqlServerInstanceName> Properties dialog, select the **Certificate** tab, and then select or import the required certificate.
4. Click **Apply**.

 Certificates from trusted certificate authorities should be used for Production environments. However, a self-signed certificate could be used for Proof of Concept, or Development environments. It is important that the fully qualified domain name (FQDN) used by SQL Server matches the FQDN defined in the certificate. **If these do not match, a connection to the database will not be established and your installation will not function correctly.** For information on using and configuring self-signed certificates, see [Self-signed certificates](#) in the Blue Prism Hub installation guide.

In addition to the databases installed by the Hub installer, your Blue Prism database must also use SSL encryption, using a certificate that the Hub server trusts, such as from a trusted certificate authority.

- 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 certificates](#) for 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 15](#).
- 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
<p>RabbitMQ 3.11.9, 3.11.10, 3.12.12</p> <p>For more information, see <a href="#">Downloading and Installing RabbitMQ</a>.</p>	<p><a href="#">Install the Message Broker server on page 20</a></p>
<p>Erlang/OTP <a href="#">24.x</a> or <a href="#">25.x</a></p> <p>The version of Erlang that you require is dependent on the RabbitMQ version you intend to use. For more information, see <a href="#">RabbitMQ Erlang Version Requirements</a>.</p>	
<p>IIS 10.0</p> <p>Included with Windows Server 2016, 2019 and 2022.</p>	<p><a href="#">Install and configure the web server on page 25</a></p>
<p>ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle)</p> <p><a href="https://dotnet.microsoft.com/download/dotnet/6.0">https://dotnet.microsoft.com/download/dotnet/6.0</a> - Select the version you require. Under <b>ASP.NET Core Runtime</b>, select <b>Hosting Bundle</b>.</p>	
<p>.NET Desktop Runtime 6.0.9 or 6.0.10</p> <p><a href="https://dotnet.microsoft.com/download/dotnet/6.0">https://dotnet.microsoft.com/download/dotnet/6.0</a> - Select the version you require. Under <b>.NET Desktop Runtime</b>, select the appropriate download.</p>	
<p>.NET Framework 4.8</p> <p><a href="https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0">https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0</a></p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> This is installed by default on Windows Server 2022. You only need to install the .NET Framework if you are using Windows Server 2016 Datacenter or Windows Server 2019.</p> </div>	
<p>Blue Prism Hub 4.7</p> <p>Download Hub from any of the following product download pages on the Blue Prism Portal:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automation Lifecycle Management</a></li> <li>• <a href="#">Decision</a></li> <li>• <a href="#">Interact</a></li> </ul>	
<p>Authentication Server SAML 2.0 extension</p> <p>Download from the <a href="#">Digital Exchange</a> - This is an optional installer. It is only required if you intend to use SAML 2.0 authentication.</p>	<p>See the installation guide on the <a href="#">Digital Exchange</a>.</p>

## 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 4.7 Download from the <a href="#">Blue Prism Portal</a> .	<a href="#">Install Blue Prism Interact</a>
Blue Prism Interact Remote API.bprelease file Download from the <a href="#">Blue Prism Portal</a> .	<a href="#">Install and configure the Interact Web API service</a>

## Minimum hardware requirements


The information below details the minimum hardware requirements recommended for effectively installing and running Hub and Interact 4.7. 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 - A minimum of 100 eDTUs are required during installation. This can be lowered to 50 eDTUs following installation.
- 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 or 2022

### Web server

- Intel Dual Xeon Processor
- 8 GB RAM
- Windows Server 2016 Datacenter or 2019 or 2022
- 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	✓	✓
Windows Server 2022	✓	✓

 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)	✓	✓	✓

#### Note:

- SQL Express is only appropriate for non-production environments, such as for the purposes of proof of concept exercises.
- SQL Server must be configured to use SSL encryption. If your organization does not already use SSL encryption (you have been running your environment without certificates for your SQL Server, or you have been using a self-signed certificate), your organization should obtain a certificate from a trusted certificate authority and import it into SQL Server to enable this. For more information, see [Microsoft's documentation](#).

For steps on importing certificates into SQL Server, see [Prerequisites on page 8](#).

 Certificates from trusted certificate authorities should be used for Production environments. However, a self-signed certificate could be used for Proof of Concept, or Development environments. It is important that the fully qualified domain name (FQDN) used by SQL Server matches the FQDN defined in the certificate. **If these do not match, a connection to the database will not be established and your installation will not function correctly.** For information on using and configuring self-signed certificates, see [Self-signed certificates](#).

The following are also supported:

- Azure SQL Database - A minimum of 100 eDTUs are required during installation. This can be lowered to 50 eDTUs following installation.
- 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 3.11.9, 3.11.10, 3.12.12
- Erlang/OTP 24.x or 25.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.

 Blue Prism aims to fully test new RabbitMQ versions against the latest Hub version within two months of the general availability of that software. If any subsequent Hub development is required to support a new RabbitMQ version, any updates will be incorporated into a future release of Hub as determined by our release cycle.

## Web server

The following software is required on the Web server:

- .NET Framework 4.8 - Installed by default on Windows Server 2022.
- IIS 10.0
- ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle)
- .NET Desktop Runtime 6.0.9 or 6.0.10

 Interact 4.7 only supports the versions of ASP.NET Core Runtime and .NET Desktop Runtime shown above. If you use a later version, such as 7.x.x, you may experience issues.


See [Install and configure the web server on page 25](#) for more information.

## Web browser on client machines

The latest versions of the following web browsers are supported by Interact:

- Google Chrome
- Microsoft Edge (Chromium-based)

To enable Active Directory users to log into Interact using a Chrome or Edge browser, the browsers **must be configured for Integrated Windows Authentication**.

 Microsoft Internet Explorer and Mozilla Firefox are not supported.

## 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	ladaDB

## 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	<p>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).</p> <p>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.</p>
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:

<b>Database server</b>	<p>Port 1433 to allow SQL Server Connectivity from the Web Server.</p> <p>If the SQL Server instance is a named instance, it will also require:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• UDP Port 1434 for the SQL Server Browser Service to allow SQL Server Connectivity from the Web Server.</li> </ul>
<b>Message Broker server</b>	<p>Port 5672 to allow RabbitMQ Messaging connectivity.</p> <p>Port 15672 to allow RabbitMQ Management Console connectivity.</p>
<b>Web server</b>	<p>Port 443 to allow HTTPS connectivity.</p>
<b>Digital Workers</b>	<p>Port 443 to allow HTTPS connectivity.</p>

 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.

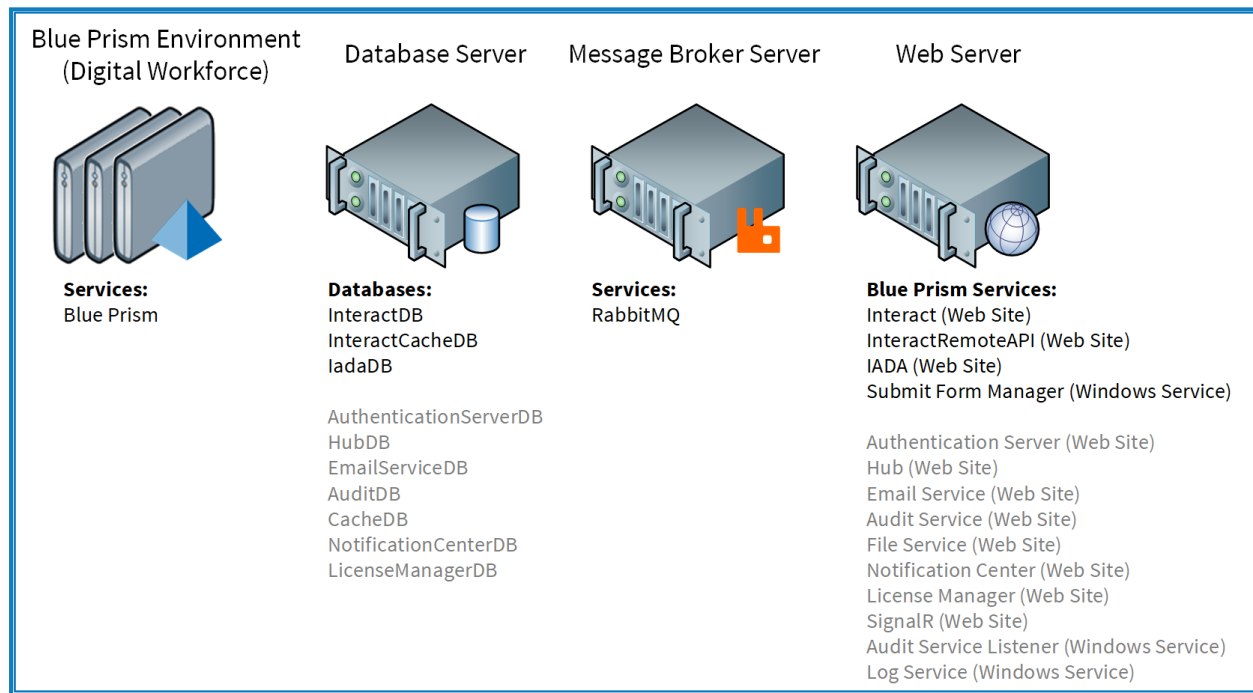
 Prior to following this guidance, ensure that you have fully considered the information in [Preparation](#).


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.

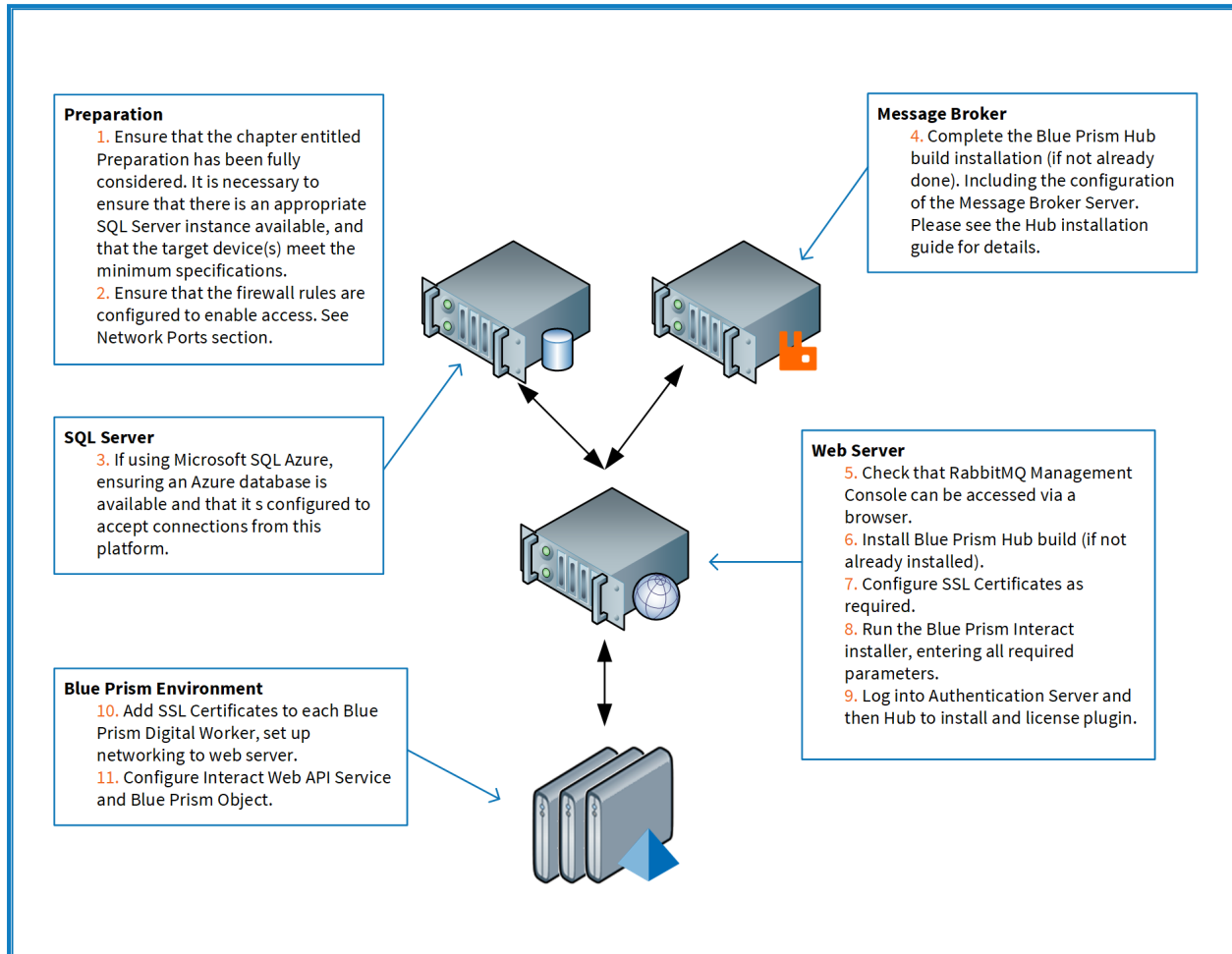
The diagram below illustrates the typical architecture for an environment.



 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>.

🔗 For software versions, see [Software requirements on page 13](#).

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.

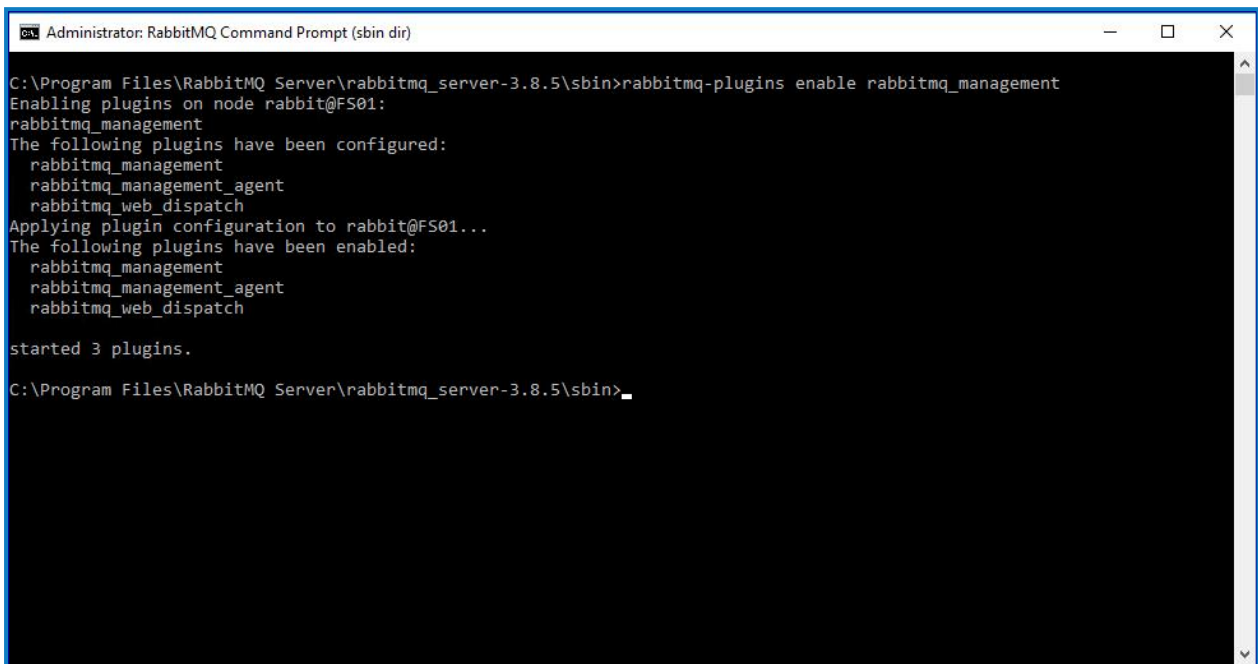
🔗 For more information, see [Downloading and Installing RabbitMQ](#).

▶ To watch this installation step, see our [RabbitMQ installation video](#).

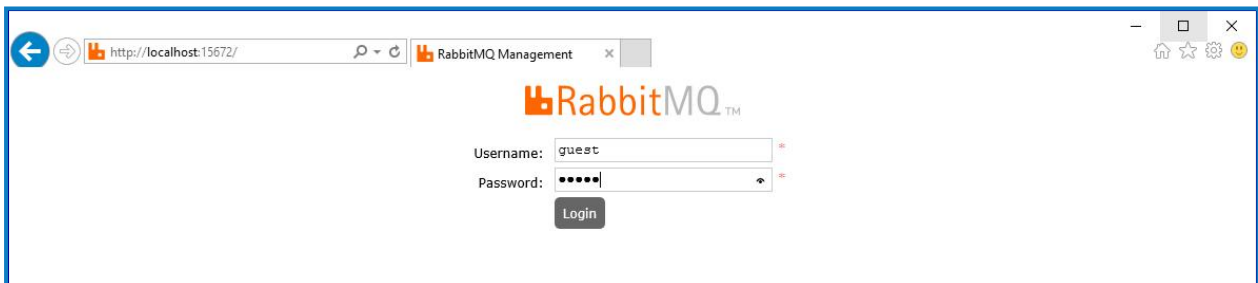
3. Configure Windows Firewall to enable inbound traffic to Ports 5672 and 15672.
4. From the Start menu, under the RabbitMQ Server folder, select the RabbitMQ Command Prompt (sbin dir).

- In the RabbitMQ Command Prompt window, type the following command:

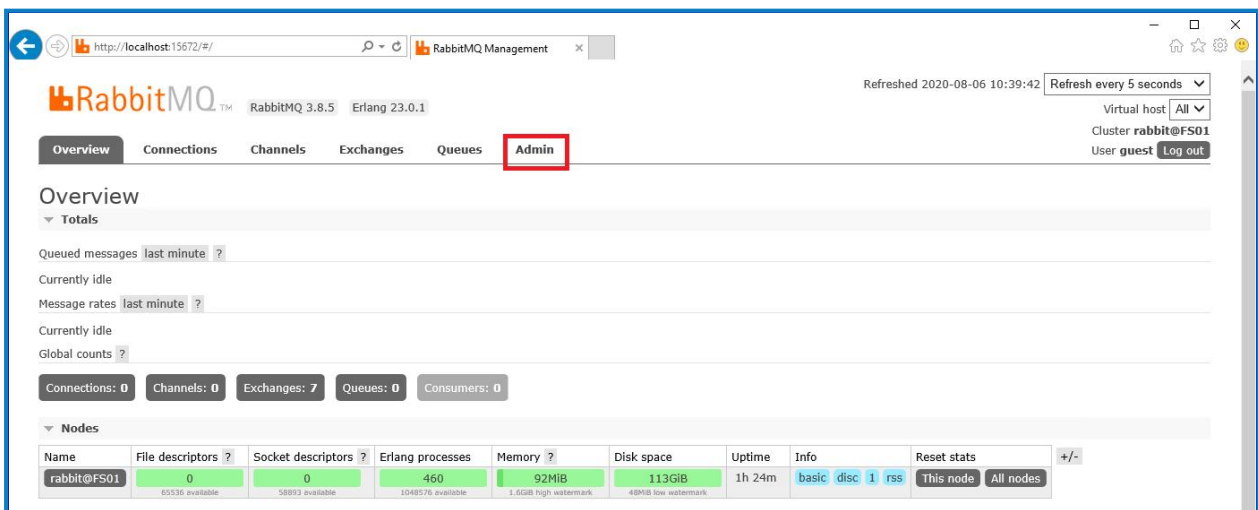
```
rabbitmq-plugins enable rabbitmq_management
```



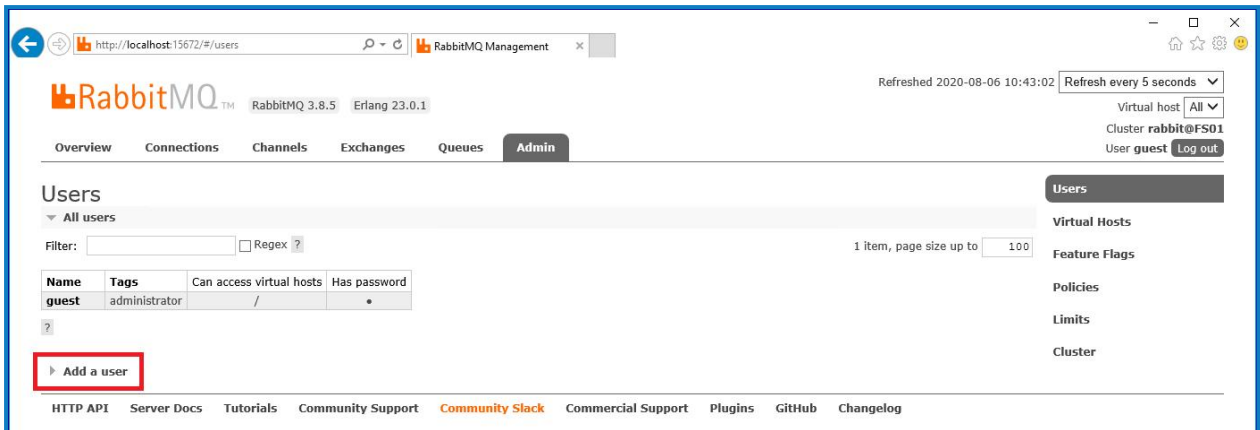
- Launch a browser and navigate to the following URL: <http://localhost:15672>
- In the RabbitMQ console, log on with the default credentials of guest/guest.




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



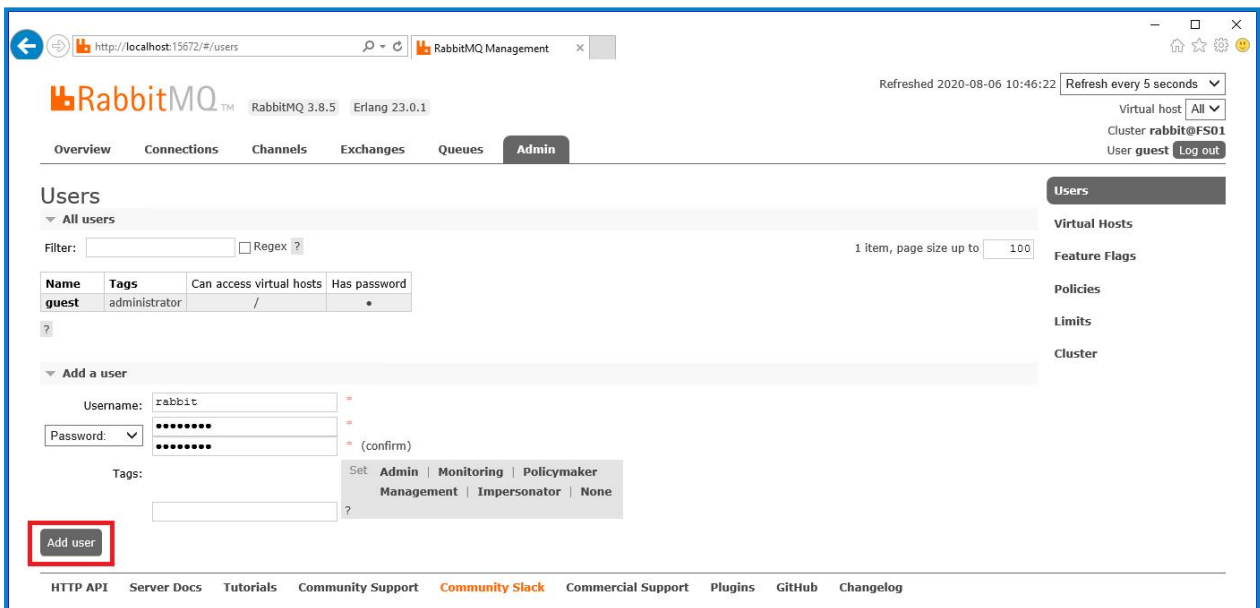
9. Click **Add a user**.



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.

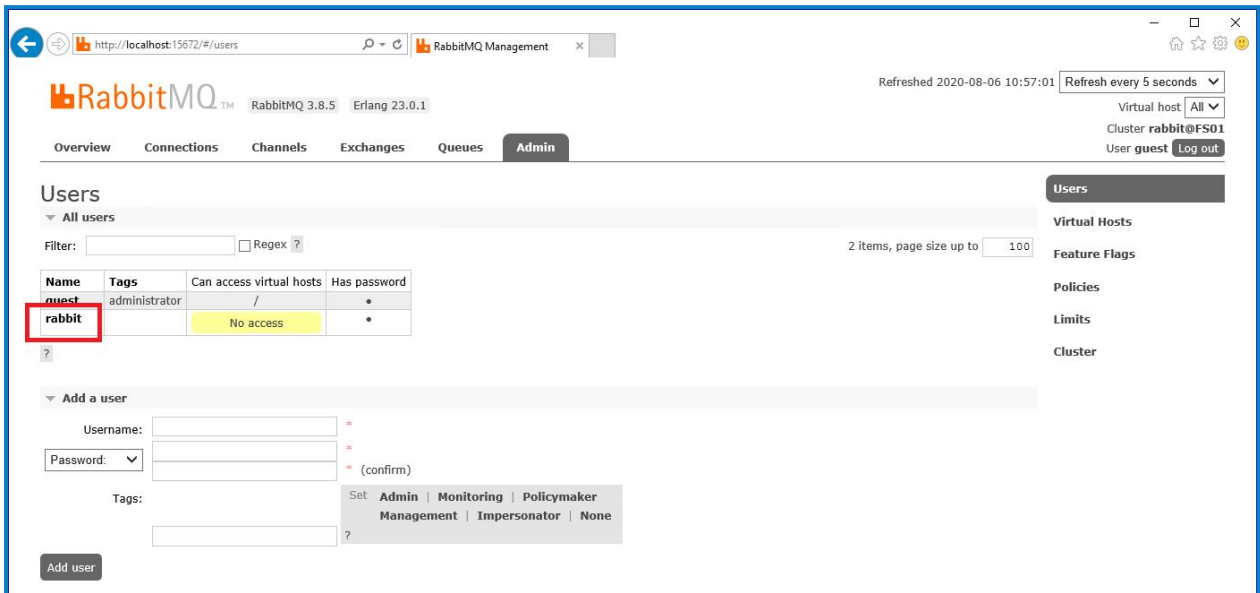
 The following characters must not be used for the password when creating the RabbitMQ user  
# / : ? @ \ ` " \$ ' .

11. Click **Add User**.

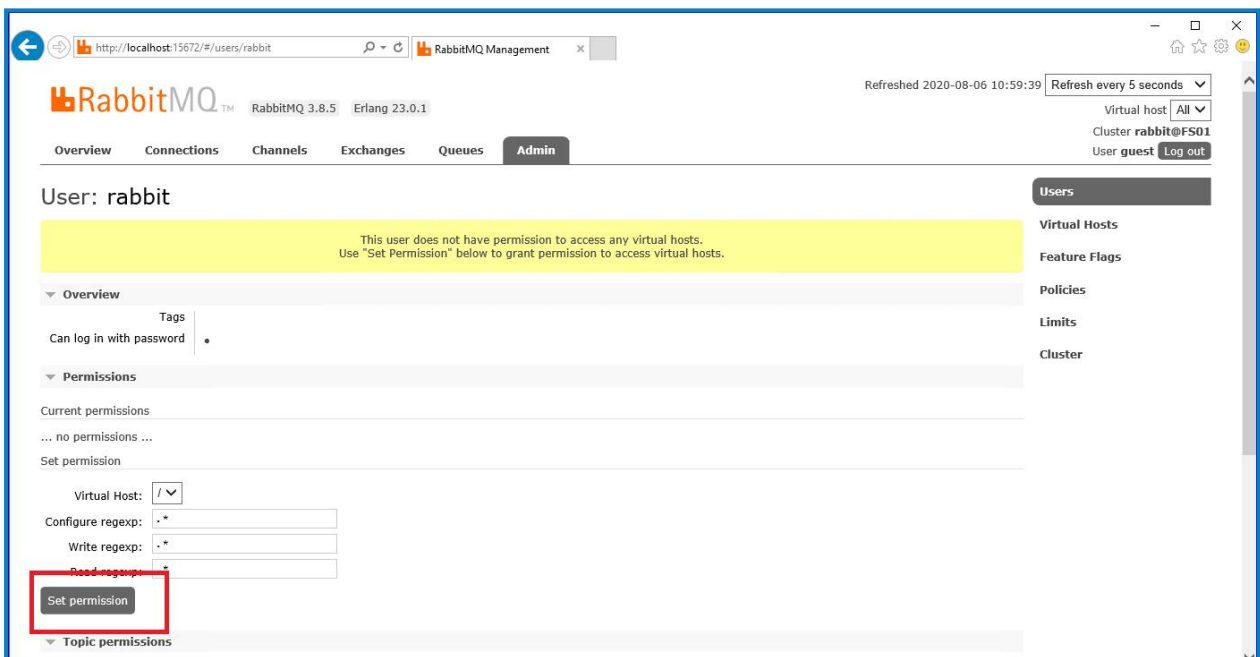


The next step is to set the permissions for the user.

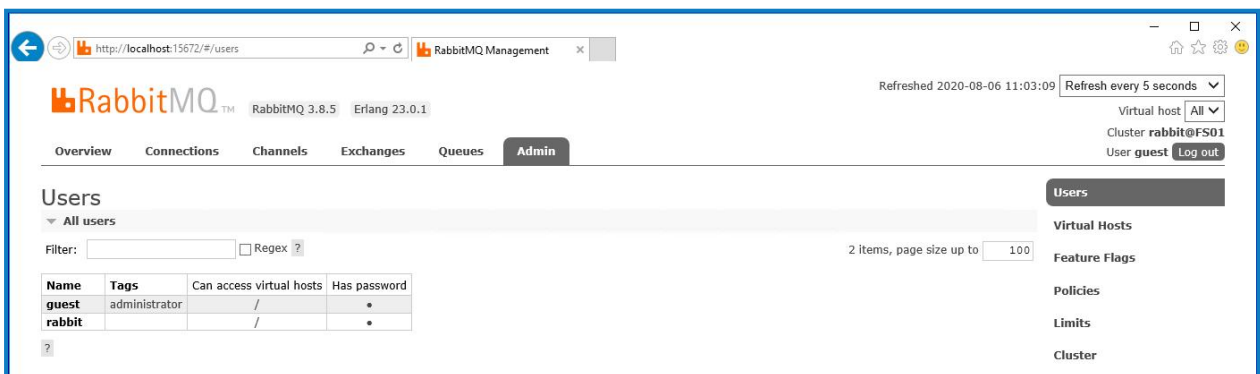
12. Click on the username of the user that you just created.




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 96](#).




## 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. [Install the Authentication Server SAML 2.0 extension](#) - This is only required if you intend to use SAML 2.0 authentication.

 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, Web-Windows-Auth -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.

 When generating a certificate, enter the host name in lowercase characters. If you do not use all lowercase, you may experience a naming mismatch between the name in the certificate and the host name when using the Hub installer. This could result in the certificate failing to be applied and the installer preventing you from progressing with the installation.

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)
<b>Websites with a user interface for use by end-users</b>	
Blue Prism - Authentication Server	https://authentication.local
Blue Prism - Hub	https://hub.local
<b>Websites for use by the application only (services)</b>	
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
<b>Websites with a UI for use by end-users</b>	
Blue Prism - Interact	https://interact.local
<b>Websites for use by the application only (services)</b>	
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.

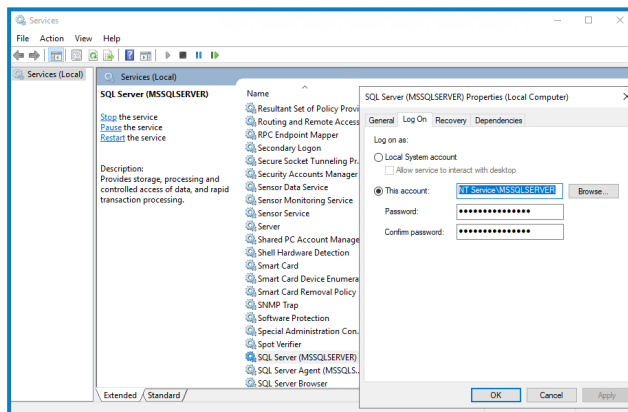
To generate and apply a self-signed certificate for SQL Server:

 Microsoft provide a script that can be used to generate a self-signed certificate for SQL Server. For more information, see [Microsoft's documentation](#). It is important that the fully qualified domain name (FQDN) used by the SQL Server matches the FQDN defined in the certificate. **If these do not match, a connection to the database will not be established and your installation will not function correctly.**

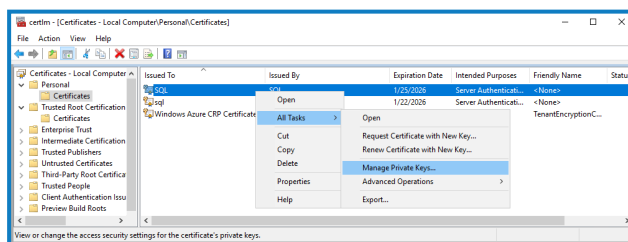
1. Run PowerShell as an administrator and execute the [Microsoft script](#) with the information for your SQL Server.

This generates the certificate and installs it on the SQL Server.

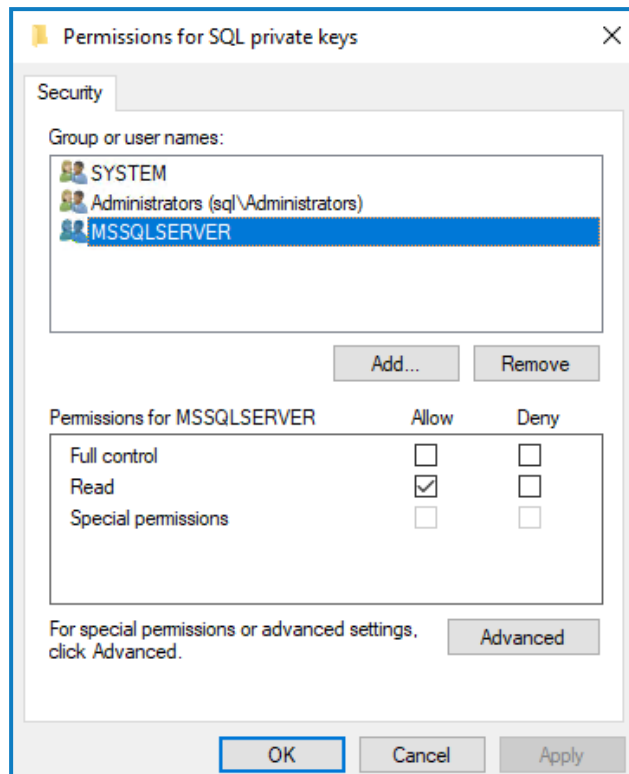
2. On your SQL Server:
  - a. Enable access to the certificate's private key for the SQL Server service account. To do this:
    - i. If you do not already know it, find your service account name for your SQL Server. This is shown on the Log On tab of the SQL Server Properties, which can be accessed from Services on your SQL Server.



- ii. On your SQL Server, open Certificate Manager.
- iii. Expand **Personal**, then expand **Certificates**, right-click **SQL**, and then select **All Tasks** and click **Manage Private Keys...**

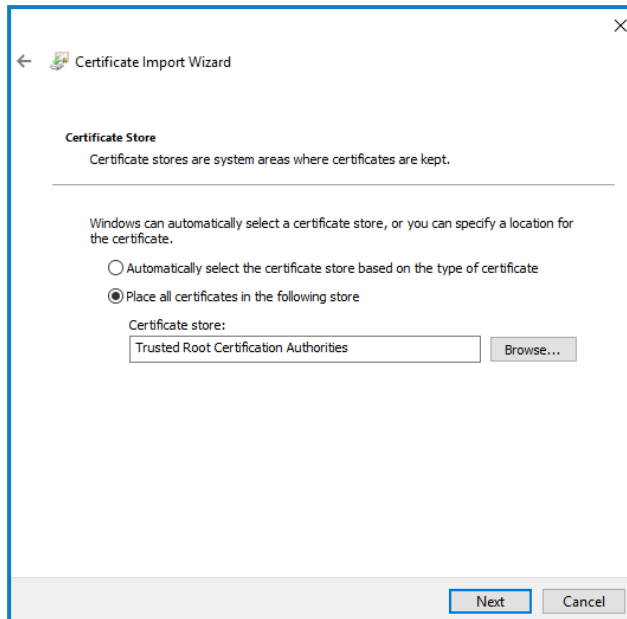


- iv. In the Permissions for SQL private keys dialog, add your SQL Server service account with Read permissions. For example:



- v. Click **OK** to apply the changes and close the dialog.
- b. Enable SSL on your SQL Server and specify the certificate. To do this:
    - i. From the Windows task bar, open **SQL Server Configuration Manager**.
    - ii. In the SQL Server Configuration Manager, expand **SQL Server Network Configuration** and right-click **Protocols for <SqlServerInstanceName>**, and then click **Properties**.
    - iii. In the Protocols for <SqlServerInstanceName> Properties dialog, select the **Certificate** tab, and then select or import the required certificate.
    - iv. Click **Apply**.
    - v. Click **OK** to close the Properties dialog.
  - c. Restart the SQL Server service.
  - d. Copy the certificate C:\sqlservercert.cer. You will need to add this to the Hub and Interact website host servers.
3. On the website host servers:
    - a. Paste the sqlservercert.cer into the website host servers for Hub and Interact.
    - b. Add the certificate to the server's Trusted Root Certification Authorities certificate store. To do this:
      - i. Double-click on the certificate and click **Install Certificate...**  
The Certificate Import Wizard displays.
      - ii. On the Welcome page, select **Local Machine** under **Store Location** and click **Next**.

- iii. On the Certificate Store page, select **Place all certificates in the following store** and enter **Trusted Root Certification Authorities**.



- iv. Click **Next** and follow the wizard through to completion.

- c. Test the connection from the website host server to the SQL Server.

To generate a self-signed certificate for a website:


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.

 When generating a certificate, enter the host name (`[Website]`) in lowercase characters. If you do not use all lowercase, you may experience a naming mismatch between the name in the certificate and the host name when using the Hub installer. This could result in the certificate failing to be applied and the installer preventing you from progressing with the installation.

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 the website 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)
```

 XXXXXXXXXXXX should be replaced with the host server name.

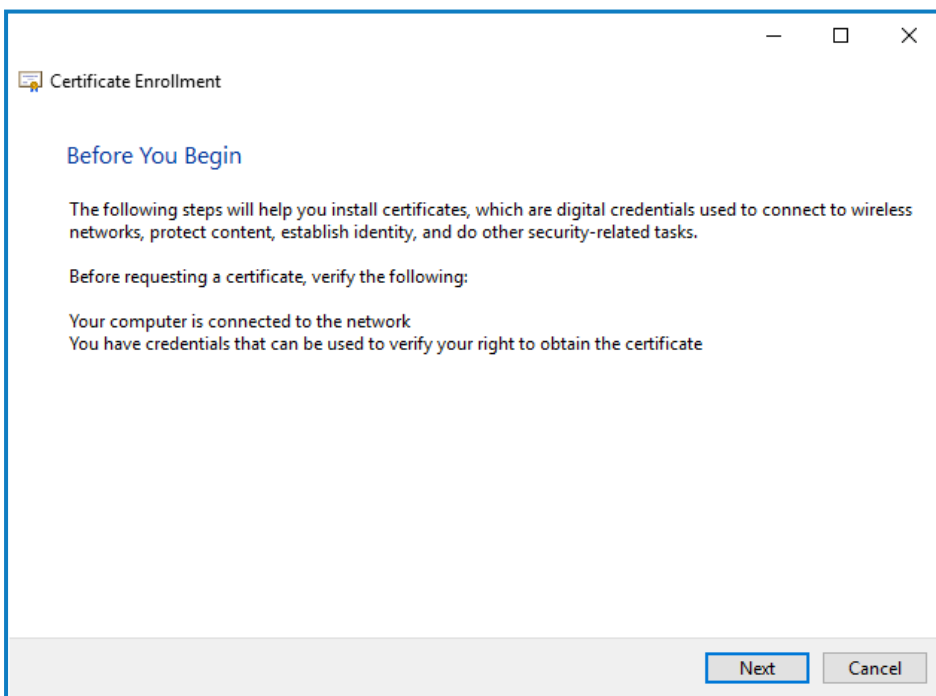
Once created, open the Local Machine certificate manager (certlm) and copy and paste the certificate into the trusted root certificate store.

### Create an offline certificate request

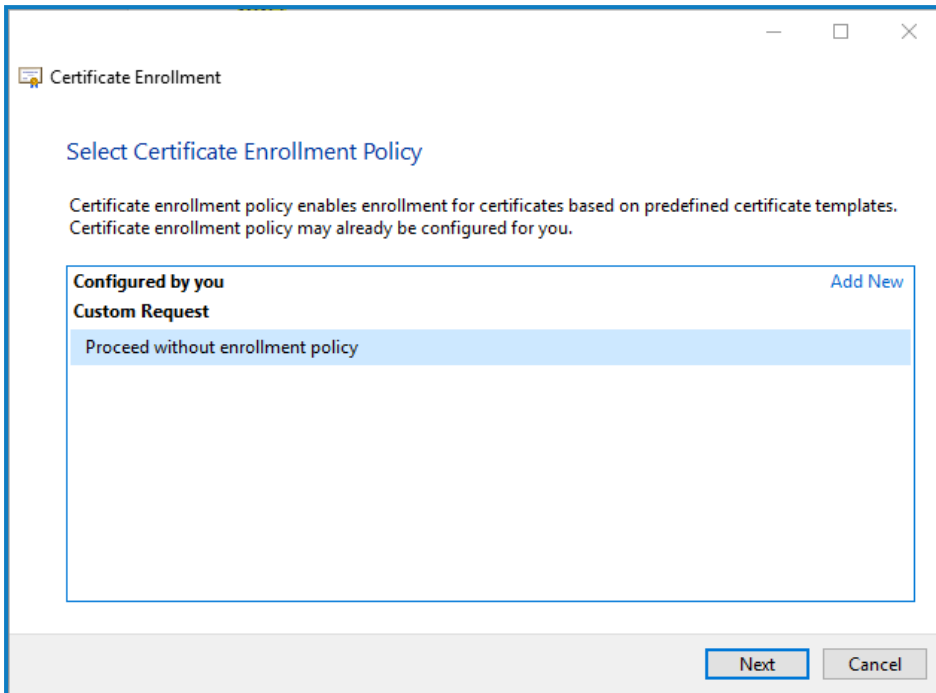
To create an offline certificate request, for each certificate follow this procedure:

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.



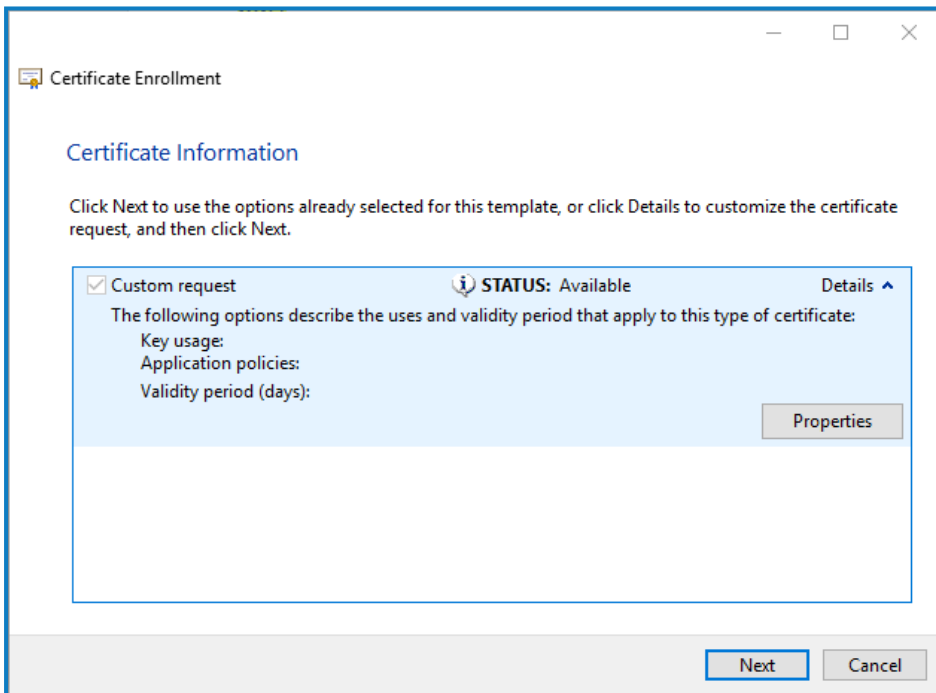
3. Click **Next**.



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	<p>Download the following components and store them in a temporary location, for example, C:\temp:</p> <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle) <a href="https://dotnet.microsoft.com/download/dotnet/6.0">https://dotnet.microsoft.com/download/dotnet/6.0</a> - Select the version you require. Under <b>ASP.NET Core Runtime</b>, select <b>Hosting Bundle</b>.</li> <li>• .NET Desktop Runtime 6.0.9 or 6.0.10 <a href="https://dotnet.microsoft.com/download/dotnet/6.0">https://dotnet.microsoft.com/download/dotnet/6.0</a> - Select the version you require. Under <b>.NET Desktop Runtime</b>, select the appropriate download.</li> <li>• .NET Framework 4.8 <a href="https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0">https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0</a></li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> This is installed by default on Windows Server 2022. You only need to install the .NET Framework if you are using Windows Server 2016 Datacenter or Windows Server 2019.</p> </div>
2	<p>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:</p> <p>For Windows Server 2016 and Windows Server 2019:</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait start-process "C:\temp\ndp48-x86-x64-allos-enu.exe" /q -wait</pre> </div> <p>For Windows Server 2022:</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait</pre> </div> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Ensure the file name and file path match the files that were stored in step 1.</p> </div>
3	<p>Restart your server before installing Blue Prism Hub to ensure the components are fully installed and registered.</p>

 To watch this installation step, see our [.NET installation video](#).

## Install Blue Prism Hub

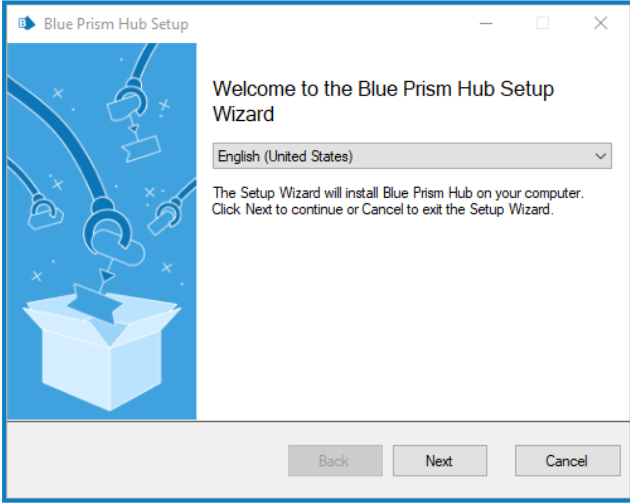
Before you install Blue Prism Hub:

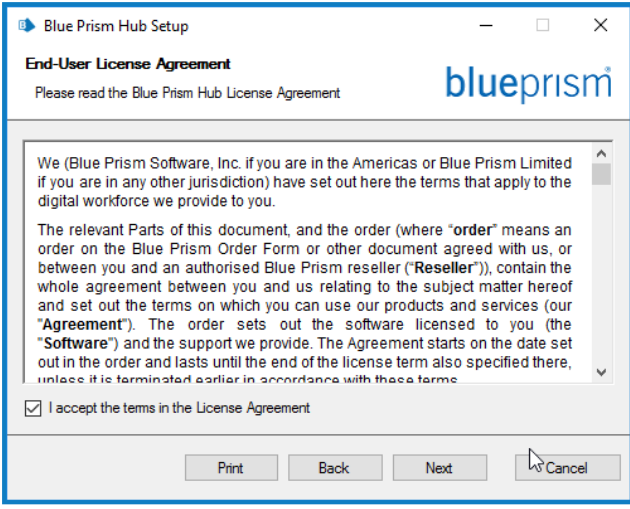
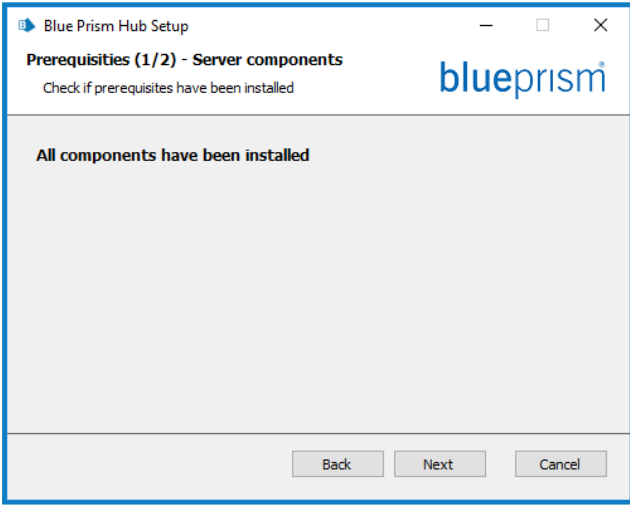
- If you have purchased ALM, Decision or Interact, you will need your Customer ID during this Hub installation. This can be found in the email that was sent to you when you purchased ALM, Decision or Interact.
- If you want to use the Blue Prism Decision plugin in Hub, you will need to install the Blue Prism Decision Model Service container on a Docker host before running the Hub install wizard. For more information, see [Install Blue Prism Decision](#).
- 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.

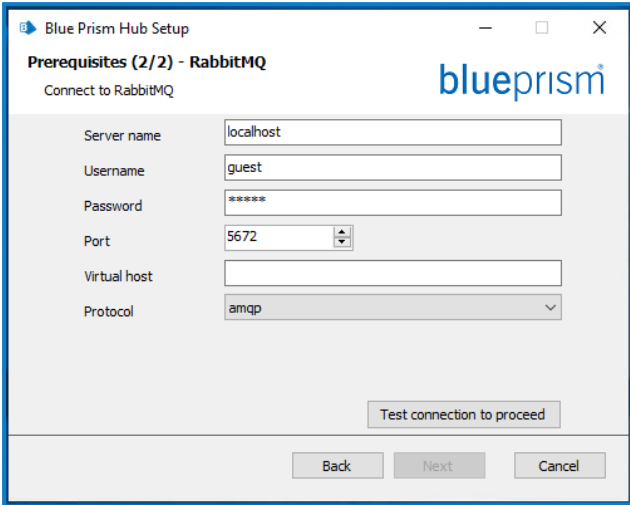


▶ To watch the Hub installation and configuration process, see our [Blue Prism Hub installation video](#).

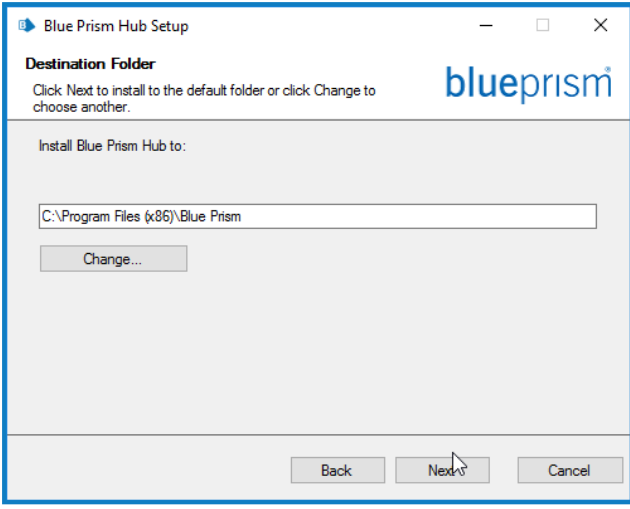
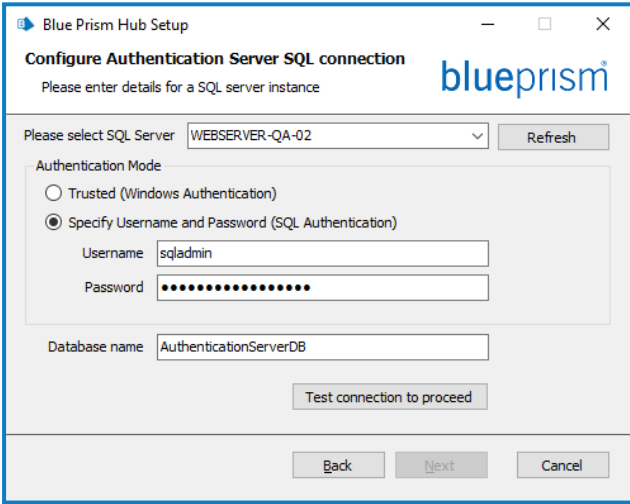

The steps below detail the process for installing the Blue Prism Hub software. This includes the Authentication Server, Hub, and other associated services. The installation process will create any new databases that are required.

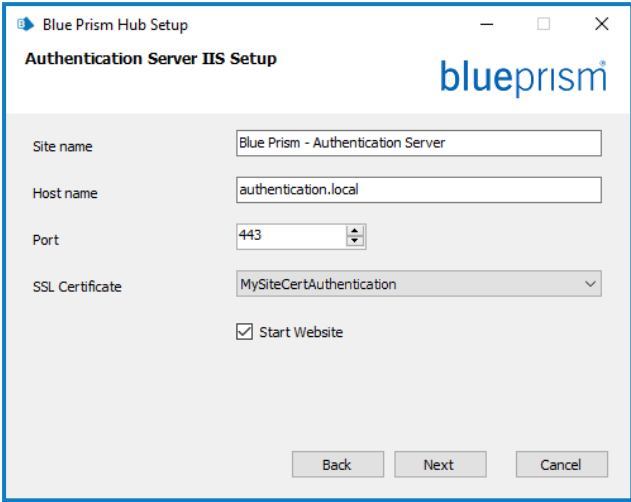


Download and run the Blue Prism Hub installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer must be run with administrator rights.

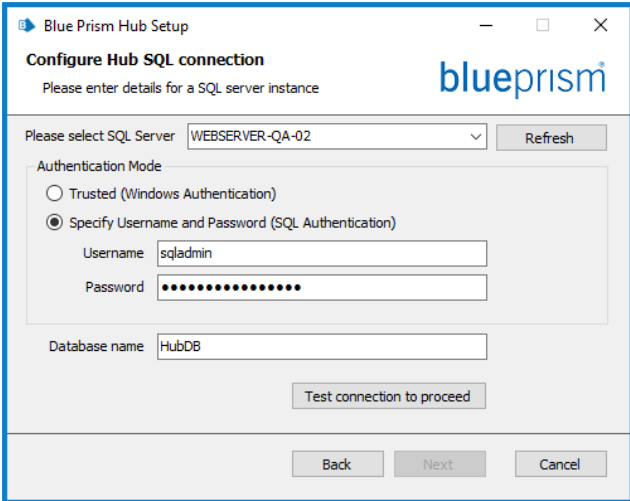

Step	Installer page	Details
1		<p><b>Welcome</b></p> <p>If required, select another language for the installer from the drop-down list. The default language is English (United States). Click <b>Next</b>.</p>

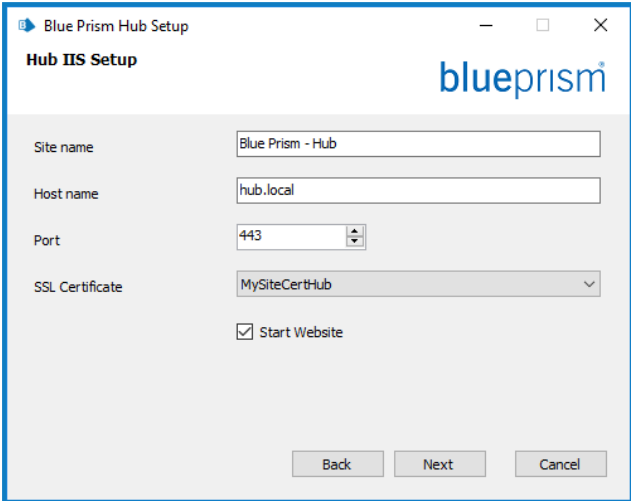

Step	Installer page	Details
<p>2</p>		<p><b>License agreement</b></p> <p>Read the End-User License Agreement and if you agree to the terms, select the check box.</p>
<p>3</p>		<p><b>Prerequisites 1 - Server components</b></p> <p>The installer checks that the prerequisites have been installed. Those that are not installed are identified. You cannot proceed until all the prerequisites are installed.</p> <p>If there are uninstalled prerequisites, cancel the installer and install the missing components before restarting the installer. Otherwise, proceed with the installation.</p>

Step	Installer page	Details
<p>4</p>		<h3>Prerequisites 2 - RabbitMQ</h3> <p>Enter the server name or IP address of the Message Broker server and the credentials of the user you created.</p> <div data-bbox="903 443 1461 607" style="border: 1px solid #0070C0; padding: 5px;"> <p> The default message queuing port is 5672. This should only be changed if the default ports have been changed by your IT support organization.</p> </div> <p>By default, the <b>Virtual host</b> 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.</p> <p>In <b>Virtual host</b>, 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 <a href="#">RabbitMQ website - Virtual Hosts</a>.</p> <p>From the <b>Protocol</b> 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 <a href="#">RabbitMQ website - TLS Support</a>.</p> <div data-bbox="903 1496 1461 1733" style="border: 1px solid #0070C0; padding: 5px;"> <p> 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 <a href="#">Troubleshoot a Hub installation on page 96</a>.</p> </div> <p>Click <b>Test connection</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

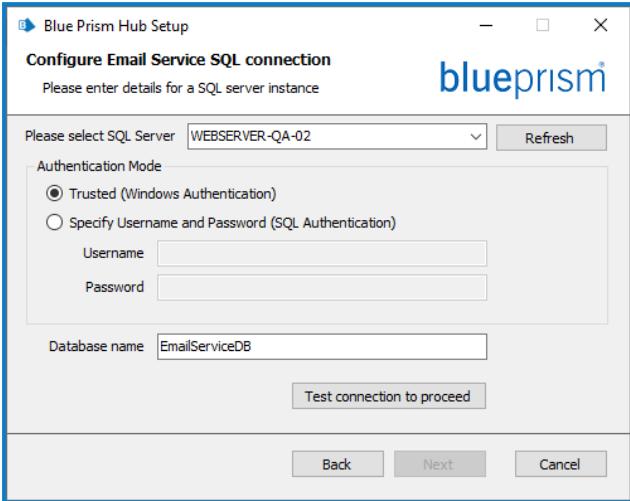

Step	Installer page	Details
<p>5</p>		<p><b>Destination folder</b></p> <p>Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the <b>Change</b> button.</p>
<p>6</p>		<p><b>Authentication Server SQL connection</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid orange; padding: 10px; margin: 10px 0;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

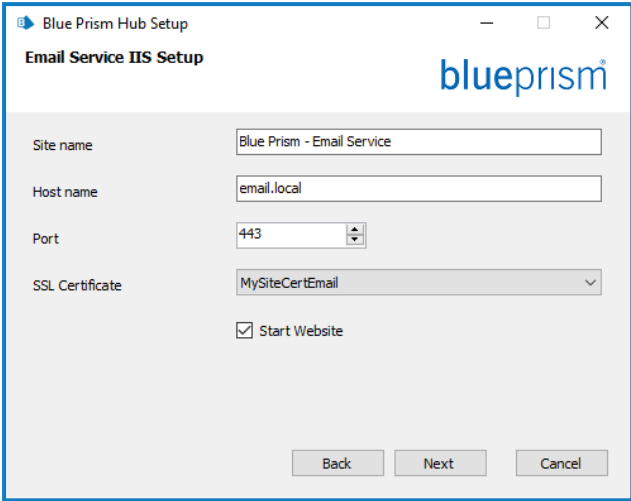

Step	Installer page	Details
<p>7</p>		<h3>Authentication Server IIS setup</h3> <p>Configure IIS for the Authentication Server website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div data-bbox="903 864 1461 987" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div> <div data-bbox="903 1014 1461 1173" style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Once installation is complete, the IIS feature <b>Windows Authentication</b> is enabled on the Authentication Server website.</p> </div>

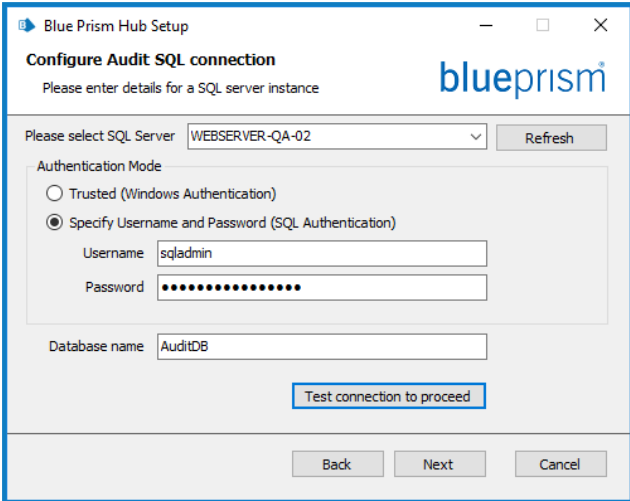

Step	Installer page	Details
<p>8</p>		<h3>Hub SQL connection</h3> <p>Configure the settings for the Hub database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

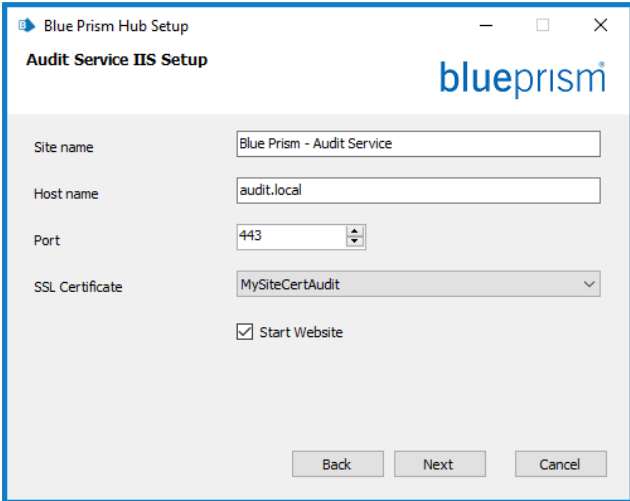

Step	Installer page	Details
<p>9</p>		<p><b>Hub IIS setup</b></p> <p>Configure the Hub website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

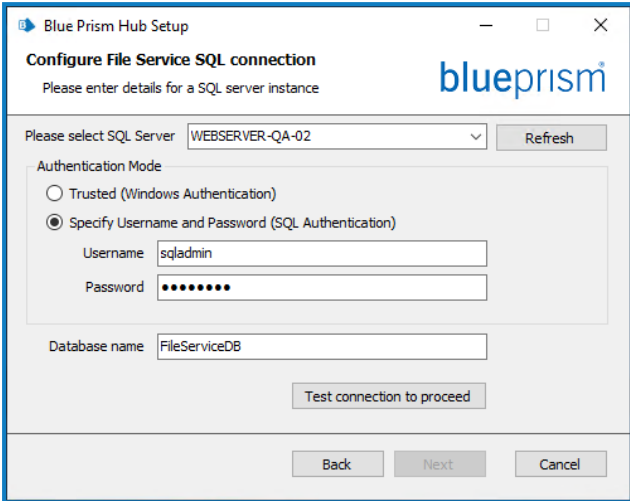



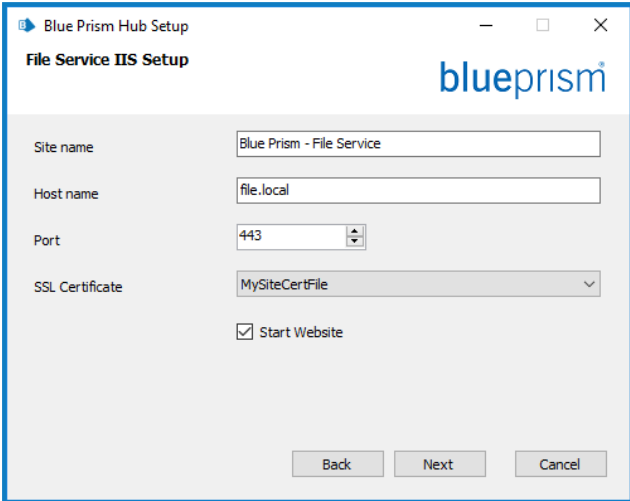

Step	Installer page	Details
<p>10</p>		<h3>Email Service SQL connection</h3> <p>Configure the settings for the Email Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

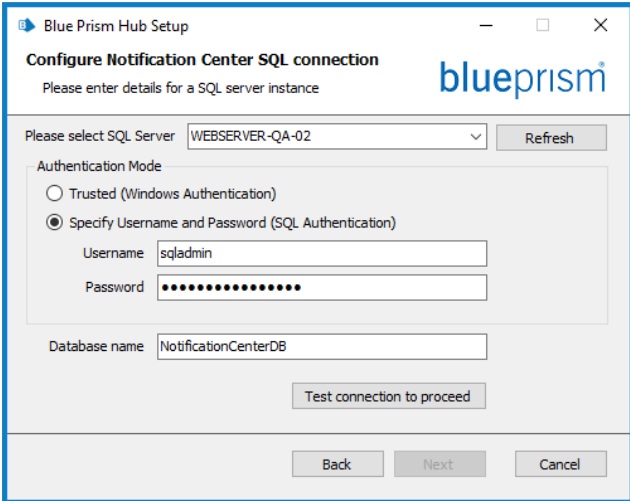

Step	Installer page	Details
<p>11</p>		<p><b>Email Service IIS setup</b></p> <p>Configure the Email Service website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

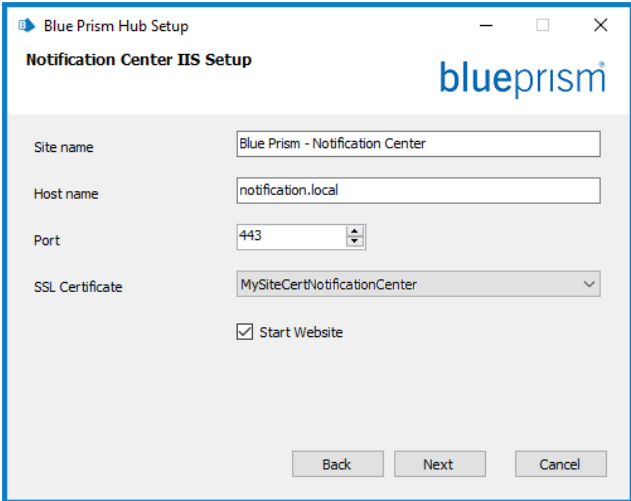

Step	Installer page	Details
<p>12</p>		<p><b>Audit SQL connection configuration</b></p> <p>Configure the settings for the Audit database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

Step	Installer page	Details
<p><b>13</b></p>		<p><b>Audit Service IIS setup</b></p> <p>Configure the Audit Service website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

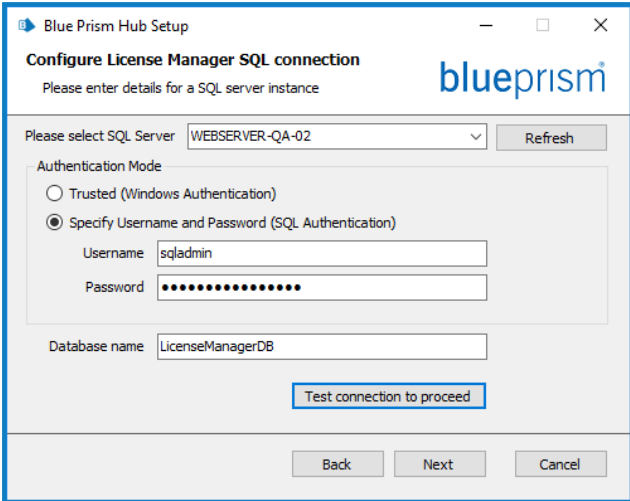

Step	Installer page	Details
<p>14</p>		<h3>File Service SQL connection configuration</h3> <p>Configure the settings for the File Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

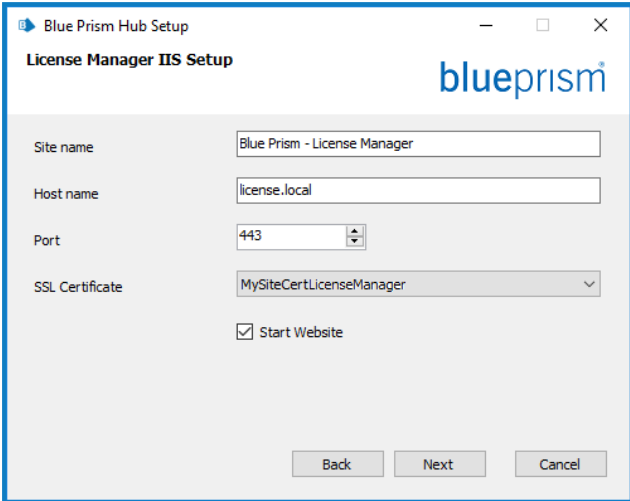

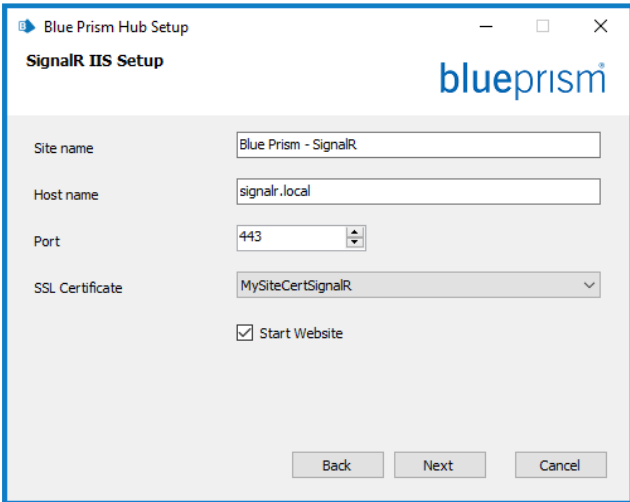

Step	Installer page	Details
<p>15</p>		<p><b>File Service IIS setup</b></p> <p>Configure the File Service website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

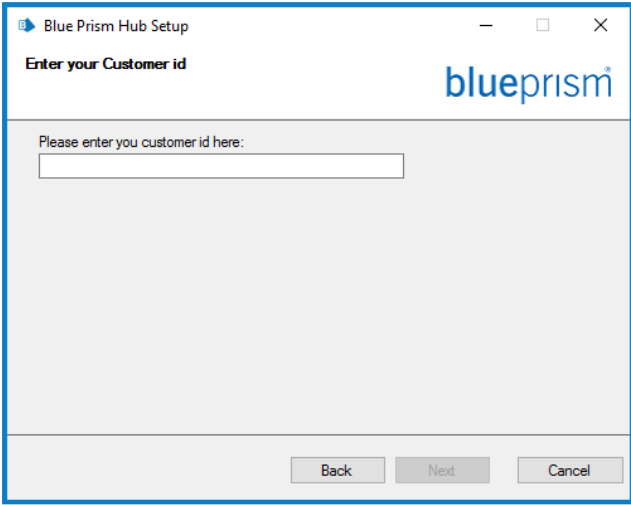
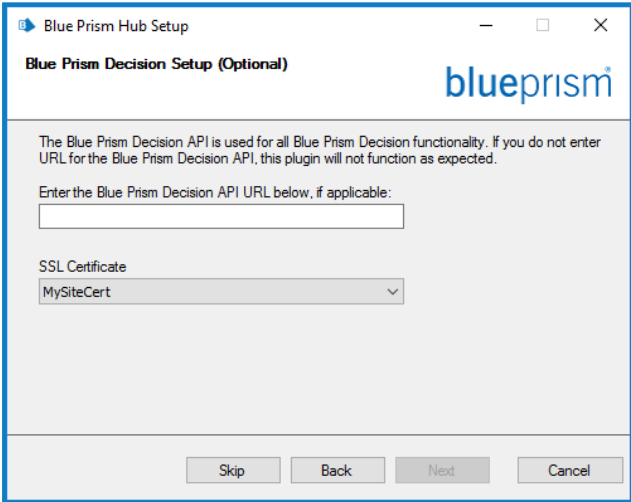

Step	Installer page	Details
<p>16</p>		<h3>Notification Center SQL connection</h3> <p>Configure the settings for the Notification Center database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

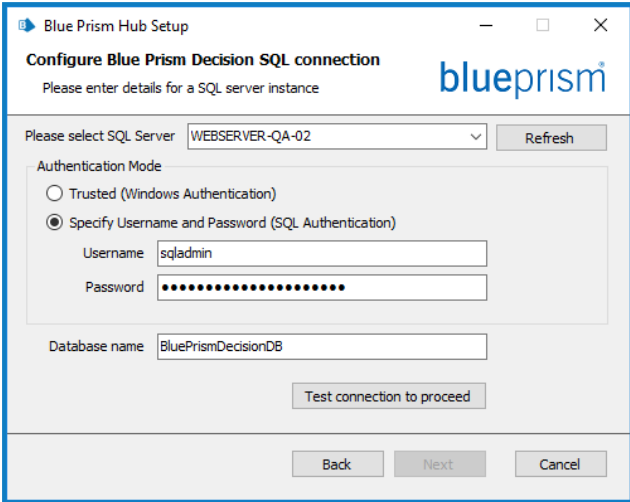

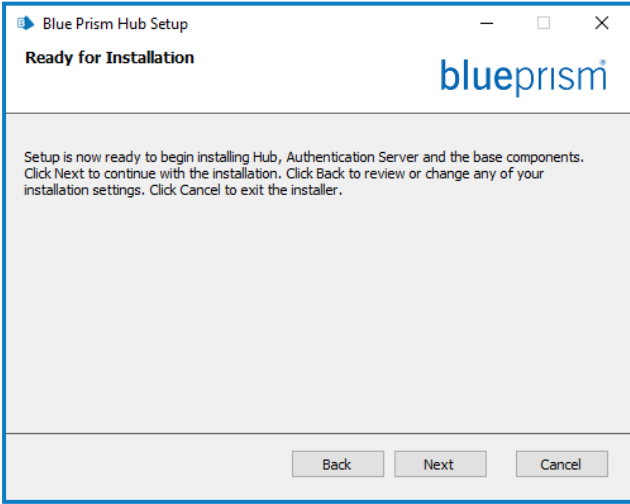
Step	Installer page	Details
<p>17</p>		<h3>Notification Center IIS setup</h3> <p>Configure the Notification Center website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

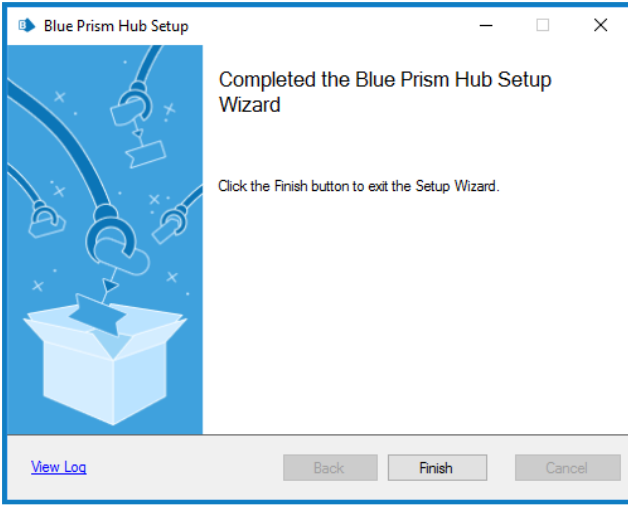


Step	Installer page	Details
<p>18</p>		<h3>License Manager SQL connection</h3> <p>Configure the settings for the License Manager database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>

Step	Installer page	Details
<p>19</p>		<p><b>License Manager IIS setup</b></p> <p>Configure the License Manager website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>
<p>20</p>		<p><b>SignalR IIS setup</b></p> <p>Configure the SignalR website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

Step	Installer page	Details
<p>21</p>		<p><b>Enter your Customer Id</b></p> <p>Enter your customer identifier. This identifier is supplied to you by Blue Prism when you receive your product license for ALM or Interact.</p> <p>If you have not purchased a licensed plugin, you can enter your own value.</p> <p>If you later purchase a licensed plug, your customer ID will need to be changed within the configuration file. For more information, see <a href="#">Troubleshoot a Hub installation on page 96</a>.</p>
<p>22</p>		<p><b>Blue Prism Decision Setup (Optional)</b></p> <p>If you want to use Blue Prism Decision, you need to:</p> <ul style="list-style-type: none"> <li>• Enter the URL for the Blue Prism Decision Model Service container followed by the port number. The URL should be in the format <code>https://&lt;FQDN&gt;:&lt;port number&gt;</code>, for example, <code>https://decision.blueprism.com:50051</code>.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p> The URL must match the FQDN that was specified in the certificate. The port number must match the port that was defined when the container was set to run. For more information, see <a href="#">Install Blue Prism Decision</a>.</p> </div> <ul style="list-style-type: none"> <li>• Select the appropriate SSL Certificate.</li> </ul> <p>If you do not want to use Blue Prism Decision, click <b>Skip</b>. The <a href="#">Ready for Installation</a> screen displays.</p>

Step	Installer page	Details
<p>23</p>		<p><b>Blue Prism Decision SQL connection</b></p> <p>Configure the settings for the Blue Prism Decision database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot a Hub installation on page 96</a> for further details.</p>
<p>24</p>		<p><b>Ready for Installation</b></p> <p>Click <b>Next</b> to install Hub.</p>

Step	Installer page	Details
25		<p><b>Installation complete</b></p> <p>If the installation fails, the <b>View Log</b> option gives details of the error that was encountered. For more information, see <a href="#">Troubleshoot a Hub installation on page 96</a>.</p>

### Install the Authentication Server SAML 2.0 extension

If your organization intends to use SAML 2.0 authentication for your users, you must install the Authentication Server SAML 2.0 extension on your web server where Hub and Authentication Server are installed. For more information, see the [Authentication Server SAML 2.0 Extension 4.7 Installation Guide](#) on the Digital Exchange.

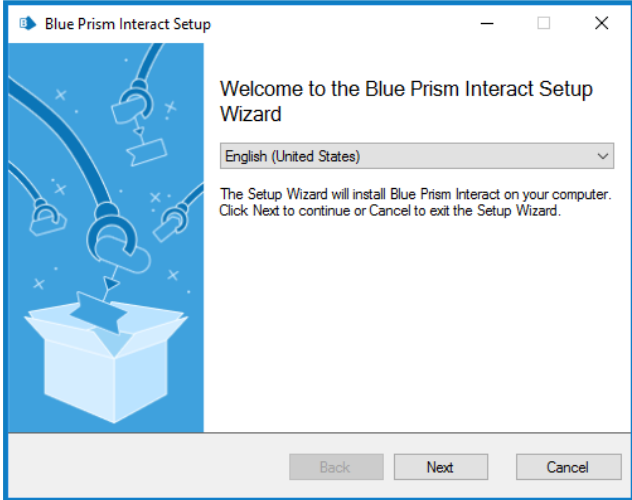
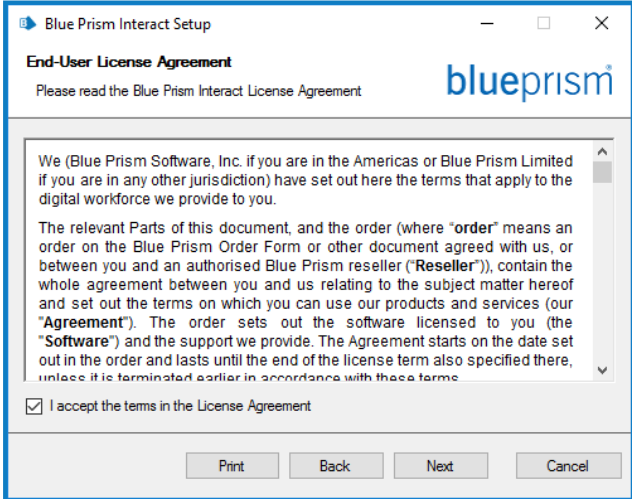
If your organization does not intend to use SAML 2.0 authentication for your users, you do not need to install anything further.

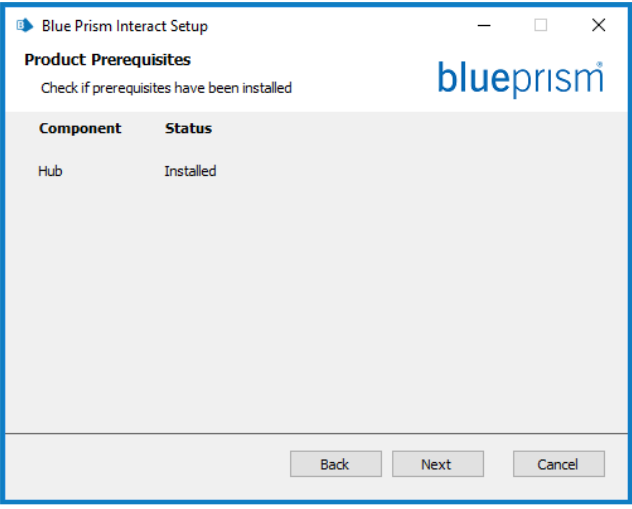

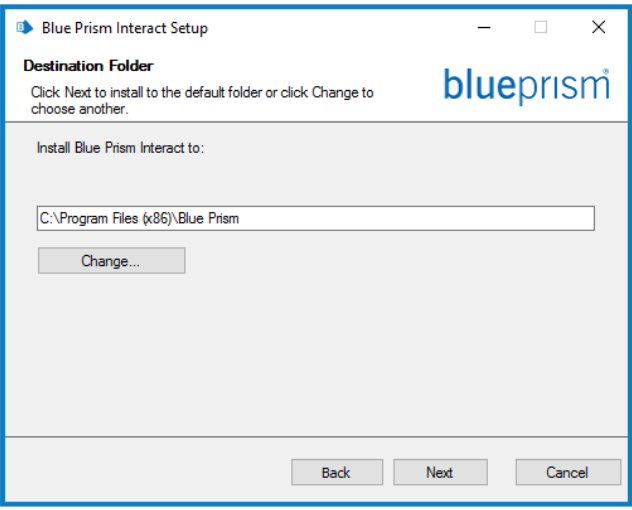
## Install Blue Prism Interact

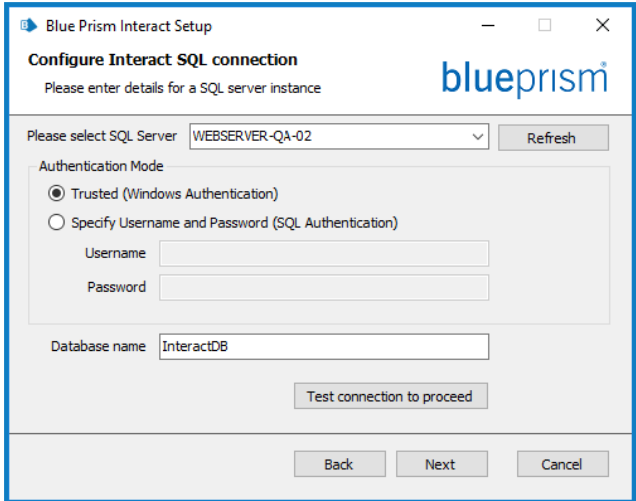

The steps below detail the process for installing the Blue Prism Interact software. This assumes that [Blue Prism Hub](#) has been installed which includes the Authentication Server, Hub, and other associated services.

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.

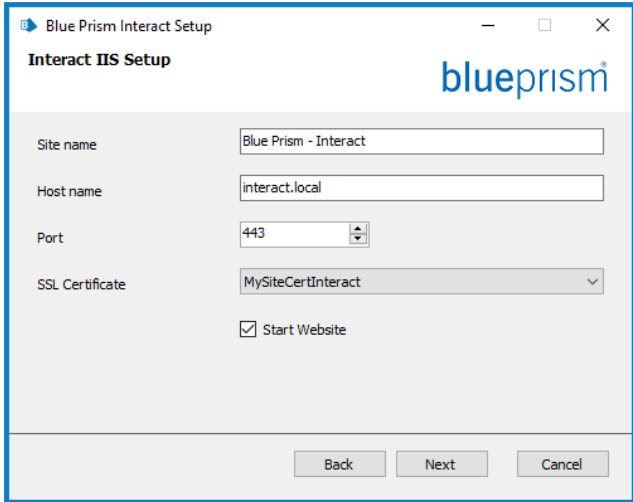

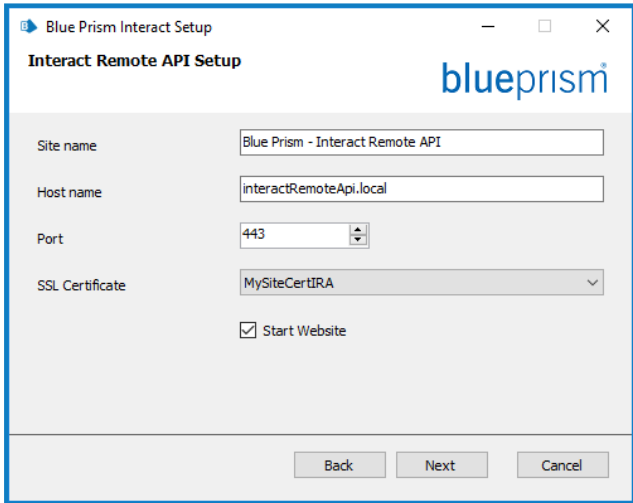

▶ To watch the Interact installation and configuration process, see our [Blue Prism Interact installation video](#).

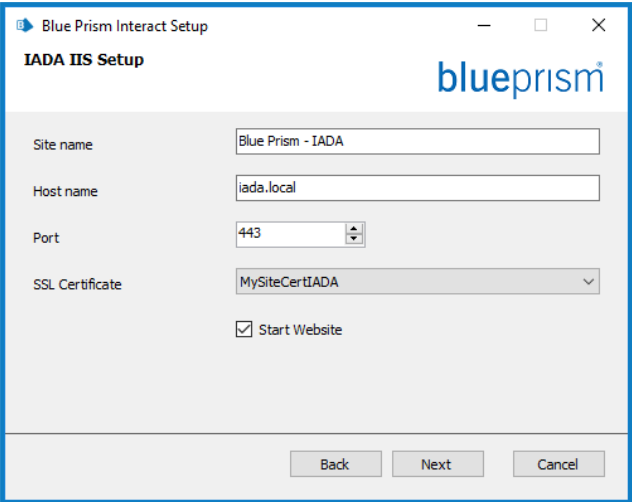

Step	Installer page	Details
1		<p><b>Welcome</b></p> <p>If required, select another language for the installer from the drop-down list. The default language is English (United States).</p> <p>Click <b>Next</b>.</p>
2		<p><b>License agreement</b></p> <p>Read the End-User License Agreement and if you agree to the terms, select the check box.</p>

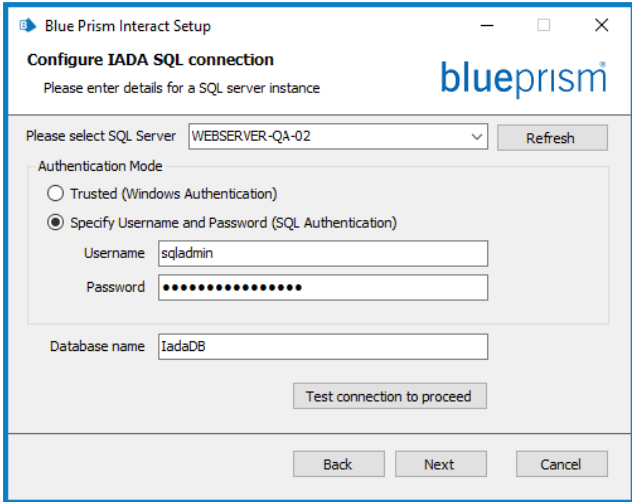

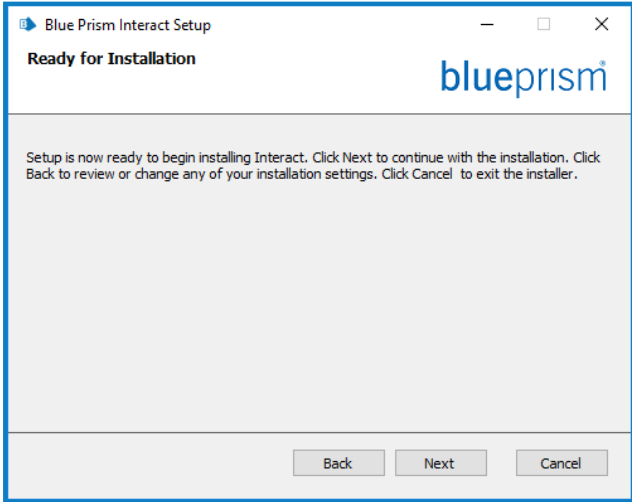
Step	Installer page	Details
<p>3</p>		<p><b>Product prerequisites</b></p> <p>The installer checks that the prerequisites have been installed. If the installer finds any prerequisites missing these will be notified to you. Otherwise, continue with the installation.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> You cannot proceed unless all prerequisites have been installed.</p> </div>
<p>4</p>		<p><b>Destination folder</b></p> <p>Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the <b>Change</b> button.</p>

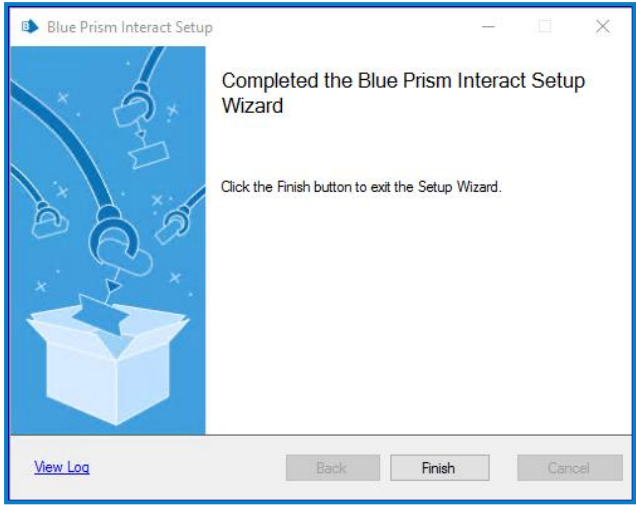
Step	Installer page	Details
<p><b>5</b></p>		<p><b>Configure Interact SQL configuration</b></p> <p>Configure the settings for the Interact Database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on page 60</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot an Interact installation on page 89</a> for further details.</p>



Step	Installer page	Details
<p>6</p>		<p><b>Interact IIS setup</b></p> <p>Configure the Interact website. You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>
<p>7</p>		<p><b>Interact Remote API setup</b></p> <p>You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

Step	Installer page	Details
<p>8</p>		<p><b>IADA IIS setup</b> You need to:</p> <ul style="list-style-type: none"> <li>• Enter a site name.</li> <li>• 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.</li> <li>• Enter the port number.</li> <li>• Select the appropriate SSL certificate.</li> <li>• Leave <b>Start Website</b> selected, unless you do not want the website to automatically start at the end of the installation.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The <b>Next</b> button is only activated if the URL you have entered matches the one configured in the certificate.</p> </div>

Step	Installer page	Details
<p>9</p>		<p><b>Configure IADA SQL configuration</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>• If <b>Windows Authentication</b> is selected, the account must have the appropriate permissions. See <a href="#">Installing using Windows Authentication on the next page</a> for further information.</li> <li>• If <b>SQL Authentication</b> is selected, enter the username and password.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.</p> </div> <p>The database name can be left as the default value or changed as required.</p> <p>Click <b>Test connection to proceed</b> 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 <a href="#">Troubleshoot an Interact installation on page 89</a> for further details.</p>
<p>10</p>		<p><b>Ready for Installation</b></p> <p>Click <b>Next</b> to install Interact.</p>


Step	Installer page	Details
11		<p><b>Installation complete</b></p> <p>If the installation fails, the <b>View Log</b> option gives details of the error that was encountered.</p> <p>For more information, see <a href="#">Troubleshooting an installation</a>.</p> <p>Click <b>Finish</b>.</p>

## 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 15](#).
- Permissions for the required certificates.
- Ownership over the IIS Application Pool.
- Ownership over the Windows services installed by Hub and Interact.

 You must assign the application pools and services to use Windows accounts before creating an environment in Hub. If you assign the accounts after creating an environment, you may experience performance issues, for example, forms created using the Interact plugin may not display to users in 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**.

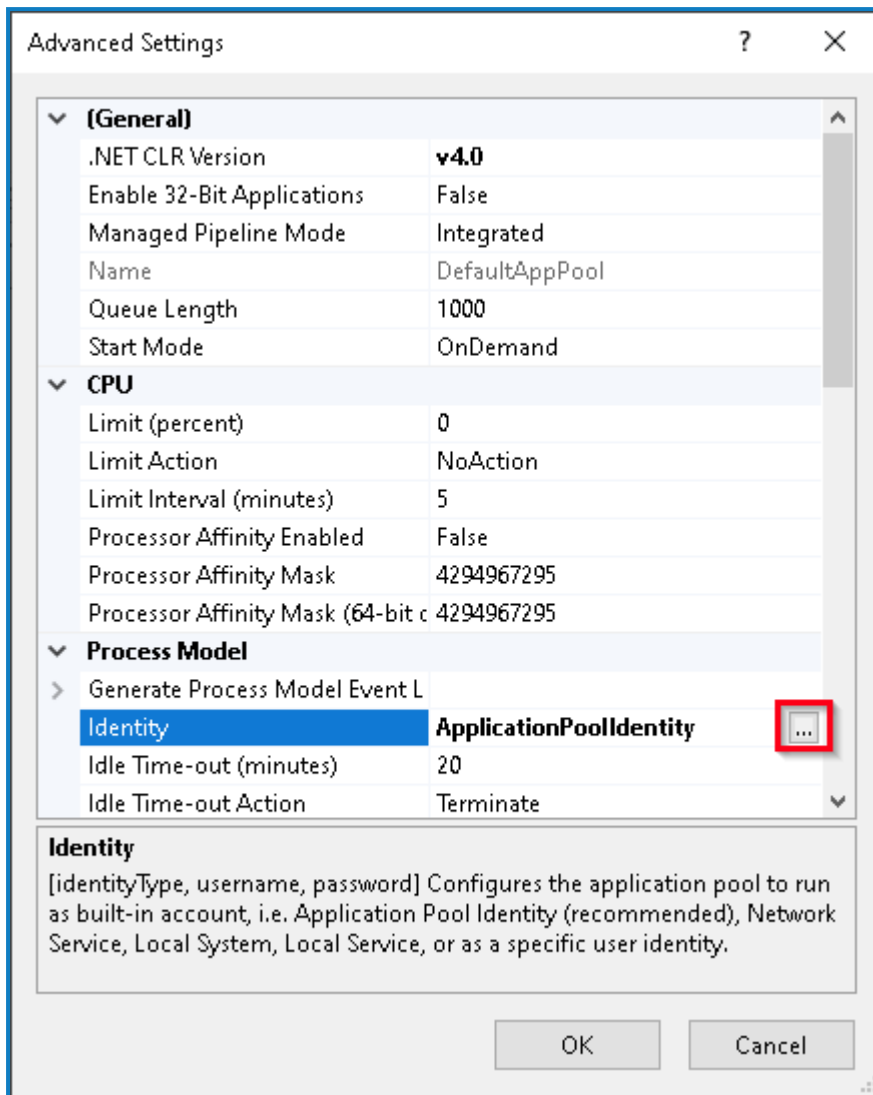
2. In the navigation pane, expand **Personal** and click **Certificates**.
3. Follow the steps below for both the BluePrismCloud\_Data\_Protection and BluePrismCloud\_IMS\_JWT certificates:
  - a. Right-click the certificate and select **All Tasks**, and click **Manage Private Keys....**  
The Permissions 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

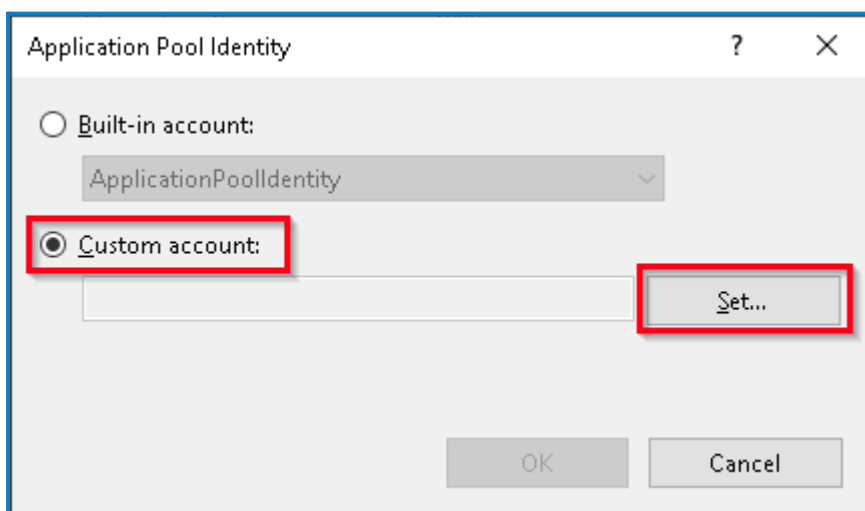
By default, the application pools are created with the identity 'ApplicationPoolIdentity'. After the installer has completed, the Windows service account will need to be allocated to manage the application pools. To do this:

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.

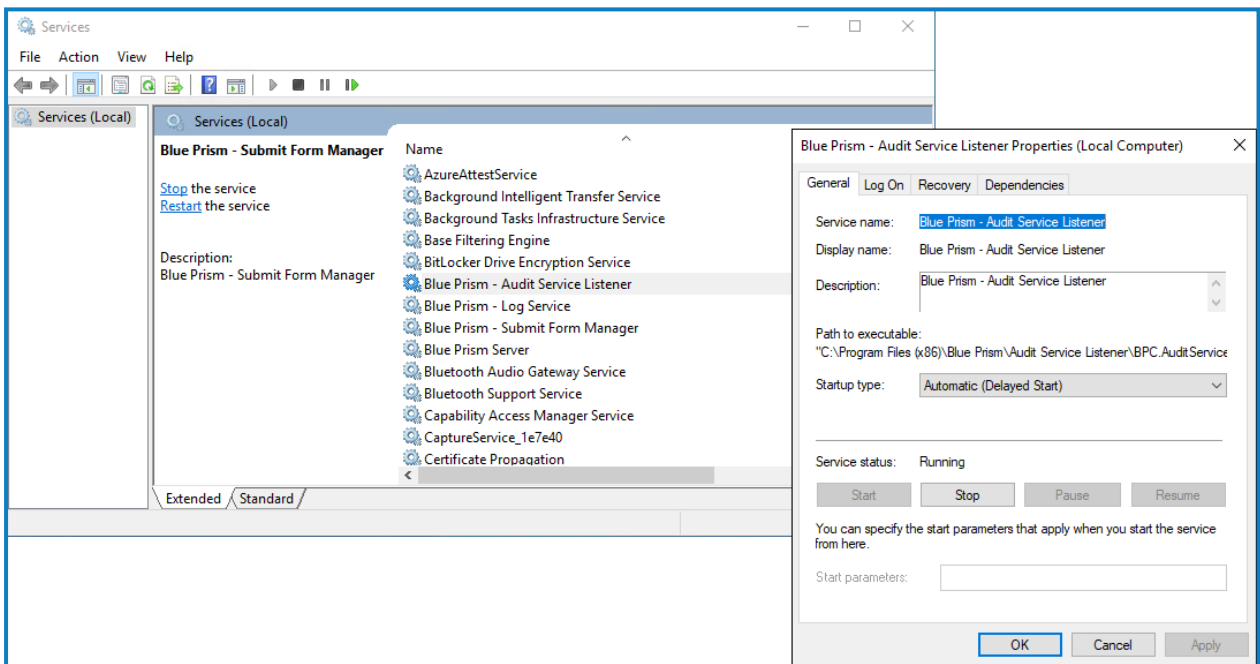
### Assigning a Windows service account to a service

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

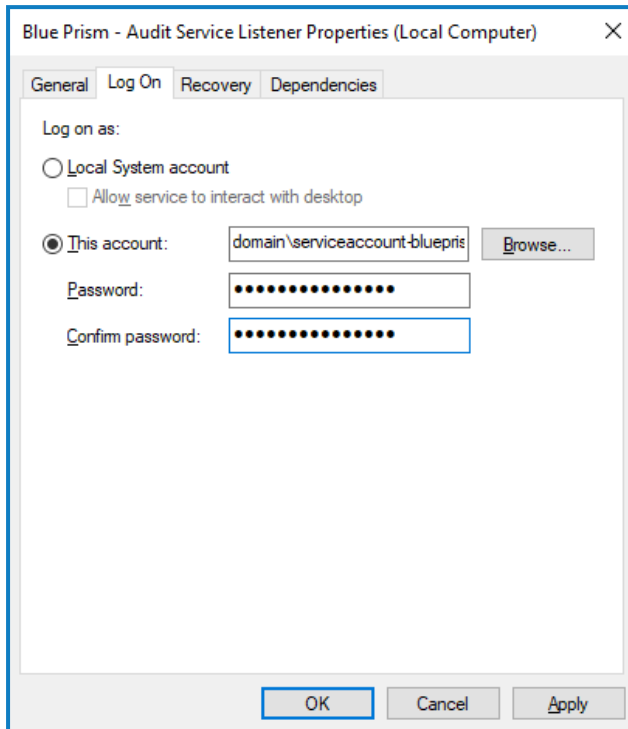
- Blue Prism - Audit Service Listener
- Blue Prism - Log Service
- Blue Prism - Submit Form Manager

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.



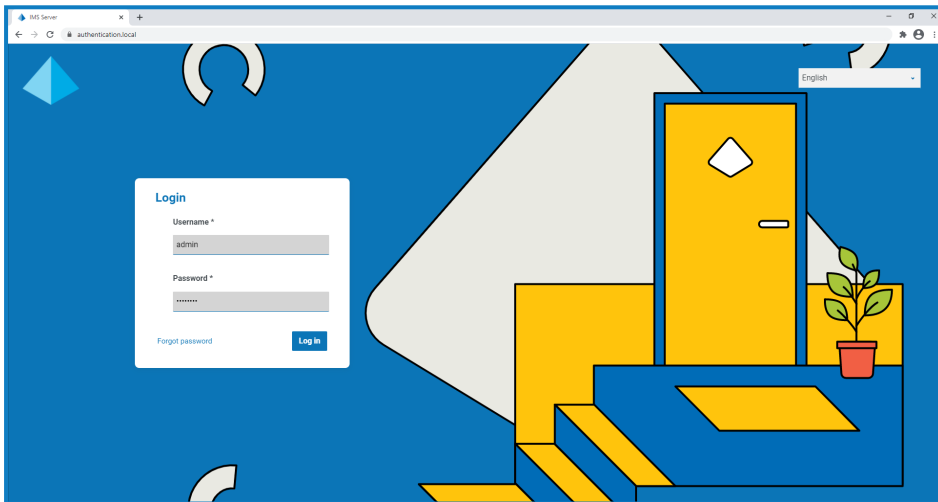
## Initial Hub configuration

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

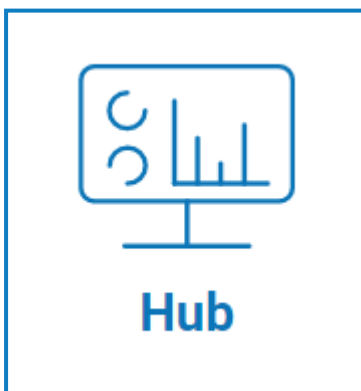
When you open the login page for Authentication Server, localization settings are automatically applied from your web browser. The login page and Hub display in the language most compatible with the language settings configured in the browser. If the language selected in your browser settings is not 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

 If you have installed your environment to use Windows Authentication, you must assign the application pools and services to use Windows accounts before creating an environment in Hub. If you do not, you may experience performance issues, for example, forms created using the Interact plugin may not display to users in Interact. For more information, see [Installing using Windows Authentication on page 60](#).


SSL encryption is used by all the databases installed as part of the Hub installer. For Hub to connect successfully to the Blue Prism database, the Blue Prism database must also be configured to use SSL encryption. For more information, see [Prerequisites on page 8](#).

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:

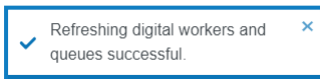
 The Timeout value is in seconds.

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 96](#) 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 96](#).

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:

The screenshot shows the 'Email configuration' dialog box. The 'Authentication' section has 'Username and password' selected. The 'SMTP host details' section includes fields for 'SMTP host', 'Port number', 'Sender email', and 'Encryption'. The 'SMTP authentication' section is set to 'Disabled'. The 'SMTP credentials' section on the right includes fields for 'Username', 'Password', and 'Test email recipient'.

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

The screenshot shows the 'Email configuration' dialog box. The 'Authentication' section has 'Microsoft OAuth 2.0' selected. The 'SMTP host details' section includes a field for 'Sender email'. The 'SMTP credentials' section on the right includes fields for 'Application ID', 'Directory ID', 'Client secret', and 'Test email recipient'.

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 96](#) for more information.

For more information about configuring email settings, see [Hub Administrator 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 on the next page](#).

### 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 on the next page](#).
- If your organization does not want to use the same user accounts, only configure the authentication settings in Hub. See [Authentication settings on the next page](#).

 To watch the configuration steps, see our [Configure Authentication Server video](#).

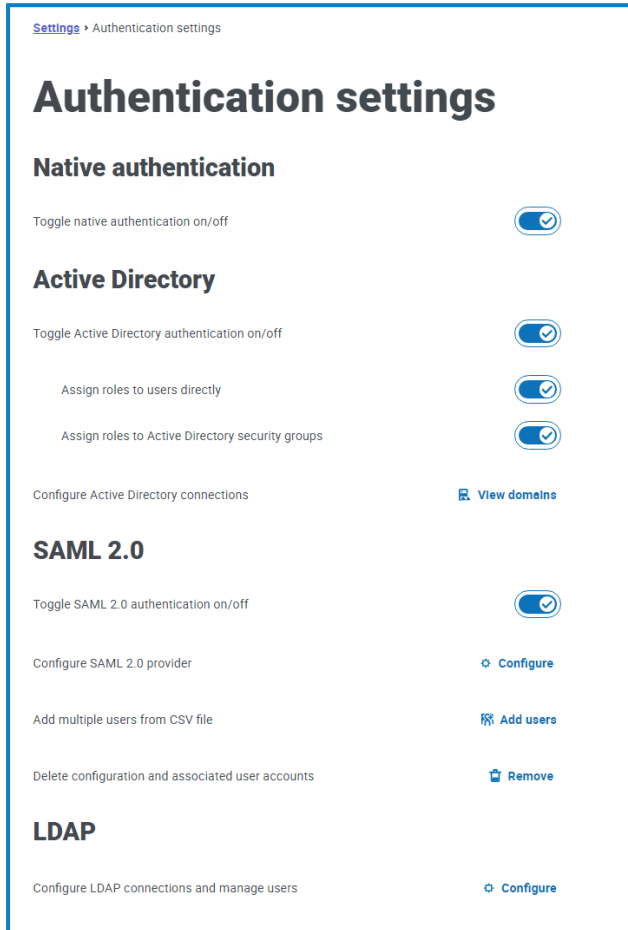
## Authentication settings

Authentication settings for a Hub environment can be configured on the Authentication settings page.

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. Select the authentication type(s) you want to use, and the associated options if required.
  - **Native authentication** - This is enabled by default in new environments or when upgrading Hub.
  - **Active Directory** - This can only be enabled if the server hosting Authentication Server is a member of an Active Directory domain. If enabled, Active Directory domains and user role management can also be configured.
  - **SAML 2.0** - This option is only visible on the Authentication settings page if the Authentication Server SAML 2.0 extension has been installed on the host web server where Authentication Server is installed.
  - **LDAP** - To enable LDAP authentication at least one LDAP connection must be created.

Based on your organization's requirements, you have the following options:


- Enable all authentication types.
- Disable one or more authentication types; this can only be done while there is at least one administrator user in the system that is configured to log in with a different authentication type than the type(s) being disabled.



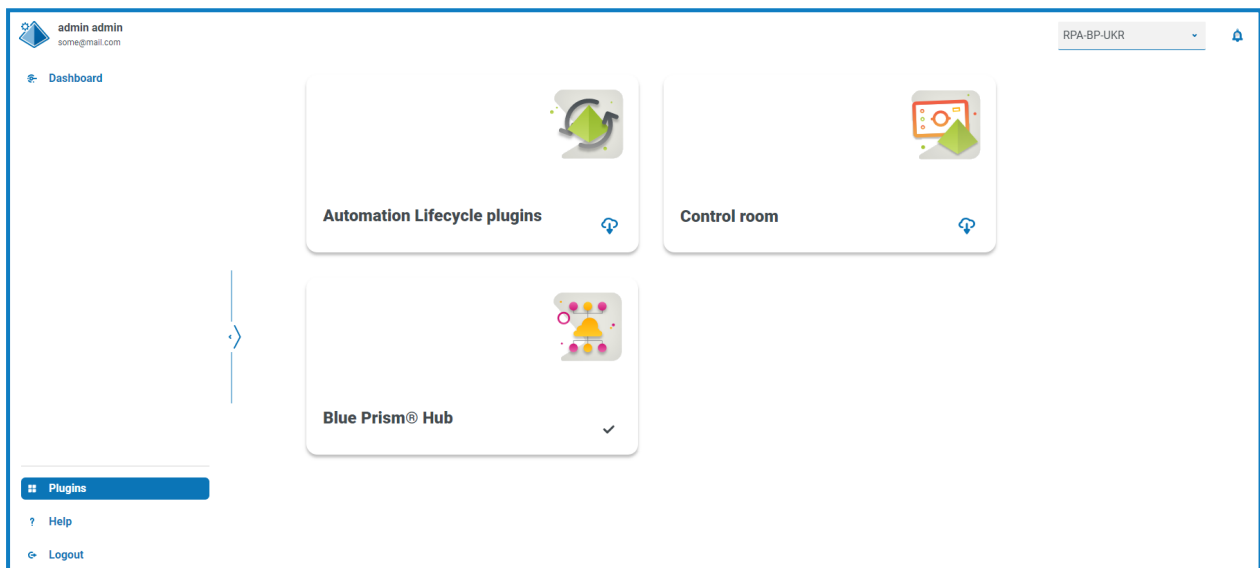
 For more information about configuring authentication settings, see the [Hub Administrator Guide](#).

## 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.

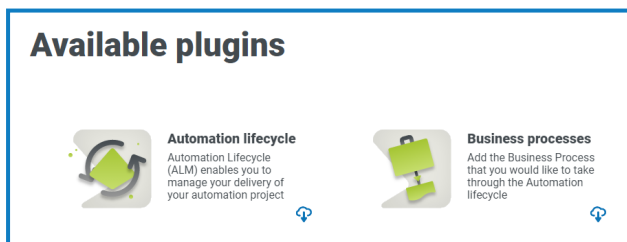
 To watch this installation step, see our [Business Processes plugin installation video](#).

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



3. Click **Automation lifecycle**.

The available plugin components display.



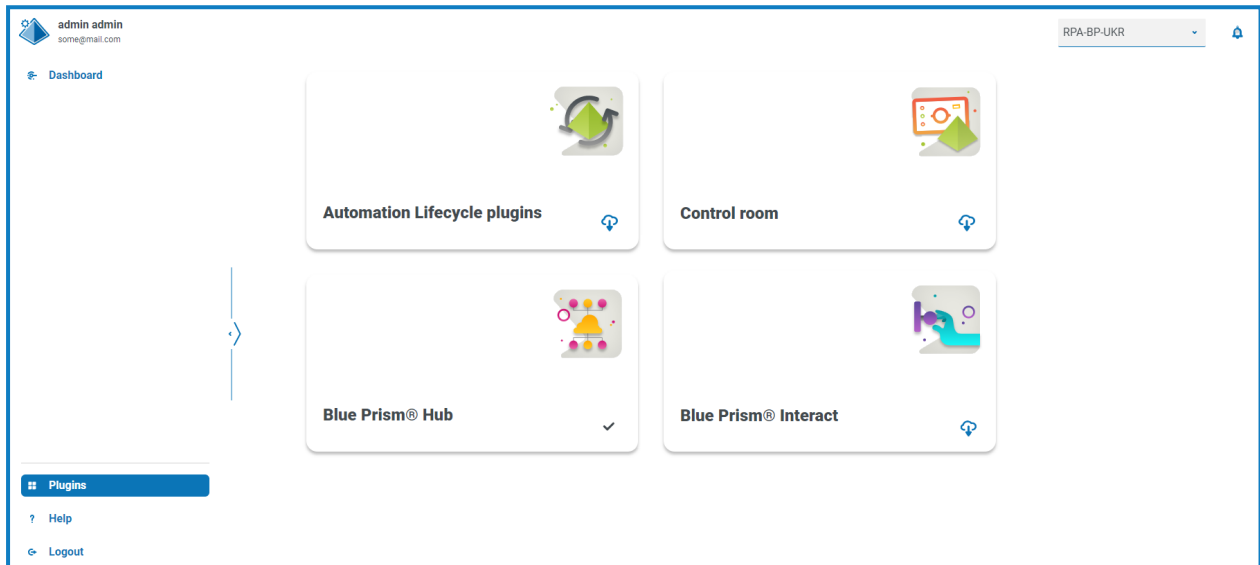
4. Click the download icon in the bottom corner of the **Business processes** tile to initiate the install.  
The site restarts.

## 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](#)

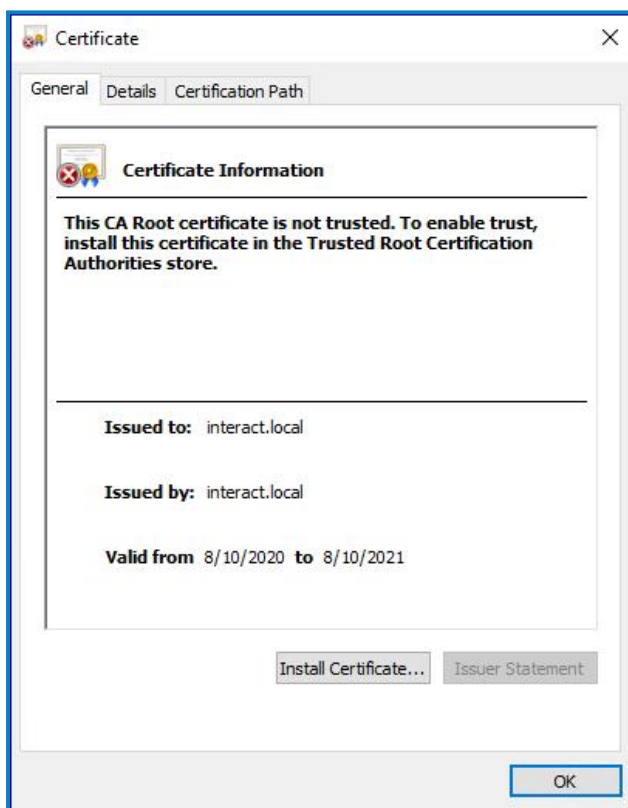
These instructions assume that the user is familiar with Blue Prism.

### Install SSL certificates

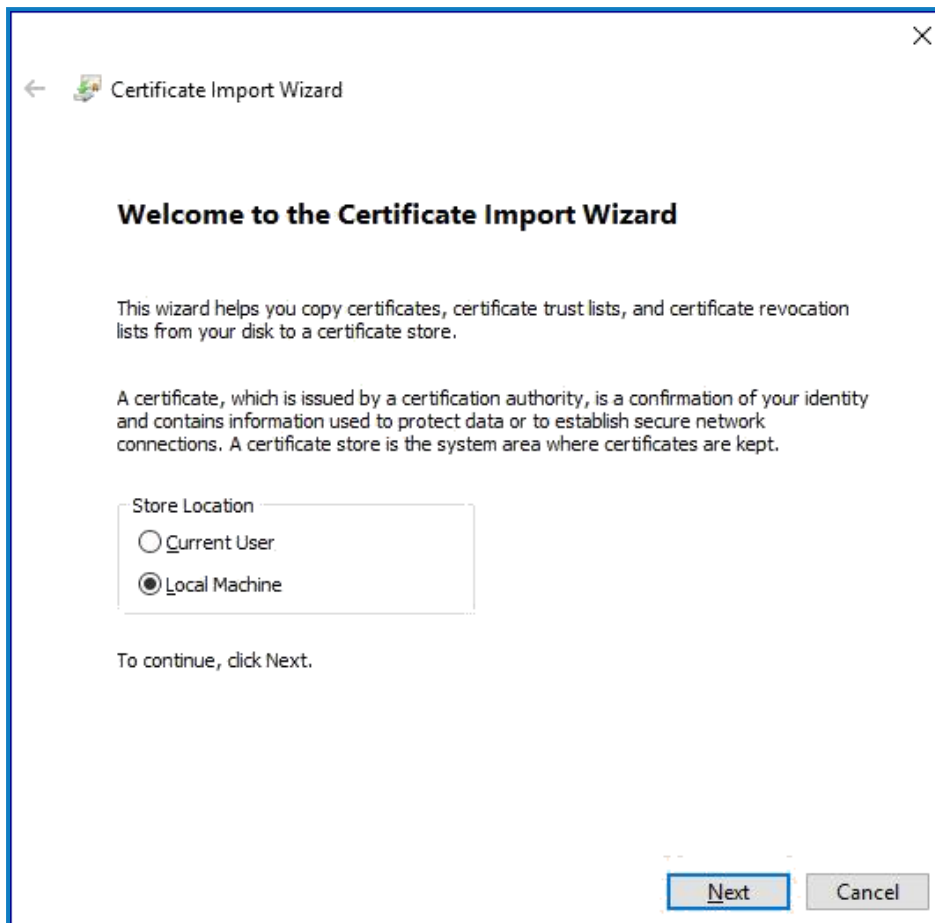
On each Digital Worker, log in and copy across the SSL Certificates for Interact, IADA, Interact Remote API, Authentication Server, and SignalR.

 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.

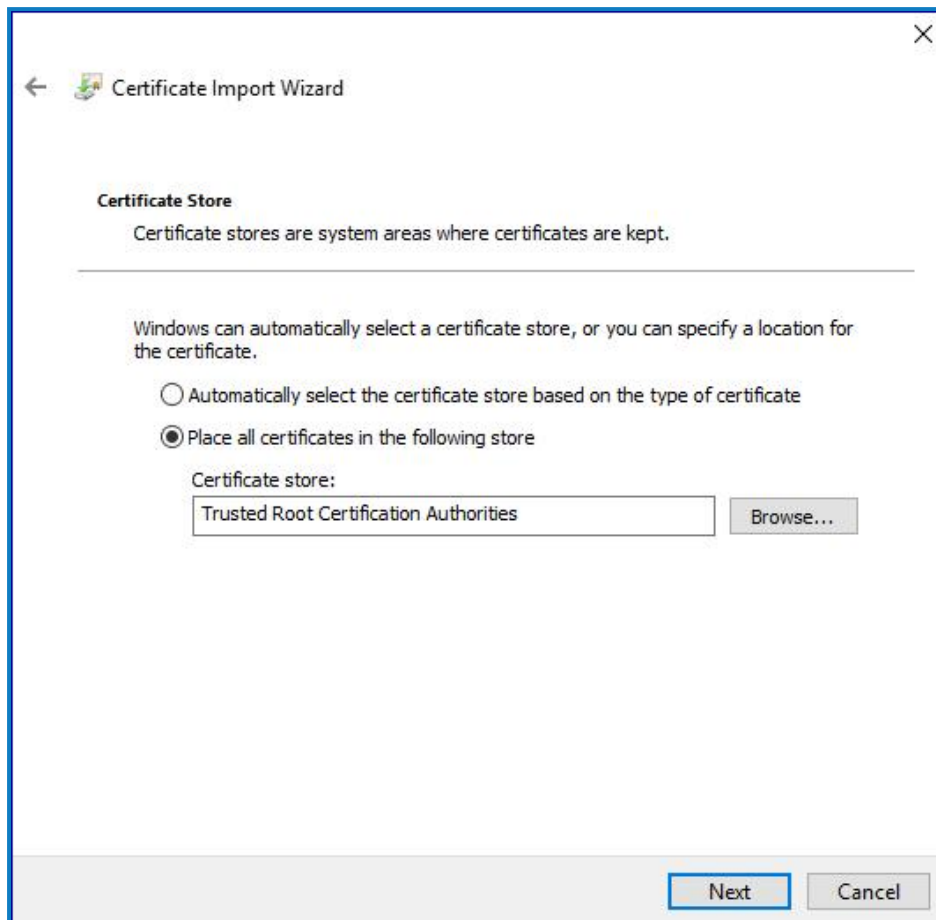
1. Double-click each SSL Certificate and select **Install Certificate**.



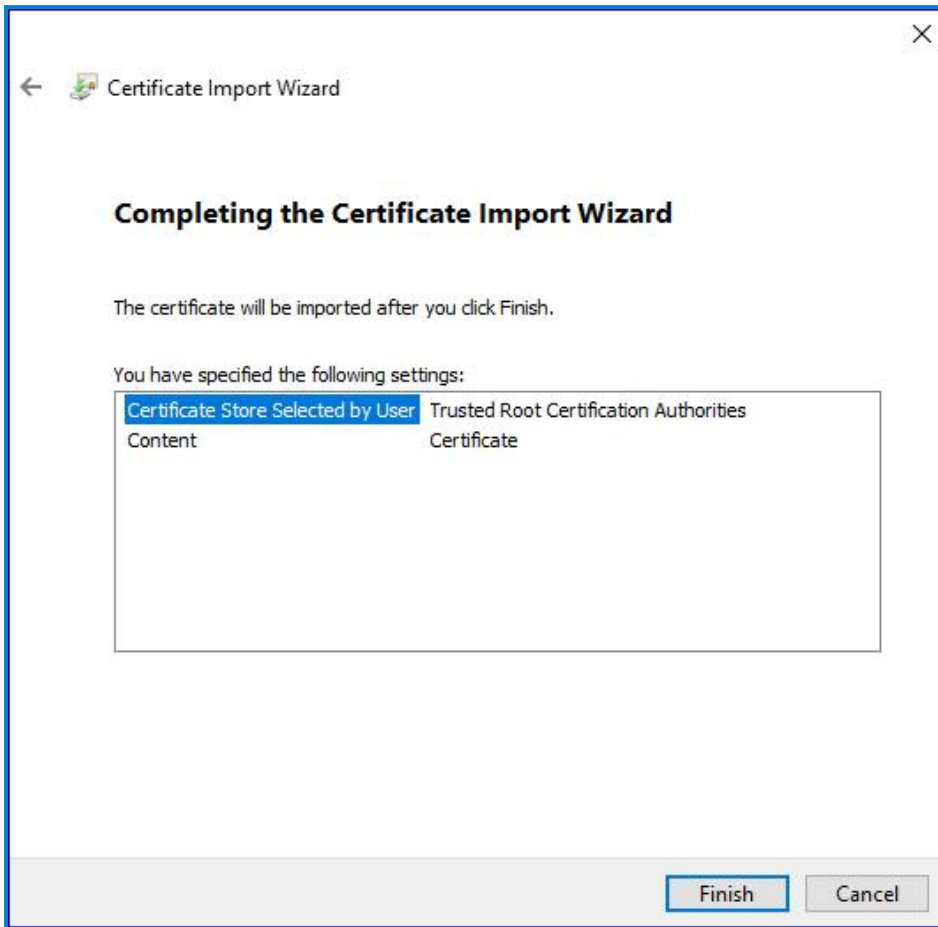
## 2. Change the Store location to Local Machine.



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. [Import the Interact API Service VBO](#) into Blue Prism.
3. [Set up the credentials](#) for the Interact Web API service account in Blue Prism.
4. [Configure the Interact API Service](#) 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.

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

**Add a service account**

**ID \***  
Client ID which uniquely identifies the client application to the identity provider.  
InteractRemoteAPI

**Name \***  
Client name in the Authentication Server database.  
InteractRemoteAPI

**Permissions**  
The API(s) to which the client has access.

- Blue Prism API
- Authentication Server API
- Interact Remote API
- Decision API
- Director API

Create service account

- 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.

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

**Add a service account**

Your service account has been successfully created. The secret for this service account displays below.

**Secret**  
You can copy the secret to your clipboard using the Copy to Clipboard icon.

.....

Show secret

OK

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

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


## Import the VBO

- Download the Interact API Service release file from the [Blue Prism Portal](#).
- 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](#).

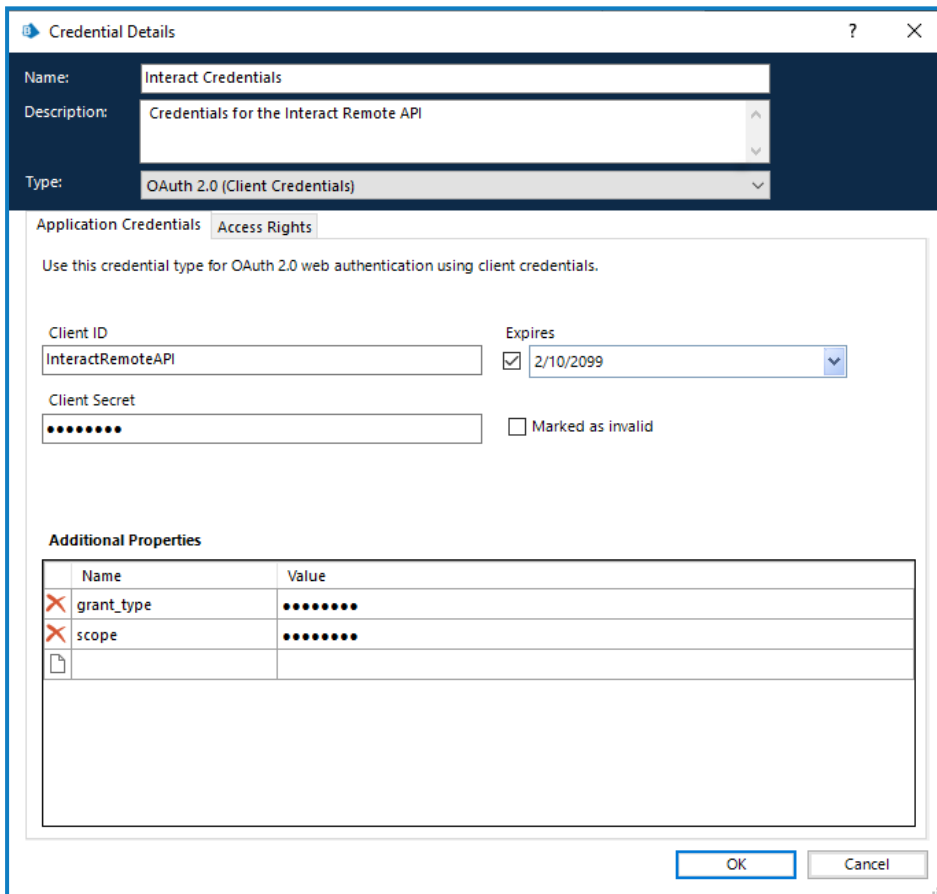


### Set up credentials in Blue Prism

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 75](#), for example, *InteractRemoteAPI*.

 The client ID is case sensitive. You must ensure you enter the client ID in the same case as defined in the service account.

- d. In **Client Secret**, enter the secret key that was generated for the service account.

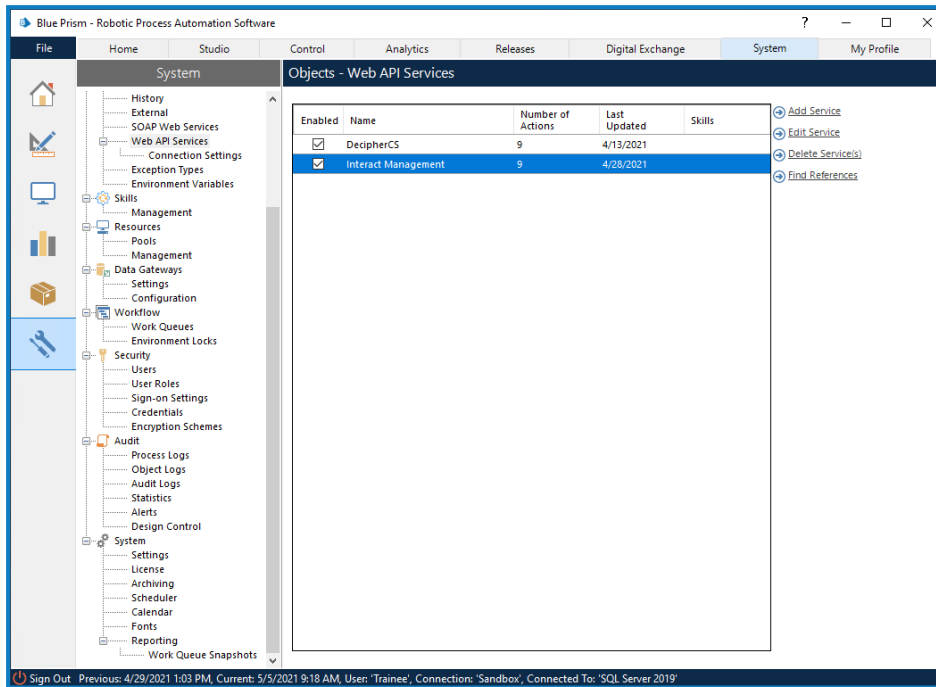


4. On the Access Rights tab of the Credential Details dialog, set up the required access permissions.
5. Click **OK**.

## Configure the web service

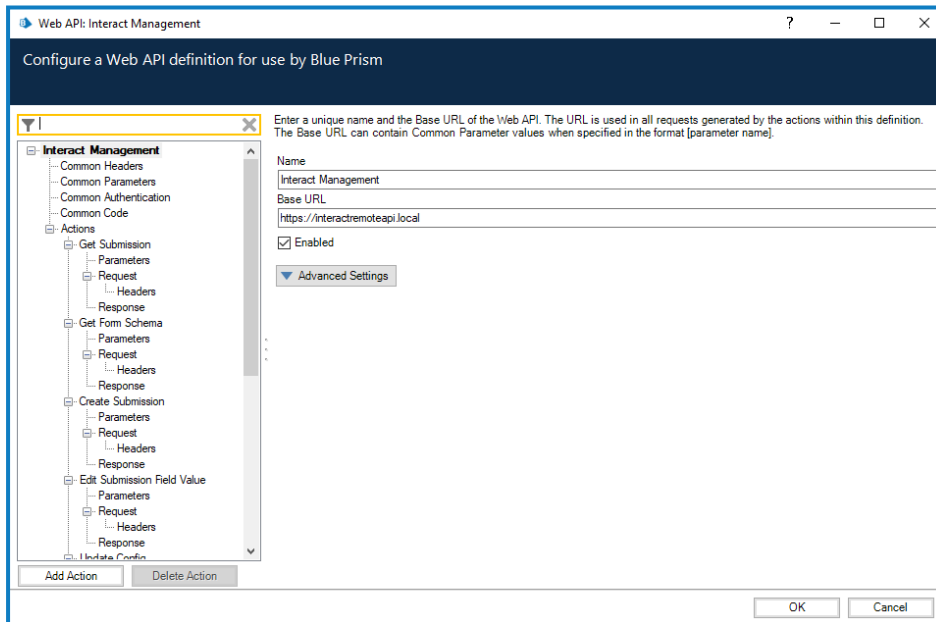
1. In Blue Prism, select **System** and then click **Objects > Web API Services**.

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,

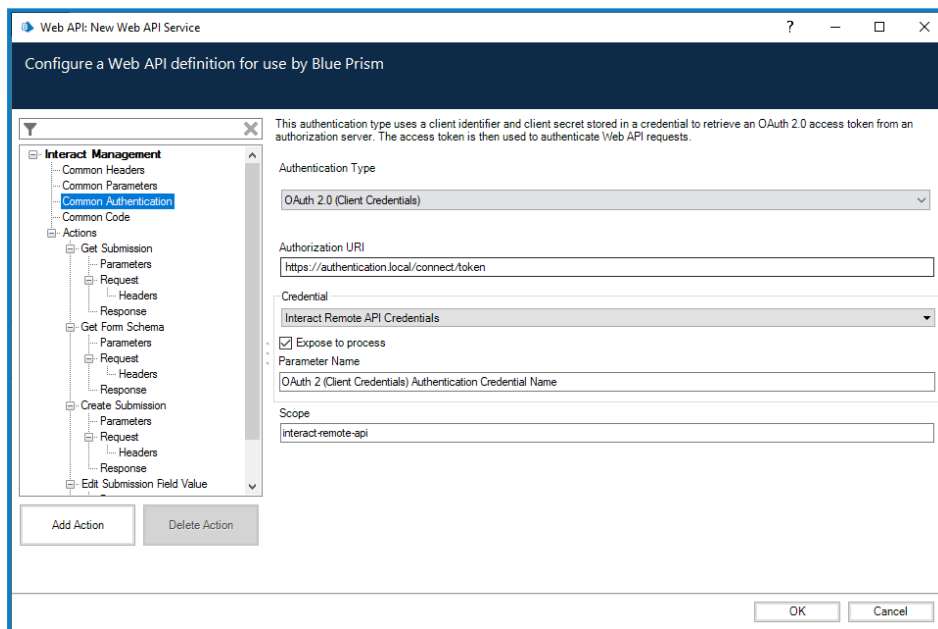
`https://authentication.blueprism.com/connect/token.`

 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 81](#).



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

## Verify an installation

This section provides a simple scenario to test that the basic components of the Interact installation are operating as expected. This verification process requires that:


- A connection to a Blue Prism database has been configured in Hub, see [Database settings on page 66](#) for more information.
- A valid work queue exists in the Blue Prism environment that can be used for this test.
- The Interact API Service is installed and configured in Blue Prism, see [Configure Digital Workers on page 75](#) for more information.

The verification steps include:

- Verifying that Interact can submit information to a work queue in Blue Prism:
  - [Creating a business process inside Hub](#) - Every form is linked to a business process.
  - [Creating an Interact form](#) - Create a new form with one page and one field to use for the verification test.
  - [Adding the form to a role](#) - Provide a user with access to the form in Interact.
  - [Submitting the form and ensuring that it appears in a queue within Blue Prism](#).
- Verifying that Blue Prism can provide information back to Interact:
  - [Creating a simple Blue Prism process](#).


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

If you experience problems whilst verifying the installation, see [Troubleshooting an installation](#).


 If you have installed your environment to use Windows Authentication, you must assign the application pools and services to use Windows accounts, and then create an environment in Hub, before carrying out this verification. If you do not, the forms created in the Interact plugin will not be displayed to users in Interact. For more information, see [Installing using Windows Authentication on page 60](#) and [Initial Hub configuration on page 65](#).

## Create a business process inside Hub

1. [Log into Authentication Server](#) using an administrator user account and select **Hub**.
2. On the left navigation bar, select **Automation lifecycle** and click **Business Processes**.
3. Click **Add new**.
4. Enter a unique identifier and a name for the business process. Optionally, enter a description.
5. If required, enter any additional notes and click **Create business process**.


 For more information on creating business process, see the [Automation Lifecycle Management user guide](#).

## Create an Interact Form

 You must create a form that has a minimum of one page with one field.

1. In Hub, on the left navigation bar, select **Interact** and click **Forms**.
2. Select **Create form** to create a new Interact form.
3. Select the business process you created from the drop-down list if it is not already selected.

4. Enter a name for the Interact Form and a description, for example, *Test Form*.
5. Under **Delivery method**, select **Queue**.
6. Select the environment from the drop-down list, and then select the required queue name.

 If the required queue is not displayed in the list, click the refresh icon to update the queues.

7. Leave the **Priority**, **SLA**, **Email** and **Interact role** blank.
8. Leave the **Default approval type** set to **None**.
9. In **Category**, enter a name for the category. For example, *TestCategory*.
10. Select an icon from the preset icons to represent the Form in Interact.
11. Click **Create form**.  
The Edit form page displays.
12. Click **Create page**.  
The Create page panel displays.
13. Enter a name and description for the new page, and click **Save**.  
The Edit form page displays showing the page you have created.
14. Click the ellipsis (...) on the page that you just created, and click **Create field**.  
The Choose capture type dialog displays.
15. Click **Text**.
16. On the Create text page, enter *TestTextField* in the **Label** field, leave everything else as default.
17. Click **Create field**.
18. On the Edit form page, click **Save**.
19. In the Increase minor panel, enter an update note and click **Save**.

 For more information on creating business process, see the [Interact plugin user guide](#).


## Add the form to a role

1. In Hub, click your profile icon to open the Settings page, and then click **Roles and permissions**.  
The Roles and permissions page displays.
2. Click **Create role**.  
The Create role section displays.
3. Enter a role name, such as *Interact Test Role*. Optionally, enter a description.
4. Change the **Role type** to **Interact**.
5. In **Add form**, select the form you have just created from the drop-down list. If you have used the example name used in [Create an Interact Form on the previous page](#), this will be **Test form**.
6. In **Add user**, select the user(s) who you want to have access to the Form that you have created. Add the administrator user you are using as a minimum.
7. Click **Save**.
8. Log out of Hub.


 For more information on deploying business process, see the [Interact plugin user guide](#).

## Submit the form to a work queue in Blue Prism

1. Log into **Authentication Server** using the credentials of a member in the role that you assigned to the form and select **Interact**.

 For the purposes of the test, you can use either the administrator assigned to the role or a user. Only members of the role are able to see the form in Interact, regardless of their administrative privileges.

2. Click on the form that you just created (**Test Form**).  
The form displays with the single text field shown.
3. Enter some text into the field and then click **Submit**.
4. Log into Blue Prism and check whether there is an item in the work queue specified when creating the form.

 For more information on using Interact as an end user, see the [Interact user guide](#).

This completes the verification of the installation proving that Interact can communicate with Blue Prism. The next step is to verify that Blue Prism can provide information back to Interact.

## Create a simple Blue Prism process

You can use one of the following two processes. Both of these demonstrate communication between Blue Prism and Interact. These processes show:

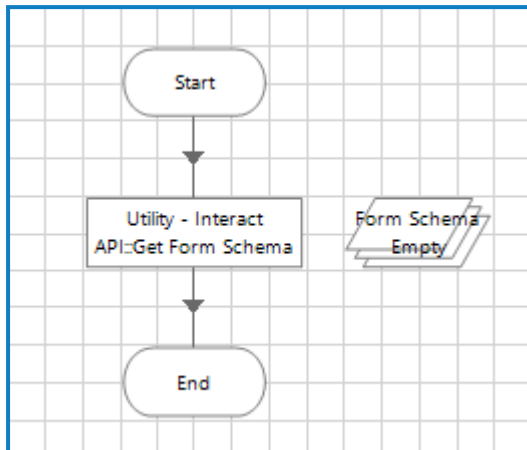
- **Option 1** - Blue Prism can query and receive a response from Interact, in this case, the form name.
- **Option 2** - Blue Prism can change a value in a form, with the change displayed in Interact.

### Option 1: Retrieve the form name

1. Create a process in Blue Prism.
2. Add an action to your process and set the following properties:
  - a. Set the **Business Object** to **Utility - Interact API**.
  - b. Set the **Action** to **Get Form Schema**.
  - c. On the Input tab, in the **Form Name Value**, enter the name of the form you created between double quotation marks, for example, *"Test Form"*.
  - d. On the Output tab, generate the default Form Schema collection.

3. Connect the Action stage to the Start and End stages.

Your process should look similar to this:



4. Run the process.
5. Once complete, open the Form Schema collection and select the **Current Values** tab. This should reflect the content of the form - in this case just one TestTextField Text field.

### Option 2: Change a field value

This process requires there to be an item in the work queue - one was submitted as part of [Submit the form to a work queue in Blue Prism on the previous page](#).

1. Create a process in Blue Prism.
2. Add three actions to your process and set the following properties:

Action 1:

- a. Set the **Business Object** to **Work Queues**.
- b. Set the **Action** to **Get Next Item**.
- c. On the Input tab, in the **Queue Value**, enter the name of the queue to which you submitted the form. This was specified in [Create an Interact Form on page 84 in step 6](#). The queue name must be entered between double quotation marks, for example, *"InteractQueue"*.
- d. On the Output tab, generate the default Data collection and Item ID field.

Action 2:

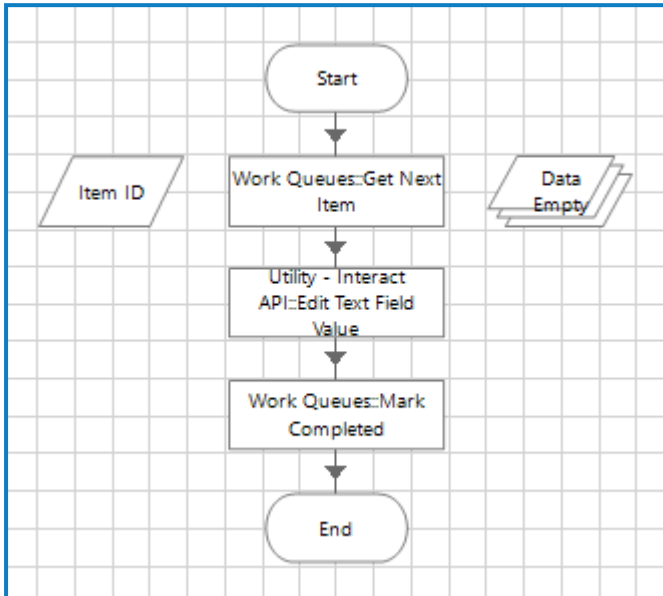
- a. Set the **Business Object** to **Utility - Interact API**.
- b. Set the **Action** to **Edit Text Field Value**.
- c. On the Input tab, enter the following values:
  - For **Submission Id**, enter *[Data.\_requestId]*.
  - For **Field Name**, enter the name for the field between double quotation marks, for example, *"TestTextField"*.
  - For **Field Value**, enter the phrase between double quotation marks that you want to pass back to Interact, for example, *"some sample text in the field"*.

Action 3:

- a. Set the **Business Object** to **Work Queues**.
- b. Set the **Action** to **Mark Completed**.

- c. On the Input tab, in the **Item ID** value, enter `[Item ID]`. This is the Text data type generated by the first action.
3. Connect the Action stages together and to the Start and End stages.

Your process should look similar to this:



4. Run the process.
5. Once complete:
  - a. Open the queues in Blue Prism. The previously submitted form should be marked as complete.
  - b. Open Interact, select **History**, click the ellipsis (...) next to the submitted form and click **View**. The form should display the text sent from Blue Prism.

### Verification complete

This completes the verification of the installation proving that Blue Prism can communicate with Interact, and Interact with Blue Prism.



You can now remove any test items you created, such as:

- Deleting the work queue if it is no longer required - see [Workflow - work queues](#).
- Deleting the form from the Interact plugin - see the [Interact plugin user guide](#).
- Deleting the business process - see the [Automation Lifecycle Management user guide](#).
- Deleting the test role - see the [Hub administrator guide](#).



## 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 SQL Server hosting the database has a valid certificate applied.
  - 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.
  - That the SQL Server has a valid certificate applied.

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.
- **SSL Encryption** - Ensure that the SQL Server has a valid certificate. For more information, see [Prerequisites on page 8](#).
- **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 15](#).
- 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**.

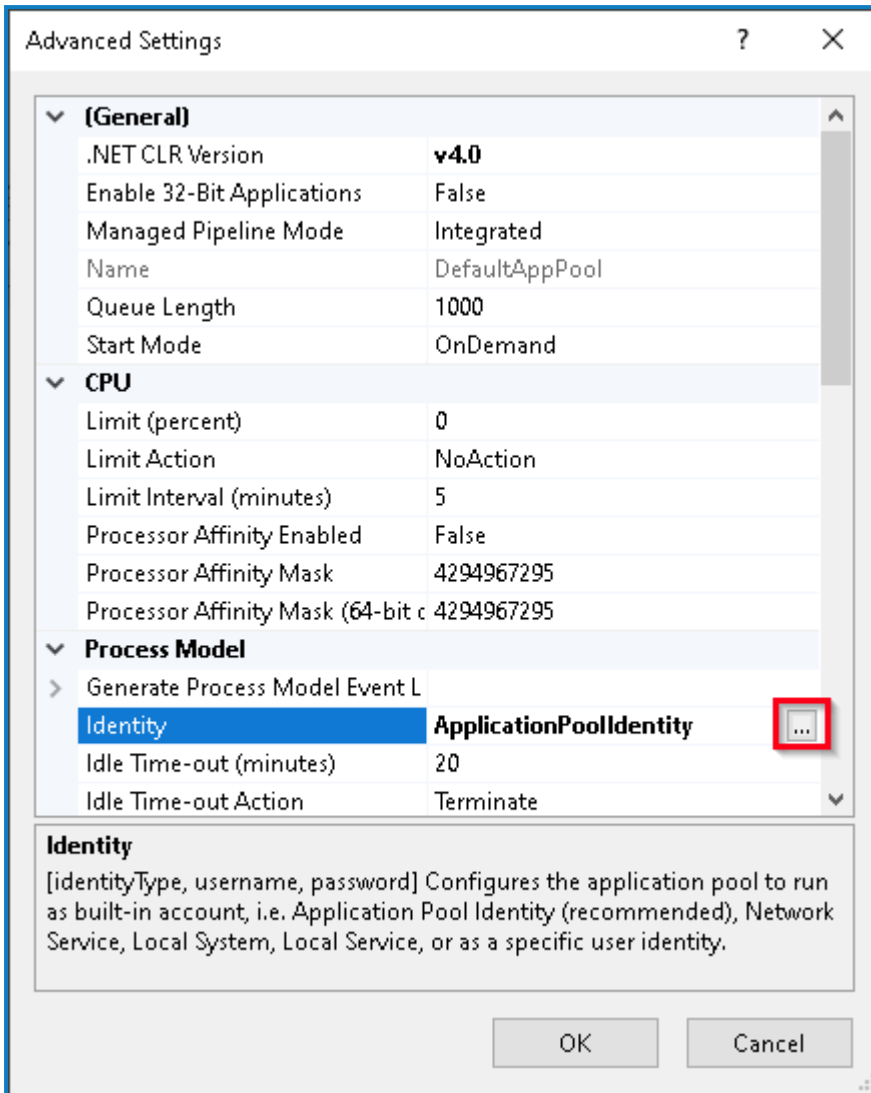
2. In the navigation pane, expand **Personal** and click **Certificates**.
3. Follow the steps below for both the BluePrismCloud\_Data\_Protection and BluePrismCloud\_IMS\_JWT certificates:
  - a. Right-click the certificate and select **All Tasks**, and click **Manage Private Keys....**  
The Permissions 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

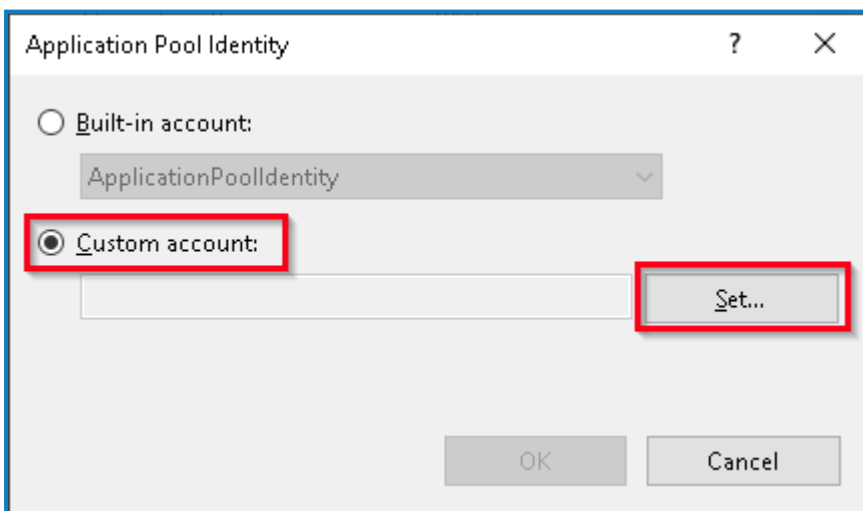
By default, the application pools are created with the identity 'ApplicationPoolIdentity'. After the installer has completed, the Windows service account will need to be allocated to manage the application pools. To do this:

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.

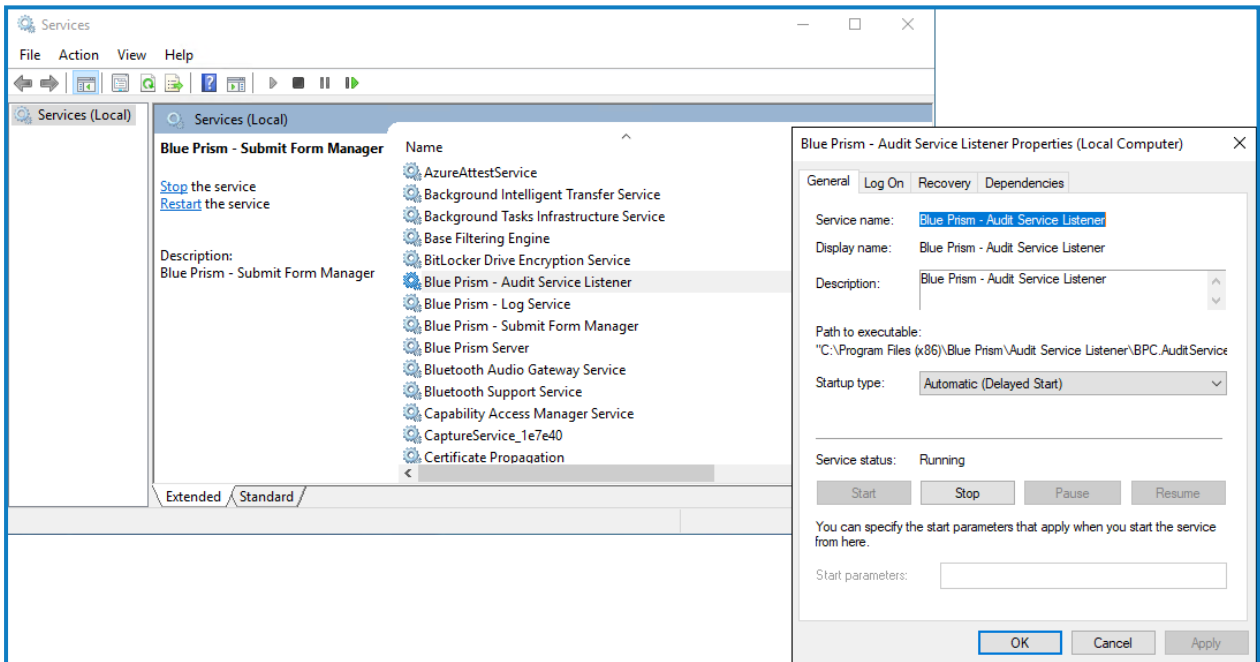
### Assigning a Windows service account to a service

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

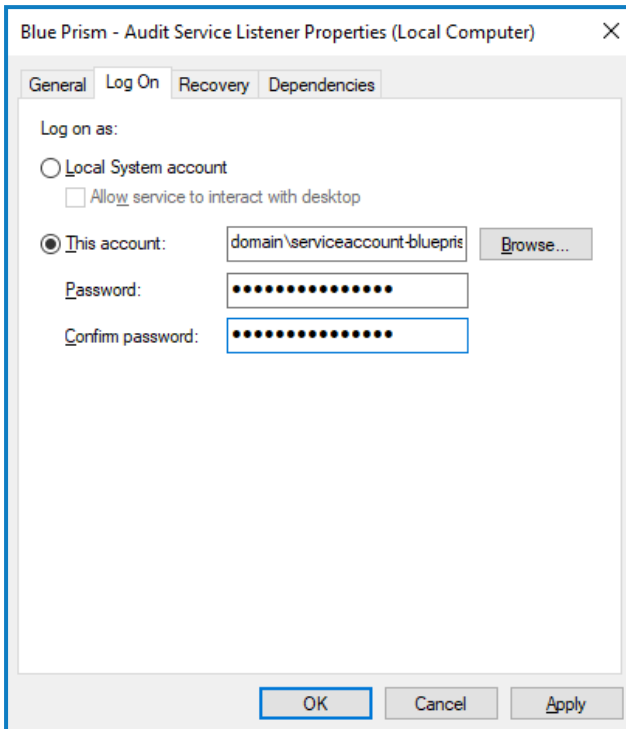
- Blue Prism - Audit Service Listener
- Blue Prism - Log Service
- Blue Prism - Submit Form Manager

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.

## Messages stuck in RabbitMQ

If a submission is not added to the expected Blue Prism Enterprise work queue, this may be because the submission has not been passed through the Message Broker server (running RabbitMQ) correctly.

If there is a system outage of Hub or Interact, Interact Form submissions may be sent to a RabbitMQ error queue instead of the appropriate message queue in RabbitMQ (which then directs the submissions to the work queues in Blue Prism Enterprise). Your system administrator (with access to RabbitMQ) will need to move the submission out of the error queue.

For information on moving Interact Form submissions from the RabbitMQ error queue, refer to this knowledge base article: [How to move Interact Form Submissions from a RabbitMQ error queue](#).

Another cause of messages becoming stuck in RabbitMQ is where IADA has failed to process the messages and update the queues. IADA has a dependency on the IIS Application Initialization feature, which should have been installed by default during the installation process. However, if it has not been installed, you can do so as follows:

1. On the web server where Interact and IADA are installed, open the Server Manager. To do this, type *Server* in the search box on the Windows task bar, and then click **Server Manager**.
2. Click **Add roles and features**.  
 The Add Roles and Features Wizard displays.
3. Click **Next** until you reach the Server Roles page.

4. Expand **Web Server (IIS)**, expand **Web Server**, expand **Application Development**, and then select **Application Initialization**.
5. Click **Next** until you reach the Confirm installation selections page.
6. Click **Install**.
7. Once the installation is complete, restart the web server.

## 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 SQL Server hosting the database has a valid certificate applied.
  - 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.
  - That the SQL Server has a valid certificate applied.

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.
- SSL Encryption - Ensure that the SQL Server has a valid certificate. For more information, see .
- 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.

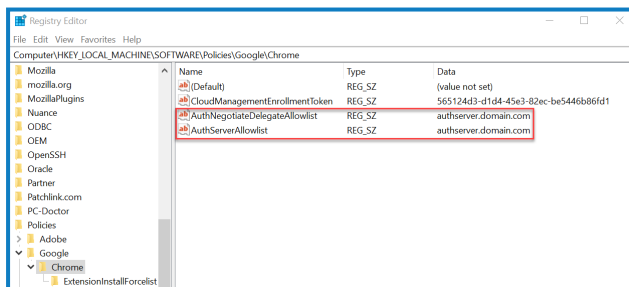
To overcome this, after the removal process has been run, either delete or clean the databases so that any previous paths have been deleted or use alternatives database names during the reinstallation.

## Configure browsers for Integrated Windows Authentication

In the event that Active Directory users cannot log into Blue Prism Hub post installation, check that you have configured the supported web browsers for Integrated Windows Authentication so that the currently logged-in users can be retrieved from the client machine. The configuration steps are different for each web browser supported by Hub.

### Configure Google Chrome


1. Close any open instances of Chrome.
2. Open Registry Editor and enter the following in the top bar:  
*Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Google\Chrome*
3. Right-click the Chrome folder and select **New > String Value**.
4. Add the following string values: *AuthNegotiateDelegateAllowlist* and *AuthServerAllowlist*.
5. Right-click each string value in turn and select **Modify**.
6. In the **Value data** field for both string values, enter the host name of the Authentication Server website, for example, *authserver.domain.com*, and click **OK**.

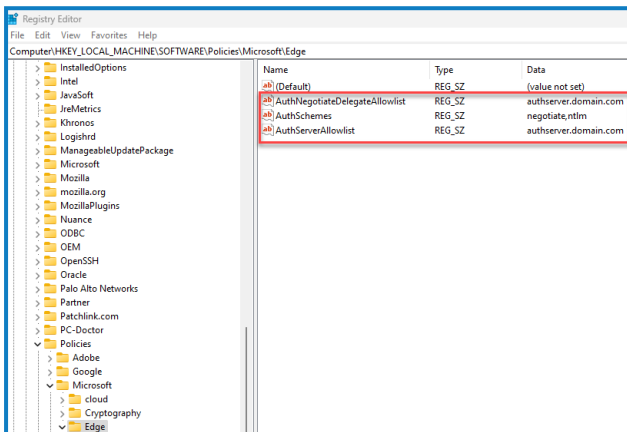


### Configure Microsoft Edge

1. Close any open instances of Edge.
2. Open Registry Editor and enter the following in the top bar:  
*Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Edge*
3. Right-click the Edge folder and select **New > String Value**.
4. Add the following string values: *AuthNegotiateDelegateAllowlist*, *AuthServerAllowlist*, and *AuthSchemes*.
5. Right-click each string value in turn and select **Modify**.

- In the **Value data** field for `AuthNegotiateDelegateAllowlist` and `AuthServerAllowlist`, enter the host name of the Authentication Server website, for example, `authserver.domain.com`, and click **OK**.
- In the **Value data** field for `AuthSchemes`, enter `negotiate, ntlm` and click **OK**. For more information, see the [Microsoft documentation on Microsoft Edge policies](#).

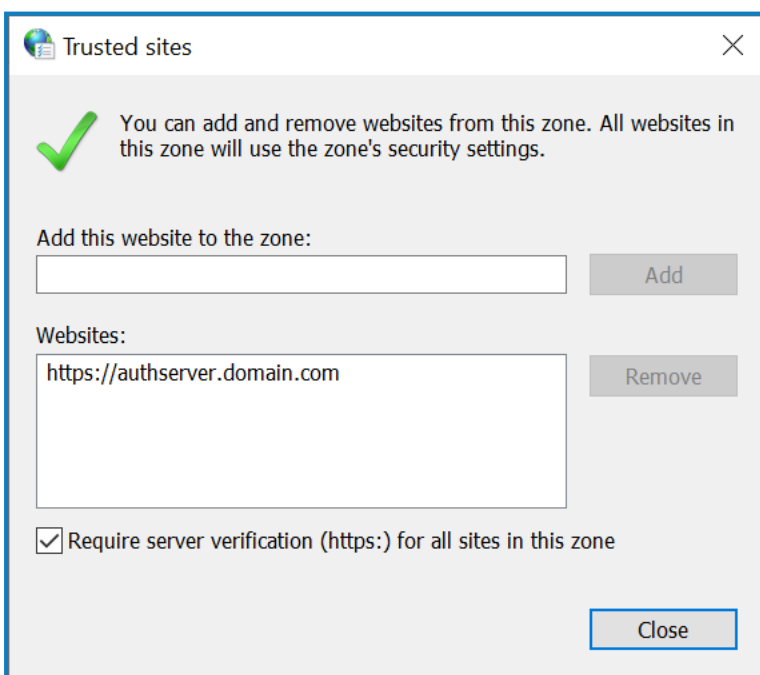
 This string value is not required if your organization is only set up for Kerberos authentication, see [below](#) for more information.



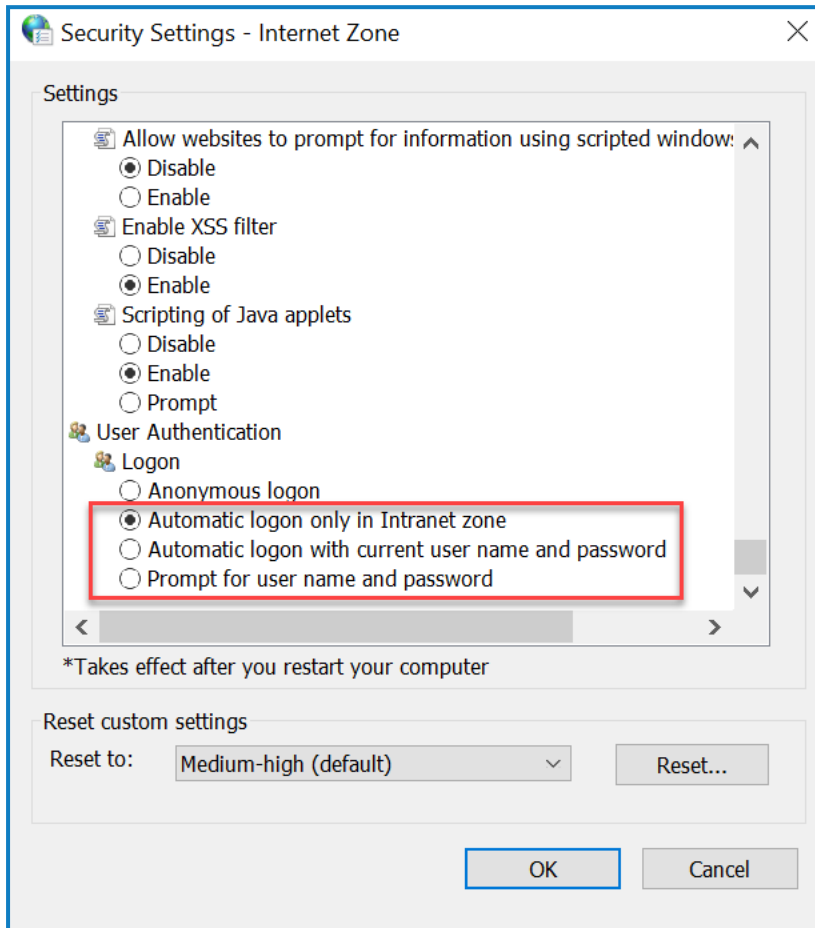
Alternatively, you can follow these steps for Microsoft Edge:

- Close any open instances of Edge.
- Navigate to **Control Panel > Network and Internet > Internet Options**.
- On the **Advanced** tab, under **Security**, select **Enable Integrated Windows Authentication**.
- On the **Security** tab, click **Trusted Sites > Sites**.
- In the **Trusted sites** dialog, enter the URL for Authentication Server (for example, `https://authserver.domain.com`) in the **Add this website to the zone** field and click **Add**.

The URL displays in the **Websites** field.



6. Click **Close**.
7. On the Security tab in the Internet Options dialog, click **Trusted Sites > Custom Level**.
8. Under **User Authentication > Logon**, confirm that **Anonymous logon** is not selected. Instead, use any of the settings that allows the browser to pick up user credentials, as shown below.



9. Click **OK**.

## Configure Kerberos authentication

The steps above will not suffice if Windows New Technology LAN Manager (NTLM) authentication has been disabled for your environment. In this case, you must also [configure Kerberos authentication](#) and a [service principal name \(SPN\)](#). Depending on your organization's setup, you might need to also [add a Microsoft Edge WebView2 registry key](#). For more information, see the Microsoft documentation on [NTLM](#) and [Kerberos](#) authentication.

1. On the web server, open Internet Information Services (IIS) Manager.
2. From the list of connections, select **Blue Prism - Authentication Server**.  
This is the default site name - if you have used a custom site name, select the appropriate connection.
3. Under IIS, double-click **Authentication**.  
The Authentication page displays.
4. Select **Windows Authentication** (make sure it is set to *Enabled*) and then click **Providers....**  
The Providers dialog displays.

5. Add one or more providers from the list of available providers, based on your organization's setup, and click **OK**.

### Configure service principal name (SPN)

A service principal name (SPN) will also need to be configured and registered for the Authentication Server URL to ensure Kerberos authentication works correctly. See the [Microsoft documentation](#) on this topic for further details, including required permissions. This is an essential step to review with your organization's IT team to ensure that the `Setspn` command does not fail to execute due to missing account permissions.

1. Open Command Prompt as an administrator on the web server and run the applicable command below.

If the Blue Prism - Authentication Server application pool is running as a Local System account, use:

```
Setspn -S HTTP/WEBSITE_URL COMPUTER_HOSTNAME
```

If the Blue Prism - Authentication Server application pool is running as a service account, use:

```
Setspn -S HTTP/WEBSITE_URL DOMAIN/Username
```



HTTP covers both HTTP and HTTPS. Do not change the command to include HTTPS specifically as the configuration will fail.

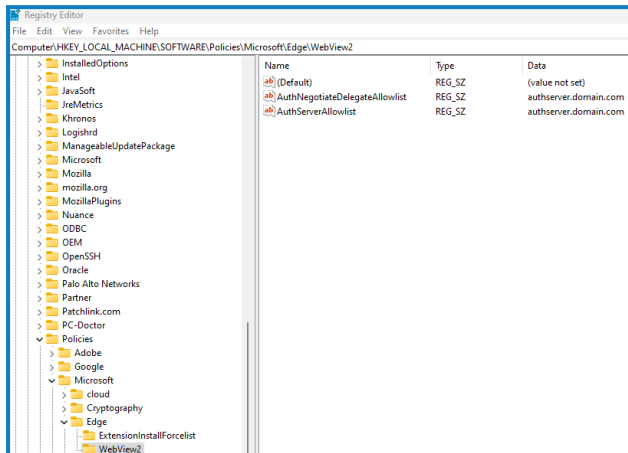
2. Run `klint purge` to refresh the Kerberos tickets.
3. Log into Authentication Server to verify that Kerberos authentication is working correctly.

### Add a Microsoft Edge WebView2 registry key

If your organization is only set up for Kerberos authentication, and Authentication Server is also used to log into Blue Prism Enterprise, a registry key for the [Microsoft Edge WebView2 browser](#) must be added:

1. Close any open instances of Edge.
2. Open Registry Editor and enter the following in the top bar:  
`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge`
3. Right-click the Edge folder and select **New > Key**.
4. Name the new key **WebView2**.
5. Right-click the WebView2 folder and add the following string values:  
`AuthNegotiateDelegateAllowlist` and `AuthServerAllowlist`.
6. Right-click each string value in turn and select **Modify**.

7. In the **Value data** field for `AuthNegotiateDelegateAllowlist` and `AuthServerAllowlist`, enter the host name of the Authentication Server website, for example, `authserver.domain.com`, and click **OK**.



## 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.

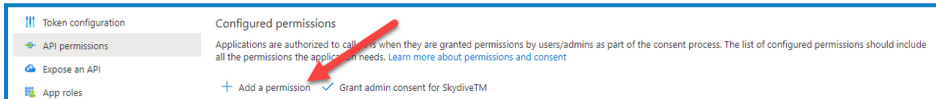
The web server must start up after the RabbitMQ services have all started. If the web server services start before the RabbitMQ service is ready, then going into the SMTP settings in Hub will result in a 'something went wrong' message.

## Saving the SMTP setting returns an error when using OAuth 2.0

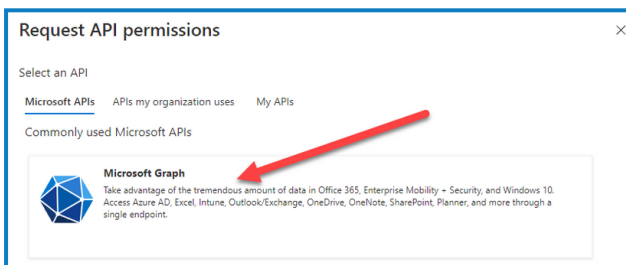
If you receive an error when saving a email configuration using OAuth 2.0, check that the Mail.Send permission is configured for the application in Azure Active Directory.

To add the Mail.Send permission:

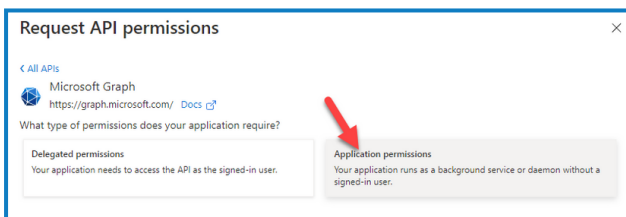
1. In Azure Active Directory, open the application properties for the application that you are linking Hub to.
2. Click **API permissions**.
3. Click **Add a permission**.



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

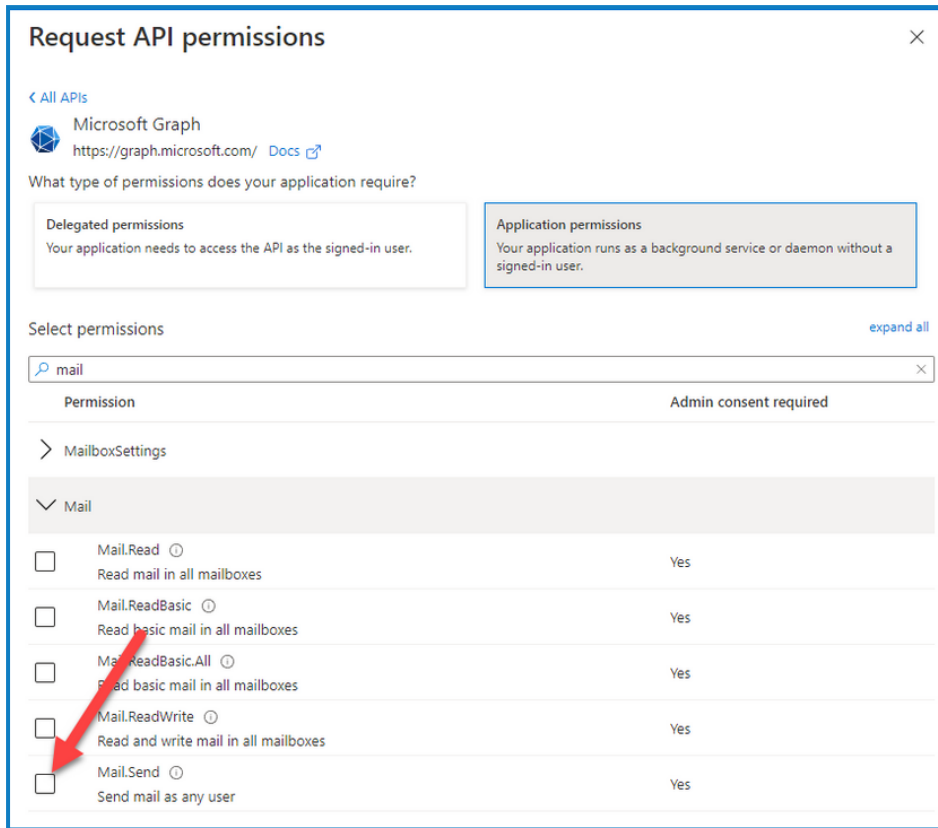


5. Under Microsoft Graph, click **Application permissions**.

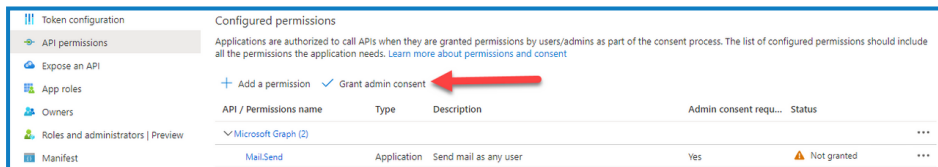


6. Type *Mail* in the search field and press Enter.

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.

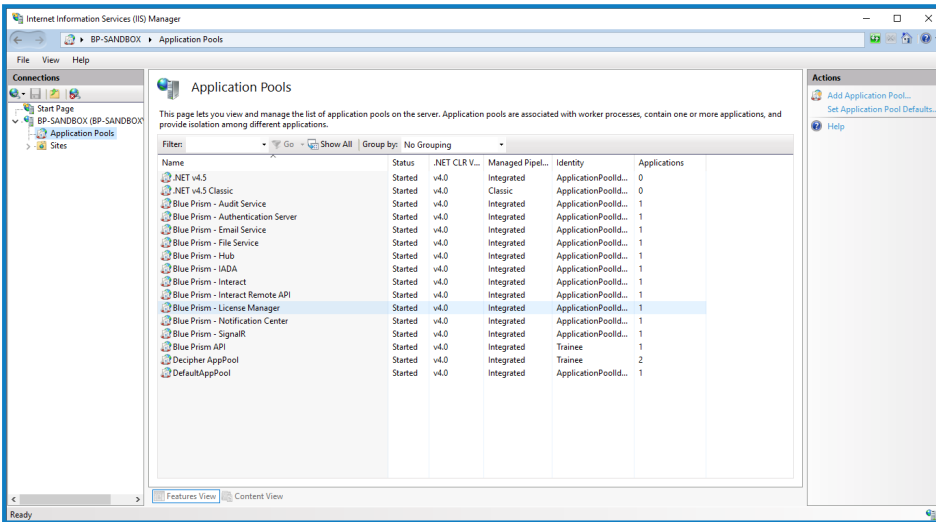


To restart License Manager:

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.

## Uninstall Interact

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

To completely uninstall Interact 4.7, 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

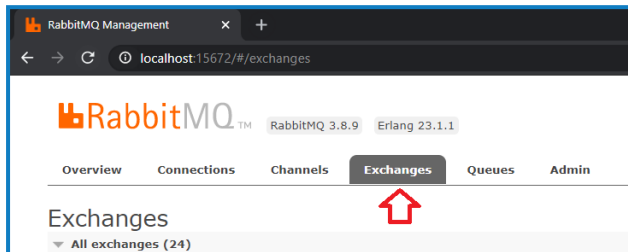
You should only remove databases for test systems. If you are contemplating removing a database for a system that had been in production, you should consider whether the data needs to be archived by your organization or used for audit purposes.

 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.

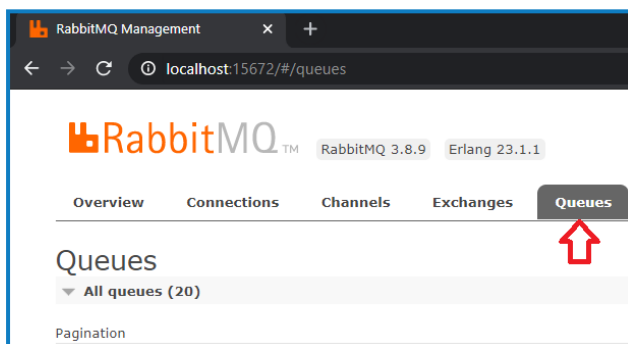
1. Delete, or archive, the database for the Interact application.

## 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:
  - `bpc.interact.*`
4. Click **Queues**.



5. Find and remove the following items:
  - `bpc.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