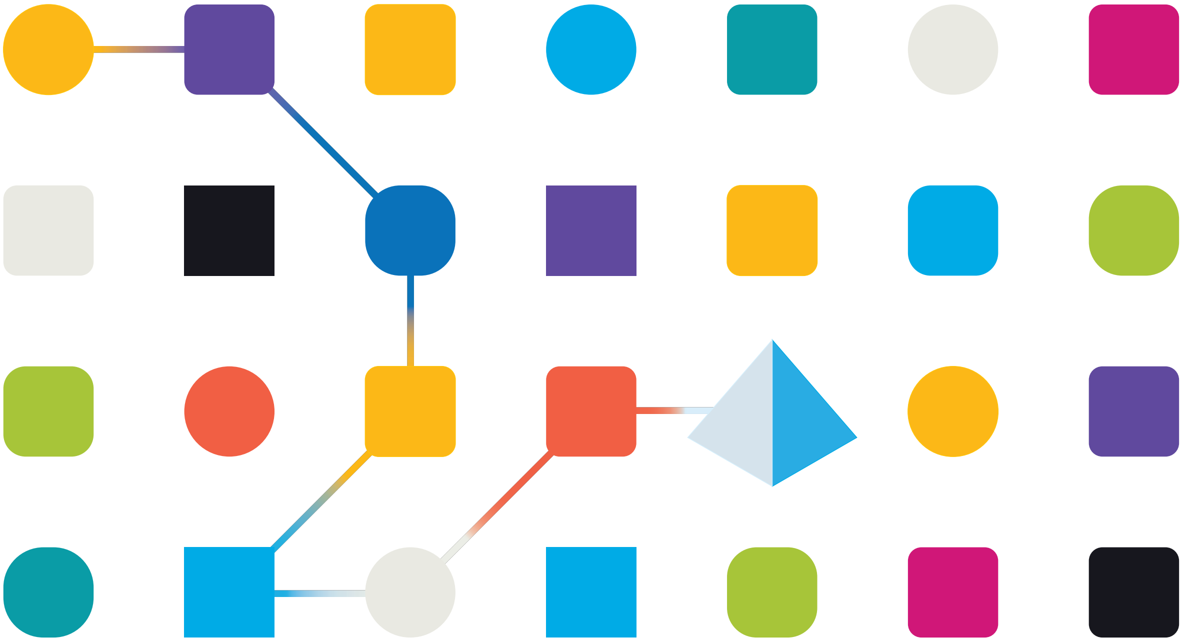
Hub 4.7

Install Guide

Document Revision: 8.2



Trademarks and Copyright

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

Contents

Installing Hub

This guide provides guidance on the process to follow when installing Blue Prism® Hub.

A number of more advanced topics are also included within this guide to provide information on troubleshooting installations and configuring advanced settings and options. It is assumed that the person carrying out an installation of Hub has prior knowledge or experience with Blue Prism, configuring SSL Certificates, and RabbitMQ.

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 to version 4.7 of Blue Prism Hub.

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

Upgrading Hub

If upgrading from an earlier version of Hub 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 Hub installation videos.

Related guidance

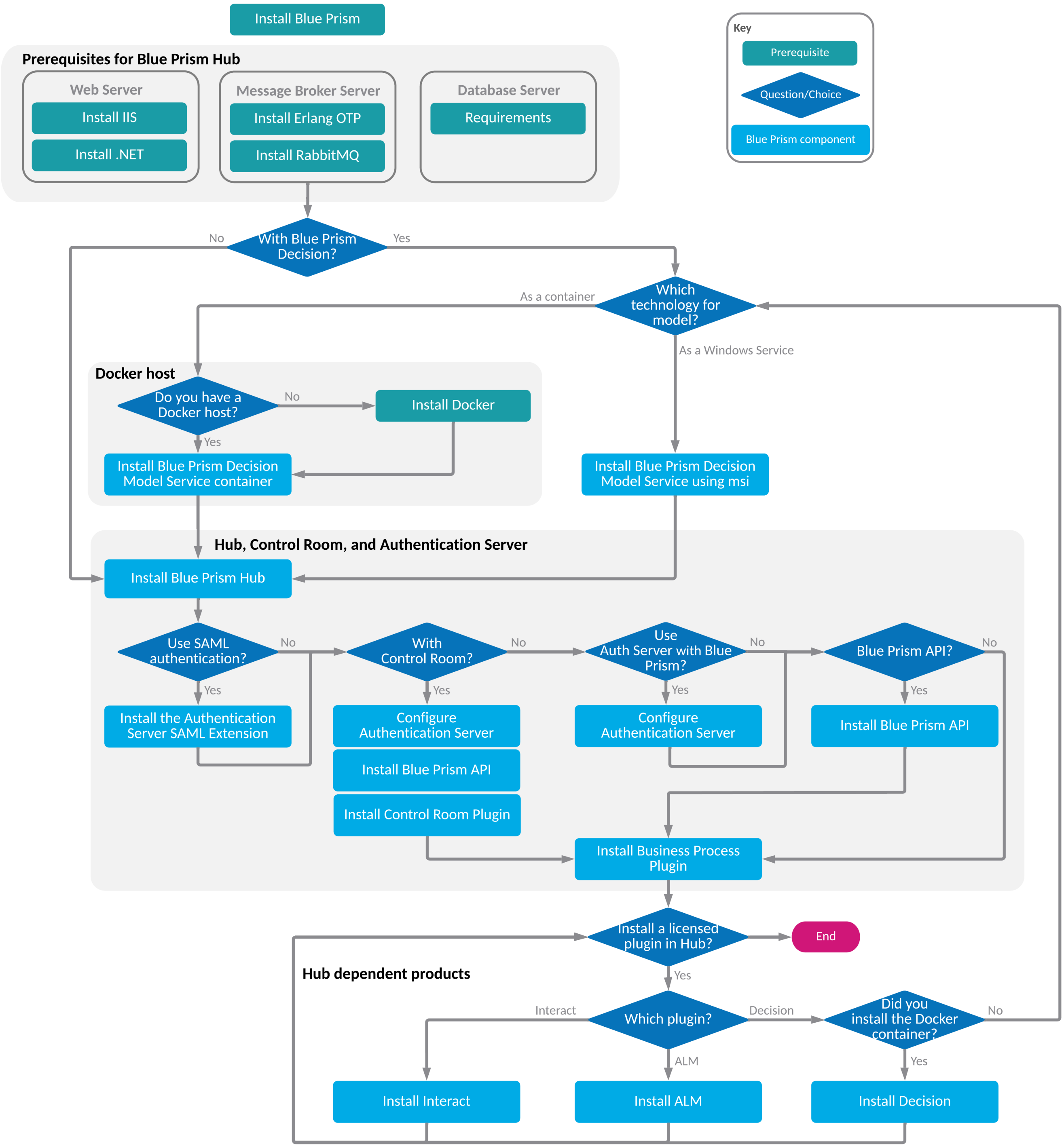
The following documents provide further information on specific aspects of the implementation of Hub and its plugins.

Document Title	Description
Hub User Guide	A document aimed at Hub users explaining how to get the best out of Hub.
Hub Administrator Guide	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.
Authentication Server Configuration Guide	A document explaining how to configure Authentication Server for Blue Prism Hub and Blue Prism user authentication.
Authentication Server SAML 2.0 Extension 4.7 Installation Guide	A document explaining how to install the SAML 2.0 extension. This is required if your organization wants to use SAML 2.0 authentication. This link takes you to the Digital Exchange, where the guide can be accessed in PDF format.
ALM User Guide	A document explaining how to use the Automation Lifecycle Management (ALM) plugin. This is a licensed product.

Document Title	Description
Control Room User Guide	A document explaining how to use the Control Room plugin. This plugin is freely available and compatible with Blue Prism 7.0 or later.
Decision Install Guide	A document explaining the steps required to install Blue Prism Decision. This is a licensed product.
Decision User Guide	A document explaining how to use the Decision plugin. This is a licensed product.
Interact Install Guide	A document explaining the steps required to install Interact. This is a licensed product.
Interact Plugin User Guide	A document explaining how to use the Interact plugin to create forms for the Interact web application. This is a licensed product.
Interact Web Application User Guide	A document explaining how to use the Interact web application as an end user. This is a licensed product.
Wireframer User Guide	A document explaining how to use the Wireframer option, which is part of the ALM plugin. This is a licensed product.

Install process overview

The diagram below provides a visual representation of the install process up to Hub 4.7:


Install Blue Prism
Prerequisites for Blue Prism Hub
Web Server
Install IIS
Install .NET
Message Broker Server
Install Erlang OTP
Install RabbitMQ
Database Server
Requirements
Key
Prerequisite
Question/Choice
Blue Prism component
No
With Blue Prism Decision?
Yes
As a container
Which technology for model?
As a Windows Service
Docker host
Do you have a Docker host?
No
Install Docker
Yes
Install Blue Prism Decision Model Service container
Install Blue Prism Decision Model Service using msi
Hub, Control Room, and Authentication Server
Install Blue Prism Hub
Use SAML authentication?
No
Yes
Install the Authentication Server SAML Extension
With Control Room?
No
Yes
Configure Authentication Server
Install Blue Prism API
Install Control Room Plugin
Use Auth Server with Blue Prism?
No
Yes
Configure Authentication Server
Blue Prism API?
No
Yes
Install Blue Prism API
Install Business Process Plugin
Install a licensed plugin in Hub?
End
Yes
Hub dependent products
Interact
Which plugin?
Decision
ALM
Install Interact
Install ALM
Did you install the Docker container?
No
Yes
Install Decision

Preparation

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

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, and so on. Administrator-level access is required during the installation process. See Minimum SQL permissions on page 18 for more details.
- A Message Broker Server must be available hosting RabbitMQ Message Broker. See Install the Message Broker server on page 24 for more details.
- A Web Server for the Hub installation. See the Prerequisites on the next page for further information.
- Administrator access to the devices where Blue Prism Hub 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. DNS should be available to all components.
- 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 on page 16 for details.

Prerequisites

See Software requirements and permissions on page 16 for details of software requirements and minimum SQL permissions.

Installing Hub 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 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.

- 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 29 for more information.

- You will be creating the following websites - you should define the URLs based on your organizations domain:

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

⚠ 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.

- 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. For more information, see Configure SSL certificates on page 30.
- Your Customer ID - During the installation process, you will be asked to enter your Customer ID. This can be found in the email that was sent to you when you purchased ALM, Decision or Interact for use with Hub.

If you are only installing Control Room, you will not need a Customer ID. Customer IDs are only provided with, and required by, ALM, Decision or Interact.

- When using Windows Authentication, defined Windows Service Accounts are required for use with the Blue Prism environment. This is so that Windows Services and Application Pools can be configured correctly for the websites created during the Hub installation. For more information, see Installing using Windows Authentication on page 58.
- 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. The Application Pool for Hub will also need access to the BPC_SQL_CERTIFICATE certificate. 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 18.
- 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.

- The Group Policy settings for Script Execution must be set to RemoteSigned at machine level (the highest level) during installation. These settings are required to allow the installer to run signed Powershell scripts, and not by Hub itself, so when the installation is complete you can return the settings to their former values if necessary.

  To determine whether you need to temporarily update the Script Execution settings, run the command `Get-ExecutionPolicy -List` (for more information, see Get-ExecutionPolicy), and check the output. If either MachinePolicy or UserPolicy is **not** set to RemoteSigned, you must update the settings as follows:

  1. In the Group Policy Editor, navigate to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows PowerShell**.
  2. Double-click the **Turn on Script Execution option**.

     The Turn on Script Execution screen displays.
  3. Select **Enabled**, and in the Execution Policy dropdown, select **Allow local scripts and remote signed scripts**.
  4. Click **OK**, and close the Group Policy Editor.
  5. Force a policy update, either by rebooting the machine, or by running a `gpupdate /force` command.
  6. Run `Get-ExecutionPolicy -List` again to confirm that the policy change has taken effect (MachinePolicy should now be set to RemoteSigned).

Software download list

Blue Prism Hub

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

Software and reference link	Related guidance
RabbitMQ 3.11.9, 3.11.10, 3.12.12 For more information, see Downloading and Installing RabbitMQ.	Install the Message Broker server on page 24
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 more information, see RabbitMQ Erlang Version Requirements.	
IIS 10.0 Included with Windows Server 2016, 2019 and 2022.	Install and configure the web server on page 29
ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle) https://dotnet.microsoft.com/download/dotnet/6.0 - Select the version you require. Under **ASP.NET Core Runtime**, select **Hosting Bundle**.	
.NET Desktop Runtime 6.0.9 or 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 - Select the version you require. Under **.NET Desktop Runtime**, select the appropriate download.	
.NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 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.	
Blue Prism Hub 4.7 Download Hub from any of the following product download pages on the Blue Prism Portal: • Automation Lifecycle Management • Decision • Interact	
Authentication Server SAML 2.0 extension Download from the Digital Exchange - This is an optional installer. It is only required if you intend to use SAML 2.0 authentication.	See the installation guide on the Digital Exchange.

Blue Prism Decision

Blue Prism Decision is a license-controlled plugin in Hub. If your organization intends to use Decision, you will need to download the following in addition to the downloads listed in Blue Prism Hub on the previous page.

> The Decision Model Service is available using two different technologies:
>
> - As a Windows service
> - As a Linux container
>
> Only one of these needs to be installed. You should download the version that most suits your organization's technical infrastructure.

Software and link	Related guidance
OpenSSL https://www.openssl.org/source/ This is an optional download that enables you to create self-signed SSL certificates. This should only be used for POC/POV/Dev environments.	See the OpenSSL website.
To run the Decision Model Service using the container:	
Docker Engine is the minimum that is required to run the Decision container. https://www.docker.com/products/container-runtime Blue Prism recommends that your production environment uses a Linux server as the host. For POC or Dev environments, a Windows server can be used running Docker Desktop. https://www.docker.com/products/docker-desktop	For more information about installing Docker: • On a Linux server, see the Docker help: Install Docker Engine. • On a Windows server, see the Docker help: Install Docker Desktop on Windows.
Blue Prism Decision Model Service container Download from Docker Hub.	Install Blue Prism Decision
To run the Decision Model Service as a Windows service:	
Blue Prism Decision Model Service MSI. Download from the Blue Prism Portal.	Install Blue Prism Decision
To use Decision with Blue Prism:	
Blue Prism Decision API.bprelease file Download from the Blue Prism Portal.	Install Blue Prism Decision

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 page 12.

Software and reference link	Related guidance
Blue Prism Interact 4.7 Download from the Blue Prism Portal.	Install Blue Prism Interact
Blue Prism Interact Remote API.bprelease file Download from the Blue Prism Portal.	Install and configure the Interact Web API service

Minimum hardware requirements

The information below details the minimum hardware requirements recommended for effectively installing and running Hub 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 8

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 9.

  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 24 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

> ⚠ Hub 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 29 for more information.

Web browser on client machines

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

- Google Chrome
- Microsoft Edge (Chromium-based)

To enable Active Directory users to log into Hub 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

Hub itself does not require Blue Prism to be available. However, some of the components or plugins with Hub do require Blue Prism. These are:

- Authentication Server - Requires Blue Prism 7.1.2 or later.
- Blue Prism® Automation Lifecycle Management (ALM) - Requires Blue Prism 6.4.0 or later.
- Control Room - Requires Blue Prism 7.1.0 or later.
- Blue Prism® Decision - Requires Blue Prism 6.4.0 or later.
- SS&C | Blue Prism® Interact - Requires Blue Prism 6.4.0 or later.

Minimum SQL permissions

The minimum SQL permissions for a user required to connect to the database during the installation process must have the appropriate privileges to create or configure the databases 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)

A database user required to connect to the databases during normal operation must have the minimum SQL permissions to access the Hub and Authentication Server databases. The required permissions are:

- db_datareader
- db_datawriter

When using Windows Authentication, the account set as the Identity of the Application Pools requires access to the Blue Prism database for Hub Control Room and Interact purposes. The account must have the minimum SQL permissions to access the Blue Prism database. The required permissions are:

- db_datareader
- db_datawriter

When using SQL Authentication, the same requirements apply as for Windows Authentication, but for the SQL account specified in the installation parameters.

For more information, see Default application information below.

Default application information

The information below shows the applications that are created by the 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. In addition:

- IIS APPPOOL\ Blue Prism - Authentication Server and IIS APPPOOL\ Blue Prism - SignalR will also require access to the BluePrismCloud_IMS_JWT certificate.
- IIS APPPOOL\ Blue Prism - Hub will also require access to the BPC_SQL_CERTIFICATE certificate.

> If using Windows Authentication to authenticate with SQL Server, we recommend that a dedicated Active Directory user is assigned to the Identity of the IIS Application Pool (the default names are shown in the tables below). You must ensure that this Application Pool user is set to use the Region **English (United States)**. To do this, open Control Panel > Clock and Region > Region, set the **Format** to **English (United States)** for the Application Pool user.

Hub 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 - Authentication Server	IIS APPPOOL\ Blue Prism - Authentication Server	dbcreator / sysadmin	db_datawriter / db_datareader	AuthenticationServerDB
Blue Prism - Hub	IIS APPPOOL\ Blue Prism - Hub	dbcreator / sysadmin	For the first login and initial configuration: dbcreator / sysadmin Subsequent logins: db_datawriter / db_datareader	HubDB
Blue Prism - Email Service	IIS APPPOOL\ Blue Prism - Email Service	dbcreator / sysadmin	db_datawriter / db_datareader	EmailServiceDB
Blue Prism - Audit Service	IIS APPPOOL\ Blue Prism - Audit Service	dbcreator / sysadmin	db_datawriter / db_datareader	AuditDB
Blue Prism - File Service	IIS APPPOOL\ Blue Prism - File Service	dbcreator / sysadmin	db_datawriter / db_datareader	FileServiceDB
Blue Prism - Notification Center	IIS APPPOOL\ Blue Prism - Notification Center	dbcreator / sysadmin	db_datawriter / db_datareader	NotificationCenterDB
Blue Prism - License Manager	IIS APPPOOL\ Blue Prism - License Manager	dbcreator / sysadmin	db_owner Or db_datawriter / db_datareader with execute permissions (see below)	LicenseManagerDB
Blue Prism - SignalR	IIS APPPOOL\ Blue Prism - SignalR	N/A	N/A	N/A

When the application is running, the License Manager requires appropriate permissions to execute stored procedures. If you do not want to use db_owner as the permission level, you can use db_datawriter/db_datareader and run the following SQL script to provide the required level to that user:

```
USE [LicenseManagerDB]
GRANT EXECUTE to "IIS APPPOOL\Blue Prism - License Manager"
```

Where:

- [LicenseManagerDB] is the database name for License manager.
- `"IIS APPPOOL\Blue Prism - License Manager"` is the username.

Hub 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 - Audit Service Listener	NT AUTHORITY\ SYSTEM	dbcreator / sysadmin	db_datawriter / db_datareader	AuditDB
Blue Prism - Log Service	NT AUTHORITY\ SYSTEM	N/A	N/A	N/A

Multi-device deployment considerations

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

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

Network ports

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

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

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

Typical deployment

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

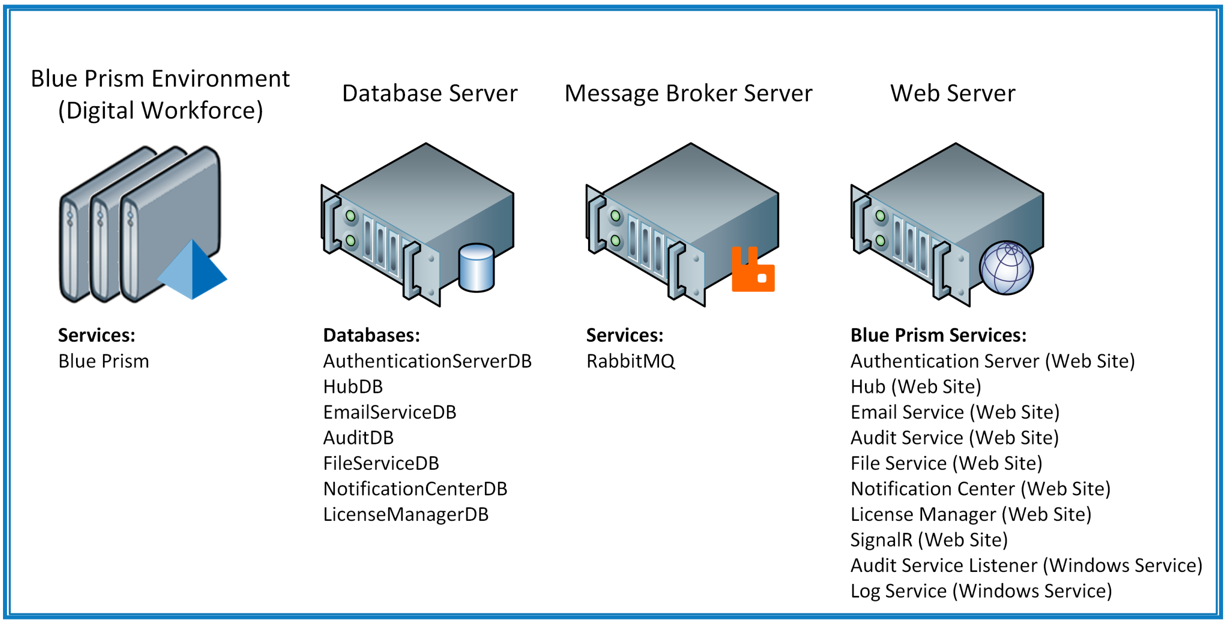
Prior to following this guidance, ensure that you have fully considered the information in Preparation on page 8.

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

- Blue Prism Environment (Digital Workforce)
- Database Server (SQL Server)
- Message Broker Server
- Web Server

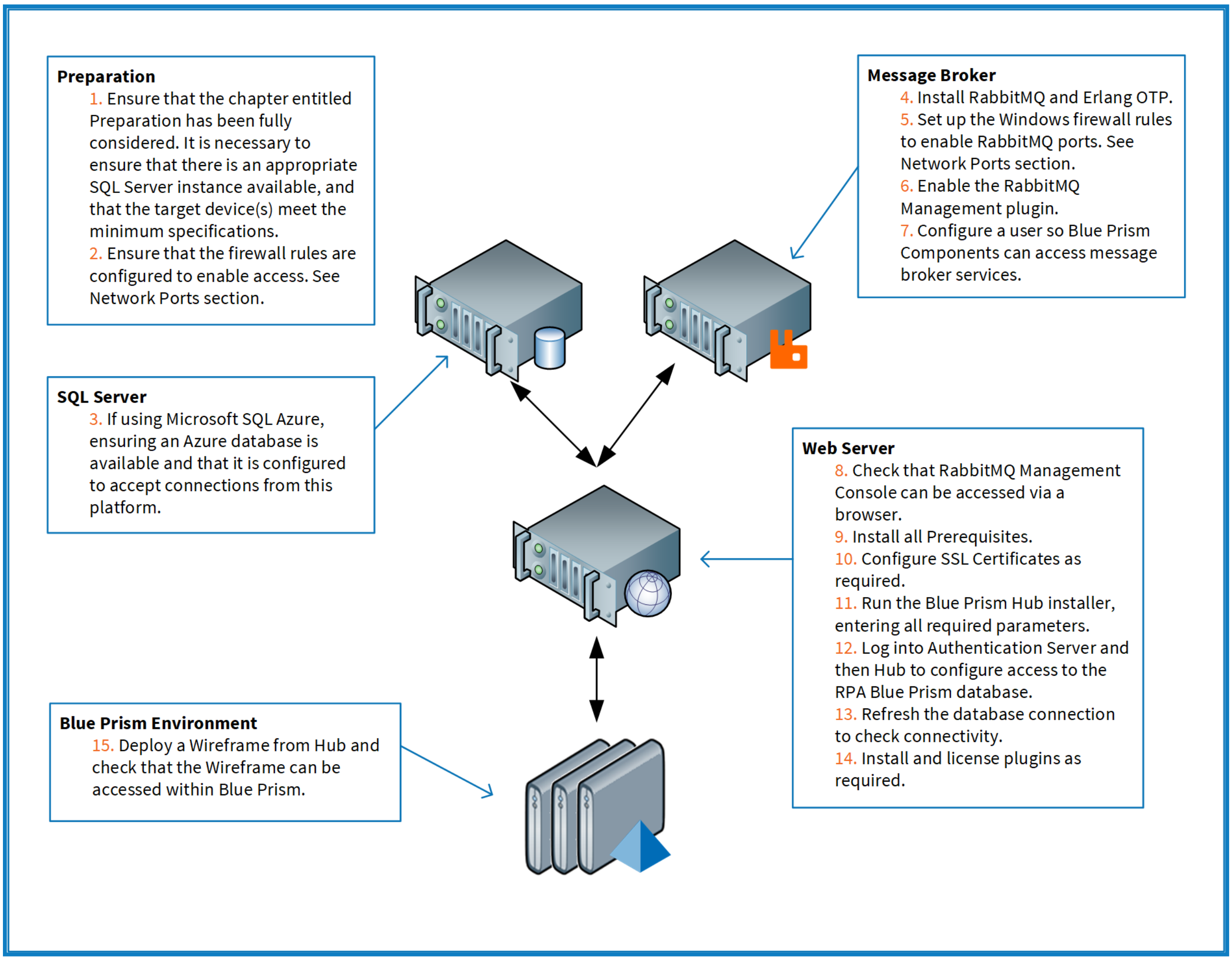
The Message Broker Server and SQL Server instances must be pre-configured prior to the installation of Blue Prism Hub.

The diagram below illustrates the typical architecture for an environment.



Overview of typical installation steps

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



Preparation

1. Ensure that the chapter entitled Preparation has been fully considered. It is necessary to ensure that there is an appropriate SQL Server instance available, and that the target device(s) meet the minimum specifications.
2. Ensure that the firewall rules are configured to enable access. See Network Ports section.

SQL Server

3. If using Microsoft SQL Azure, ensuring an Azure database is available and that it is configured to accept connections from this platform.

Message Broker

4. Install RabbitMQ and Erlang OTP.
5. Set up the Windows firewall rules to enable RabbitMQ ports. See Network Ports section.
6. Enable the RabbitMQ Management plugin.
7. Configure a user so Blue Prism Components can access message broker services.

Web Server

8. Check that RabbitMQ Management Console can be accessed via a browser.
9. Install all Prerequisites.
10. Configure SSL Certificates as required.
11. Run the Blue Prism Hub installer, entering all required parameters.
12. Log into Authentication Server and then Hub to configure access to the RPA Blue Prism database.
13. Refresh the database connection to check connectivity.
14. Install and license plugins as required.

Blue Prism Environment

15. Deploy a Wireframe from Hub and check that the Wireframe can be accessed within Blue Prism.

If you experience problems whilst installing, see Troubleshoot a Hub installation on page 71.

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 16.

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

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

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

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

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

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

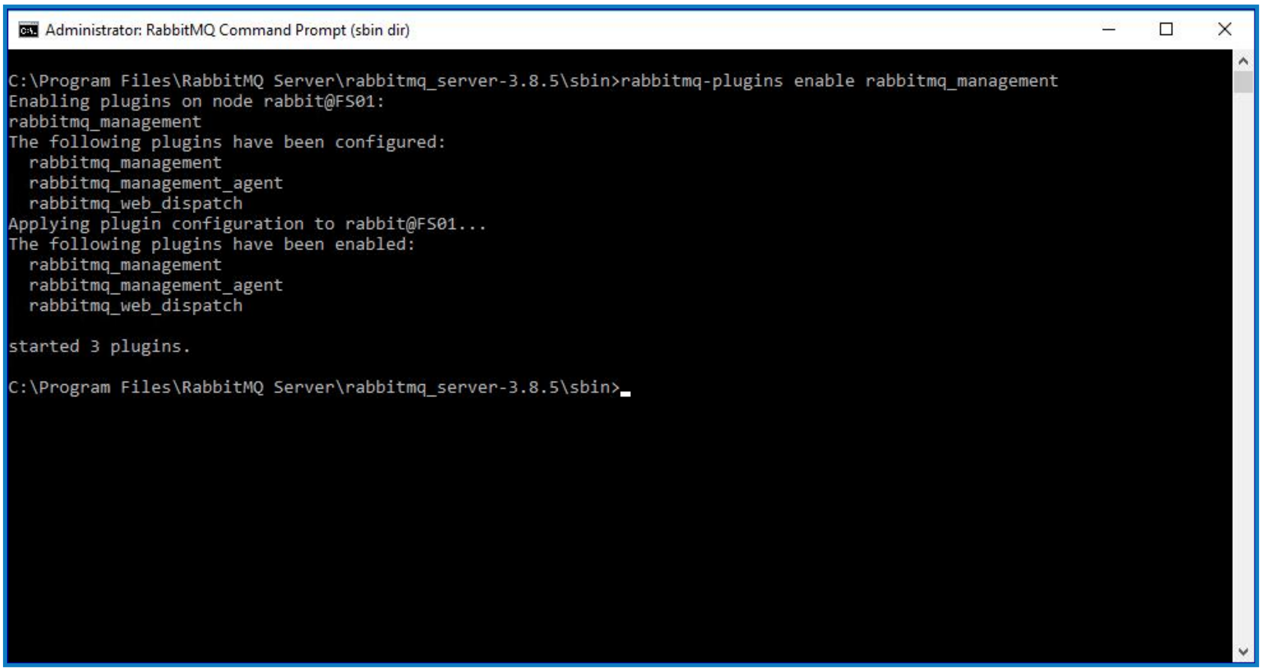
   For more information, see Downloading and Installing RabbitMQ.

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

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

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

```
rabbitmq-plugins enable rabbitmq_management
```



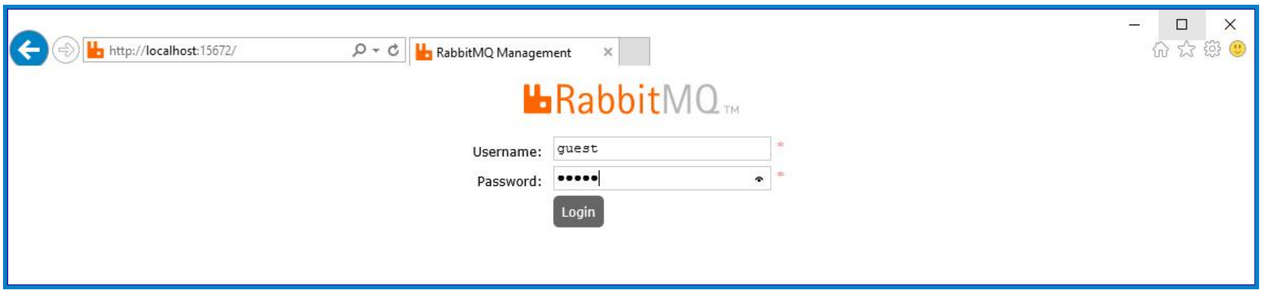
```
C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.5\sbin>rabbitmq-plugins enable rabbitmq_management
Enabling plugins on node rabbit@FS01:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch
Applying plugin configuration to rabbit@FS01...
The following plugins have been enabled:
  rabbitmq_management
  rabbitmq_management_agent
  rabbitmq_web_dispatch

started 3 plugins.

C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.5\sbin>_
```

6. Launch a browser and navigate to the following URL: http://localhost:15672

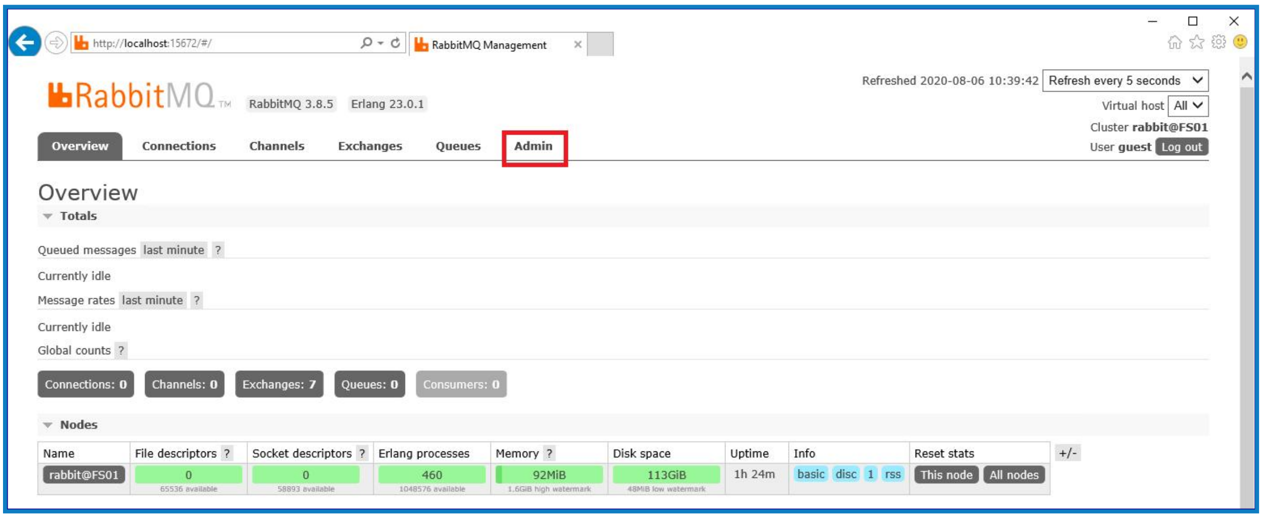
7. In the RabbitMQ console, log on with the default credentials of guest/guest.



Username: guest *

Password: ••••• *

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



RabbitMQ 3.8.5 Erlang 23.0.1

Refreshed 2020-08-06 10:39:42 Refresh every 5 seconds

Virtual host All

Cluster rabbit@FS01

User guest

Overview

Totals

Queued messages last minute ?

Currently idle

Message rates last minute ?

Currently idle

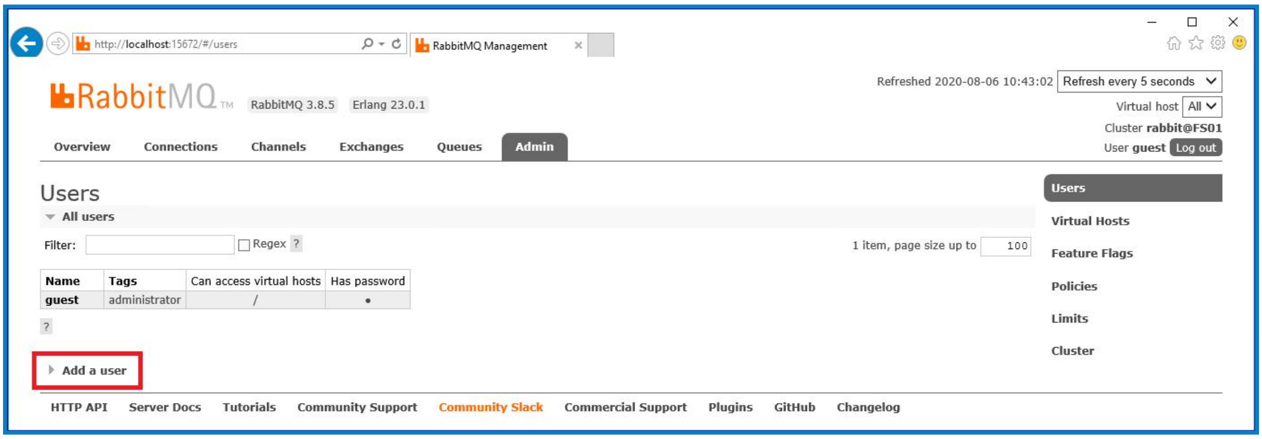
Global counts ?

Connections: 0 Channels: 0 Exchanges: 7 Queues: 0 Consumers: 0

Nodes

Name	File descriptors ?	Socket descriptors ?	Erlang processes	Memory ?	Disk space	Uptime	Info	Reset stats	+/-
rabbit@FS01	0 65536 available	0 58893 available	460 1048576 available	92MiB 1.6GiB high watermark	113GiB 48MiB low watermark	1h 24m	basic disc 1 rss	This node All nodes	

9. Click **Add a user**.



RabbitMQ 3.8.5 Erlang 23.0.1

Refreshed 2020-08-06 10:43:02 Refresh every 5 seconds

Virtual host All

Cluster **rabbit@FS01**

User **guest**

Users

All users

Filter: □ Regex ?

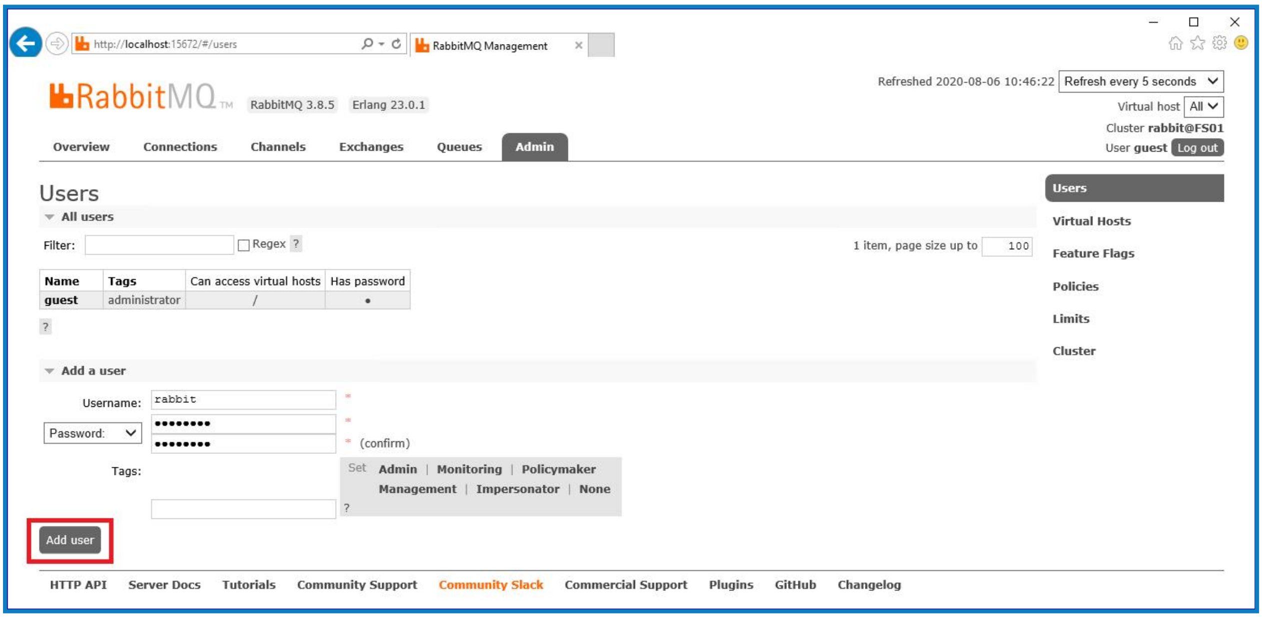
1 item, page size up to 100

Name	Tags	Can access virtual hosts	Has password
guest	administrator	/	•

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**.



RabbitMQ 3.8.5 Erlang 23.0.1

Refreshed 2020-08-06 10:46:22 Refresh every 5 seconds

Virtual host All

Cluster **rabbit@FS01**

User **guest**

Users

All users

Filter: □ Regex ?

1 item, page size up to 100

Name	Tags	Can access virtual hosts	Has password
guest	administrator	/	•

Add a user

Username: rabbit *

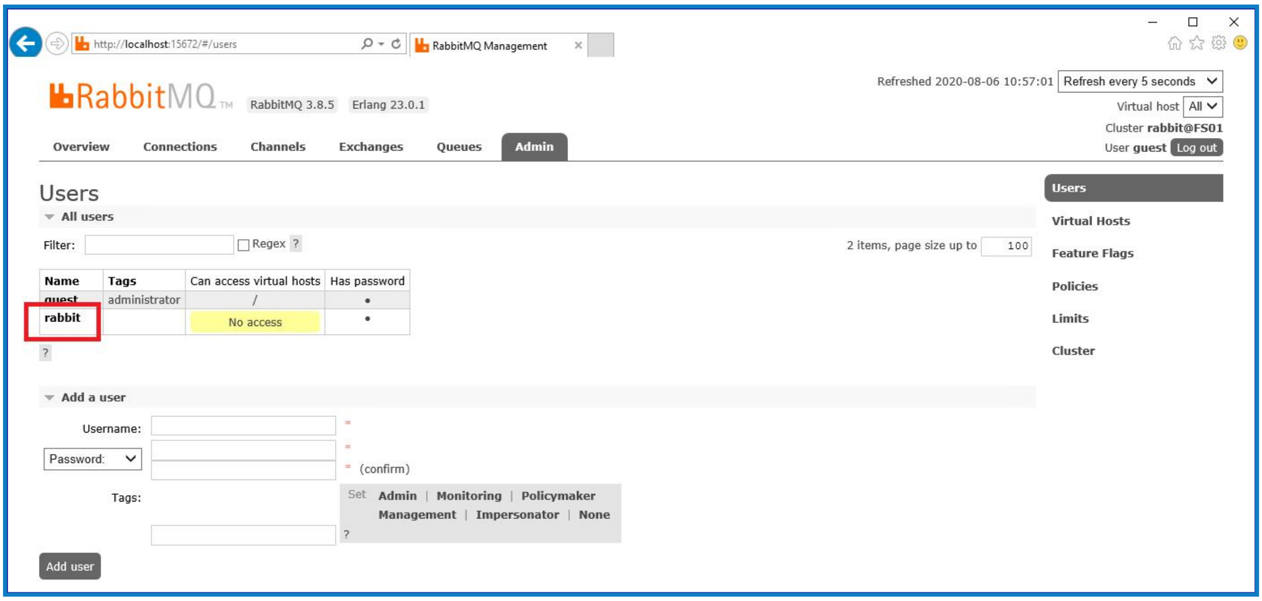
Password: •••••••• *

•••••••• * (confirm)

Tags: Set Admin | Monitoring | Policymaker | Management | Impersonator | None ?

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

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


http://localhost:15672/#/users
RabbitMQ Management
RabbitMQ™ RabbitMQ 3.8.5 Erlang 23.0.1
Overview Connections Channels Exchanges Queues Admin
Users
Virtual Hosts
Feature Flags
Policies
Limits
Cluster
Add user

Refreshed 2020-08-06 10:57:01 Refresh every 5 seconds
Virtual host All
Cluster rabbit@FS01
User guest Log out

Users

All users

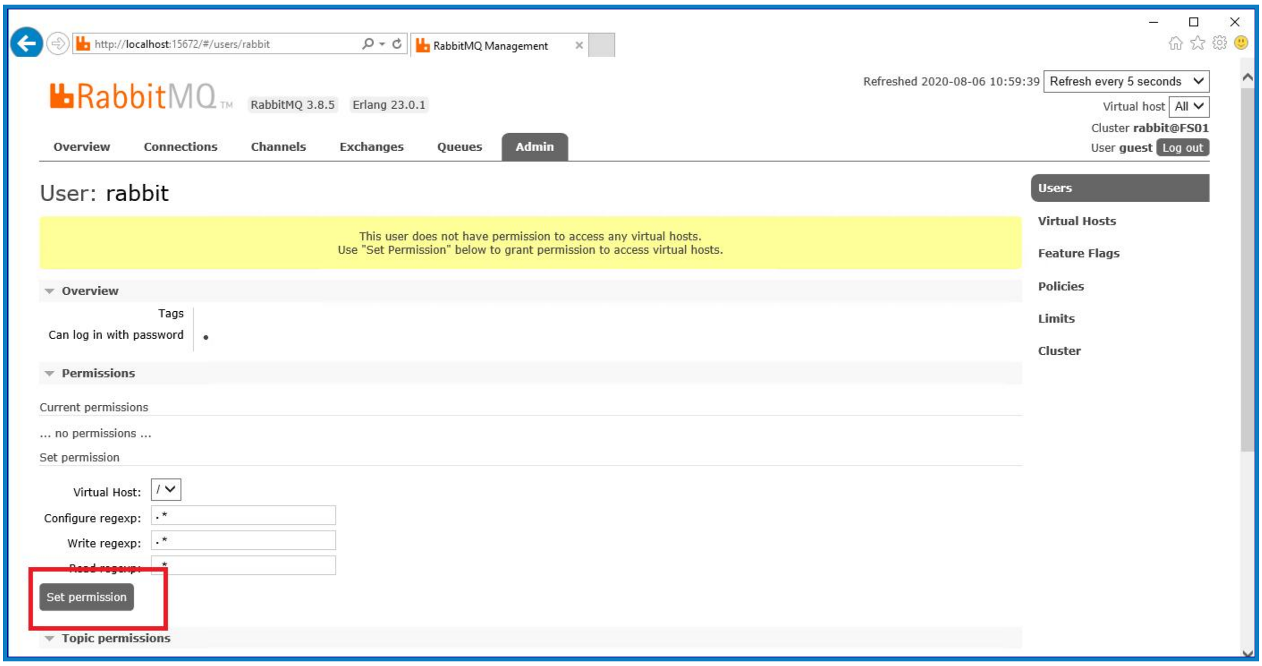
Filter: □ Regex ?   2 items, page size up to 100

Name	Tags	Can access virtual hosts	Has password
guest	administrator	/	•
rabbit		No access	•

Add a user

Username: *
Password: *
* (confirm)
Tags: Set Admin \| Monitoring \| Policymaker Management \| Impersonator \| None ?

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


http://localhost:15672/#/users/rabbit
RabbitMQ Management
RabbitMQ™ RabbitMQ 3.8.5 Erlang 23.0.1
Overview Connections Channels Exchanges Queues Admin
Users
Virtual Hosts
Feature Flags
Policies
Limits
Cluster
Set permission

Refreshed 2020-08-06 10:59:39 Refresh every 5 seconds
Virtual host All
Cluster rabbit@FS01
User guest Log out

User: rabbit

This user does not have permission to access any virtual hosts.
Use "Set Permission" below to grant permission to access virtual hosts.

Overview

Tags
Can log in with password •

Permissions

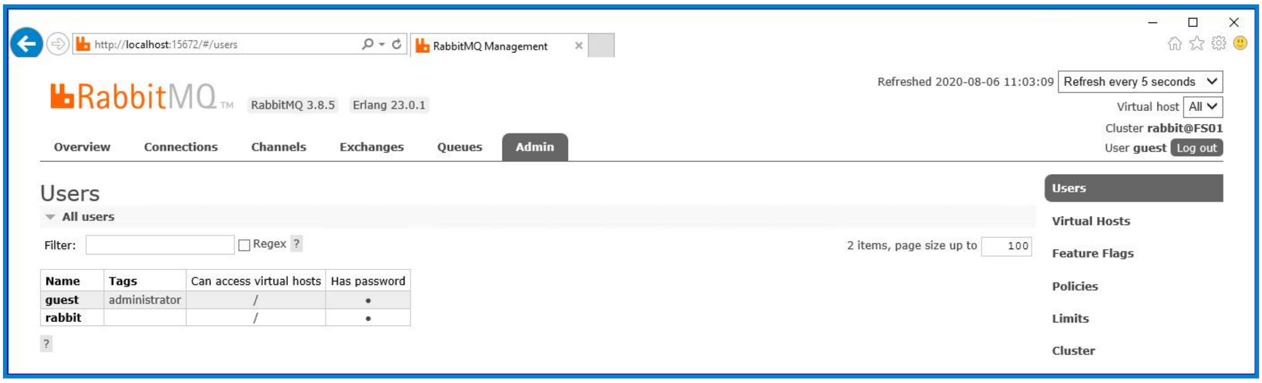
Current permissions
... no permissions ...

Set permission

Virtual Host: /
Configure regexp: .*
Write regexp: .*
Read regexp: .*

Topic permissions

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


http://localhost:15672/#/users
RabbitMQ Management
RabbitMQ™ RabbitMQ 3.8.5 Erlang 23.0.1
Overview Connections Channels Exchanges Queues Admin
Users
Virtual Hosts
Feature Flags
Policies
Limits
Cluster

Refreshed 2020-08-06 11:03:09 Refresh every 5 seconds
Virtual host All
Cluster rabbit@FS01
User guest Log out

Users

All users

Filter: □ Regex ?   2 items, page size up to 100

Name	Tags	Can access virtual hosts	Has password
guest	administrator	/	•
rabbit		/	•

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 71.

Install and configure the web server

Before installing the Hub web server, ensure you have read the information in Preparation on page 8.

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 table below details the required SSL certificates.

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

⚠ 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.**

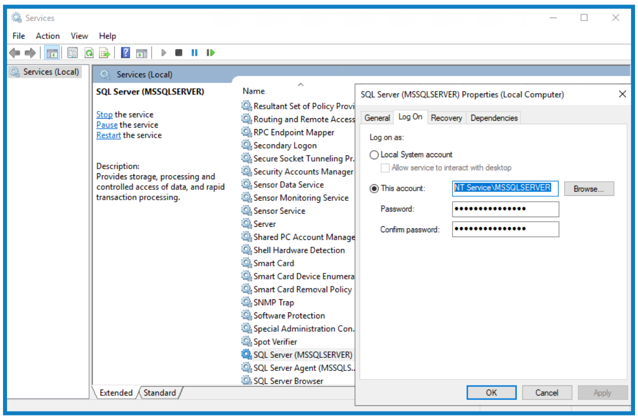
1. Run PowerShell as an administrator and execute the Microsoft script with the information for your SQL Server.

   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.



SQL Server (MSSQLSERVER)

Stop the service
Pause the service
Restart the service

Description:
Provides storage, processing and controlled access of data, and rapid transaction processing.

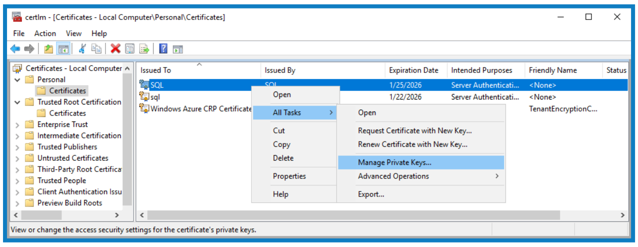
SQL Server (MSSQLSERVER) Properties (Local Computer)

Log on as:

○ Local System account
□ Allow service to interact with desktop
● This account: NT Service\MSSQLSERVER
Password: •••••••••••••••
Confirm password: •••••••••••••••

      ii. On your SQL Server, open Certificate Manager.

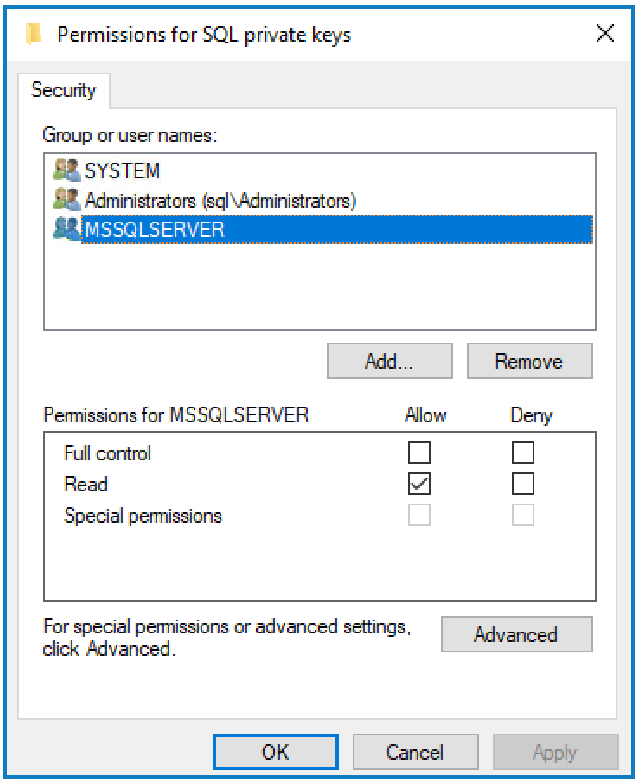
      iii. Expand **Personal**, then expand **Certificates**, right-click **SQL**, and then select **All Tasks** and click **Manage Private Keys...**


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certifica
Trusted People
Client Authentication Issu
Preview Build Roots
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
SQL	SQL	1/25/2026	Server Authenticati...	<None>	
sql		1/22/2026	Server Authenticati...	<None>	
Windows Azure CRP Certificate				TenantEncryptionC...	

View or change the access security settings for the certificate's private keys.

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



Group or user names:

- SYSTEM
- Administrators (sql\Administrators)
- MSSQLSERVER

Permissions for MSSQLSERVER	Allow	Deny
Full control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

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.

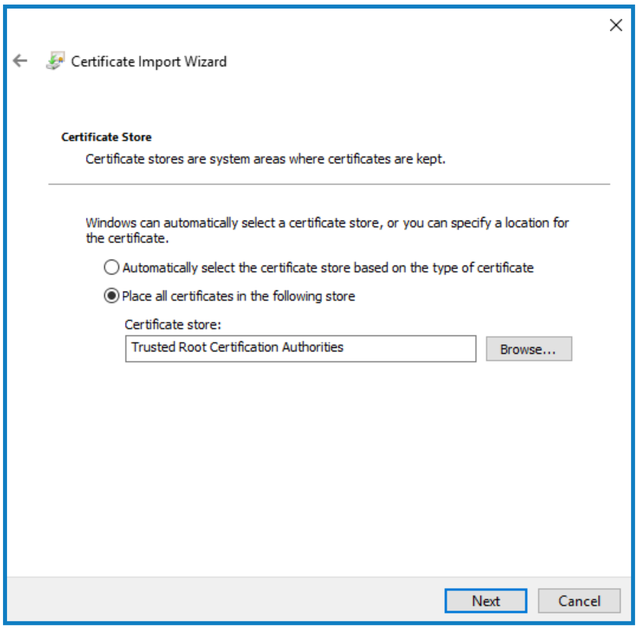
b. Add the certificate to the server's Trusted Root Certification Authorities certificate store. To do this:

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**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

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
XXXXXXXXXXX,authentication.local,hub.local,email.local,audit.local,file.local,signalr.local,notifi
cation.local,license.local -FriendlyName "TheOneCert" -NotAfter (Get-Date).AddYears(10)
```

> XXXXXXXXXXX should be replaced with the host server name.

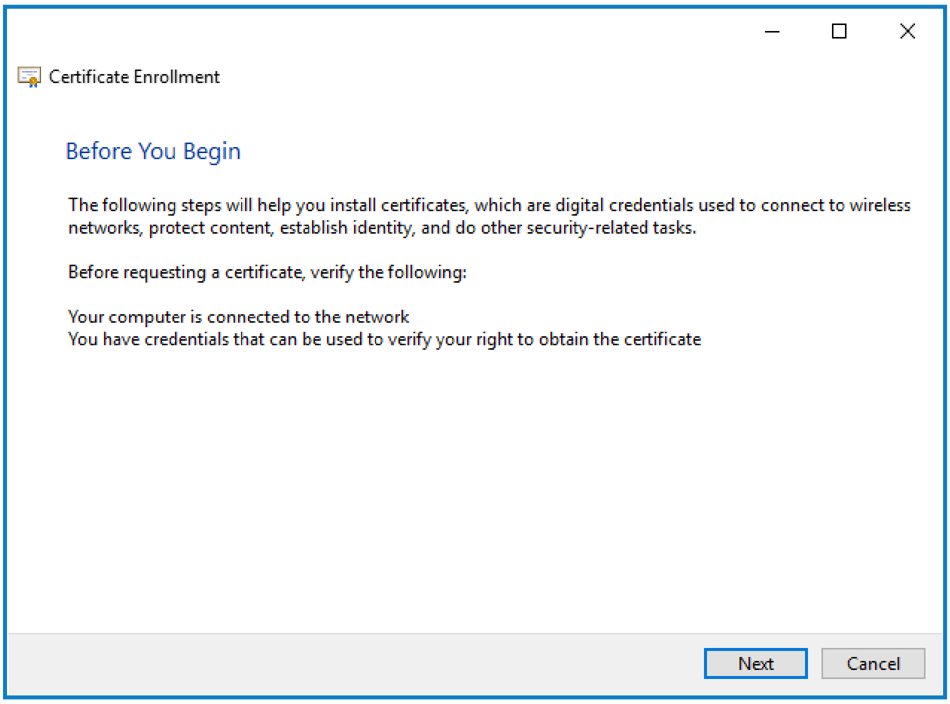
Once created, open the Local Machine certificate manager (certlm) and copy and paste the certificate into the trusted root certificate store.

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.



Certificate Enrollment

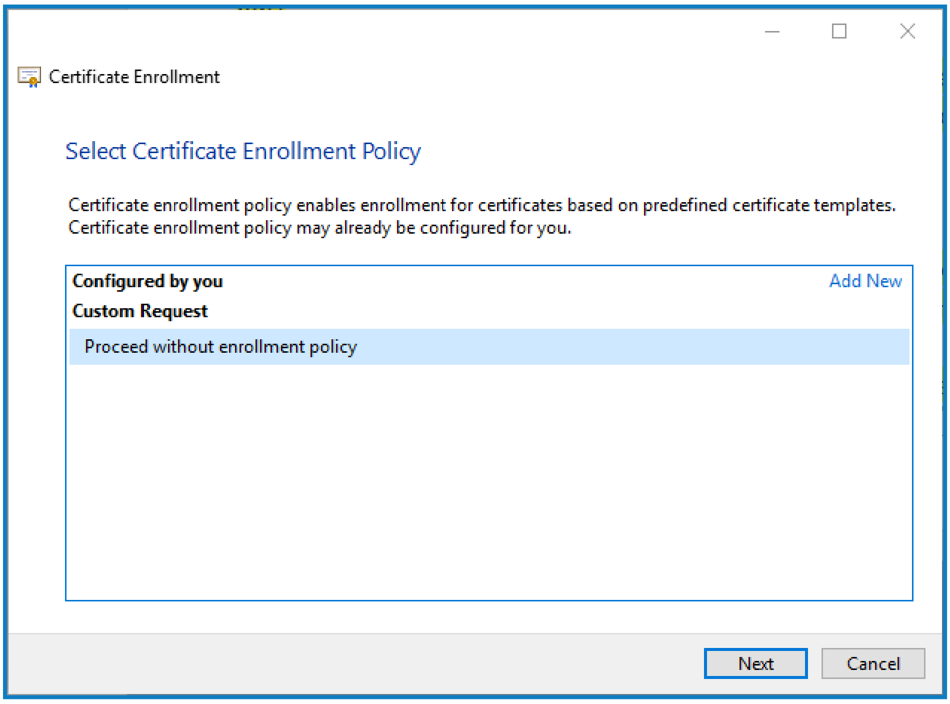
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

3. Click **Next**.



Certificate Enrollment

Select Certificate Enrollment Policy

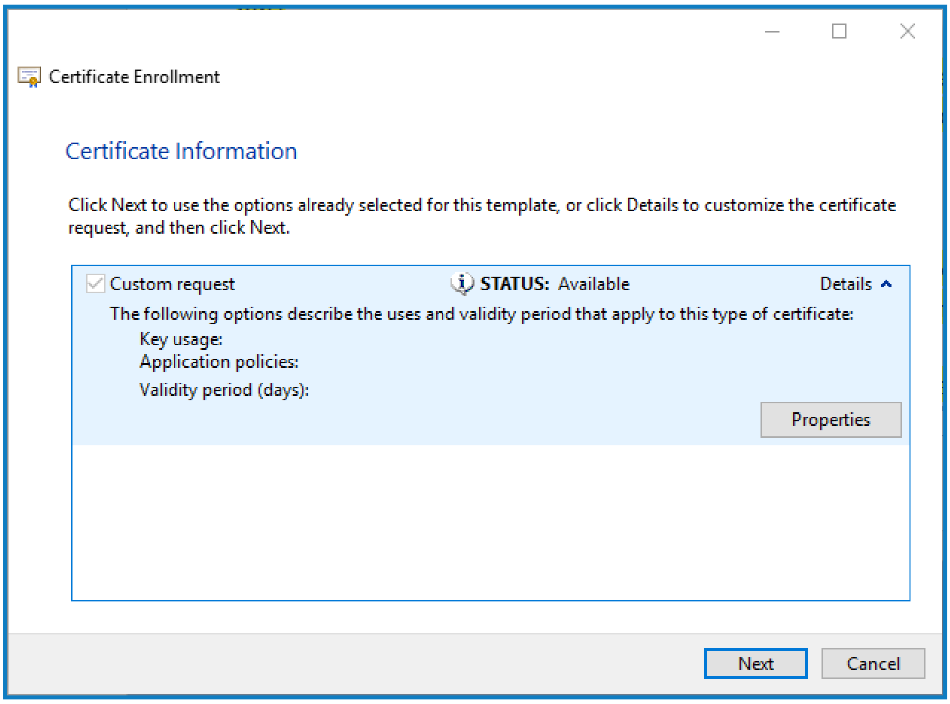
Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by you

Custom Request

Proceed without enrollment policy

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**.



Certificate Enrollment

Certificate Information

Click Next to use the options already selected for this template, or click Details to customize the certificate request, and then click Next.

☑ Custom request **STATUS:** Available

The following options describe the uses and validity period that apply to this type of certificate:

Key usage:

Application policies:

Validity period (days):

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

   The CN (common name) will display in the right-hand panel.

9. On the Extensions tab, click **Extended Key Usage**, select **Server Authentication** and click **Add**.
10. On the Private Key tab, click **Key options**, select a key size of your choice and select **Make private key exportable**.
11. Still on the Private Key tab, click **Hash Algorithm** and select a suitable Hash (optional).
12. Click **OK**.

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

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

Install .NET Core Components

The .NET Core components must be downloaded and installed.

Step	Details
1	Download the following components and store them in a temporary location, for example, C:\temp: - ASP.NET Core Runtime 6.0.9 or 6.0.10 (Windows Hosting Bundle) https://dotnet.microsoft.com/download/dotnet/6.0 - Select the version you require. Under **ASP.NET Core Runtime**, select **Hosting Bundle**. - .NET Desktop Runtime 6.0.9 or 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 - Select the version you require. Under **.NET Desktop Runtime**, select the appropriate download. - .NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 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.

2	To install the .NET dependencies, run each of the following commands using the PowerShell command prompt, waiting until each completes, before running the next command:
	For Windows Server 2016 and Windows Server 2019:
	`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`
	For Windows Server 2022:
	`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`
	Ensure the file name and file path match the files that were stored in step 1.

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

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

Install Blue Prism Hub

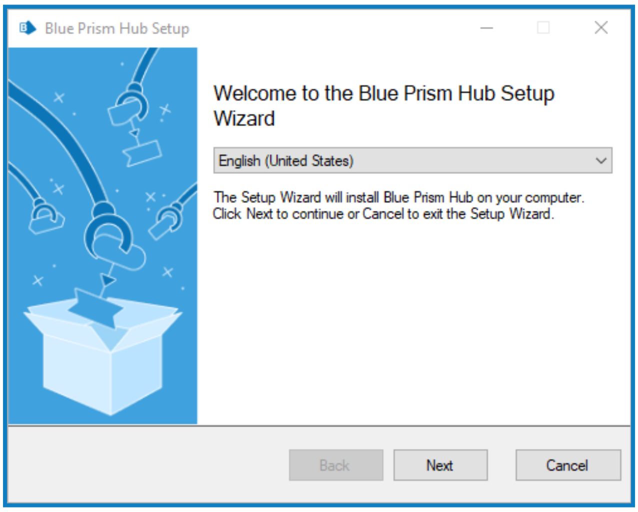
Before you install Blue Prism Hub:

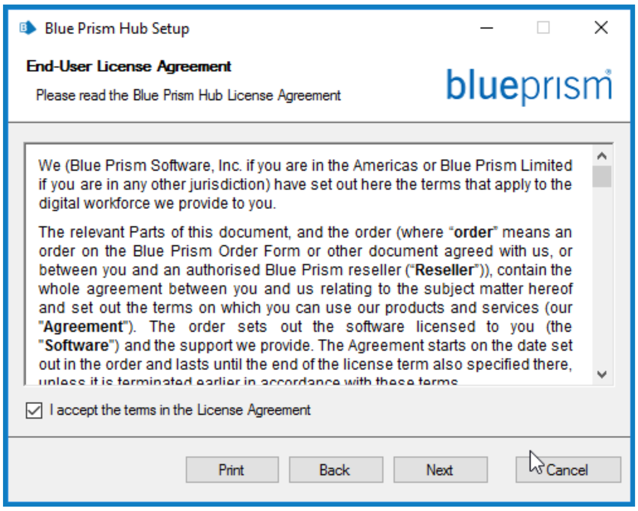
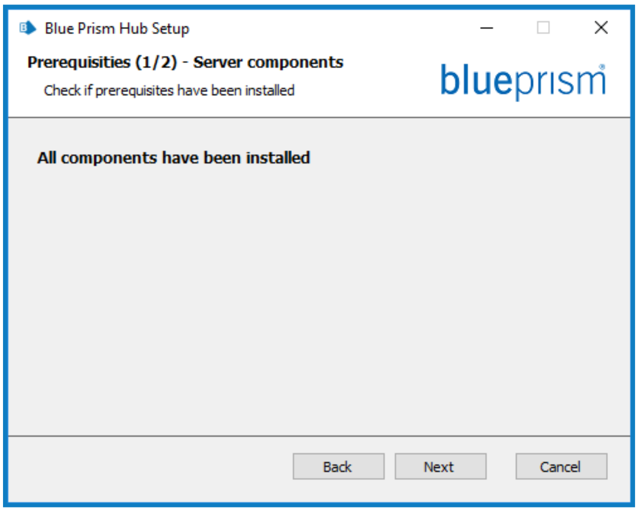
- If you have purchased ALM, Decision or Interact, you will need your Customer ID during this Hub installation. This can be found in the email that was sent to you when you purchased ALM, Decision or Interact.
- If you want to use the Blue Prism Decision plugin in Hub, you will need to install the Blue 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.

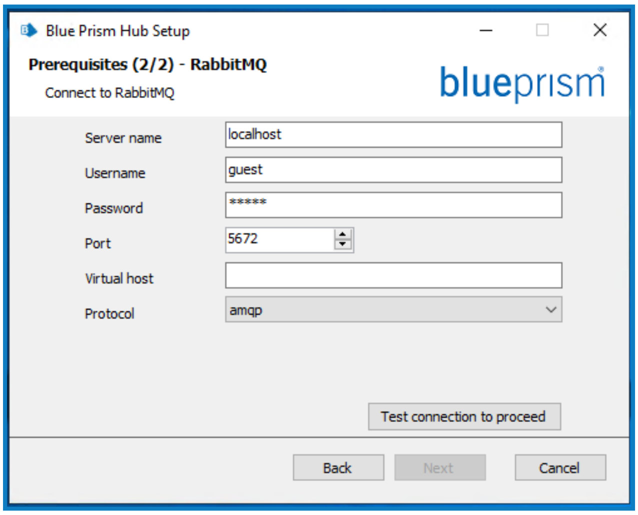
▶ To watch the Hub installation and configuration process, see our Blue Prism Hub installation video.

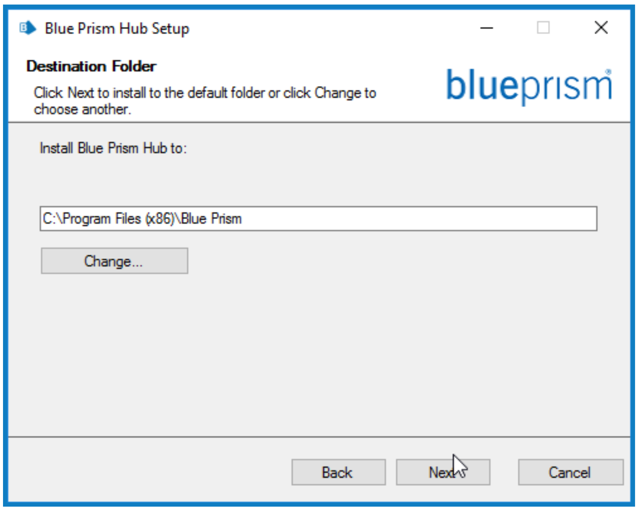
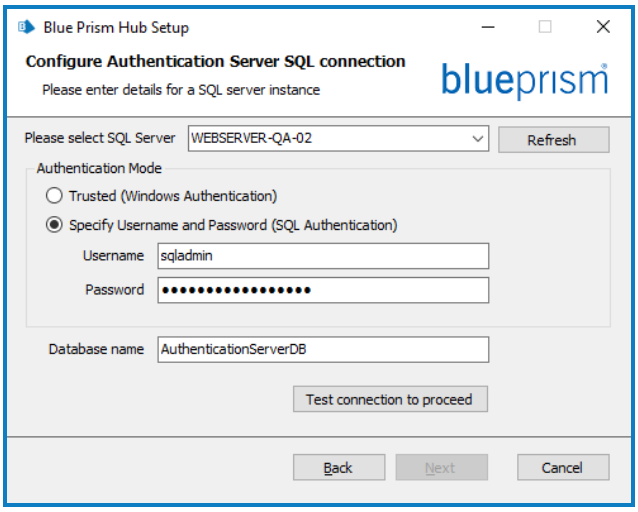
The steps below detail the process for installing the Blue Prism Hub software. This includes the Authentication Server, Hub, and other associated services. The installation process will create any new databases that are required.

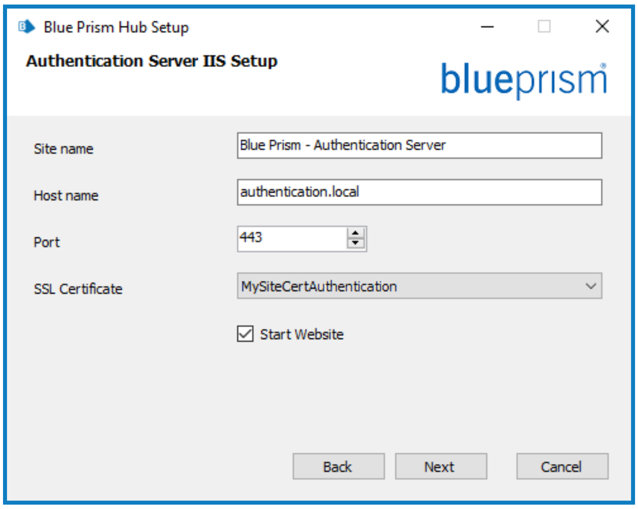
Download and run the Blue Prism Hub installer, available from the Blue Prism Portal, and progress through the installer as shown below. The installer must be run with administrator rights.

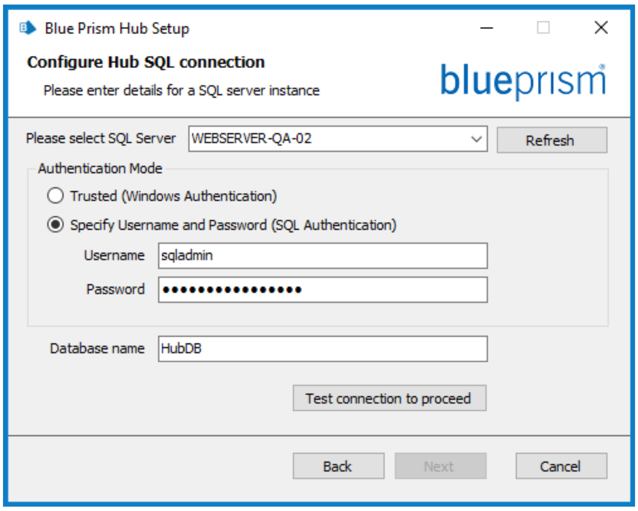
Step	Installer page	Details
1	 Blue Prism Hub Setup Welcome to the Blue Prism Hub Setup Wizard English (United States) The Setup Wizard will install Blue Prism Hub on your computer. Click Next to continue or Cancel to exit the Setup Wizard. 	**Welcome** If required, select another language for the installer from the drop-down list. The default language is English (United States). Click **Next**.

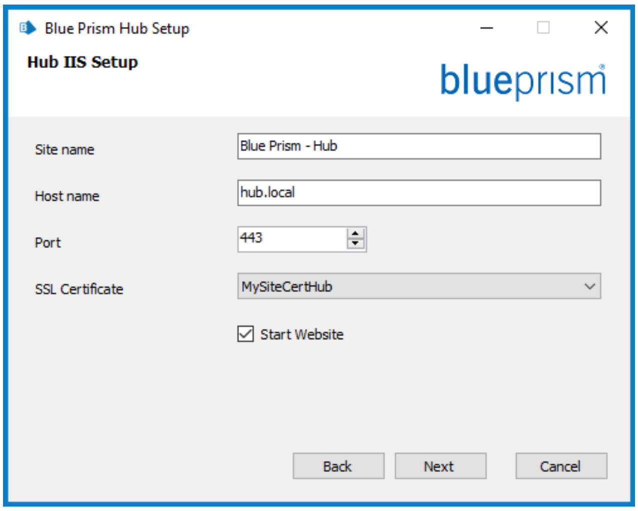
Step	Installer page	Details
2	 Blue Prism Hub Setup **End-User License Agreement** Please read the Blue Prism Hub License Agreement We (Blue Prism Software, Inc. if you are in the Americas or Blue Prism Limited if you are in any other jurisdiction) have set out here the terms that apply to the digital workforce we provide to you. The relevant Parts of this document, and the order (where "**order**" means an order on the Blue Prism Order Form or other document agreed with us, or between you and an authorised Blue Prism reseller ("**Reseller**")), contain the whole agreement between you and us relating to the subject matter hereof and set out the terms on which you can use our products and services (our "**Agreement**"). The order sets out the software licensed to you (the "**Software**") and the support we provide. The Agreement starts on the date set out in the order and lasts until the end of the license term also specified there, unless it is terminated earlier in accordance with these terms ☑ I accept the terms in the License Agreement 	**License agreement** Read the End-User License Agreement and if you agree to the terms, select the check box.
3	 Blue Prism Hub Setup **Prerequisities (1/2) - Server components** Check if prerequisites have been installed **All components have been installed** 	**Prerequisites 1 - Server components** The installer checks that the prerequisites have been installed. Those that are not installed are identified. You cannot proceed until all the prerequisites are installed. If there are uninstalled prerequisites, cancel the installer and install the missing components before restarting the installer. Otherwise, proceed with the installation.

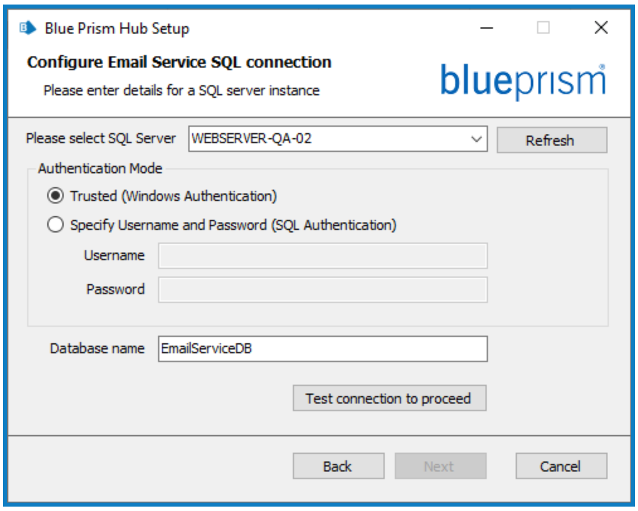
Step	Installer page	Details
4	 Blue Prism Hub Setup **Prerequisites (2/2) - RabbitMQ** Connect to RabbitMQ Server name: localhost Username: guest Password: ***** Port: 5672 Virtual host: Protocol: amqp blueprism Test connection to proceed Back Next Cancel	**Prerequisites 2 - RabbitMQ** Enter the server name or IP address of the Message Broker server and the credentials of the user you created. The default message queuing port is 5672. This should only be changed if the default ports have been changed by your IT support organization. By default, the **Virtual host** field is blank. You can leave this as blank and the connection will be made to the RabbitMQ root. Alternatively, if you have virtual hosts set up in RabbitMQ, you can connect to a specific host. In **Virtual host**, enter the name of the virtual host on RabbitMQ that you want to connect to. The virtual host must already exist on RabbitMQ, you cannot enter a new name as this installer will not create a new virtual host. Further information about virtual hosts can be found on the RabbitMQ website - Virtual Hosts. From the **Protocol** drop-down list, select the protocol you want to use. You can select either AMQP or AMQPS. If you select AMQPS, an additional field displays for you to enter the certificate that should be used for the connection. Further information about TLS configuration and certificates can be found on the RabbitMQ website - TLS Support. If you are using AMQPS, you will need to give the Blue Prism IIS application pools full control of the RabbitMQ certificate. For more information, see Troubleshoot a Hub installation on page 71. Click **Test connection** to verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

Step	Installer page	Details
5	 Blue Prism Hub Setup **Destination Folder** Click Next to install to the default folder or click Change to choose another. Install Blue Prism Hub to: C:\Program Files (x86)\Blue Prism 	**Destination folder** Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the **Change** button.
6	 Blue Prism Hub Setup **Configure Authentication Server SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: ••••••••••••••••• Database name: AuthenticationServerDB blueprism Refresh Test connection to proceed Back Next Cancel	**Authentication Server SQL connection** Configure the settings for the Authentication Server database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

Step	Installer page	Details
7	 **Authentication Server IIS Setup** Site name: Blue Prism - Authentication Server Host name: authentication.local Port: 443 SSL Certificate: MySiteCertAuthentication ☑ Start Website	**Authentication Server IIS setup** Configure IIS for the Authentication Server website. You need to: - Enter a site name. - Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. - Enter the port number. - Select the appropriate SSL certificate. - Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate. Once installation is complete, the IIS feature **Windows Authentication** is enabled on the Authentication Server website.

Step	Installer page	Details
8	 Blue Prism Hub Setup **Configure Hub SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 [Refresh] Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: •••••••••••••••• Database name: HubDB [Test connection to proceed] [Back] [Next] [Cancel]	**Hub SQL connection** Configure the settings for the Hub database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: • If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. • If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

Step	Installer page	Details
9	 Blue Prism Hub Setup **Hub IIS Setup** Site name: Blue Prism - Hub Host name: hub.local Port: 443 SSL Certificate: MySiteCertHub ☑ Start Website 	**Hub IIS setup** Configure the Hub website. You need to: • Enter a site name. • Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

<table>
<tr><th>Step</th><th>Installer page</th><th>Details</th></tr>
<tr>
<td>10</td>
<td>


Blue Prism Hub Setup

Configure Email Service SQL connection

Please enter details for a SQL server instance

Please select SQL Server: WEBSERVER-QA-02

Authentication Mode

● Trusted (Windows Authentication)

○ Specify Username and Password (SQL Authentication)

Username:

Password:

Database name: EmailServiceDB

</td>
<td>

Email Service SQL connection

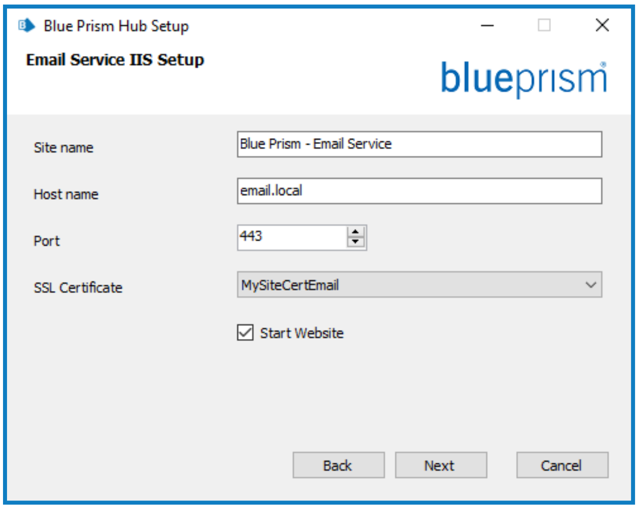
Configure the settings for the Email Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:

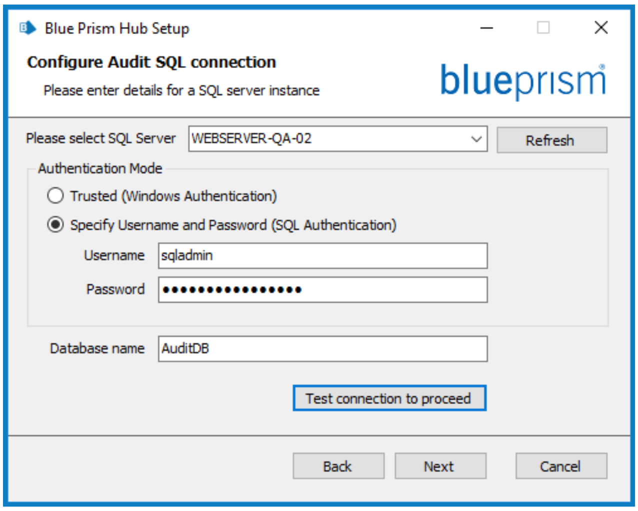
- If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information.
- If **SQL Authentication** is selected, enter the username and password.

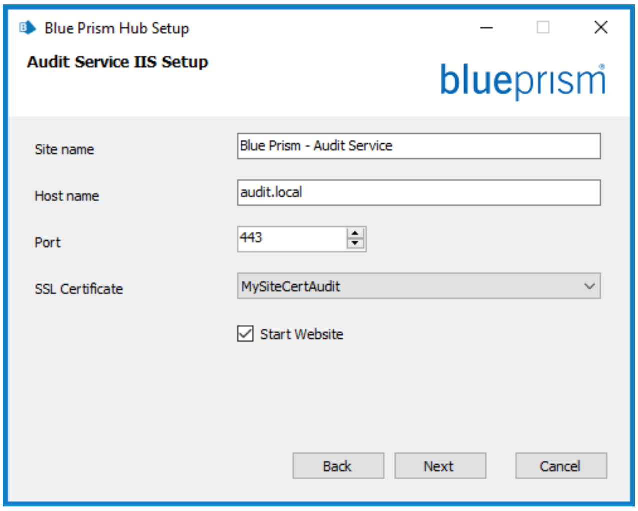
> ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.

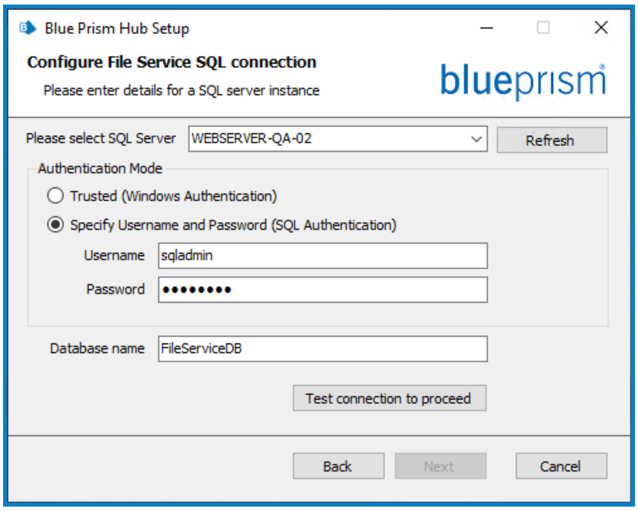
The database name can be left as the default value or changed as required.

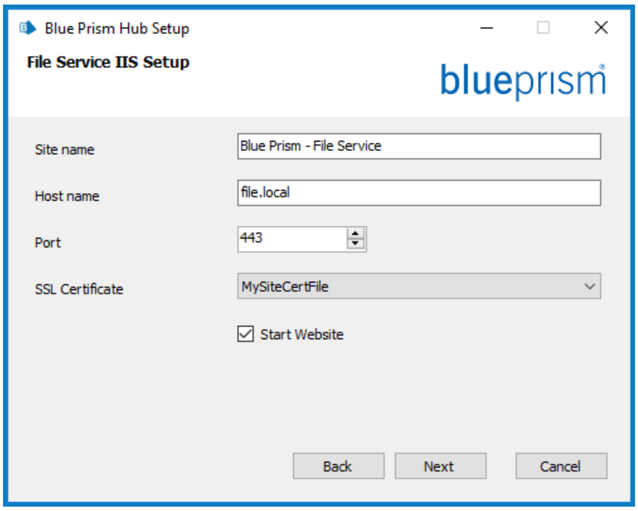
Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.
</td>
</tr>
</table>

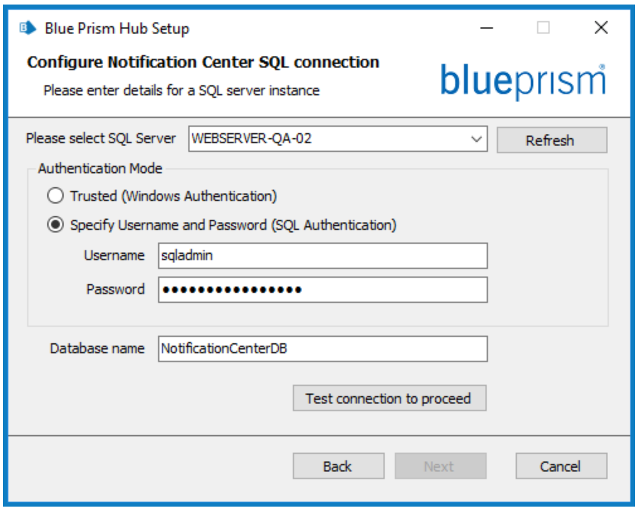
Step	Installer page	Details
11	 Blue Prism Hub Setup **Email Service IIS Setup** Site name: Blue Prism - Email Service Host name: email.local Port: 443 SSL Certificate: MySiteCertEmail ☑ Start Website 	**Email Service IIS setup** Configure the Email Service website. You need to: - Enter a site name. - Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. - Enter the port number. - Select the appropriate SSL certificate. - Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

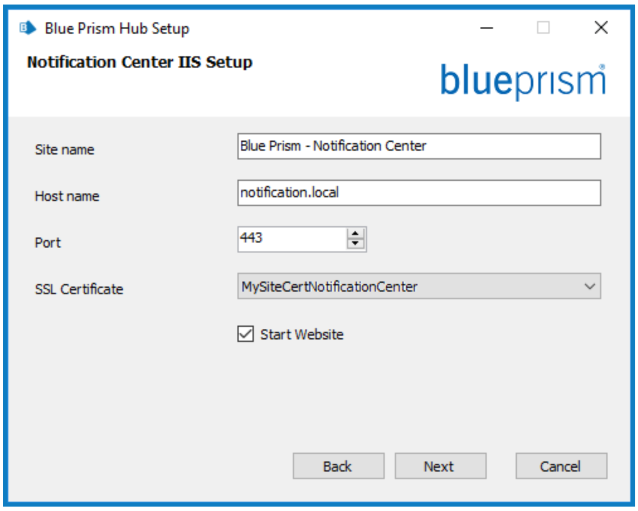
Step	Installer page	Details
12	 Blue Prism Hub Setup **Configure Audit SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: ●●●●●●●●●●●●●●●● Database name: AuditDB	**Audit SQL connection configuration** Configure the settings for the Audit database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

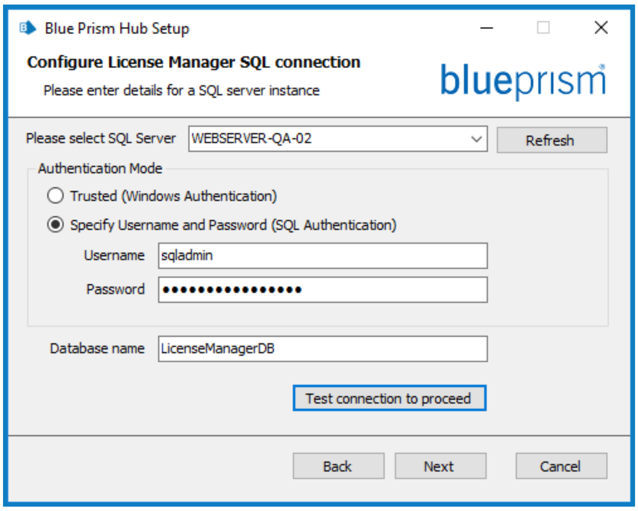
Step	Installer page	Details
13	 Blue Prism Hub Setup **Audit Service IIS Setup** Site name: Blue Prism - Audit Service Host name: audit.local Port: 443 SSL Certificate: MySiteCertAudit ☑ Start Website 	**Audit Service IIS setup** Configure the Audit Service website. You need to: - Enter a site name. - Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. - Enter the port number. - Select the appropriate SSL certificate. - Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

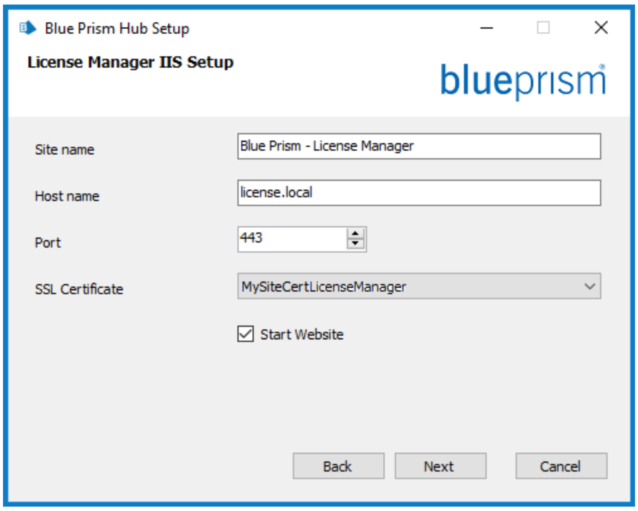
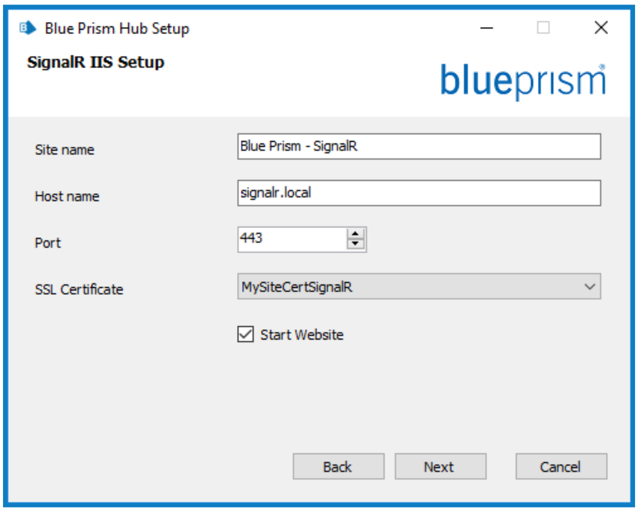
Step	Installer page	Details
14	 Blue Prism Hub Setup **Configure File Service SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: •••••••• Database name: FileServiceDB blueprism Refresh Test connection to proceed Back Next Cancel	**File Service SQL connection configuration** Configure the settings for the File Service database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

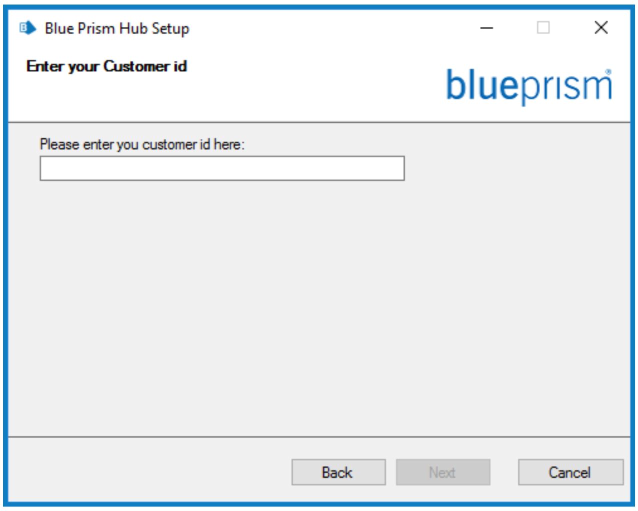
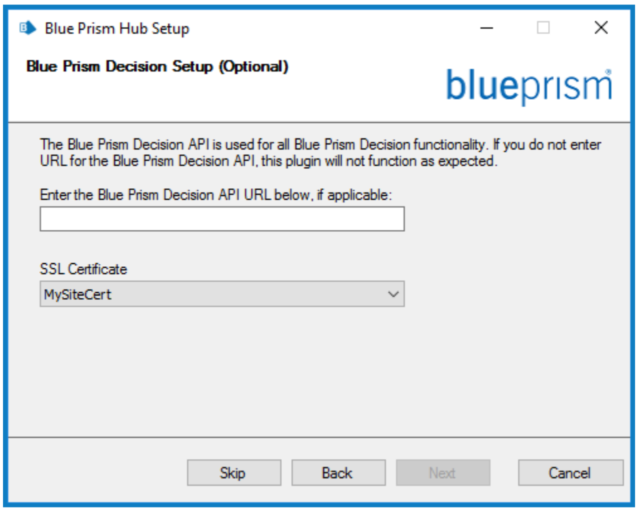
Step	Installer page	Details
15	 Blue Prism Hub Setup **File Service IIS Setup** Site name: Blue Prism - File Service Host name: file.local Port: 443 SSL Certificate: MySiteCertFile ☑ Start Website 	**File Service IIS setup** Configure the File Service website. You need to: • Enter a site name. • Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

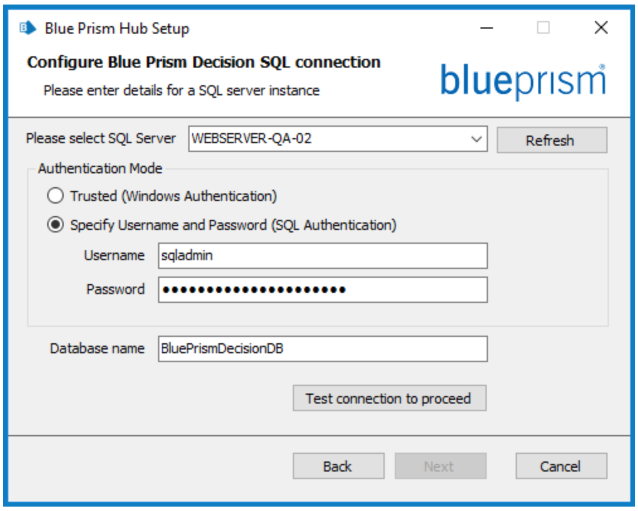
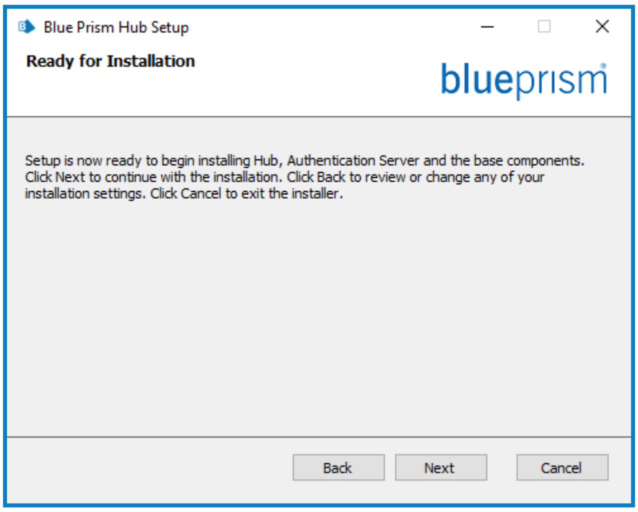
Step	Installer page	Details
16	 Blue Prism Hub Setup **Configure Notification Center SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: •••••••••••••••• Database name: NotificationCenterDB blueprism Refresh Test connection to proceed Back Next Cancel	**Notification Center SQL connection** Configure the settings for the Notification Center database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

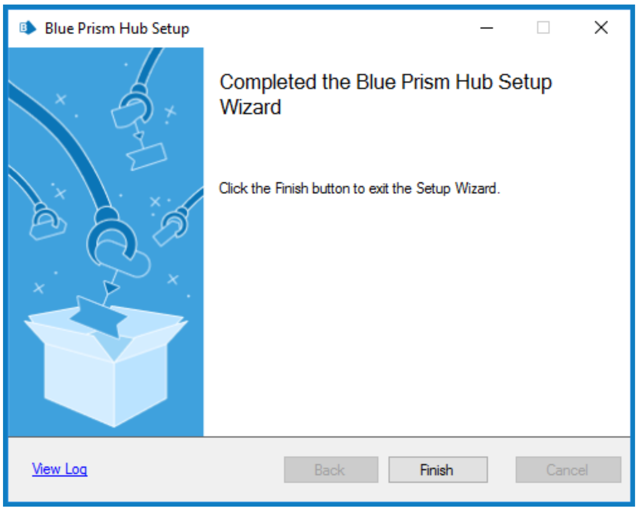
Step	Installer page	Details
17	 Blue Prism Hub Setup **Notification Center IIS Setup** Site name: Blue Prism - Notification Center Host name: notification.local Port: 443 SSL Certificate: MySiteCertNotificationCenter ☑ Start Website Back Next Cancel	**Notification Center IIS setup** Configure the Notification Center website. You need to: • Enter a site name. • Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. • Enter the port number. • Select the appropriate SSL certificate. • Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

Step	Installer page	Details
18	 Blue Prism Hub Setup **Configure License Manager SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 [Refresh] Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: ●●●●●●●●●●●●●●●● Database name: LicenseManagerDB [Test connection to proceed] [Back] [Next] [Cancel]	**License Manager SQL connection** Configure the settings for the License Manager database by providing the SQL Server host name or IP address, and the credentials for the account to create the database: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.

Step	Installer page	Details
19	 Blue Prism Hub Setup **License Manager IIS Setup** Site name: Blue Prism - License Manager Host name: license.local Port: 443 SSL Certificate: MySiteCertLicenseManager ☑ Start Website 	**License Manager IIS setup** Configure the License Manager website. You need to: - Enter a site name. - Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. - Enter the port number. - Select the appropriate SSL certificate. - Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.
20	 Blue Prism Hub Setup **SignalR IIS Setup** Site name: Blue Prism - SignalR Host name: signalr.local Port: 443 SSL Certificate: MySiteCertSignalR ☑ Start Website 	**SignalR IIS setup** Configure the SignalR website. You need to: - Enter a site name. - Enter a host name - This will be used as the URL for the site. Ensure that you consider your DNS and Domain structure when choosing a host name. - Enter the port number. - Select the appropriate SSL certificate. - Leave **Start Website** selected, unless you do not want the website to automatically start at the end of the installation. The **Next** button is only activated if the URL you have entered matches the one configured in the certificate.

Step	Installer page	Details
21	 Blue Prism Hub Setup **Enter your Customer id** Please enter you customer id here: 	**Enter your Customer Id** Enter your customer identifier. This identifier is supplied to you by Blue Prism when you receive your product license for ALM or Interact. If you have not purchased a licensed plugin, you can enter your own value. If you later purchase a licensed plug, your customer ID will need to be changed within the configuration file. For more information, see Troubleshoot a Hub installation on page 71.
22	 Blue Prism Hub Setup **Blue Prism Decision Setup (Optional)** The Blue Prism Decision API is used for all Blue Prism Decision functionality. If you do not enter URL for the Blue Prism Decision API, this plugin will not function as expected. Enter the Blue Prism Decision API URL below, if applicable: SSL Certificate MySiteCert 	**Blue Prism Decision Setup (Optional)** If you want to use Blue Prism Decision, you need to: • Enter the URL for the Blue Prism Decision Model Service container followed by the port number. The URL should be in the format https://<FQDN>:<port number>, for example, https://decision.blueprism.com:50051. 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 Install Blue Prism Decision. • Select the appropriate SSL Certificate. If you do not want to use Blue Prism Decision, click **Skip**. The Ready for Installation screen displays.

Step	Installer page	Details
23	 Blue Prism Hub Setup **Configure Blue Prism Decision SQL connection** Please enter details for a SQL server instance Please select SQL Server: WEBSERVER-QA-02 Authentication Mode ○ Trusted (Windows Authentication) ● Specify Username and Password (SQL Authentication) Username: sqladmin Password: •••••••••••••••••••• Database name: BluePrismDecisionDB blueprism Refresh Test connection to proceed Back Next Cancel	**Blue Prism Decision SQL connection** 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: - If **Windows Authentication** is selected, the account must have the appropriate permissions. See Installing using Windows Authentication on page 58 for further information. - If **SQL Authentication** is selected, enter the username and password. ⚠ You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database. The database name can be left as the default value or changed as required. Click **Test connection to proceed** to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot a Hub installation on page 71 for further details.
24	 Blue Prism Hub Setup **Ready for Installation** Setup is now ready to begin installing Hub, Authentication Server and the base components. Click Next to continue with the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the installer. 	**Ready for Installation** Click **Next** to install Hub.

Step	Installer page	Details
25	 Blue Prism Hub Setup Completed the Blue Prism Hub Setup Wizard Click the Finish button to exit the Setup Wizard. 	**Installation complete** If the installation fails, the **View Log** option gives details of the error that was encountered. For more information, see Troubleshoot a Hub installation on page 71.

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.

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 18.
- Permissions for the required certificates.
- Ownership over the IIS Application Pool.
- Ownership over the Windows services installed by Hub.

⚠ 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:

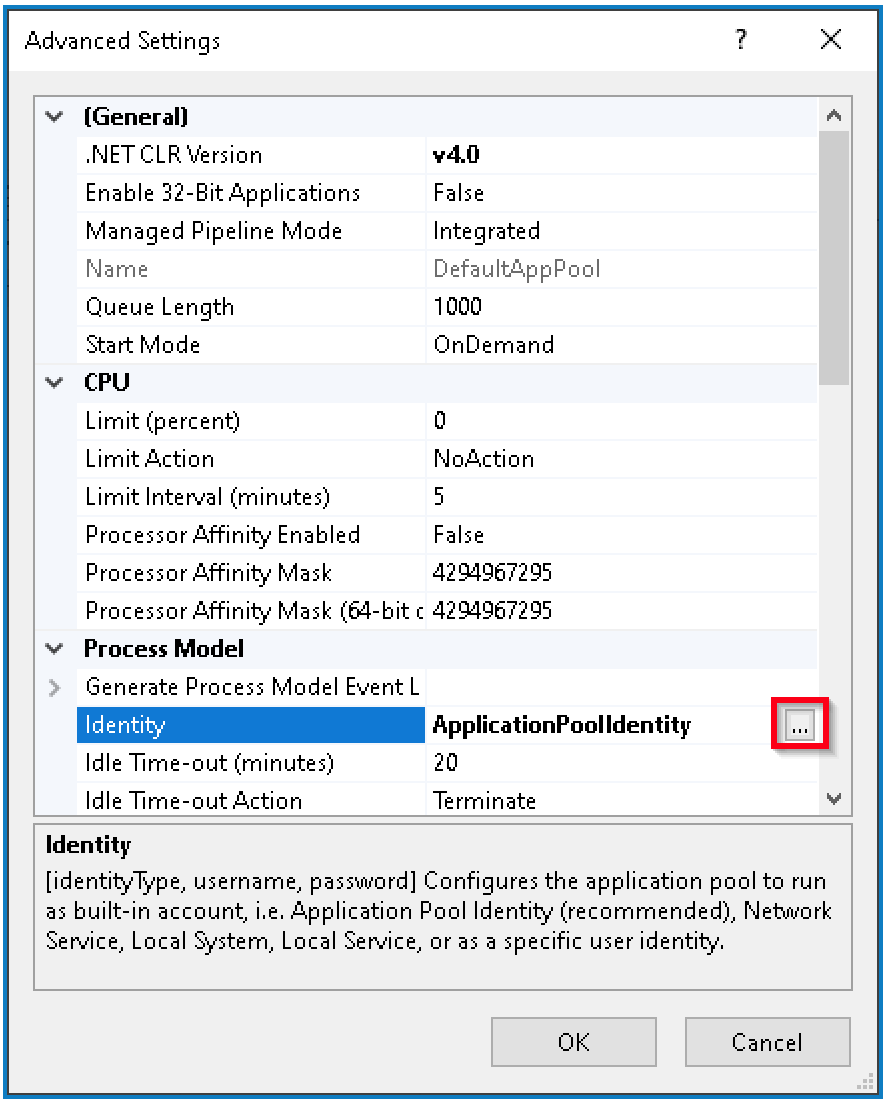
1. On the web server, open Internet Information Services (IIS) Manager.
2. In the Connections panel, expand the host and select **Application Pools**.
3. Review the **Identity** column values.

   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.

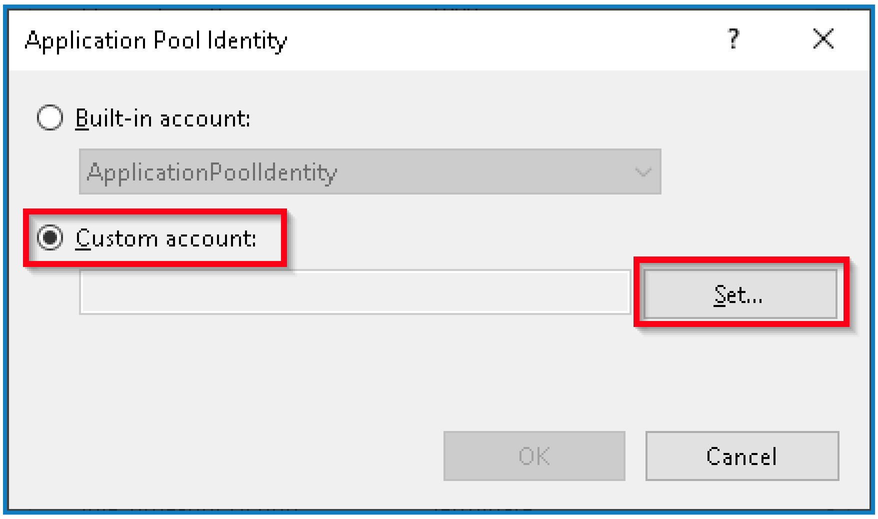
5. Select the **Identity** setting then click the **...** (ellipsis) button:



(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

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.

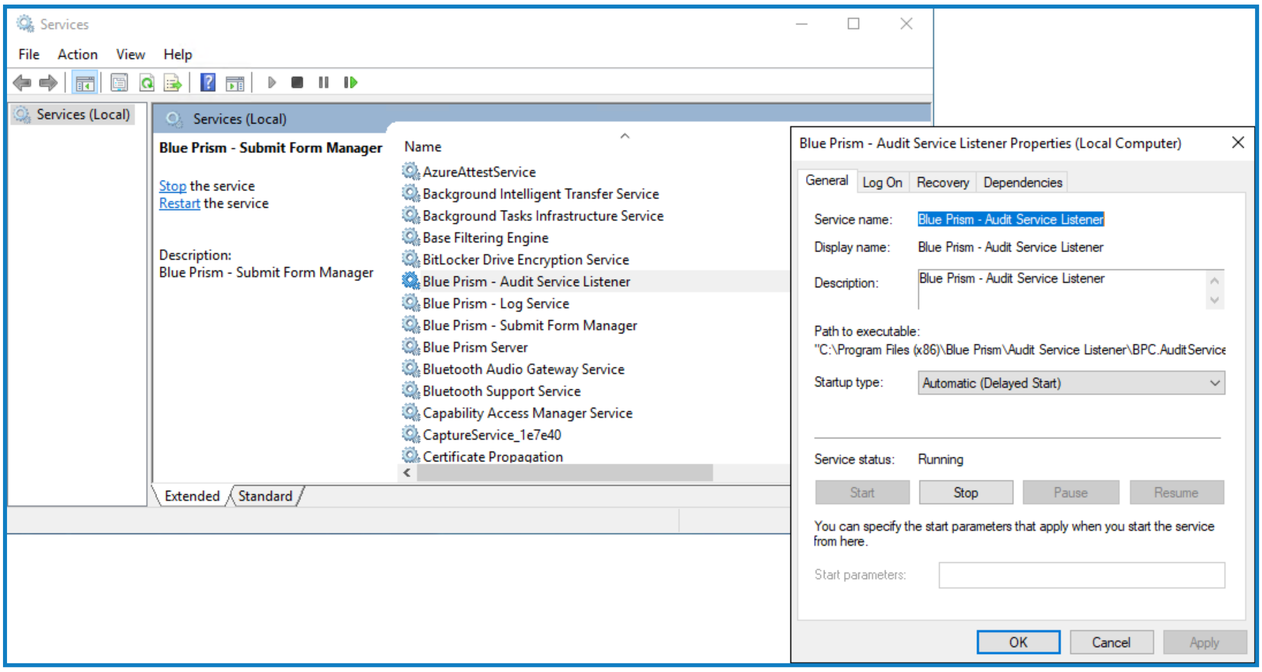
Assigning a Windows service account to a service

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

- Blue Prism - Audit Service Listener
- Blue Prism - Log Service

To do this:

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



Blue Prism - Submit Form Manager

Stop the service
Restart the service

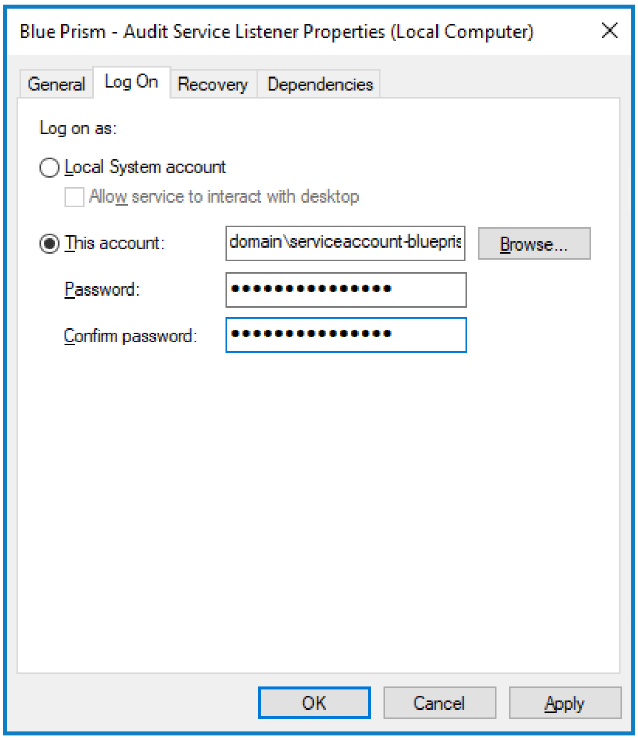
Description:
Blue Prism - Submit Form Manager

Name
AzureAttestService
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BitLocker Drive Encryption Service
Blue Prism - Audit Service Listener
Blue Prism - Log Service
Blue Prism - Submit Form Manager
Blue Prism Server
Bluetooth Audio Gateway Service
Bluetooth Support Service
Capability Access Manager Service
CaptureService_1e7e40
Certificate Propagation

Blue Prism - Audit Service Listener Properties (Local Computer)

Service name: Blue Prism - Audit Service Listener
Display name: Blue Prism - Audit Service Listener
Description: Blue Prism - Audit Service Listener
Path to executable:
"C:\Program Files (x86)\Blue Prism\Audit Service Listener\BPC.AuditService
Startup type: Automatic (Delayed Start)
Service status: Running
You can specify the start parameters that apply when you start the service from here.
Start parameters:

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.



Blue Prism - Audit Service Listener Properties (Local Computer)

Log on as:
○ Local System account
□ Allow service to interact with desktop
● This account: domain\serviceaccount-bluepris
Password: •••••••••••••••
Confirm password: •••••••••••••••

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

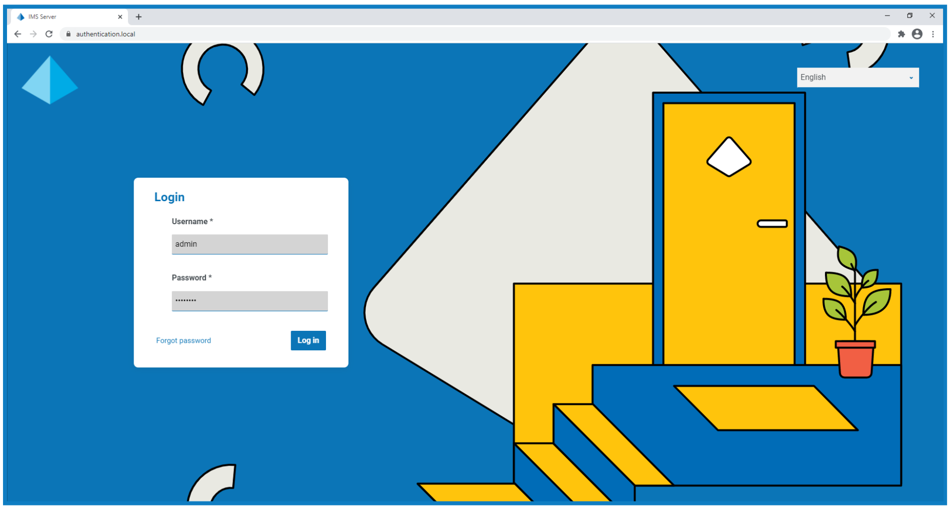
⚠ If you intend to use Blue Prism Interact, install Interact before you carry out this configuration. For more information, see the Interact install guide.

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.

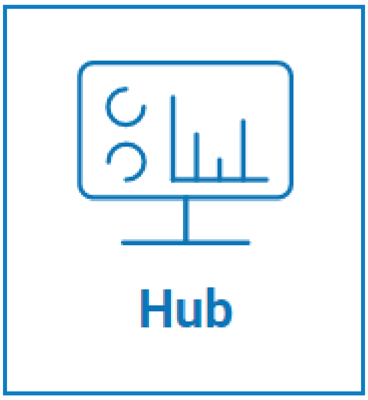
1. Launch a browser and go to the Authentication Server website, in our example: https://authentication.local



Username * admin

Password * ••••••••

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 58.

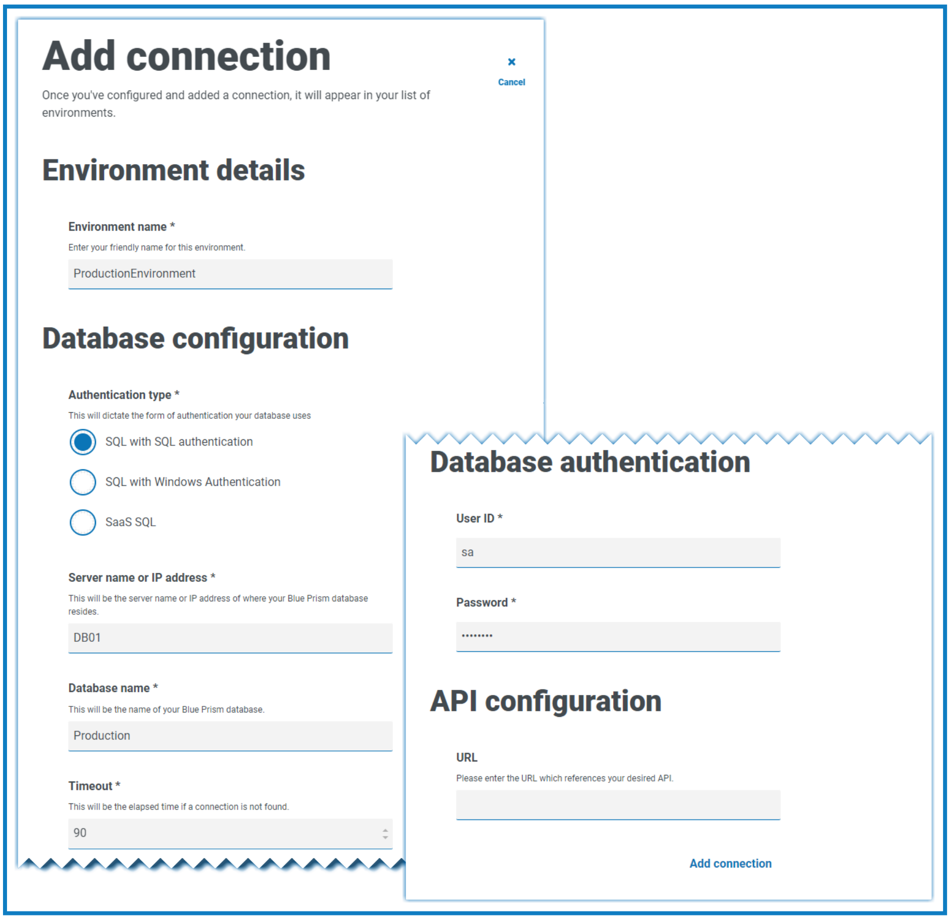
SSL encryption is used by all the databases installed as part of the Hub installer. For Hub to connect successfully to the Blue Prism database, the Blue Prism database must also be configured to use SSL encryption. For more information, see Prerequisites on page 9.

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:



Add connection

Once you've configured and added a connection, it will appear in your list of environments.

Environment details

Environment name *
Enter your friendly name for this environment.
ProductionEnvironment

Database configuration

Authentication type *
This will dictate the form of authentication your database uses
● SQL with SQL authentication
○ SQL with Windows Authentication
○ SaaS SQL

Server name or IP address *
This will be the server name or IP address of where your Blue Prism database resides.
DB01

Database name *
This will be the name of your Blue Prism database.
Production

Timeout *
This will be the elapsed time if a connection is not found.
90

Database authentication

User ID *
sa

Password *
••••••••

API configuration

URL
Please enter the URL which references your desired API.

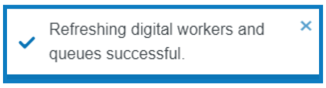
The Timeout value is in seconds.

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.



✓ Refreshing digital workers and queues successful.

   If the message does not display, see Troubleshoot a Hub installation on page 71 for more information.

Create an administrator

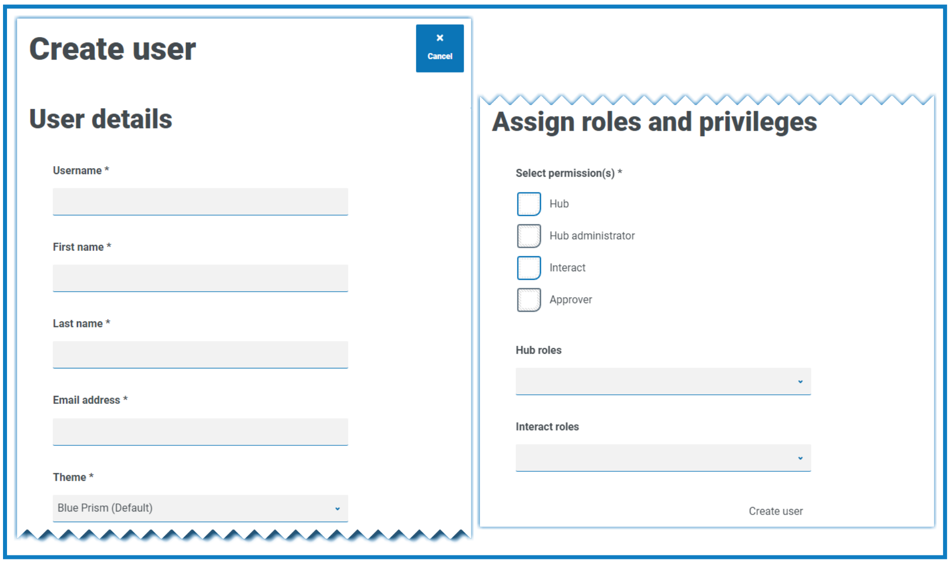
You will need to create an administrator account with valid information to finish the Hub configuration. You should not use the generic admin account to complete the configuration, this is because:

- 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.

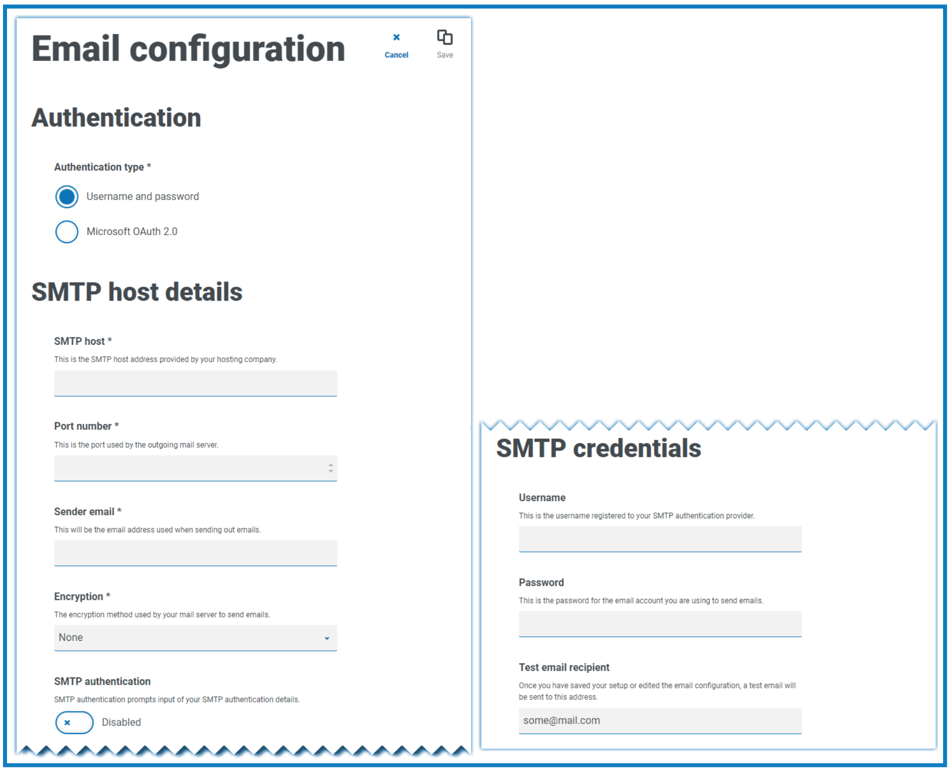
> If you are using Microsoft OAuth 2.0, the Mail.Send permission in Azure Active Directory must be enabled. This is found in the API Permission tab under the application properties in Azure Active Directory. For more information, see Troubleshoot a Hub installation on page 71.

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:



Email configuration

Authentication

Authentication type *

● Username and password

○ Microsoft OAuth 2.0

SMTP host details

SMTP host *
This is the SMTP host address provided by your hosting company.

Port number *
This is the port used by the outgoing mail server.

Sender email *
This will be the email address used when sending out emails.

Encryption *
The encryption method used by your mail server to send emails.
None

SMTP authentication
SMTP authentication prompts input of your SMTP authentication details.
Disabled

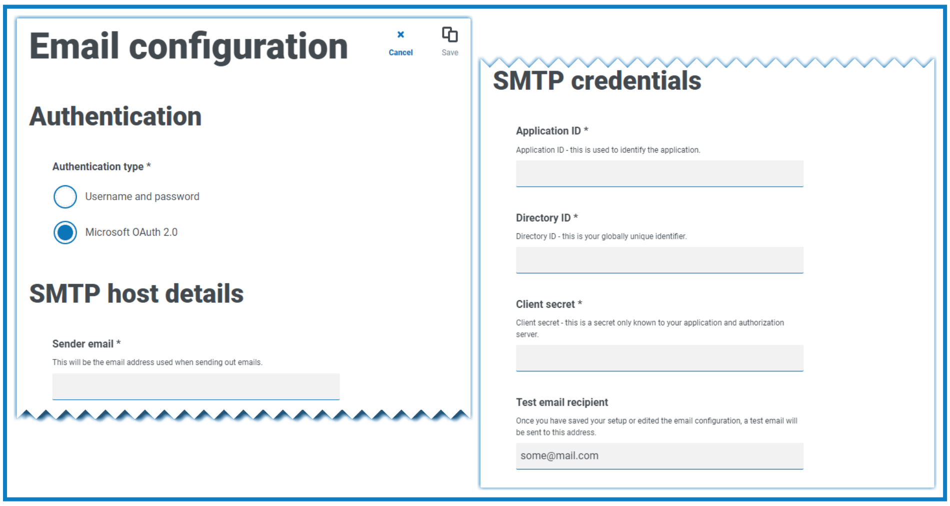
SMTP credentials

Username
This is the username registered to your SMTP authentication provider.

Password
This is the password for the email account you are using to send emails.

Test email recipient
Once you have saved your setup or edited the email configuration, a test email will be sent to this address.
some@mail.com

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



Email configuration

Authentication

Authentication type *

○ Username and password

● Microsoft OAuth 2.0

SMTP host details

Sender email *
This will be the email address used when sending out emails.

SMTP credentials

Application ID *
Application ID - this is used to identify the application.

Directory ID *
Directory ID - this is your globally unique identifier.

Client secret *
Client secret - this is a secret only known to your application and authorization server.

Test email recipient
Once you have saved your setup or edited the email configuration, a test email will be sent to this address.
some@mail.com

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 71 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.

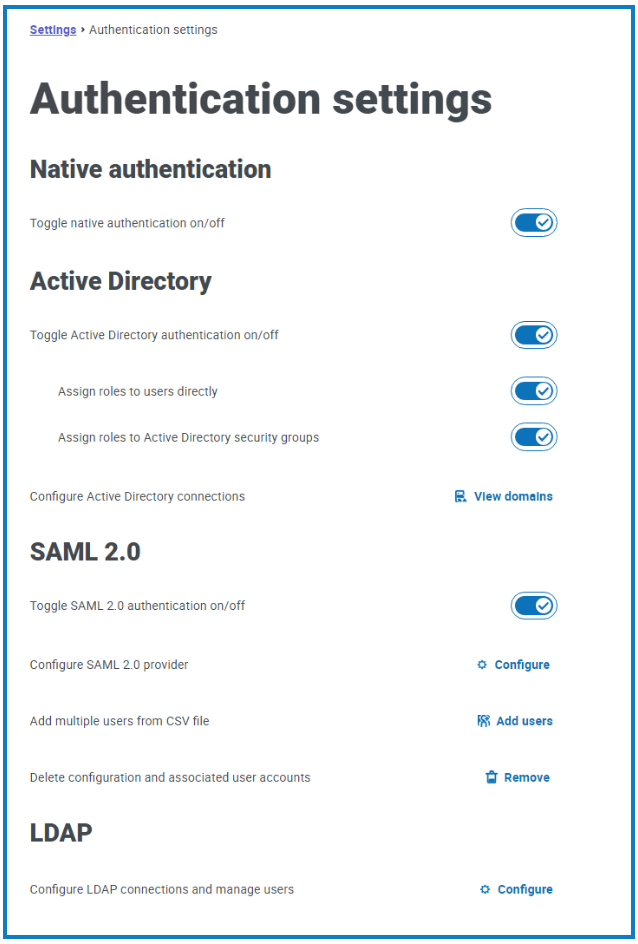
Authentication settings

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.

   Settings › Authentication settings

   # Authentication settings

   ## Native authentication

   Toggle native authentication on/off ☑

   ## Active Directory

   Toggle Active Directory authentication on/off ☑

   Assign roles to users directly ☑

   Assign roles to Active Directory security groups ☑

   Configure Active Directory connections — View domains

   ## SAML 2.0

   Toggle SAML 2.0 authentication on/off ☑

   Configure SAML 2.0 provider — Configure

   Add multiple users from CSV file — Add users

   Delete configuration and associated user accounts — Remove

   ## LDAP

   Configure LDAP connections and manage users — Configure

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.

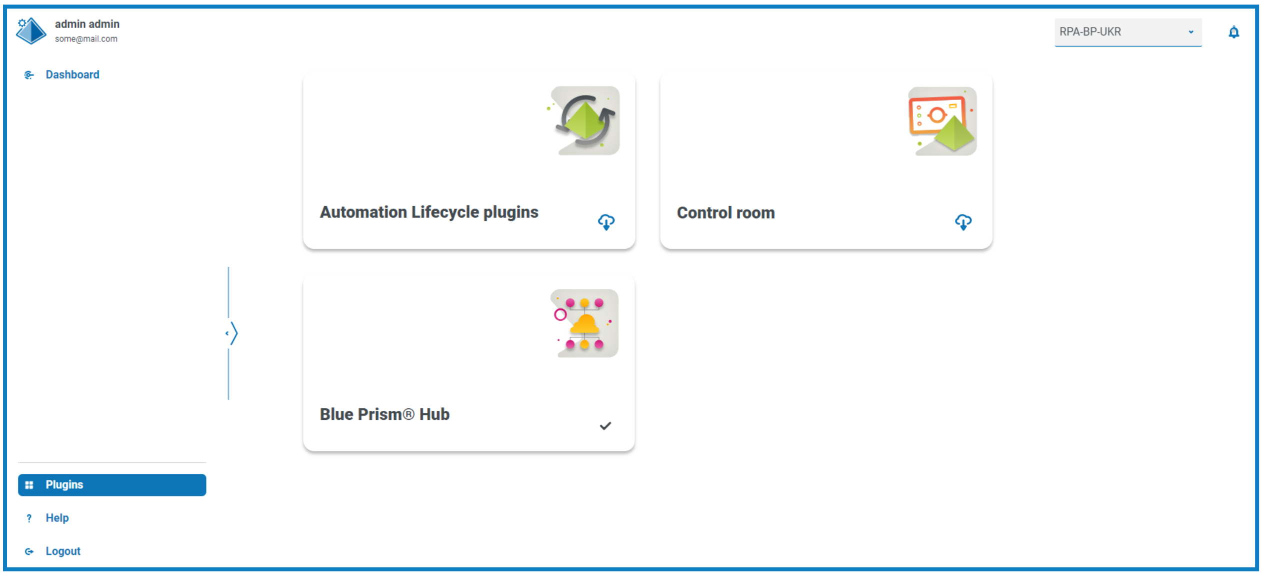
For more information about configuring authentication settings, see the Hub Administrator Guide.

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.

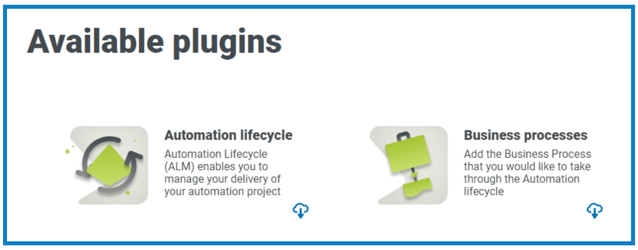
To watch this installation step, see our Business Processes plugin installation video.

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



3. Click **Automation lifecycle**.

   The available plugin components display.



Available plugins

Automation lifecycle
Automation Lifecycle (ALM) enables you to manage your delivery of your automation project

Business processes
Add the Business Process that you would like to take through the Automation lifecycle

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

   The site restarts.

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:

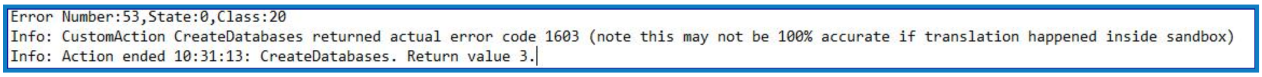
- If the database exists:
  - That it can be connected to.
  - That the SQL Server hosting the database has a valid certificate applied.
  - That the account has the rights to read, write and edit the database.
- If the database does not exist:
  - That the account has the right to create the database.
  - 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 Prerequisites on page 9.
- 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 9.

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:

   ```
   iis apppool\Blue Prism - Audit Service;
   iis apppool\Blue Prism - Authentication Server;
   iis apppool\Blue Prism - Email Service;
   iis apppool\Blue Prism - File Service;
   iis apppool\Blue Prism - Hub;
   iis apppool\Blue Prism - License Manager;
   iis apppool\Blue Prism - Notification Center;
   iis apppool\Blue Prism - SignalR;
   ```

   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.

> If you are also installing Interact, you will also need to do this for the application pools created during the Interact installation. For more information, see the Interact Install Guide.

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.

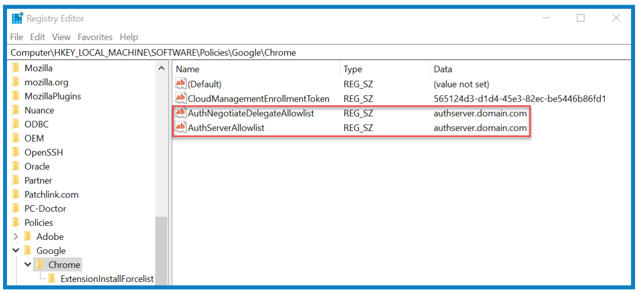
Configure browsers for Integrated Windows Authentication

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**.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome

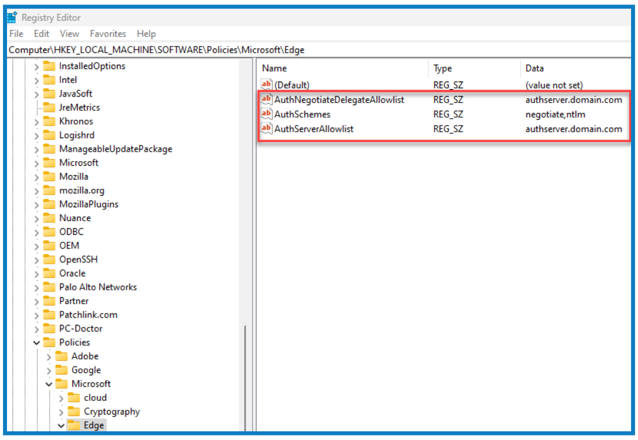
Name	Type	Data
(Default)	REG_SZ	(value not set)
CloudManagementEnrollmentToken	REG_SZ	565124d3-d1d4-45e3-82ec-be5446b86fd1
AuthNegotiateDelegateAllowlist	REG_SZ	authserver.domain.com
AuthServerAllowlist	REG_SZ	authserver.domain.com

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**.
6. 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**.
7. 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.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge

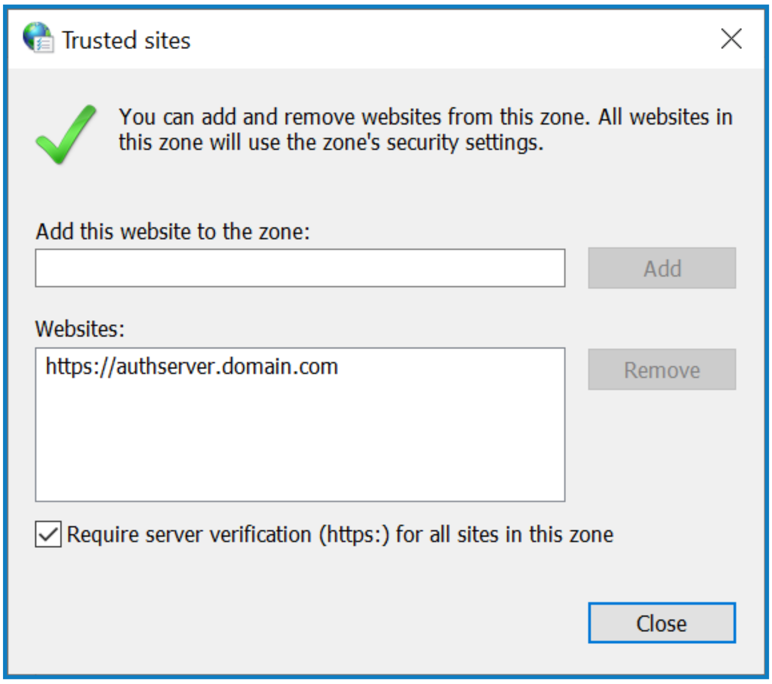
Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthNegotiateDelegateAllowlist	REG_SZ	authserver.domain.com
AuthSchemes	REG_SZ	negotiate,ntlm
AuthServerAllowlist	REG_SZ	authserver.domain.com

Alternatively, you can follow these steps for Microsoft Edge:

1. Close any open instances of Edge.
2. Navigate to **Control Panel** > **Network and Internet** > **Internet Options**.
3. On the Advanced tab, under Security, select **Enable Integrated Windows Authentication**.
4. On the Security tab, click **Trusted Sites** > **Sites**.

5. 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.



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

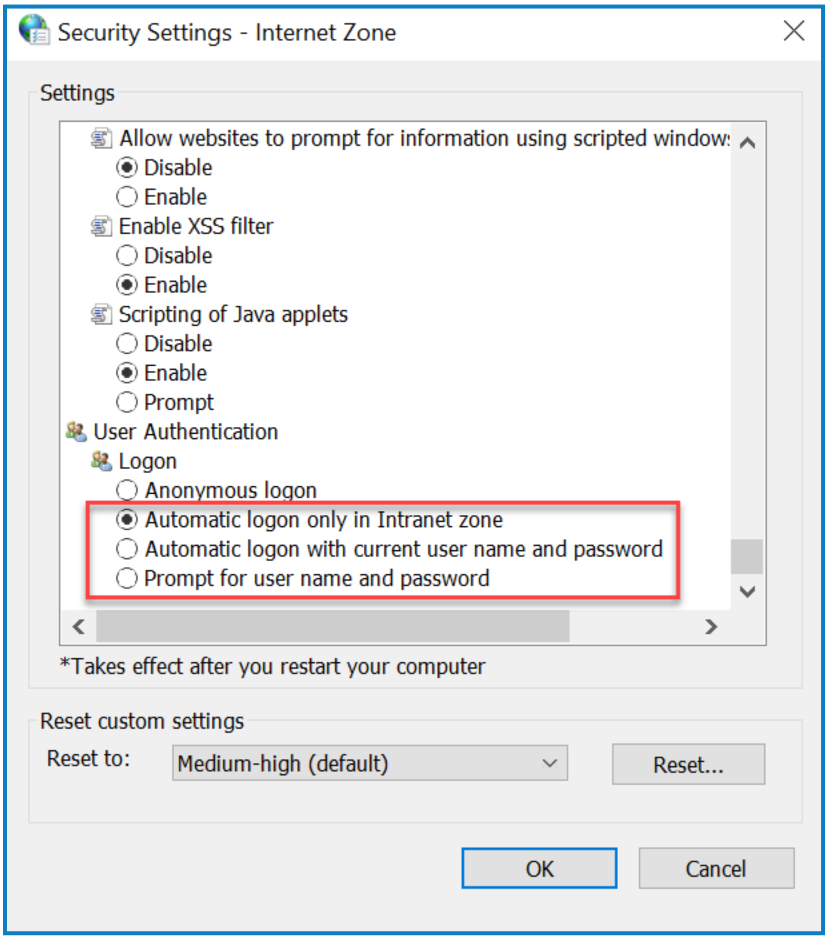
Add this website to the zone:

Websites:
https://authserver.domain.com

☑ Require server verification (https:) for all sites in this zone

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.



Security Settings - Internet Zone

Settings

- Allow websites to prompt for information using scripted window:
  - ● Disable
  - ○ Enable
- Enable XSS filter
  - ○ Disable
  - ● Enable
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt
- User Authentication
  - Logon
    - ○ Anonymous logon
    - ● Automatic logon only in Intranet zone
    - ○ Automatic logon with current user name and password
    - ○ Prompt for user name and password

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium-high (default)

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 `Klist 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

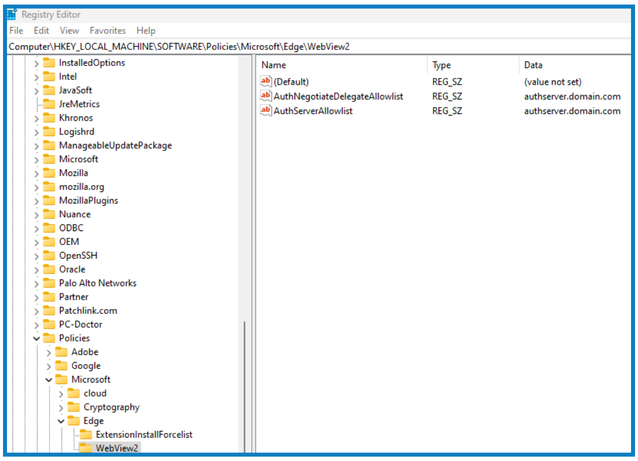
If your organization is only set up for Kerberos authentication, and Authentication Server is also used to log into Blue Prism Enterprise, a registry key for the Microsoft Edge WebView2 browser must be added:

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**.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\WebView2

Name	Type	Data
(Default)	REG_SZ	(value not set)
AuthNegotiateDelegateAllowlist	REG_SZ	authserver.domain.com
AuthServerAllowlist	REG_SZ	authserver.domain.com

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 on page 19.
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.

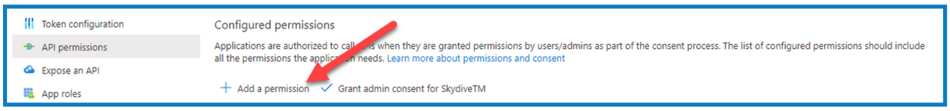
The web server must start up after the RabbitMQ services have all started. If the web server services start before the RabbitMQ service is ready, then going into the SMTP settings in Hub will result in a ‘something went wrong’ message.

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:

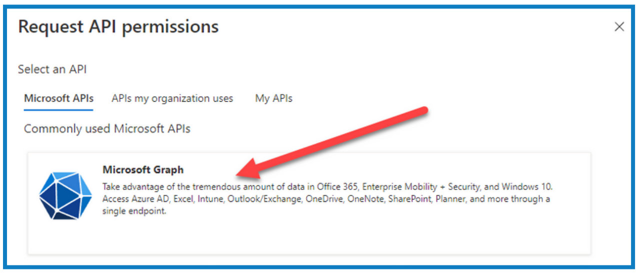
1. In Azure Active Directory, open the application properties for the application that you are linking Hub to.
2. Click **API permissions**.
3. Click **Add a permission**.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

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


Request API permissions

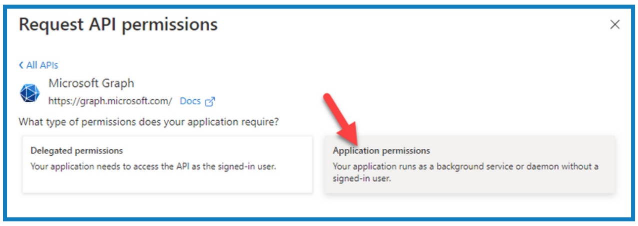
Select an API

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

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


Request API permissions

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions

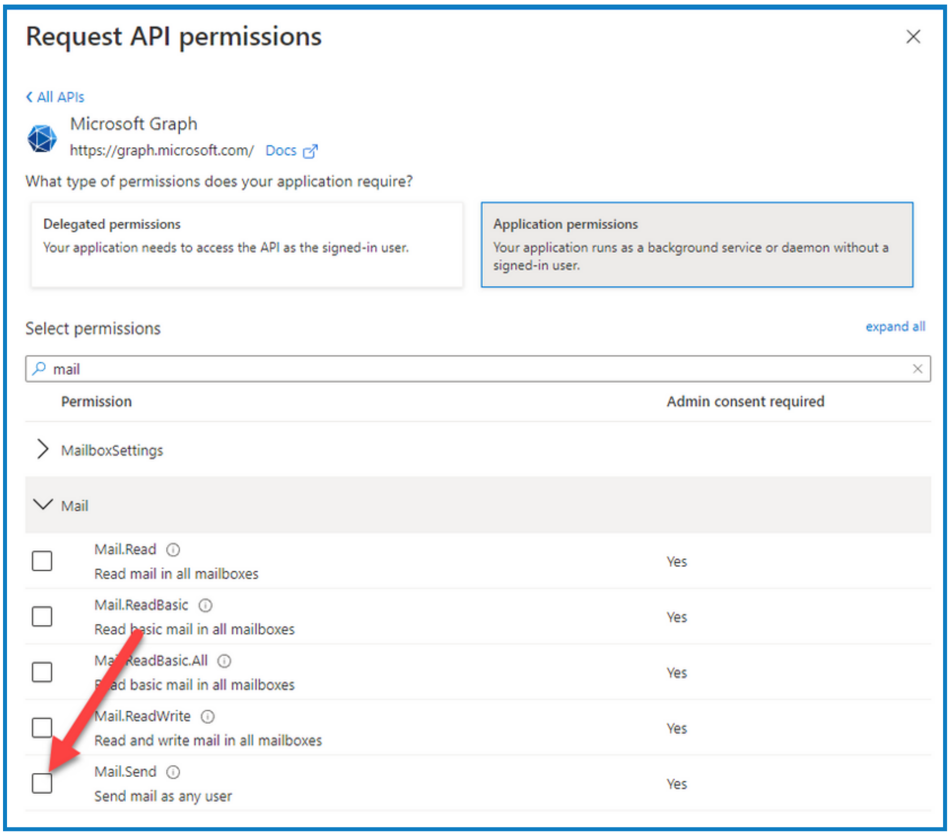
Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

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**.



Request API permissions

‹ All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

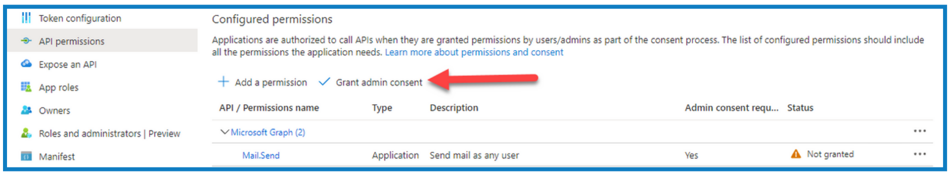
Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

mail

Permission	Admin consent required
› MailboxSettings	
⌄ Mail	
□ Mail.Read ⓘ Read mail in all mailboxes	Yes
□ Mail.ReadBasic ⓘ Read basic mail in all mailboxes	Yes
□ Mail.ReadBasic.All ⓘ Read basic mail in all mailboxes	Yes
□ Mail.ReadWrite ⓘ Read and write mail in all mailboxes	Yes
□ Mail.Send ⓘ Send mail as any user	Yes

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



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
⌄ Microsoft Graph (2)				
Mail.Send	Application	Send mail as any user	Yes	⚠ Not granted

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"
}
```

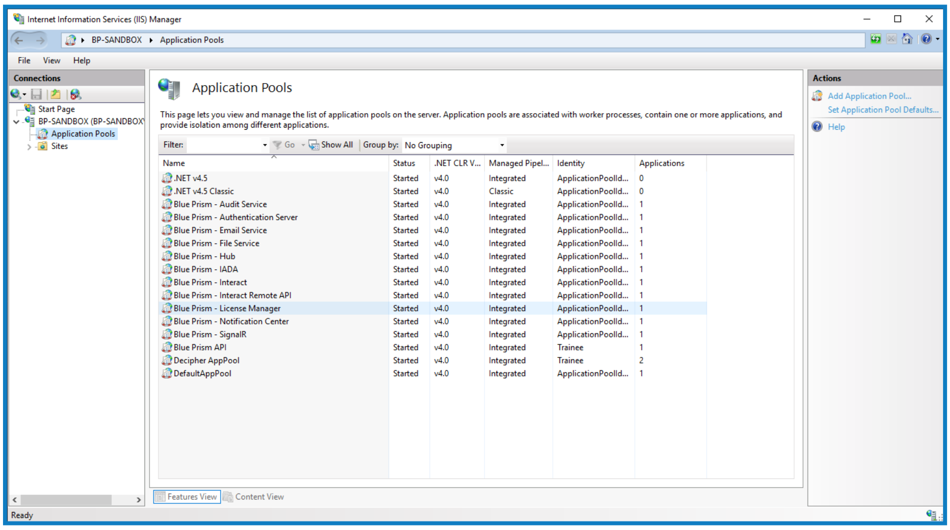
4. Save the file.

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.



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: Go Show All Group by: No Grouping

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
Blue Prism - Audit Service	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Authentication Server	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Email Service	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - File Service	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Hub	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - IADA	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Interact	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Interact Remote API	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - License Manager	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - Notification Center	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism - SignalR	Started	v4.0	Integrated	ApplicationPoolId...	1
Blue Prism API	Started	v4.0	Integrated	Trainee	1
Decipher AppPool	Started	v4.0	Integrated	Trainee	2
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	1

The License Manager restarts.

Uninstall Hub

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

To completely uninstall Hub 4.7, you need to:

1. Stop the Application Pools using IIS.
2. Remove Hub using the Programs and Features application.
3. Remove the IIS websites and Application Pools.
4. Remove the hosts.
5. Remove the databases.
6. Remove RabbitMQ data.
7. Remove the certificates.
8. 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 Hub websites on page 19.

Remove Hub using Programs and Features

> If you have also installed Interact, you will need uninstall it first using these steps by selecting Blue Prism Interact in step 3.

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 Hub.
4. Click **Uninstall**.
5. Confirm that you want to continue with the uninstall.

Remove IIS websites and Application Pools

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, expand the **Sites** node and remove the sites that still remain after removing Hub:
   - Blue Prism - License Manager.
   - Blue Prism - Notification Center.
3. In the **Connections** pane, expand the **Application Pools** node and remove the pools that still remain after removing Hub:
   - Blue Prism - License Manager.
   - Blue Prism - Notification Center.

Remove the hosts

1. Open the file `C:\Windows\System32\drivers\etc\hosts` in a text editor.
2. Delete the line with the domain License Manager. You can find this line by searching for the text *licensemanager*.
3. Delete the line with the domain Notification Center. You can find this line by searching for the text *notificationcenter*.
4. Save the file.

Remove the databases

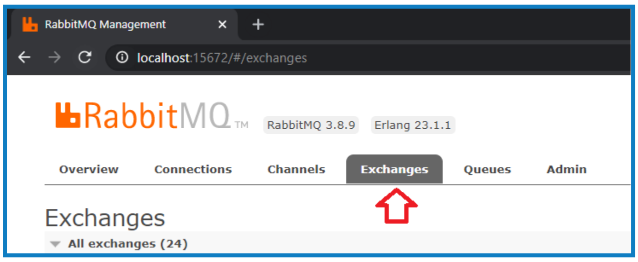
You should only remove databases for test systems. If you are contemplating removing a database for a system that had been in production, you should consider whether the data needs to be archived by your organization or used for audit purposes.

> Following the uninstall of Hub, 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 databases for the Hub and Interact (if it has been installed) applications.

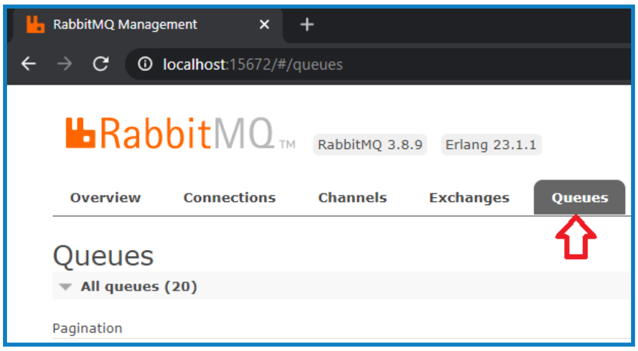
Remove RabbitMQ data

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.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*

4. Click **Queues**.



5. Find and remove the following items:
   - bpc.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*

Remove the certificates

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
   - BPC_SQL_CERTIFICATE

Remove any remaining files

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