

Hub 4.0

Install Guide

Document Revision: 1.2





Trademarks and Copyright

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

© 2024 Blue Prism Limited

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

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

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



Contents

Install Guide	i
Document Revision: 1.2	ii
Trademarks and Copyright	
Contents	iii
Installing Hub	5
Intended audience	5
Related guidance	5
Preparation	6
Planning	6
Prerequisites	7
Software download list	8
Blue Prism Hub	8
Blue Prism Interact	8
Software requirements and permissions	10
Software requirements	10
Operating system	10
Microsoft SQL Server	10
Message Broker server	10
Web server	10
Minimum SQL permissions	11
Default application information	11
Hub websites	12
Hub services	12
Multi-device deployment considerations	13
Network ports	14
Typical deployment	15
Overview of typical installation steps	15



Install the Message Broker server	17
Check RabbitMQ Message Broker connectivity	26
Install and configure the web server	28
Install the prerequisites	28
Features	28
Server roles	28
Scripted installation	29
.NET Core components	30
Scripted installation	30
Configure SSL certificates	30
Self-signed certificates	31
Scripted creation of self-signed certificates	32
Create an offline certificate request	32
Install Blue Prism Hub	36
Initial Hub configuration	61
Database settings	66
Email settings	68
Troubleshoot a Hub installation	70
Message Broker connectivity	70
Database connectivity	70
Web server	71
Starting the IMS website	71
File service	71
Windows Authentication	71
Not able to configure SMTP settings in Hub	72
Uninstall Hub	73



Installing Hub

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

Blue Prism Hub is only supported in a multi-device deployment, where the Blue Prism components are deployed across a number of devices. The reasons for this are:

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

A number of more advanced topics are also included within this guide to provide information on troubleshooting installations and configuring advanced settings and options. 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 4.0 of Blue Prism Hub.

Blue Prism Hub must be installed before attempting to install 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.

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 detailed document explaining how to get the best out of Hub, including user access, licensing plugins and customization of Hub.
Interact Install Guide	A document explaining the steps required to install Interact. This is a licensed product.
Interact User Guide	A document explaining how to use Interact. This is a licensed product.



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, IMS, Hub, Audit, and so on. Administrator-level access is required during the installation process. See "Minimum SQL permissions" on page 11 for more details.
- A Message Broker Server must be available hosting RabbitMQ Message Broker. See "Install the Message Broker server" on page 17 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 (including version 4.7.2 of .NET Framework)?
 - See "Software requirements and permissions" on page 10 for details.



Prerequisites

See "Software requirements and permissions" on page 10 for details of software requirements and minimum SQL permissions.

Installing Hub requires the following prerequisites:

• 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 23.0.1, available here: https://github.com/erlang/otp/releases/tag/OTP-23.0.1
- RabbitMQ Server 3.8.5, available here: https://github.com/rabbitmq/rabbitmq-server-/releases/tag/v3.8.5

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), IIS features, and the .NET Core components installed. These need to be preinstalled to enable a successful installation of Blue Prism Hub. These are detailed in the web server build section.
- 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.
- 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.
- 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. 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 11.
- By default, the 'Local System' account is used for services. This account must have access to application files. If using Windows Authorization for access to SQL server, this will need to be configured manually.



Software download list

Blue Prism Hub

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

Software and reference link	Related guidance
RabbitMQ 3.8.5	"Install the Message Broker server" on page 17
For more information, see <u>Downloading and Installing RabbitMQ</u> .	server on page 17
Erlang/OTP	
The version of Erlang that you require is dependent on the RabbitMQ version you intend to use. For more information, see <u>RabbitMQ Erlang Version Requirements</u> .	
IIS 10.0 Included with Windows Server 2016 and Windows Server 2019.	"Install and configure the web server" on page 28
.NET Core 3.1.3 Windows Server Hosting	
https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-	
aspnetcore-3.1.3-windows-hosting-bundle-installer	
.NET Core 3.1.3 Windows Desktop Runtime	
https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-desktop-3.1.3-windows-x64-installer	
Visual C++ Redistributable 2012 (x64)	
https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU 4/vcredist x64.exe	
.NET Framework 4.7.2	
https://dotnet.microsoft.com/download/dotnet-framework/thank- you/net472-web-installer	
Blue Prism Hub 4.0	
Download from the Blue Prism Portal.	

Blue Prism Interact

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



Software and reference link	Related guidance
Blue Prism Interact 4.0	Install Blue Prism Interact
Download from the Blue Prism Portal.	
Blue Prism Interact Remote API.bprelease file	Install and configure the
Download from the Blue Prism Portal.	Interact Web API service



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	✓	✓

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 2019 (64-bit)	✓	✓	✓

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

The following are also supported:

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

Azure SQL Database is not currently supported.

Message Broker server

The following software is required on the Message Broker server:

- RabbitMQ 3.8.5
- Erlang/OTP 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 RabbitMQ Supported Platforms.

See "Install the Message Broker server" on page 17 for more information.

Web server

The following software is required on the Web server:



- .NET Framework 4.7.2
- IIS 10.0
- .NET Core Windows Server Hosting 3.1.3
- .NET Core Windows Desktop Runtime 3.1.3
- Visual C++ Redistributable 2012 (x64)

See "Install and configure the web server" on page 28 for more information.

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 IMS 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. IIS APPPOOL\ Blue Prism – IMS will also require access to the BluePrismCloud_IMS_JWT certificate.



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 - IMS	IIS APPPOOL\ Blue Prism – IMS	dbcreator / sysadmin	db_datawriter / db_datareader	ImsDB
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	IIS APPPOOL\ Blue Prism – Email	N/A	N/A	N/A
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	CacheDB

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).	
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 Con-
Message	nectivity from the Web Server. Port 5672 to allow RabbitMQ Messaging connectivity.
Broker server	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.

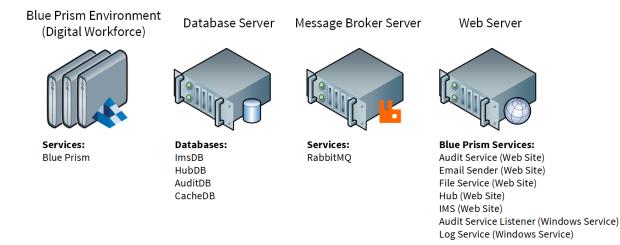
Prior to following this guidance, ensure that you have fully considered the information in "Preparation" on page 6.

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.

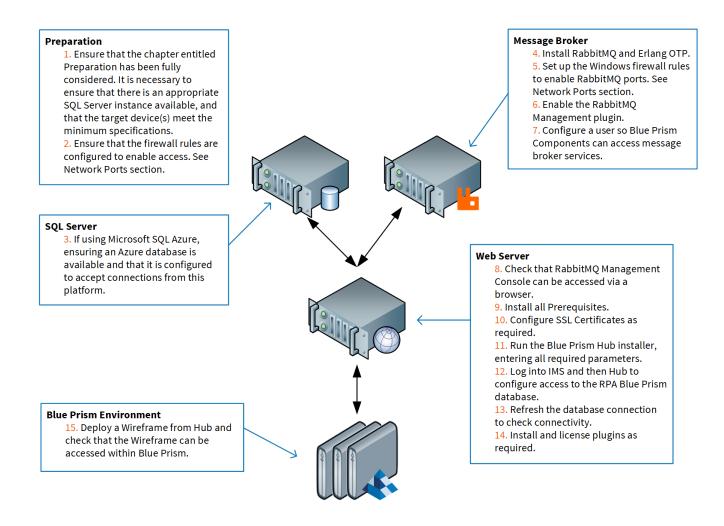
The diagram below illustrates the typical architecture for an environment.



Overview of typical installation steps

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





If you experience problems whilst installing, see "Troubleshoot a Hub installation" on page 70.



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.

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

1. Install Erlang/OTP.

For information, see the Erlang/OTP installation guide.

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

For more information, see Downloading and Installing RabbitMQ.

- 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

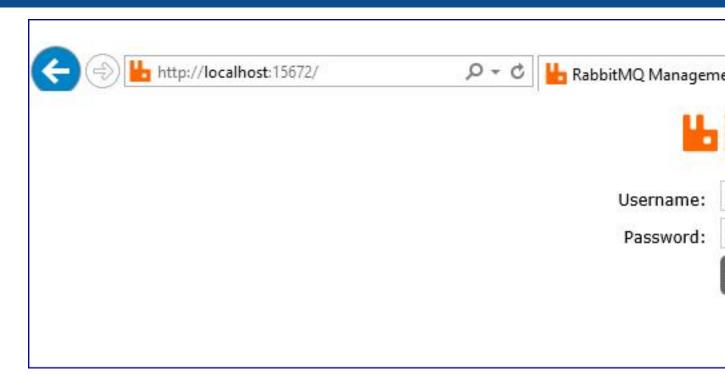


Administrator: RabbitMQ Command Prompt (sbin dir)

```
C:\Program Files\RabbitMQ Server\rabbitmq server-3.8.5\sbin>rabbi
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>_
```

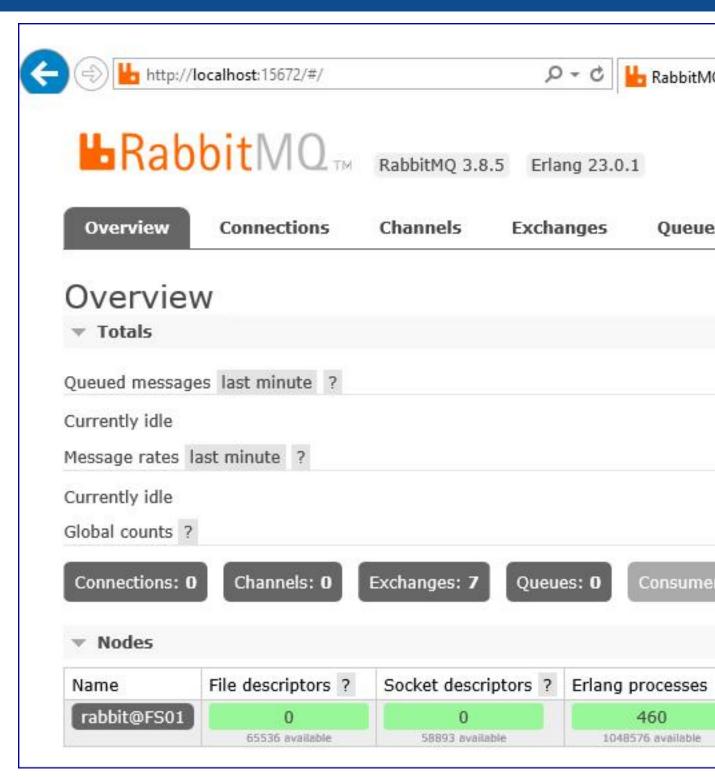
- 6. Launch a browser and navigate to the following URL: http://localhost:15672
- 7. In the RabbitMQ console, log on with the default credentials of guest/guest.





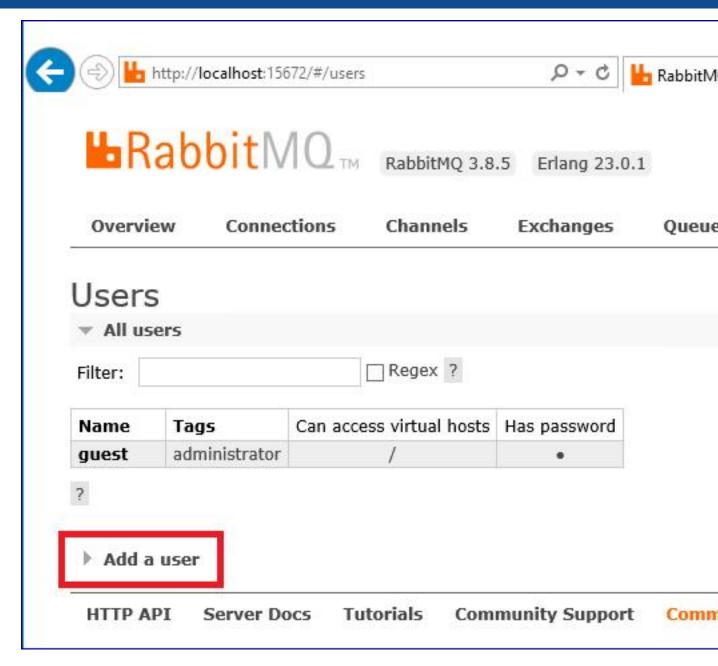
8. In the console, click **Admin**.





9. Click Add a user.



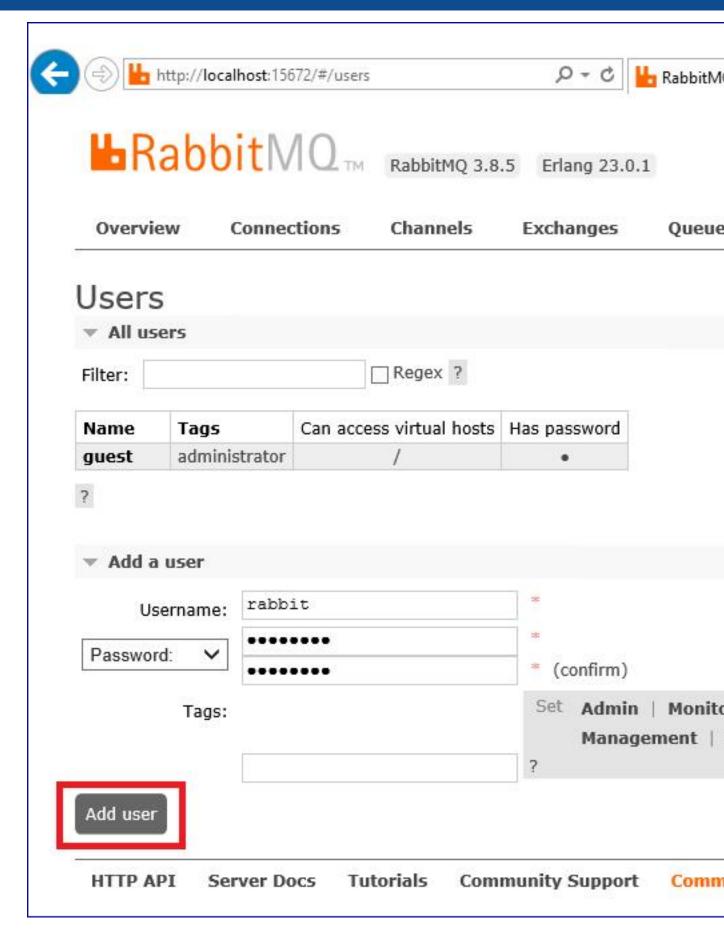


10. Enter the details for a new user, providing the username and password. The user does not require any special permissions and can be left at None.

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

11. Click Add User.



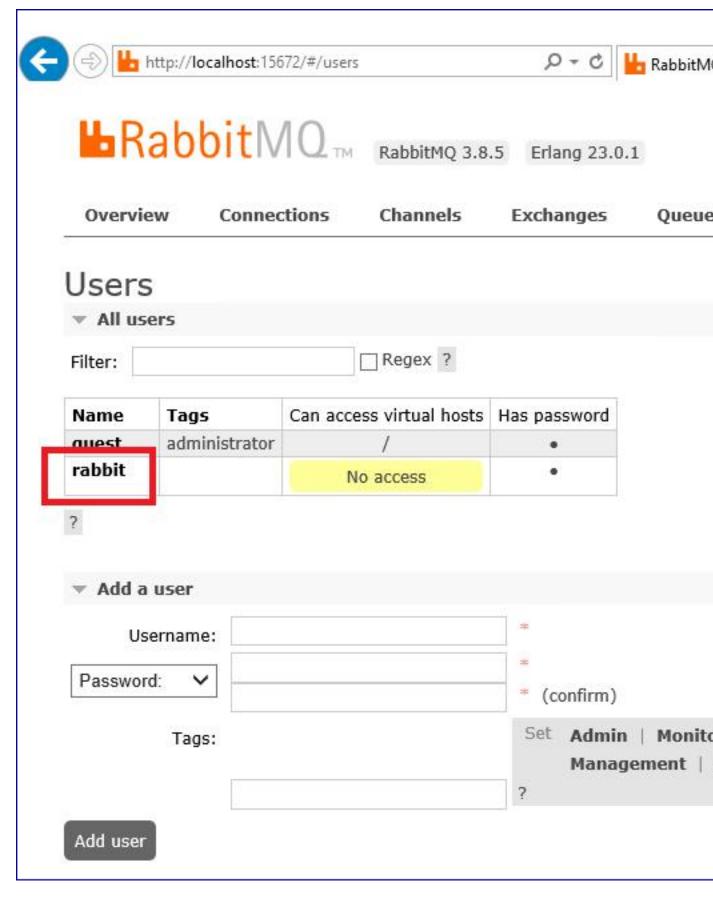




The next step is to set the permissions for the user.

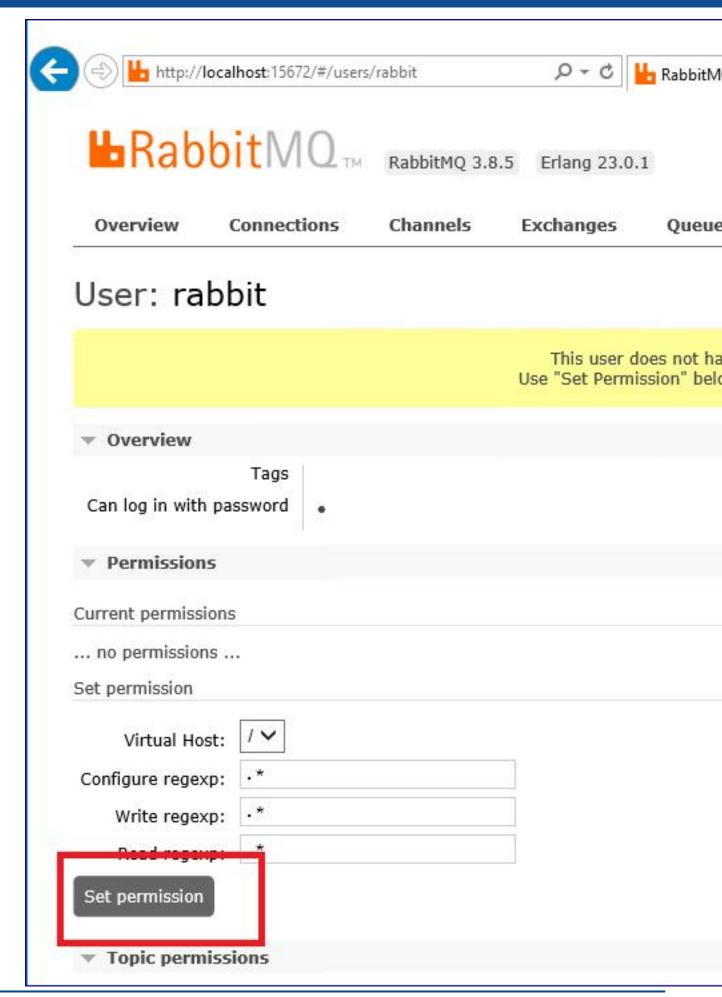
12. Click on the username of the user that you just created.





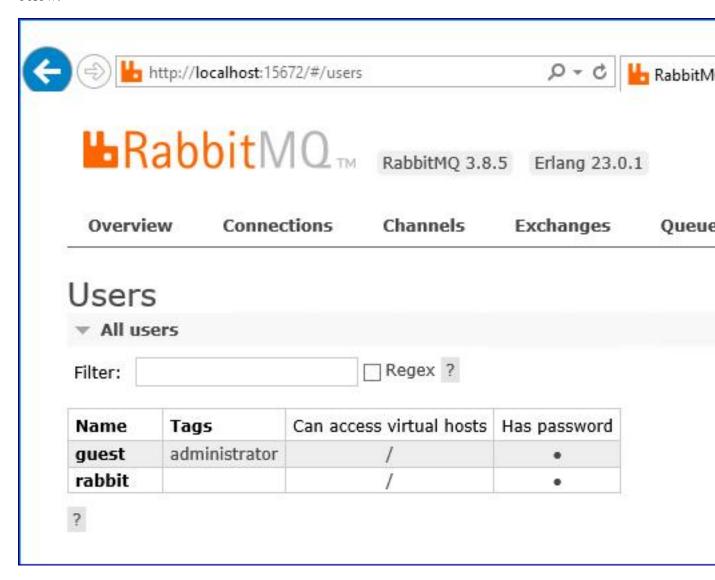
13. Click **Set Permission** to allocate the default permissions.







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



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

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

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

Check RabbitMQ Message Broker connectivity

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

The login page for RabbitMQ Management Console should display.



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

If the console does not appear, restart the RabbitMQ service. If the console still does not appear, see "Troubleshoot a Hub installation" on page 70.



Install and configure the web server

Before installing the Hub web server, ensure you have read the information in "Preparation" on page 6.

Install and configure the web server ensuring that the system can communicate with the RabbitMQ Message Broker and the prerequisites and Blue Prism Hub are installed.

The process consists of the following steps:

- 1. Install the prerequisites
- 2. Configure SSL Certificates
- 3. Install Blue Prism Hub

Install the prerequisites

The system requires IIS Web Server, IIS features and the .NET Core components to be installed. It is important that IIS is installed before installing the prerequisites below.

Install all of the features listed below before installing the .NET Core Components.

The full list of the prerequisites is detailed below, in the order listed:

Features

- Remote Server Administration Tools\Role Administration Tools\File Services Tools\File Server Resource Manager Tools
- .NET Framework 4.6 Features
- .NET Framework 4.6 Features\.NET Framework 4.6
- .NET Framework 4.6 Features ASP.NET 4.6
- .NET Framework 4.6 Features\WCF Services
- .NET Framework 4.6 Features\WCF Services\HTTP Activation
- .NET Framework 4.6 Features\WCF Services\TCP Port Sharing

Server roles

- File and Storage Services\File and iSCSI Services\File Server
- File and Storage Services\File and iSCSI Services\File Server Resource Manager
- Web Server (IIS)
- Web Server (IIS)\Web Server
- Web Server (IIS)\Web Server\Common HTTP Features
- Web Server (IIS)\Web Server\Common HTTP Features\Default Document
- Web Server (IIS)\Web Server\Common HTTP Features\Directory Browsing
- Web Server (IIS)\Web Server\Common HTTP Features\HTTP Errors
- Web Server (IIS)\Web Server\Common HTTP Features\Static Content
- Web Server (IIS)\Web Server\Common HTTP Features\HTTP Redirection
- Web Server (IIS)\Web Server\Health and Diagnostics
- Web Server (IIS)\Web Server\Health and Diagnostics\HTTP Logging
- Web Server (IIS)\Web Server\Health and Diagnostics\Logging Tools
- Web Server (IIS)\Web Server\Health and Diagnostics\Request Monitor



- Web Server (IIS)\Web Server\Health and Diagnostics\Tracing
- Web Server (IIS)\Web Server\Performance
- Web Server (IIS)\Web Server\Performance\Static Content Compression
- Web Server (IIS)\Web Server\Security
- Web Server (IIS)\Web Server\Security\Request Filtering
- Web Server (IIS)\Web Server\Security\Client Certificate Mapping Authentication
- Web Server (IIS)\Web Server\Security\IIS Client Certificate Mapping Authentication
- Web Server (IIS)\Web Server\Security\Windows Authentication
- Web Server (IIS)\Web Server\Application Development
- Web Server (IIS)\Web Server\Application Development\.NET Extensibility 4.6
- Web Server (IIS) \Web Server\Application Development\Application Initialization
- Web Server (IIS)\Web Server\Application Development\ASP
- Web Server (IIS)\Web Server\Application DevelopmentASP.NET 4.6
- Web Server (IIS)\Web Server\Application Development\ISAPI Extensions
- Web Server (IIS)\Web Server\Application Development\ISAPI Filters
- Web Server (IIS)\Management Tools
- Web Server (IIS)\Management Tools\IIS Management Console
- Web Server (IIS)\Management Tools\IIS 6 Management Compatibility
- Web Server (IIS)\Management Tools\IIS 6 Management Compatibility\IIS 6 Metabase Compatibility
- Web Server (IIS)\Management Tools\IIS Management Scripts and Tools
- Web Server (IIS)\Management Tools\Management Service

Scripted installation

Run the commands below using the PowerShell command prompt:

```
Install-WindowsFeature -Name FS-FileServer -computerName localhost
Install-WindowsFeature -Name FS-Resource-Manager -computerName localhost
Install-WindowsFeature -Name Web-Default-Doc -computerName localhost
Install-WindowsFeature -Name Web-Dir-Browsing -computerName localhost
Install-WindowsFeature -Name Web-Http-Errors -computerName localhost
Install-WindowsFeature -Name Web-Static-Content -computerName localhost
Install-WindowsFeature -Name Web-Http-Redirect -computerName localhost
Install-WindowsFeature -Name Web-Http-Logging -computerName localhost
Install-WindowsFeature -Name Web-Log-Libraries -computerName localhost
Install-WindowsFeature -Name Web-Request-Monitor -computerName localhost
Install-WindowsFeature -Name Web-Http-Tracing -computerName localhost
Install-WindowsFeature -Name Web-Stat-Compression -computerName localhost
Install-WindowsFeature -Name Web-Filtering -computerName localhost
Install-WindowsFeature -Name Web-Client-Auth -computerName localhost
Install-WindowsFeature -Name Web-Cert-Auth -computerName localhost
Install-WindowsFeature -Name Web-Windows-Auth -computerName localhost
Install-WindowsFeature -Name Web-Net-Ext45 -computerName localhost
Install-WindowsFeature -Name Web-AppInit -computerName localhost
Install-WindowsFeature -Name Web-ASP -computerName localhost
Install-WindowsFeature -Name Web-Asp-Net45 -computerName localhost
Install-WindowsFeature -Name Web-ISAPI-Ext -computerName localhost
Install-WindowsFeature -Name Web-ISAPI-Filter -computerName localhost
Install-WindowsFeature -Name Web-Mgmt-Console -computerName localhost
Install-WindowsFeature -Name Web-Scripting-Tools -computerName localhost
Install-WindowsFeature -Name Web-Mgmt-Service -computerName localhost
Install-WindowsFeature -Name Web-Metabase -computerName localhost
Install-WindowsFeature -Name RSAT-Role-Tools -computerName localhost
Install-WindowsFeature -Name RSAT-File-Services -computerName localhost
Install-WindowsFeature -Name RSAT-FSRM-Mgmt -computerName localhost
```



Install-WindowsFeature -Name NET-WCF-HTTP-Activation45 -computerName localhost -Restart

.NET Core components

• .NET Core 3.1.2 Windows Server Hosting

https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-3.1.2-windows-hosting-bundle-installer

• .NET Core 3.1.2 Windows Desktop Runtime

https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-desktop-3.1.2-windows-x64-installer

.NET Core SDK 3.1.300

https://dotnet.microsoft.com/download/dotnet-core/thank-you/sdk-3.1.300-windows-x64-installer

• Visual C++ Redistributable 2012 (x64)

https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU 4/vcredist x64.exe

.NET Framework 4.7.2

https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer

Scripted installation

To install the .NET dependencies, run the commands below using the PowerShell command prompt, updating C:\temp to the appropriate location as required:

```
start-process "C:\temp\dotnet-hosting-3.1.2-win.exe" /q -wait
start-process "C:\temp\windowsdesktop-runtime-3.1.2-win-x64.exe" /q -wait
start-process "C:\temp\dotnet-sdk-3.1.300-win-x64.exe" /q -wait
start-process "C:\temp\vcredist_x64.exe" /q -wait
start-process "C:\temp\NDP472-KB4054531-Web.exe" /q -wait
```

Configure SSL certificates

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

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

The 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 – IMS	https://ims.local	
Blue Prism – Hub	https://hub.local	
Websites for use by the application only (services)		
Blue Prism – Email Sender	https://email.local	
Blue Prism – Audit Service	https://audit.local	
Blue Prism – File Service	https://file.local	

Self-signed certificates

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

To generate a self-signed certificate:

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

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

For example:

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

This example creates a self-signed certificate called *MySiteCertIMS* in the Personal Certificates store, with the Subject *ims.local* and is valid for 10 years from the point of creation.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

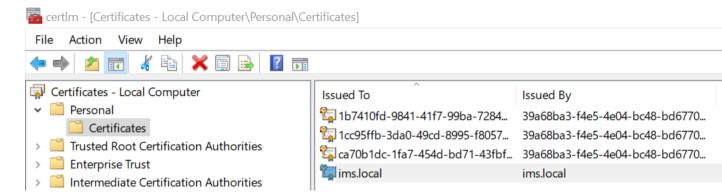
PS C:\WINDOWS\system32> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "ims

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint Subject
------
B56A10A4792784D73C2756256BEFC075D8E63919 CN=ims.local
```



- 2. Open the Manage Computer Certificates application on your web server (type **manage computer** into the search bar).
- 3. Copy and paste the certificate from Personal > Certificates to Trusted Root Certification > Certificates.



4. Repeat this process for each website.

Scripted creation of self-signed certificates

This process is not recommended for production environments.

Run the following PowerShell commands:

```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "ims.local" -
FriendlyName "MySiteCertIMS" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "hub.local" -
FriendlyName "MySiteCertHub" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "email.local" -
FriendlyName "MySiteCertEmail" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "audit.local" -
FriendlyName "MySiteCertAudit" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "file.local" -
FriendlyName "MySiteCertFile" -NotAfter (Get-Date).AddYears(10)
```

Once created, open the Local Machine certificate manager (certlm) and copy and paste the certificates 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.

Cancel

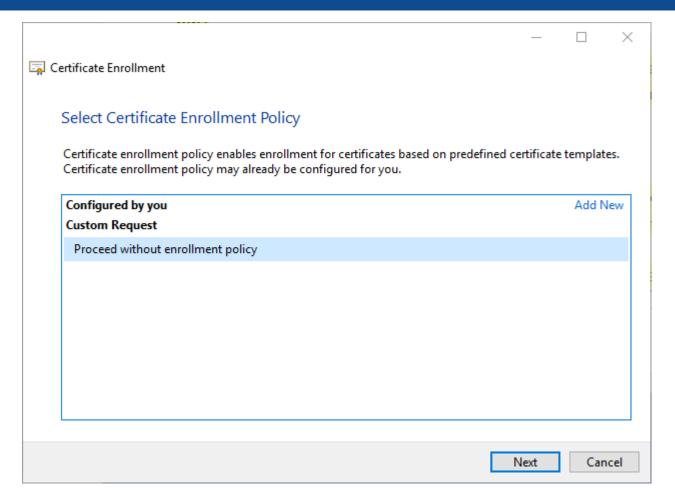
Next



		_		\times
Certificate Enrollment				
	Before You Begin			
	The following steps will help you install certificates, which are digital credentials used to networks, protect content, establish identity, and do other security-related tasks.	conne	ct to wire	less
	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			

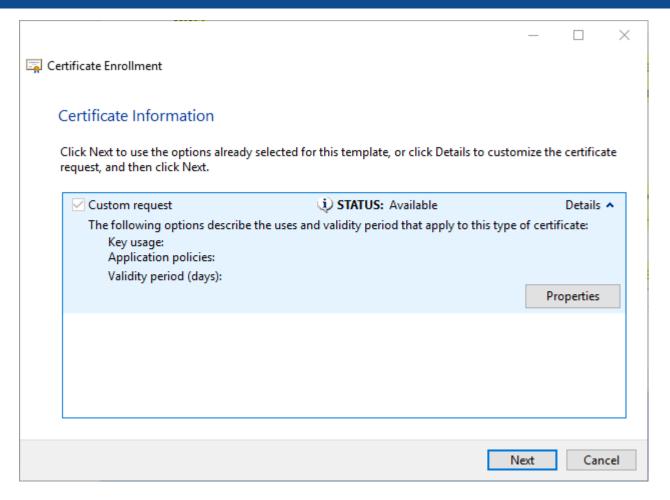
3. Click Next.





- 4. Select Proceed without enrollment policy and click Next.
- 5. On the Custom request screen, click Next.
- 6. On the Certificate Information screen, click the **Details** drop-down and click **Properties**.

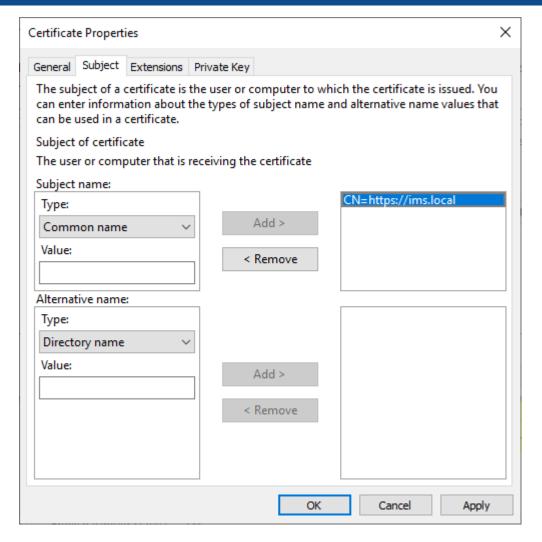




- 7. On the General tab in the Certificate Properties dialog, enter a friendly name and description based on the website this certificate will be applied to.
- 8. On the Subject tab change the subject name type to **Common name**, enter the website URL in the **Value** field and click **Add**.

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





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

You are returned to the Certificate Enrollment screen.

- 13. Click Next.
- 14. Add a file name and path and click **Finish**.

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

Install Blue Prism Hub

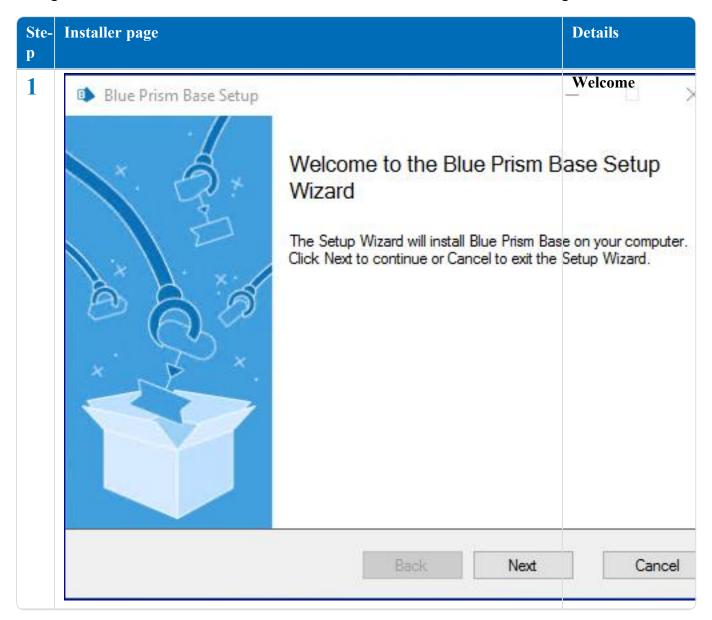
Before you install Blue Prism Hub:



• 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.

The steps below detail the process for installing the Blue Prism Hub software. This includes the Identify Management System (IMS), 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 <u>Blue Prism Portal</u>, and progress through the installer as shown below. The installer must be run with administrator rights.





1	Installer page	Details
	Blue Prism Base Setup	License agree- ment
	End-User License Agreement	Read the End-
	Please read the Blue Prism Base License Agreement	User License Agreement and if
ŀ		you agree to the terms, select the
	Common Public License Version 1.0	check box.
	THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TER COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPROD DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S OF THIS AGREEMENT.	UCTION OR
	COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPROD DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S	UCTION OR
	COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPROD DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S OF THIS AGREEMENT.	UCTION OR
	COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPROD DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S OF THIS AGREEMENT. 1. DEFINITIONS	UCTION OR



Ste- p	Installer page	Details
3	Blue Prism Base Setup Prerequisities (1/2) - Server components Check if prerequisites have been installed	Prerequisites 1 – Server components The installer
	Components IIS 8.0	checks that the statis have been Not initialled. Those
	Microsoft Windows Desktop Runtime 3.1.2 (x64) Microsoft .NET Core SDK 3.1.300 (x64)	that are not installed are iden-
	Microsoft .NET Core 3.1.2 Windows Server Hosting Microsoft Visual C++ 2012 Redistributable (x64)	not proceed until Not installed all the pre- Not installed
	File and iSCSI Services\File Server File and iSCSI Services\File Server Resource Manager	installed. Not installed If there are unin- Not installed pre-
	File Services Tools\File Server Resource Manager Tools WCF Services\HTTP Activation	Not installed pre- the installer and
	Application Development\Application Initialization	Not iring components before restarting
	Back	the installer. Otherwise, pro- ceed with the
		installation.



re- Installer page		Details
Blue Prism Base Set	up	Prerequisites 2 – RabbitMQ
Prerequisites (2/2) Connect to RabbitMQ		Enter the server name or IP S address of the
Server name	192.168.0.104	Message Broker server and the credentials of the
Username	rabbit	user you created. The default mes-
Password	******	sage queuing port is 5672. This
Port	5672	should only be changed if the default ports
		have been changed by your
	Test cor	IT support organ- nnection to proceed ization.
		Click Test connection to verify connectivity. A
	Back	Next notification will display the result
		of the test. If the test failed, see "Troubleshoot a
		Hub installation" on page 70 for further details.



te-	Installer page		Details
	Blue Prism Base Setup	3	Destination folder
	Destination Folder Click Next to install to the default folder or click Change to choose another.	♣ b	Specify the required installation folder. The default location
	Install Blue Prism Base to:		is C:\Program Files (x86)\Blue Prism, but you can choose your
	C:\Program Files (x86)\Blue Prism Change		own using the Change button.
	Back	Next	Cancel



Ste-p	Installer page		Details
6	Blue Prism Base Configure IMS S Please enter detai	AND THE PARTY AND ADDRESS OF THE PARTY.	IMS SQL connection Configure the settings for the IMS database by
	2 in a control of	1000	providing the SQL Server host name or IP address, and the credentials for the account to create the database:
	Password Database name	ImsDB	• If Win- dows Authentic- ation is
			selected, the account must have the appro- priate per- missions,
		Back Next	See Win- dows Authentic- ation" on page 71 for further inform- ation.
			If Windows Authentication is the required method, you need to switch to SQL Authentication and



Ste-p	Installer page	Details
		back again to enable the Next button.
		• If SQL Authentication is selected, enter the username and password.
		You must ensure that your data- base pass- word does not contain an equals sign (=), semi-colon
		(;), or speech marks ("). These characters are not supported, and will lead to issues
		when try- ing to con- nect to the database.



Ste- In	istaller page		Details
7	Blue Prism Base Setup IMS IIS Setup	♣ bl	IMS IIS setup Configure IIS for the IMS website. You need to:
	Site name Host name Port SSL Certificate	Blue Prism - IMS ims.local 443 TenantEncryptionCert Start Website Back Next	• Enter a site name. • Enter a host name in lower-case characters — This will be used as the URL for the site. The first part of the default host name must not be changed. You can only change the .local part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. The use of
			uppercase characters in URLs is



Ste-p	Installer page	Details
		not supported.
		 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 install-ation.

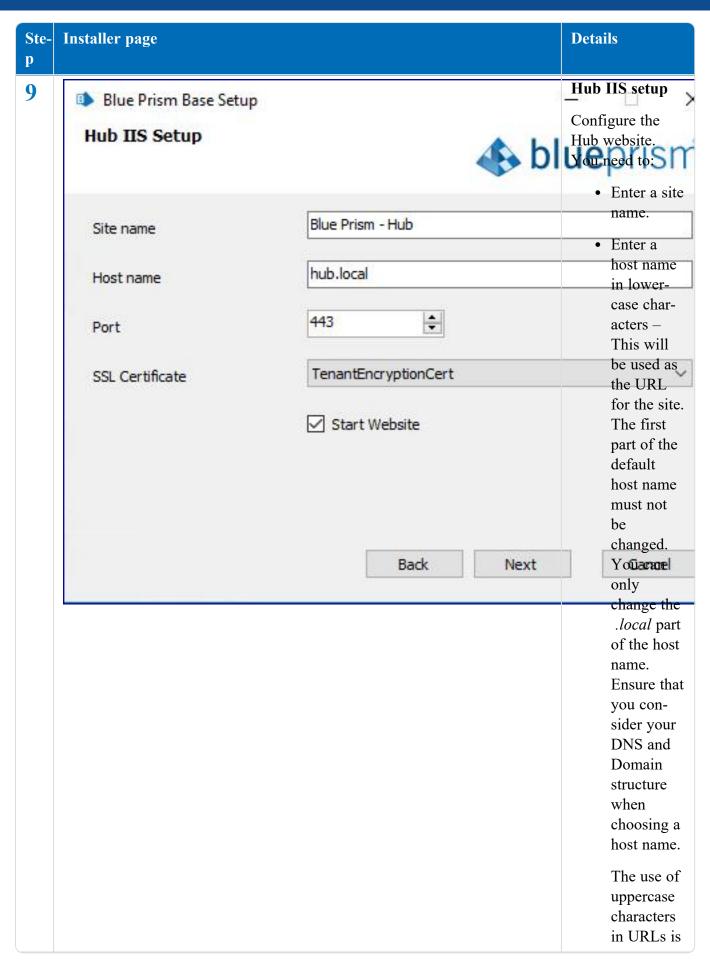


Ste-	Installer page		Details
8	Blue Prism Base	Setup	Hub SQL connection >
	Configure Hub S Please enter detail	QL connection Is for a SQL server instance	Configure the set- tings for the Hub database by
			providing the SQL Server Host name or IP address, and the credentials for the account to create the data- base: If Win- dows Authentic- ation is selected, the account must have
		Back	the appropriate permissions. See Windows Authentication" on page 71 for further information. • If SQL Authentication is selected, enter the username and password. You must



Ste-p	Installer page	Details
		ensure that your data- base pass- word does not contain an equals sign (=), semi-colon (;), or speech marks ("). These char- acters are not sup- ported, and will lead to issues when try- ing to con- nect to the database.
		The database name can be left as the default value or changed as required. Click Next to continue.







Ste-	Installer page	Details
		not supported. • 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.

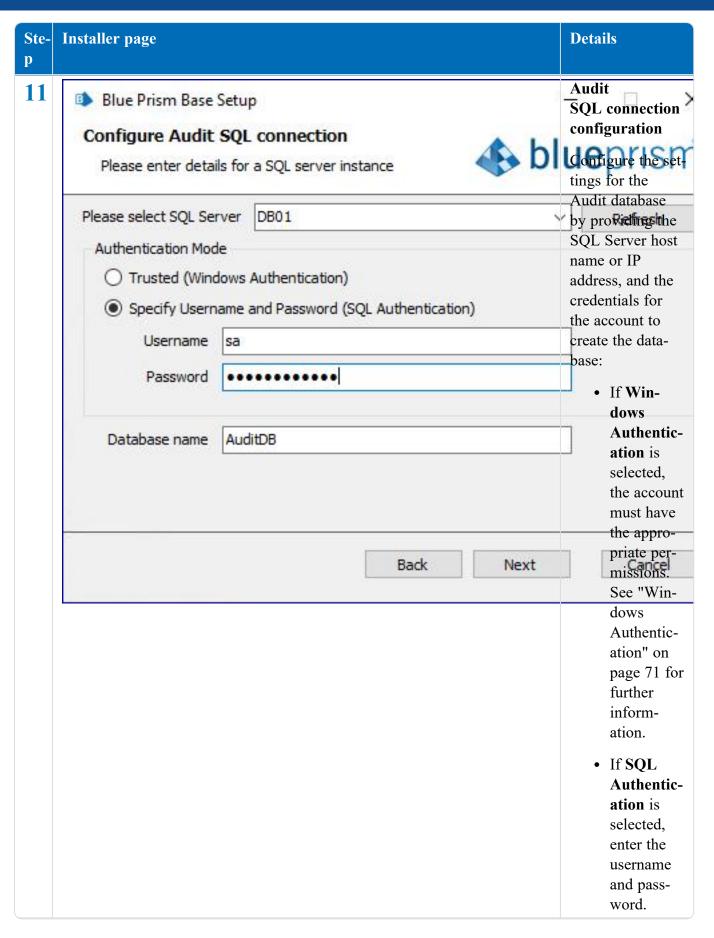


Ste-p	Installer page		Details
10	Blue Prism Base Setup Email Sender IIS Setup	♣ bl	Email Sender IIS setup Configure the Email Sender website.
	Site name	Blue Prism - Email Sender	You need to: • Enter a site name.
	Host name Port	email.local	• Enter a host name in lower- case char-
	SSL Certificate	TenantEncryptionCert ☑ Start Website Back Next	acters – This will be used as the URL for the site. The first part of the default host name must not be Cancel changed. You can only change the .local part of the host name. Ensure that you con- sider your DNS and Domain structure
			when choosing a host name. The use of uppercase



Ste-p	Installer page	Details
P		characters in URLs is not sup- ported. • Enter the port num- ber. • Select the appropriate SSL cer- tificate. • Leave Start Web- site selec- ted, unless you do not want the website to auto- matically start at the end of the install-
		ation.







Ste-p	Installer page	Details
		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.



Ste-p	Installer page		Details
12	Blue Prism Base Setup Audit Service IIS Setup	♣ bl	Audit Service IIS setup Configure the Audit Service website.
	Site name	Blue Prism - Audit Service	You need to: • Enter a site name.
	Host name Port	443 A	• Enter a host name in lower- case char-
	SSL Certificate	TenantEncryptionCert Start Website Back Next	acters — This will be used as the URL for the site. The first part of the default host name must not be Cancel changed. You can only change the .local part of the host name. Ensure that you con-
			sider your DNS and Domain structure when choosing a host name. The use of uppercase



Ste-p	Installer page	Details
P		characters in URLs is not sup- ported. • Enter the port num- ber. • Select the appropriate SSL cer- tificate. • Leave Start Web- site selec- ted, unless you do not want the website to auto- matically start at the end of the install-
		ation.

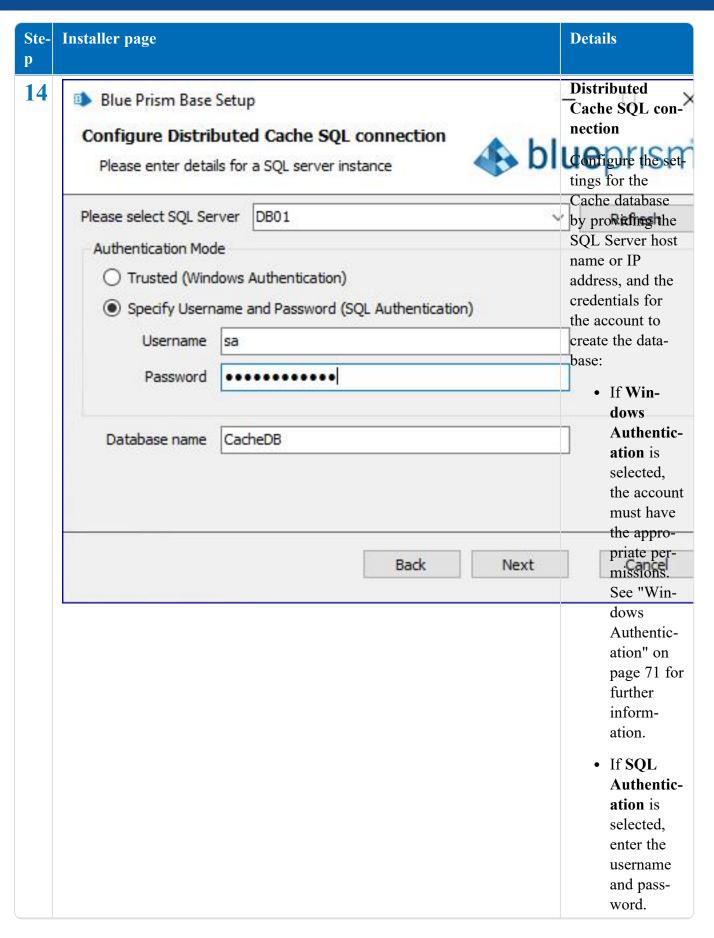


Ste-p	Installer page		Details
13	Blue Prism Base Setup File Service IIS Setup	♣ bl	File Service IIS setup Configure the File Service web- site.
	Site name Host name	Blue Prism - File Service	You need to: • Enter a site name. • Enter a
	Port	443	host name in lower- case char-
	SSL Certificate	TenantEncryptionCert Start Website Back Next	acters – This will be used as the URL for the site. The first part of the default host name must not be Cancel changed. You can
			only change the .local part of the host name. Ensure that you con- sider your DNS and Domain structure when choosing a host name. The use of uppercase



Ste-	Installer page	Details
		characters in URLs is not sup- ported.
		 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 install-ation.

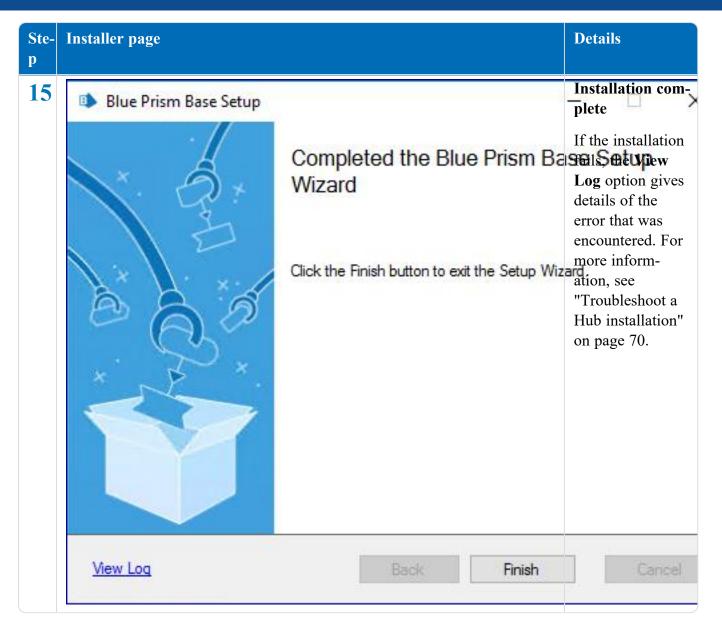






Ste-p	Installer page	Details
		You must ensure that your database password does not contain an equals sign (=), semi-colon (;), or speech marks ("). These characters are not supported, and will lead to issues when trying to connect to the database.
		The database name can be left as the default value or changed as required.







Initial Hub configuration

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

When you open the login page for IMS, 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.

I have had to repeat sections to get the pagination work in the PDF - the table seemed to be forcing it to stay together creating white space. I tried a number of things to fix it, to no avail. Now out of time. Will look again another time. For now, a snippet is in place to keep content consistent.



1. Launch a browser and go to the IMS website, in our example: https://ims.local







2. Log in using the default credentials.

Username: admin Password: Qq1234!!

For information about how to change the default password and other settings see the <u>Hub User</u> Guide.

3. Click **Hub** to launch the Hub website.



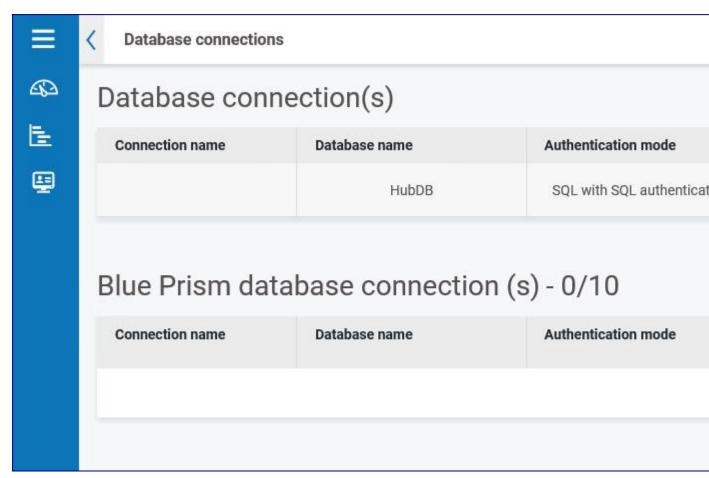




Database settings

Configure access to the Blue Prism RPA database.

1. Click on the settings cog and select **Database Settings**.



2. Click Add New and enter the details of the Blue Prism RPA database as illustrated below.



Cancel

Database settings Authentication mode * SQL with SQL authentication Server name or IP address * **DB01** Connection name * Production Database name * **RPA** Timeout * 90 User ID * sa Password * IADA URL Important: once selected you cannot change your URL iada.local



The Timeout value is in seconds.

- 3. Click Save to save your data.
- 4. To test the settings, go back into the Database settings and click on the action menu (three dots) alongside the configured database and select **Refresh**. If operational the following message displays in the top right corner of the Hub user interface, which verifies the installation. If the message is not displayed, see "Troubleshoot a Hub installation" on page 70 for more information.



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 check the email address, click on the settings cog and select Email Settings.



Email settings If you need help configuring your SMTP settings, please speak to your IT team in the first SMTP host * Port * Enter SMTP host Enter Port Sender email * Encryption * None Enter Sender email SMTP authenticate Password Username Enter Password Enter Username Send test email to some@mail.com

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 the next page for more information.

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



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

There are a number of checks that can be performed when a connection cannot be made to a SQL Server over the LAN:

- Verify Network Connectivity Ensure that all relevant devices are connected to the same network and are able to communicate.
- SQL Credentials Verify the SQL credentials and that the user has appropriate permissions on the SQL Server.
- Firewall Check that the firewalls on the servers themselves or within the network are not preventing communication.
- SQL Browser Service Ensure the SQL Browser Service on the SQL Server is enabled to allow for a SQL Instance to be found. For SQL Server Express this service is typically disabled by default.
- Enabling TCP/IP Connectivity Where remote connectivity is required for SQL, check that TCP/IP connectivity is enabled for the SQL Instance. Microsoft provide articles specific to each version of SQL that provide instructions to Enable the TCP/IP Network Protocol for SQL Server.

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

Error Number:53,State:0,Class:20
Info: CustomAction CreateDatabases returned actual error code 1603 (r
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 databases need to be cleared of any old data 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 7.

Starting the IMS website

After completing the installation if you get 'HTTP Error 500.19 on 0x8007000d' (when starting the IMS website), this is caused by the installation order of the prerequisites.

If the Windows features were not installed in their entirety before the .NET Core Component, then the .NET Core 3.1.2 Windows Server Hosting will need to be repaired or reinstalled. The file for this component is dotnet-hosting-3.1.2-win.exe.

It is recommended that all Windows features are loaded prior to the commencement of the .NET Core Component.

File service

If the File service fails to locate the imagery for IMS 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.

Windows Authentication

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

If during the installation process it was chosen to use Windows Authentication, it is recommended that a Windows service account is established with the necessary permissions to execute the tasks and operate during normal operation.

This service account will need not only the ability to perform the SQL database creation process, see "Minimum SQL permissions" on page 11, and ownership over the IIS Application Pools.



By default, the Application Pools are created with the identity 'ApplicationPoolIdentity'. After the installer has completed the established service account will need to be allocated permissions to manage the Application Pools.

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.

Not able to configure SMTP settings in Hub

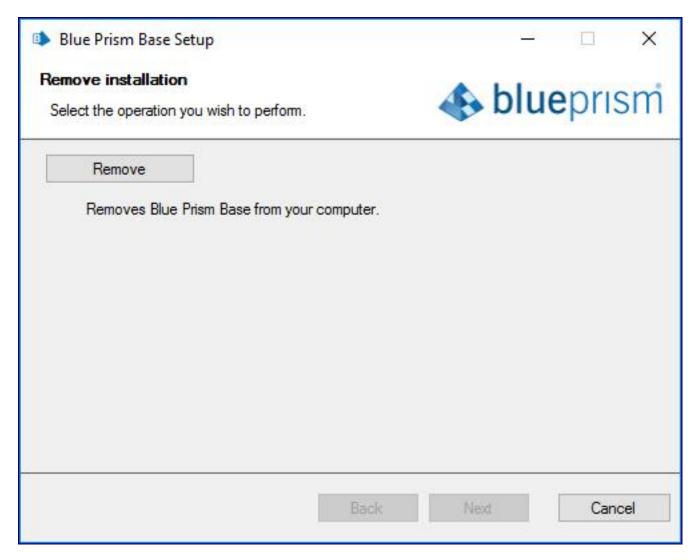
If you are unable to configure SMTP settings in Hub this is normally related to the startup order of the services.

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.



Uninstall Hub

By clicking on the Blue Prism Hub installer with the Blue Prism components installed, you are prompted to remove the installation.



When removing the installation it will remove the following items:

- IIS websites and Application Pools.
- Services.
- File structure except for top level.

It is important to note that the databases are not removed. This is to allow any potential data to be archived by the organization or used for audit purposes.

If the installation is repeated again, after a removal, and the same database names are used, then the databases should be cleared of any data prior to re-installation.