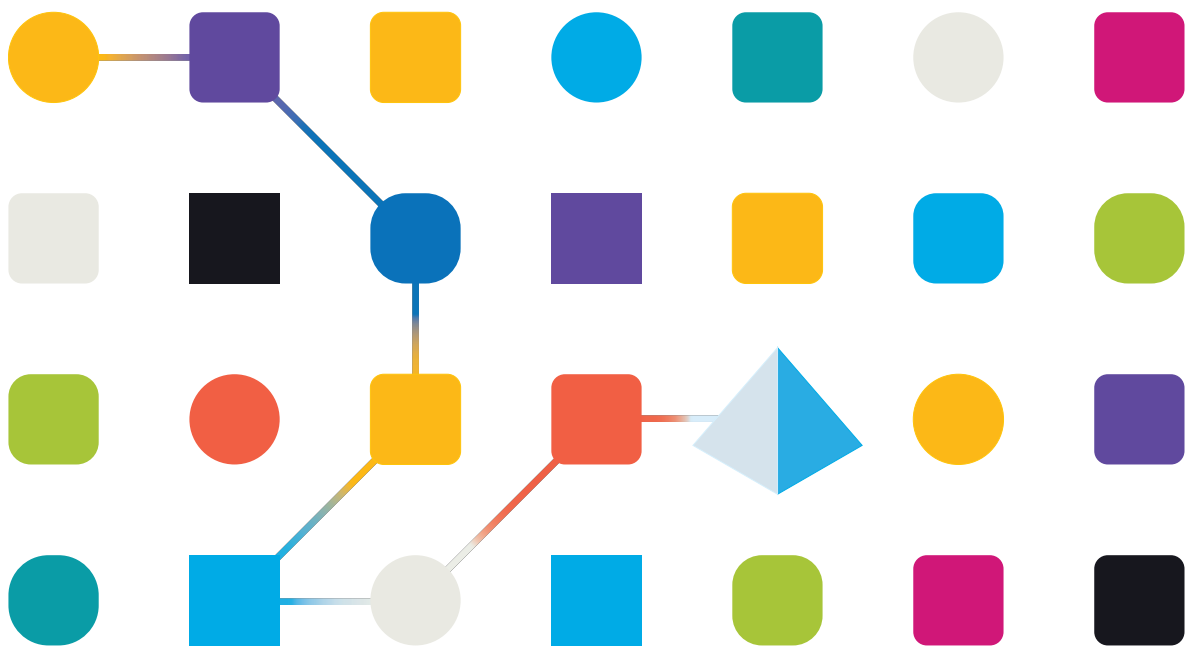


blueprism[®]

Interact 4.2 Install Guide

Document Revision: 1.5



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.

© **Blue Prism Limited, 2001 – 2021**

© “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

| | |
|---|-----------|
| Introduction | 4 |
| Upgrading Interact | 4 |
| Intended audience | 4 |
| Related documents | 4 |
| Preparation | 5 |
| Planning | 5 |
| Prerequisites | 6 |
| Software download list | 7 |
| Software requirements and permissions | 8 |
| Software requirements | 8 |
| Minimum SQL permissions | 9 |
| Default application information | 9 |
| Multi-device deployment considerations | 11 |
| Network ports | 12 |
| Typical deployment | 13 |
| Overview of typical installation steps | 14 |
| Install the Message Broker server | 15 |
| Install and configure the web server | 19 |
| Install Blue Prism Interact | 38 |
| Initial Hub configuration | 44 |
| Install the Interact plugin | 48 |
| Configure Digital Workers | 49 |
| Troubleshoot an Interact installation | 56 |
| Database connectivity | 56 |
| Web server | 56 |
| Windows Authentication | 56 |
| Troubleshoot a Hub installation | 58 |
| Message Broker connectivity | 58 |
| Database connectivity | 58 |
| Web server | 59 |
| Starting the IMS website | 59 |
| File service | 59 |
| Windows Authentication | 59 |
| Not able to configure SMTP settings in Hub | 59 |
| Updating the Customer ID after installation | 60 |
| Uninstall Interact | 61 |
| Remove Interact using Programs and Features | 61 |
| Remove any remaining files | 61 |
| Remove the databases | 61 |
| Remove RabbitMQ data | 62 |

Introduction

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

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

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

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

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

This information relates only to the version 4.2 of Blue Prism Interact.



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

Upgrading Interact

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

Intended audience

This guide is aimed at IT professionals with experience in configuring and managing networks, servers, and databases. The installation process requires familiarity with installing and configuring web servers and databases.

Related documents

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

| Document Title | Description |
|---|---|
| Hub user guide | A detailed document explaining how to get the best out of Hub, including user access, licensing plugins and customization of Hub. |
| Interact user guide | A detailed document explaining how to get the best out of Interact, including creating Forms and assigning them to Roles. |
| Interact Web API Service user guide | A document providing detailed information on how to use the Interact Web API Service and related Blue Prism Object. |

Preparation

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

Planning

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

- A SQL Server must be available to host the Blue Prism component databases, such as, IMS , Hub, Audit, Interact, InteractCache and so on. Administrator-level access is required during the installation process. See [Minimum SQL permissions](#) for more details.
- A [Message Broker server](#) must be available hosting RabbitMQ Message Broker.
- A Web Server for the co-existing Hub (see [Prerequisites on the next page](#)) and Interact installations
- Administrator access to the devices where Blue Prism Interact is to be installed must be available. All devices must meet the minimum specifications and the devices must be able to communicate with each other over the local network, including communication with your Blue Prism Database.

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? We recommend that databases are kept on separate database servers.
- Is there sufficient space and resources to host the added databases? You should check and ensure that sufficient disk space and compute resources can cope with the additional load.
- What authentication mode is required for the SQL database (SQL Native or Windows Authentication)? This is your IT organizations decision.
- Has the Message Broker server been setup and configured to support the installation of Hub? A Message Broker server is required to complete the installation of Hub.
- Do all devices where Blue Prism Hub is to be installed meet the minimum requirements (including version 4.7.2 of the .NET Framework) See [Software requirements and permissions](#) for details.

Prerequisites

See [Software requirements and permissions](#) for details of software requirements and minimum SQL permissions.

Installing Interact requires the following prerequisites:

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

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

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

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

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

- RabbitMQ Server (supported versions are 3.8.0 through to 3.8.8), available here: <https://github.com/rabbitmq/rabbitmq-server/releases/>



Installation guidance is provided here 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 19](#) for more information.
- The Interact system is a Web Server and therefore requires IIS Web Server and the .NET Core components installed. These are all installed as part of a successful installation of Blue Prism Interact using the Blue Prism Hub and the Blue Prism Interact installation media .
- 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 certificate or 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. See [Configure SSL certificates](#) for details.
- By default, the IIS Application Pools are used. Application pools must have access to the application files and two certificates that are created during installation for data protection and authorization. These certificates are BluePrismCloud_Data_Protection and BluePrismCloud_IMS_JWT are located within the default Windows certificate folder. If using Windows Authorization for access to SQL server, this will need to be configured manually.
- 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 3.8.0 to 3.8.8 For more information, see Downloading and Installing RabbitMQ . | Install the Message Broker server on page 15 |
| Erlang/OTP The version of Erlang that you require is dependent on the RabbitMQ version you intend to use. For more information, see RabbitMQ Erlang Version Requirements . | |
| IIS 10.0 Included with Windows Server 2016 and Windows Server 2019. | Install and configure the web server on page 19 |
| .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 4.2 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 4.2 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 |


Software requirements and permissions

Software requirements

The following technologies are supported for use with the software:

Operating system


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

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

Microsoft SQL server

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

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

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

The following are also supported:

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

Message Broker server

The following software is required on the Message Broker server:

- RabbitMQ 3.8.0 to 3.8.8.
- Erlang/OTP – The version of Erlang that you require is dependent on the RabbitMQ version you intend to use.

See [Install the Message Broker server on page 15](#) 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 19](#) for more information.

Blue Prism

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

Minimum SQL permissions

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

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

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

- db_datareader
- db_datawriter

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

For more information, see [Default application information below](#).

Default application information

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



For information on the Hub applications, see [Hub software requirements and permissions](#).

Interact websites

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

Interact services

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

Multi-device deployment considerations


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

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

Network ports


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

| | |
|------------------------------|---|
| 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: <ul style="list-style-type: none">• The TCP Port for the named instance (this is dynamic by default from the ephemeral range) or the defined port if a static one to allow SQL Server Connectivity from the Web Server.• UDP Port 1434 for the SQL Server Browser Service to allow SQL Server Connectivity from the Web Server. |
| Message Broker server | Port 5672 to allow RabbitMQ Messaging connectivity. Port 15672 to allow RabbitMQ Management Console connectivity. |
| Web server | Port 443 to allow HTTPS connectivity. |
| Digital Workers | Port 443 to allow HTTPS connectivity. |

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

Typical deployment

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

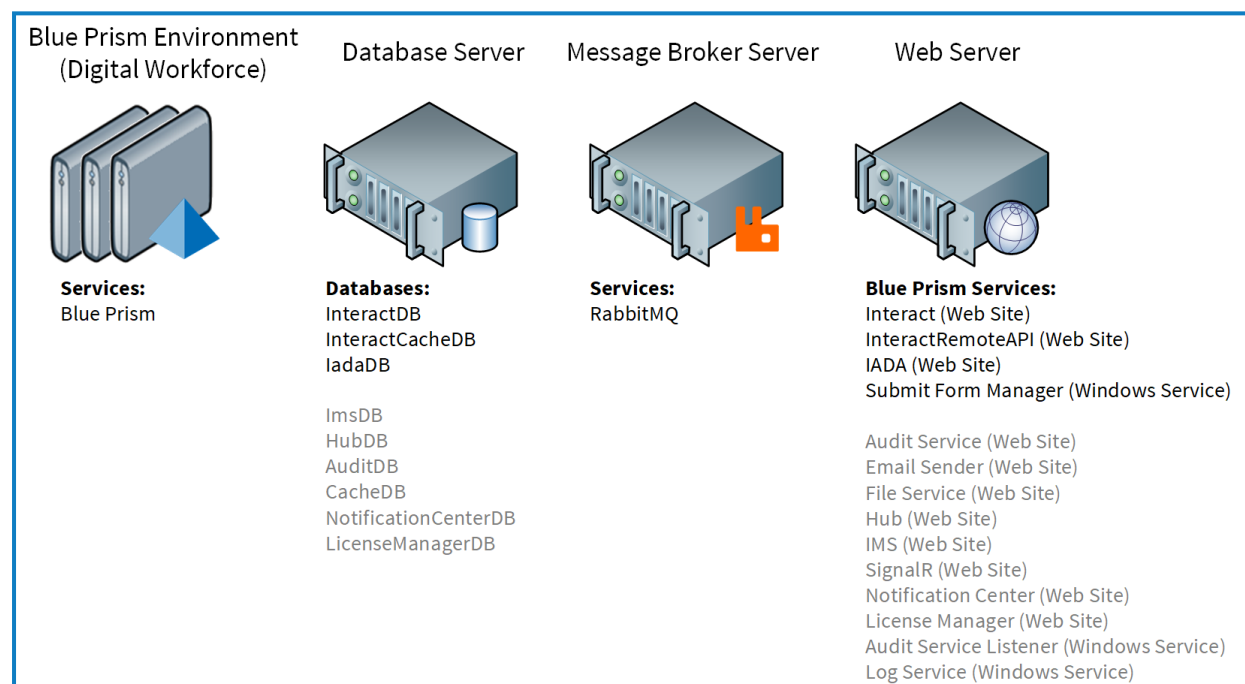
 Prior to following this guidance, ensure that you have fully considered the information in [Preparation](#).

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

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

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

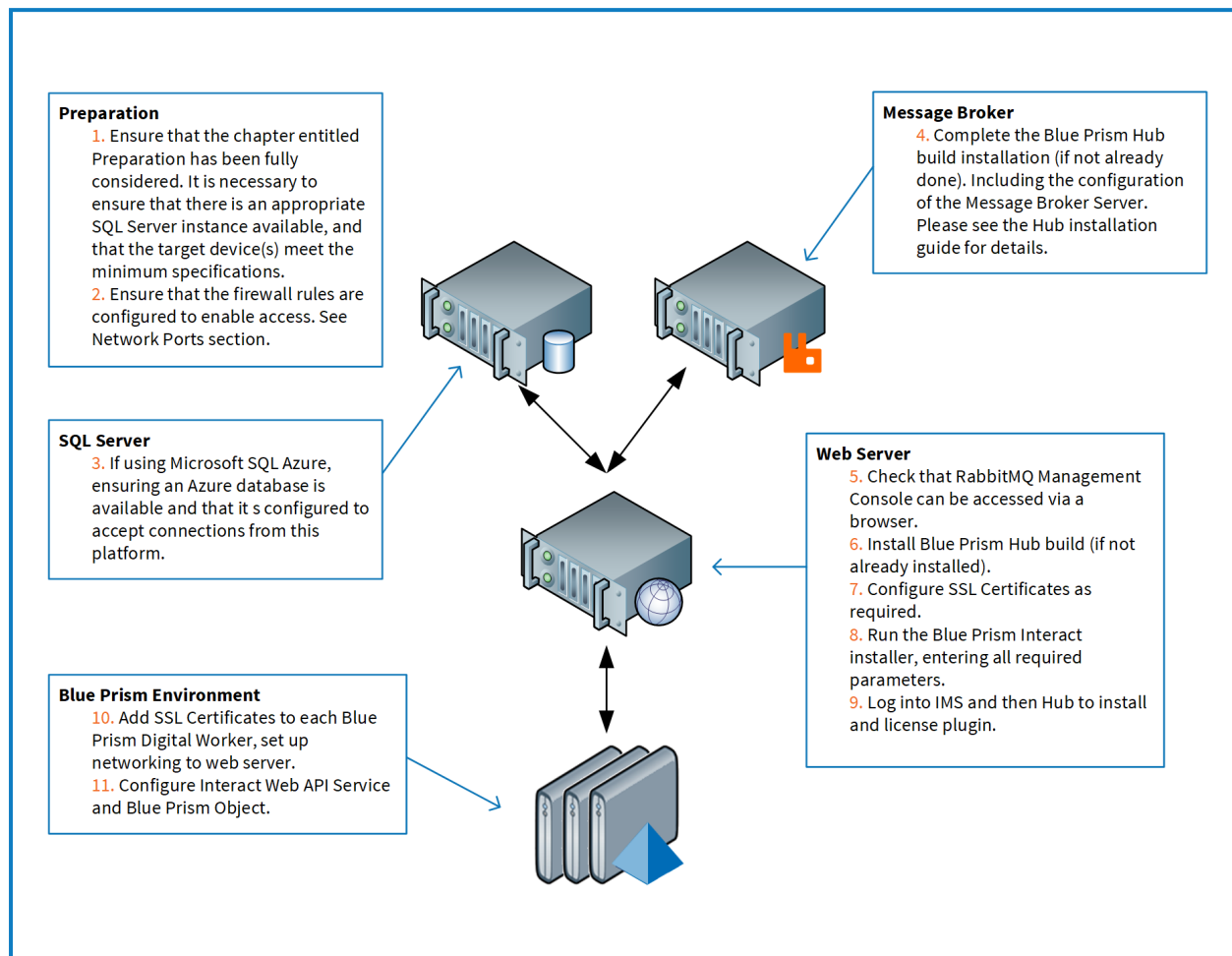
The diagram below illustrates the typical architecture for an environment.



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

Overview of typical installation steps

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



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

Install the Message Broker server

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

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

1. Install [Erlang/OTP](#).



For:

- Erlang/OTP version and support, see: [RabbitMQ Erlang Version Requirements](#).
- Installation 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
```

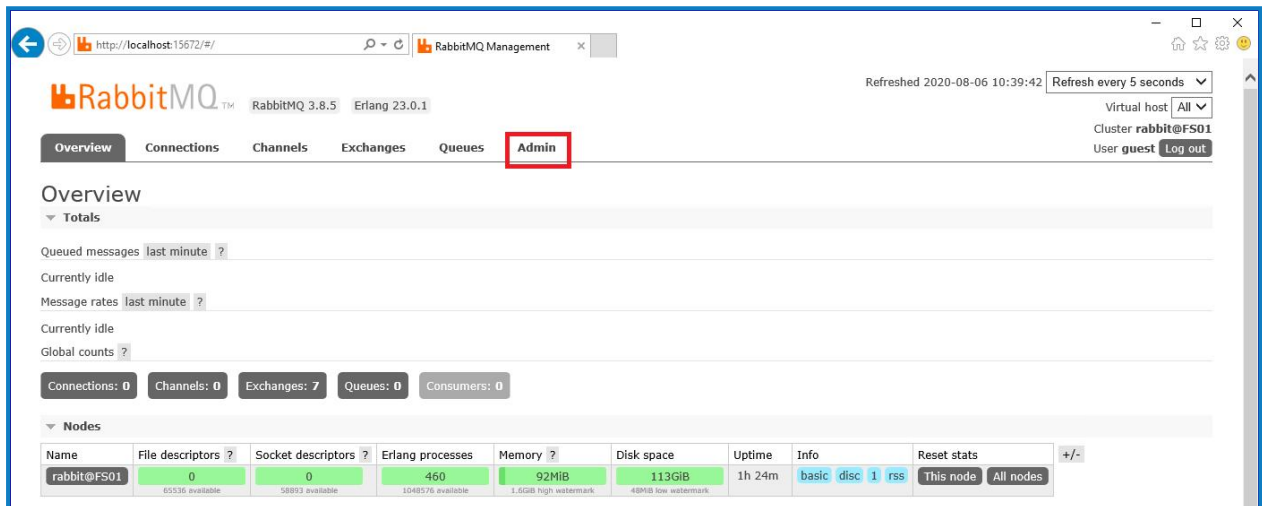
```
Administrator: RabbitMQ Command Prompt (sbin dir)
C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.5\sbin>rabbitmq-plugins enable rabbitmq_management
Enabling plugins on node rabbit@FS01:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent
  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>

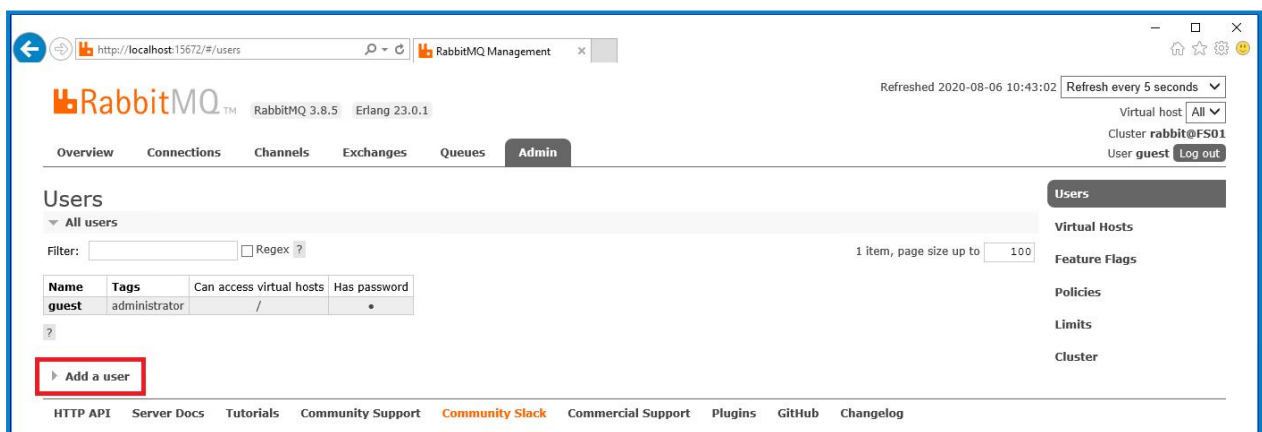
7. In the RabbitMQ console, log on with the default credentials of guest/guest.




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

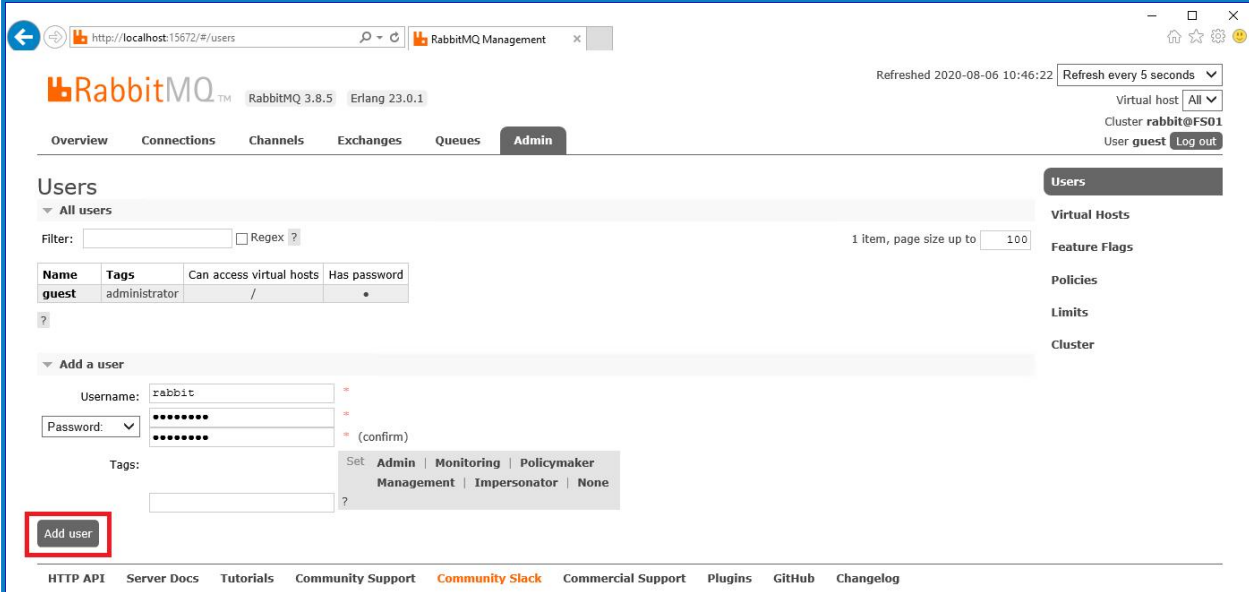


9. Click **Add a user**.



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 # / : ? @ \ ' " \$ '.

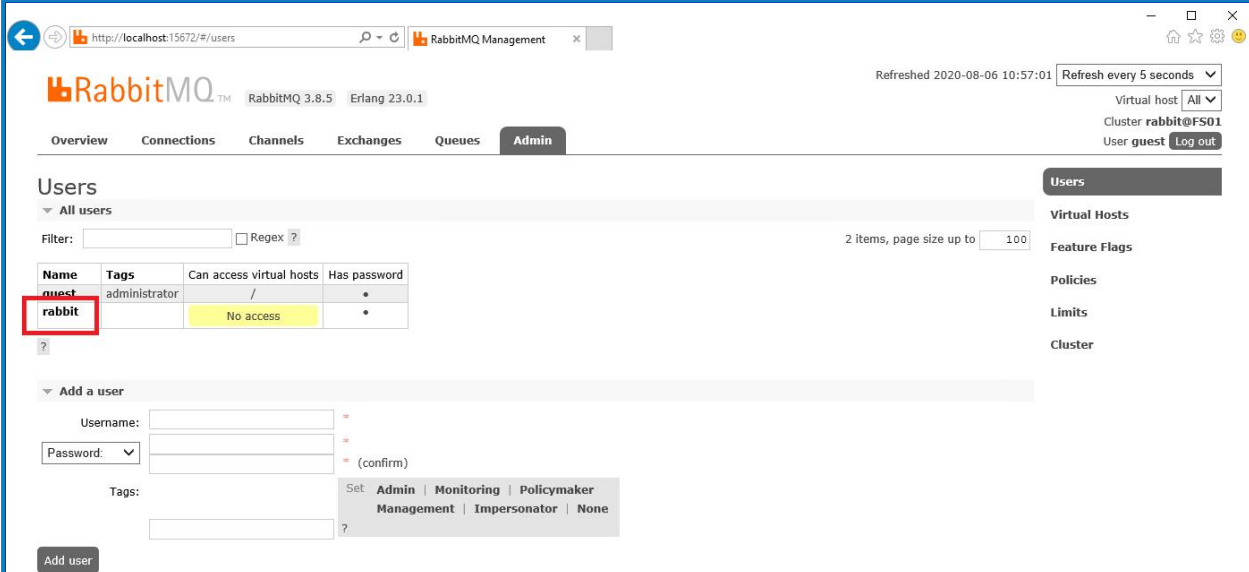
11. Click **Add User**.

The screenshot shows the RabbitMQ Management interface. The 'Admin' tab is selected. In the 'Users' section, the 'Add a user' form is visible. The 'Add user' button at the bottom left of the form is highlighted with a red rectangle. The form fields include Username (set to 'rabbit'), Password (masked with dots), and Tags (set to 'Admin', 'Monitoring', 'Policymaker', 'Management', 'Impersonator', 'None').

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

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

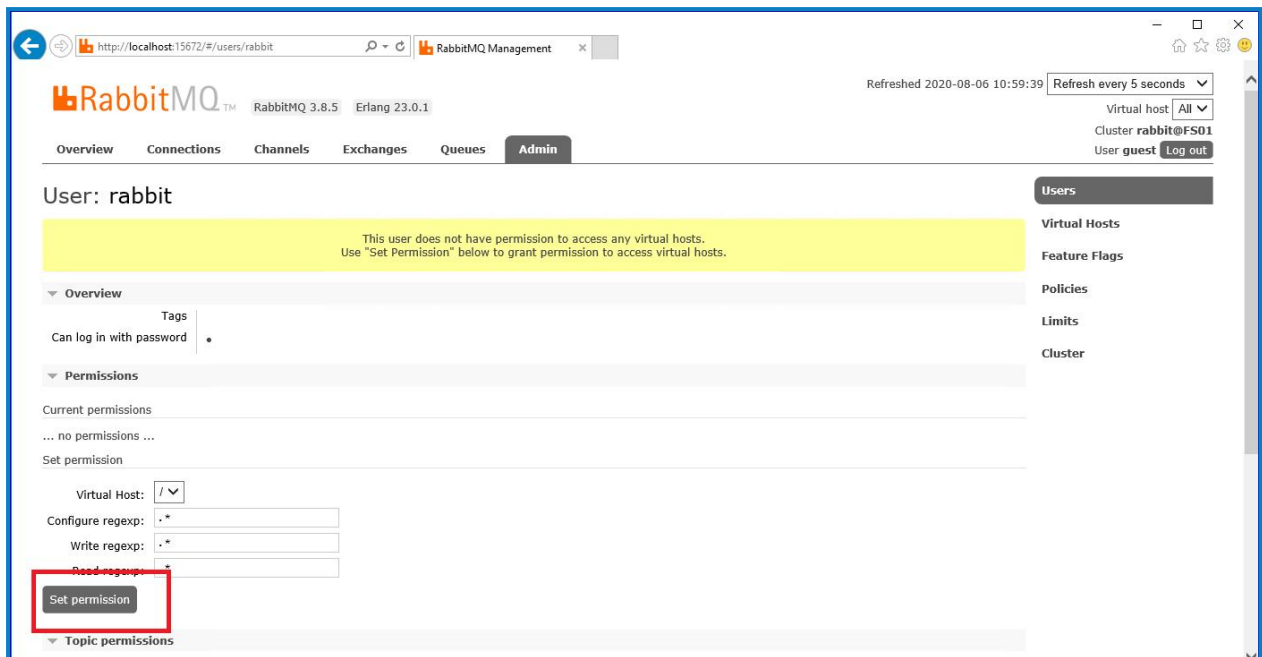
12. Click on the username of the user that you just created.



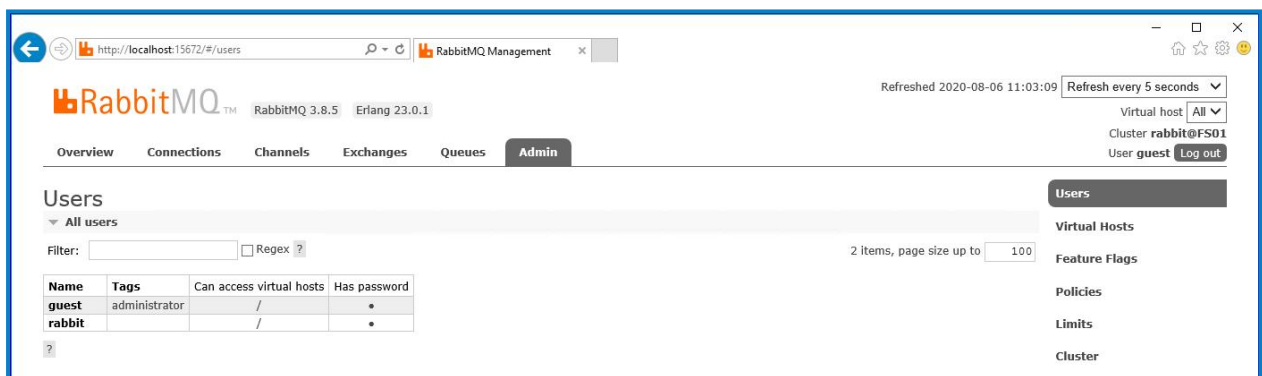
The screenshot shows the RabbitMQ Management interface. The 'Admin' tab is selected. In the 'Users' section, the 'rabbit' user is now listed in the table. The 'rabbit' username in the table is highlighted with a red rectangle. The 'Add a user' form is still visible below the table.

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


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.

Check RabbitMQ Message Broker connectivity

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

The RabbitMQ Management Console should display. You will not be able to login into the Management Console as by default the guest is restricted to local access 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 58](#).

Install and configure the web server

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](#)

 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. However, the first part of the default host name must not be changed; you can only change the *.local* part of the host name.

Install IIS

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

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

Scripted installation

Run the command below using the PowerShell command prompt:

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

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

Configure SSL certificates

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

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

The tables below details the required SSL certificates.

Hub websites:

| Website in IIS | Default URL |
|----------------------------------|----------------------------|
| Blue Prism – IMS | https://ims.local |
| Blue Prism – Hub | https://hub.local |
| Blue Prism – Email Sender | https://email.local |
| Blue Prism – Audit Service | https://audit.local |
| Blue Prism – File Service | https://file.local |
| Blue Prism – Notification Center | https://notification.local |
| Blue Prism – License Manager | https://license.local |
| Blue Prism – SignalR | https://signalr.local |

Interact websites:

| Website in IIS | Default URL |
|----------------------------------|---------------------------------|
| Blue Prism – Interact | https://interact.local |
| Blue Prism – IADA | https://iada.local |
| Blue Prism – Interact Remote API | https://interactremoteapi.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:

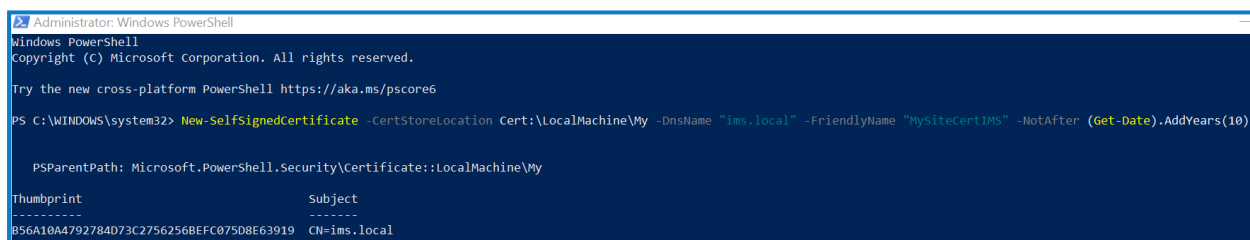
1. Run PowerShell as an administrator and use the following command, replacing `[Website]` and `[ExpiryYears]` with appropriate values:

```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "[Website].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.

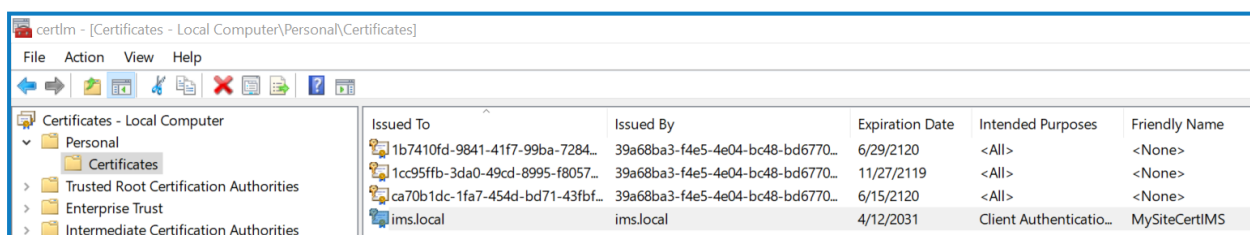
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "ims.local" -FriendlyName "MySiteCertIMS" -NotAfter (Get-Date).AddYears(10)

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

Thumbprint                               Subject
-----
856A10A4792784D73C27562568EFC075D8E63919  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.



| Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name |
|----------------------------------|-----------------------------------|-----------------|-------------------------|---------------|
| 1b7410fd-9841-41f7-99ba-7284... | 39a68ba3-f4e5-4e04-bc48-bd6770... | 6/29/2120 | <All> | <None> |
| 1cc95ffb-3da0-49cd-8995-f8057... | 39a68ba3-f4e5-4e04-bc48-bd6770... | 11/27/2119 | <All> | <None> |
| ca70b1dc-1fa7-454d-bd71-43bf... | 39a68ba3-f4e5-4e04-bc48-bd6770... | 6/15/2120 | <All> | <None> |
| ims.local | ims.local | 4/12/2031 | Client Authenticatio... | MySiteCertIMS |

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)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "signalr.local" -
FriendlyName "MySiteCertSignalR" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "notification.local" -
FriendlyName "MySiteCertNotification" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "license.local" -
FriendlyName "MySiteCertLicense" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "interact.local" -
FriendlyName "MySiteCertInteract" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "iada.local" -
FriendlyName "MySiteCertIADA" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
"interactremoteapi.local" -FriendlyName "MySiteCertIRA" -NotAfter (Get-Date).AddYears(10)
```

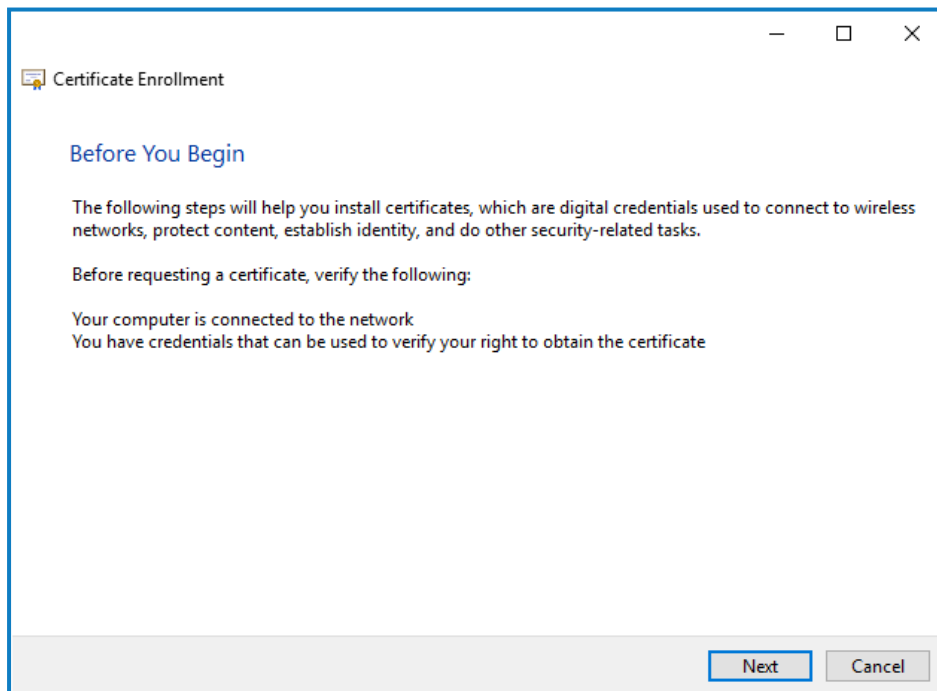
Once created, open the Local Machine certificate manager (certlm) and copy and paste the certificates into the trusted root certificate store.

Create an offline certificate request

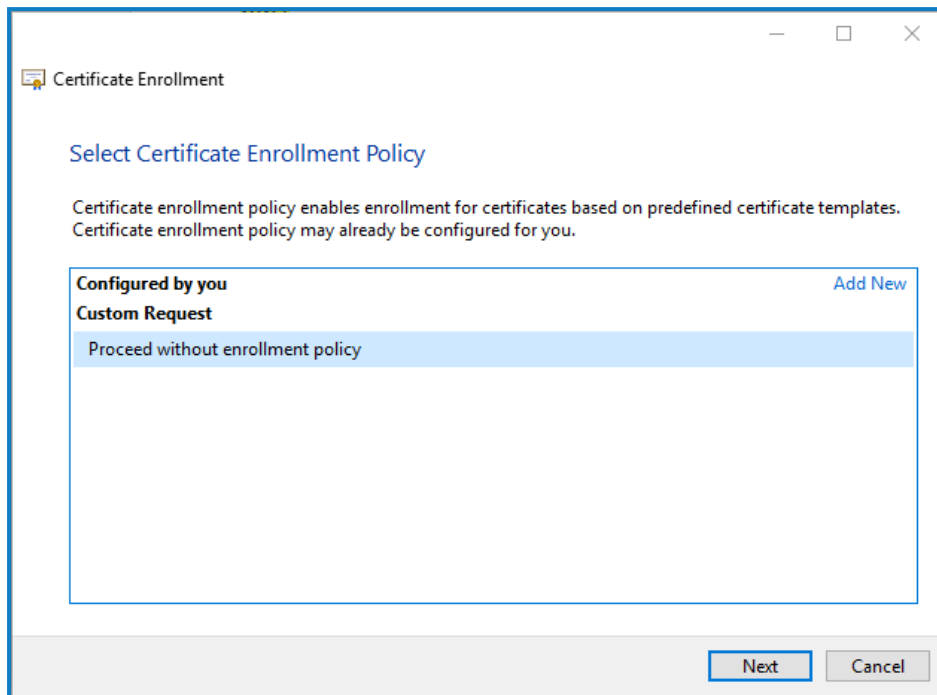
To create an offline certificate request, for each certificate follow this procedure:

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.

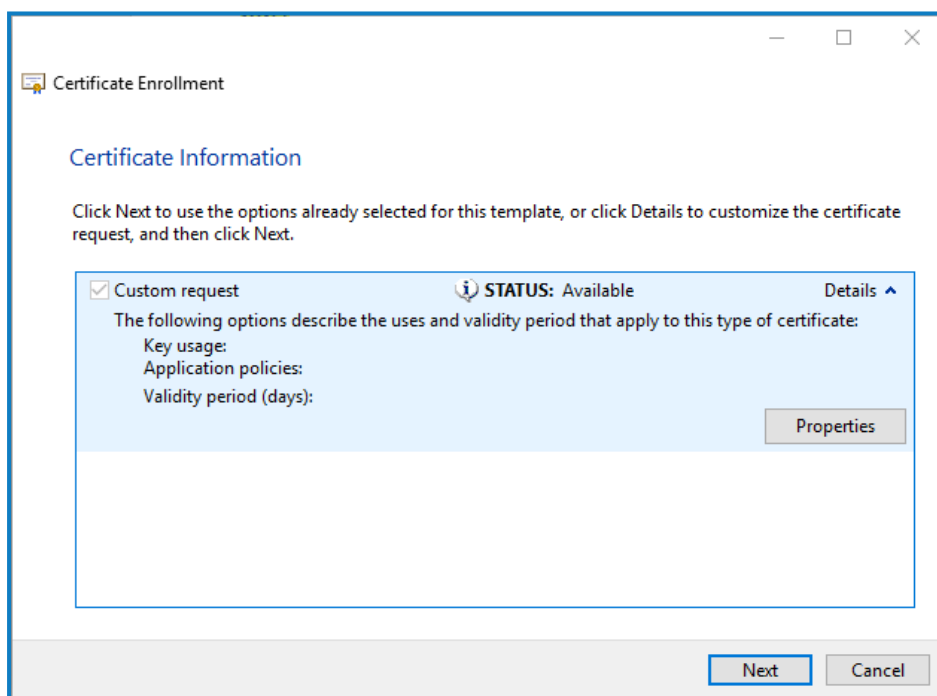
The Certificate Enrollment wizard displays.



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.

The screenshot shows the 'Certificate Properties' dialog box with the 'Subject' tab selected. The dialog has four tabs: 'General', 'Subject', 'Extensions', and 'Private Key'. The 'Subject' tab contains the following elements:


- A text box with the instruction: "The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate."
- A section titled "Subject of certificate" with the subtitle "The user or computer that is receiving the certificate".
- A "Subject name:" section with a "Type:" dropdown menu set to "Common name" and a "Value:" text box.
- An "Add >" button next to the "Value:" text box.
- A "< Remove" button below the "Add >" button.
- A list box on the right showing "CN=https://ims.local".
- An "Alternative name:" section with a "Type:" dropdown menu set to "Directory name" and a "Value:" text box.
- An "Add >" button next to the "Value:" text box.
- A "< Remove" button below the "Add >" button.
- A list box on the right (empty).
- At the bottom, there are three buttons: "OK", "Cancel", and "Apply".

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 following .NET Core components must be downloaded and installed:


| Step | Details |
|------|--|
| 1 | <p>Download the following components and store them in a temporary location, for example, C:\temp:</p> <ul style="list-style-type: none">• .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 |
| 2 | <p>To install the .NET dependencies, run each of the following commands using the PowerShell command prompt, waiting until each completes, before running the next command:</p> <pre>start-process "C:\temp\dotnet-hosting-3.1.3-win.exe" /q -wait start-process "C:\temp\windowsdesktop-runtime-3.1.3-win-x64.exe" /q -wait start-process "C:\temp\vcredist_x64.exe" /q -wait start-process "C:\temp\NDP472-KB4054531-Web.exe" /q -wait</pre> <p> Ensure the file path matches the location where the files were stored in step 1.</p> |


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

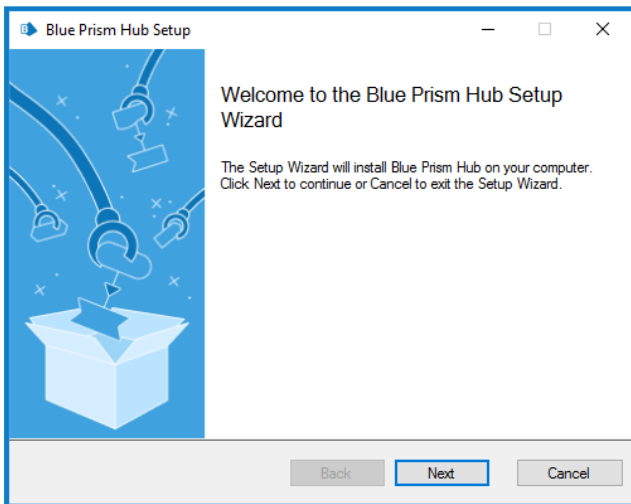
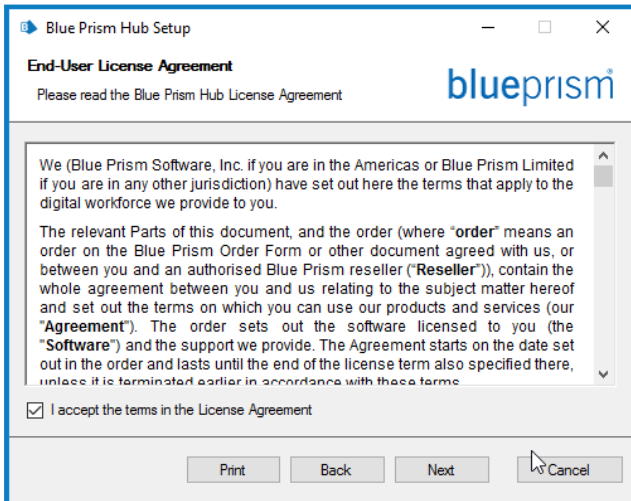
Install Blue Prism Hub

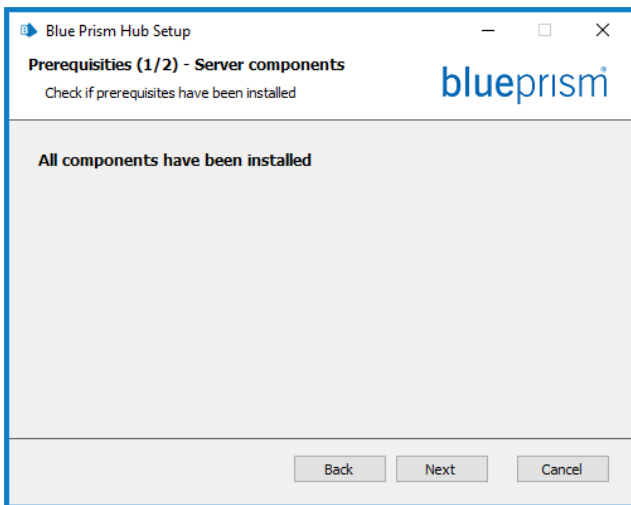
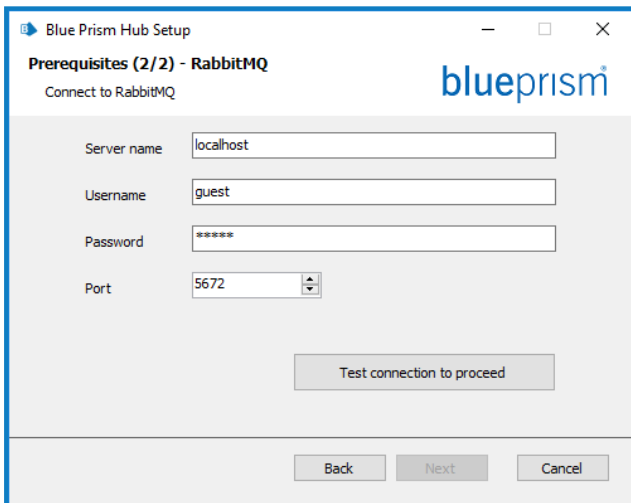

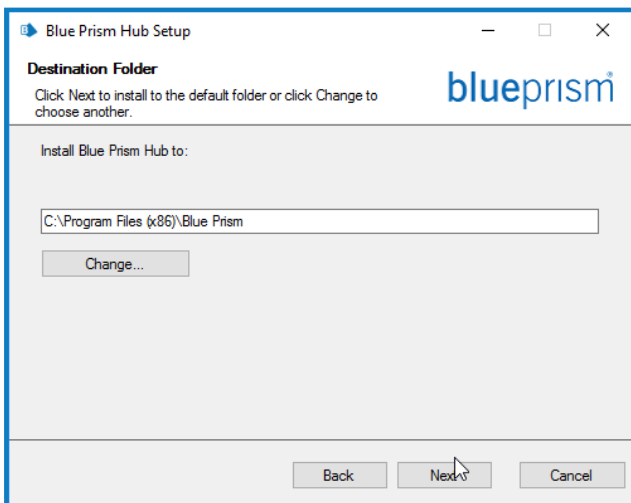
The steps below detail the process for installing the Blue Prism Hub software. This includes the Identify Management System (IMS), Hub, and other associated services. The installation process will create any new databases that are required.

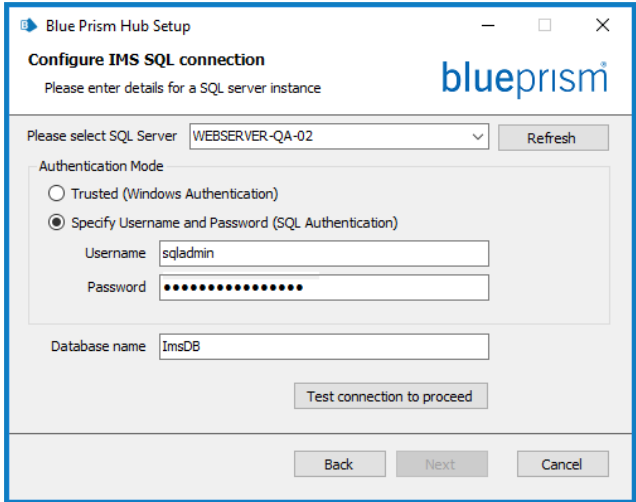
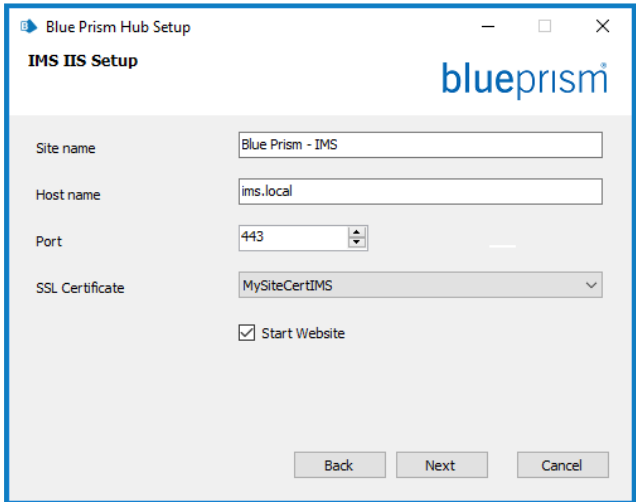

Download and run the Blue Prism Hub installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer must be run with administrator rights.

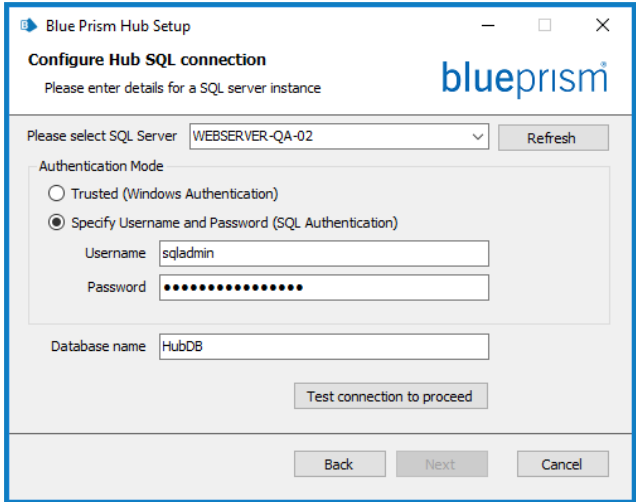
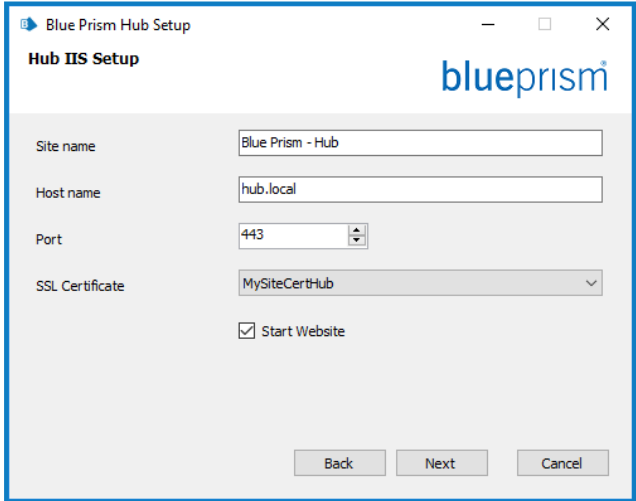

 You will need your Customer ID during this installation. This can be found in the email that was sent to you when you purchased Interact or ALM.

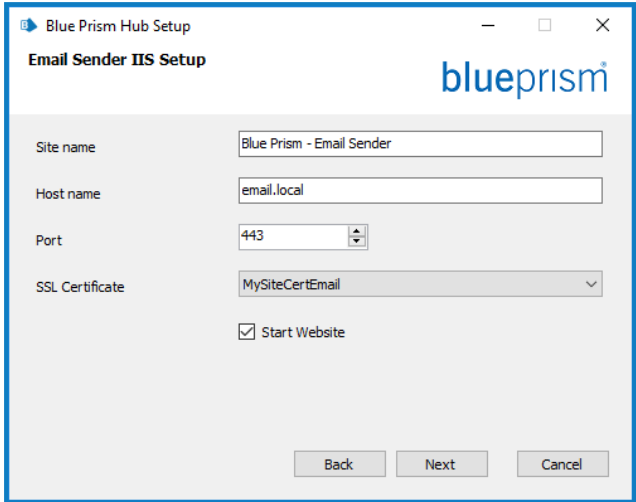

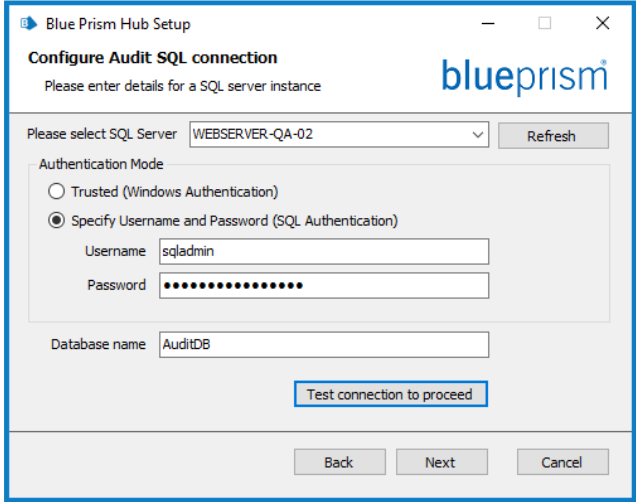
 If reinstalling Blue Prism Hub after previously using and removing it, and the same database names are to be used, it is recommended that the databases should be cleared of any old data before re-installing.

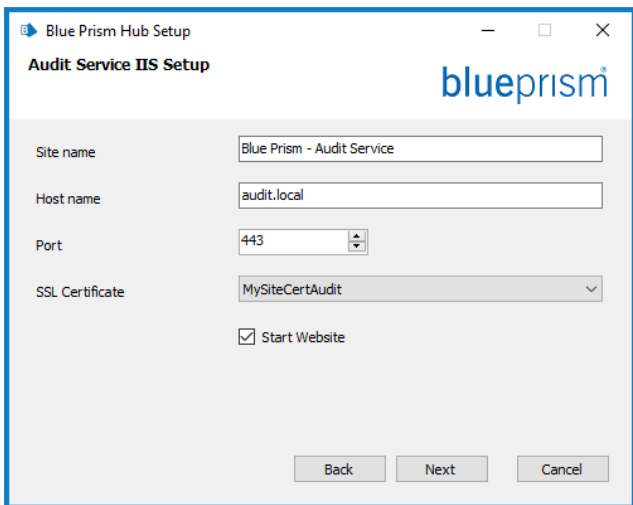

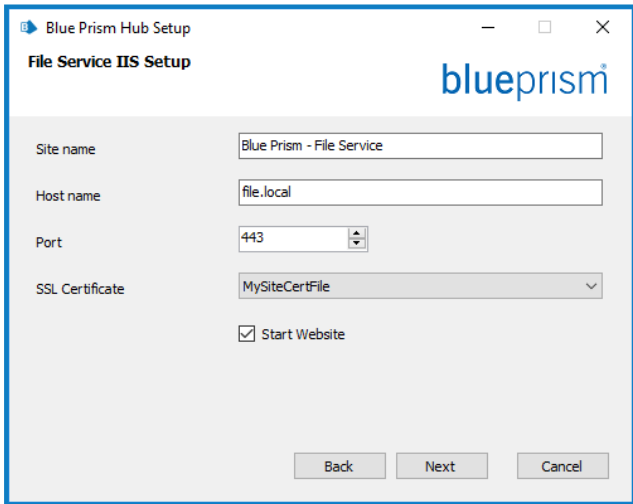

| Step | Installer page | Details |
|------|---|--|
| 1 |  <p>The screenshot shows the 'Blue Prism Hub Setup' window. It has a blue header with the title 'Blue Prism Hub Setup'. Below the title is a graphic of a blue box with a star and some abstract lines. To the right of the graphic, the text reads: 'Welcome to the Blue Prism Hub Setup Wizard. The Setup Wizard will install Blue Prism Hub on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.</p> | Welcome Click Next . |
| 2 |  <p>The screenshot shows the 'Blue Prism Hub Setup' window displaying the 'End-User License Agreement'. The title bar says 'Blue Prism Hub Setup'. Below the title bar, it says 'End-User License Agreement' and 'Please read the Blue Prism Hub License Agreement'. The Blue Prism logo is in the top right corner. The main area contains the license agreement text, which is partially visible. At the bottom, there is a checkbox labeled 'I accept the terms in the License Agreement' which is checked. Below the checkbox are four buttons: 'Print', 'Back', 'Next', and 'Cancel'.</p> | License agreement Read the End-User License Agreement and if you agree to the terms, select the check box. |

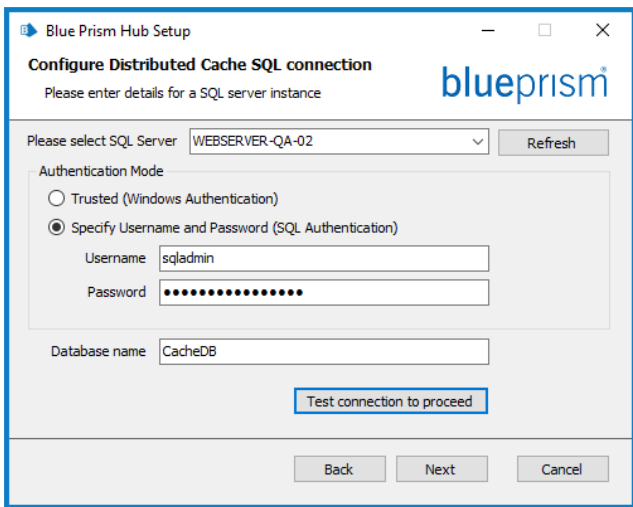
| Step | Installer page | Details |
|------|---|--|
| 3 |  | <p>Prerequisites 1 – Server components</p> <p>The installer checks that the prerequisites have been installed. Those that are not installed are identified. You cannot proceed until all the prerequisites are installed.</p> <p>If there are uninstalled prerequisites, cancel the installer and install the missing components before restarting the installer. Otherwise, proceed with the installation.</p> |
| 4 |  | <p>Prerequisites 2 – RabbitMQ</p> <p>Enter the server name or IP address of the Message Broker server and the credentials of the user you created.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> The default message queuing port is 5672. This should only be changed if the default ports have been changed by your IT support organization.</p> </div> <p>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 58 for further details.</p> |
| 5 |  | <p>Destination folder</p> <p>Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism, but you can choose your own using the Change button.</p> |

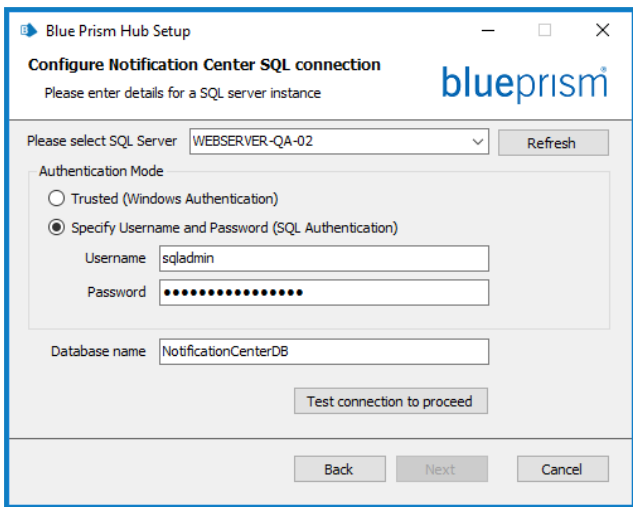
| Step | Installer page | Details |
|------|---|--|
| 6 |  | <h3>IMS SQL connection</h3> <p>Configure the settings for the IMS database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information. • If SQL Authentication is selected, enter the username and password. <p>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 58 for further details.</p> |
| 7 |  | <h3>IMS IIS setup</h3> <p>Configure IIS for the IMS website. You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <code>.local</code> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;">  The use of uppercase characters in URLs is not supported. </div> <ul style="list-style-type: none"> • Enter the port number. • Select the appropriate SSL certificate. • Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

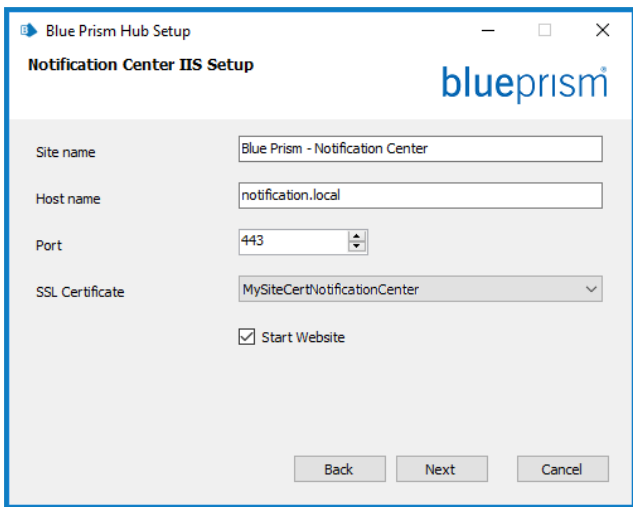

| Step | Installer page | Details |
|------|---|---|
| 8 |  | <h3>Hub SQL connection</h3> <p>Configure the settings for the Hub database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information. • If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>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 58 for further details.</p> |
| 9 |  | <h3>Hub IIS setup</h3> <p>Configure the Hub website. You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <code>.local</code> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p> The use of uppercase characters in URLs is not supported.</p> </div> <ul style="list-style-type: none"> • Enter the port number. • Select the appropriate SSL certificate. • Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

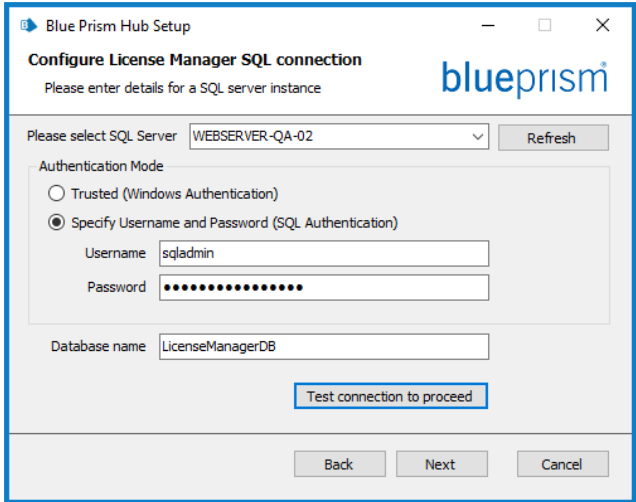
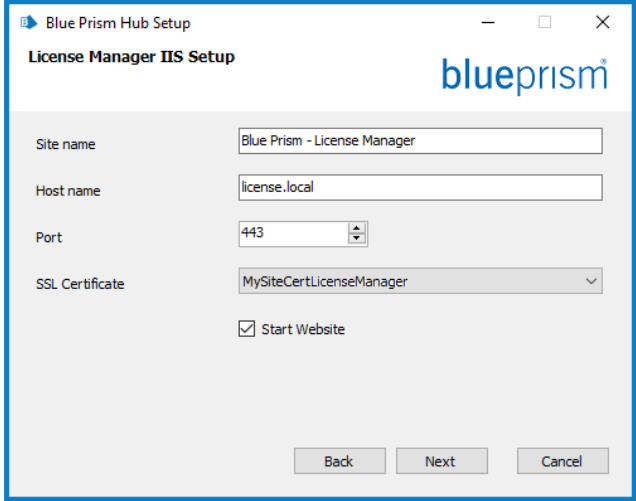

| Step | Installer page | Details |
|------|---|--|
| 10 |  | <h3>Email Sender IIS setup</h3> <p>Configure the Email Sender website. You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase characters – This will be used as the URL for the site. The first part of the default host name must not be changed. You can only change the <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;">  The use of uppercase characters in URLs is not supported. </div> <ul style="list-style-type: none"> • 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. |
| 11 |  | <h3>Audit SQL connection configuration</h3> <p>Configure the settings for the Audit database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information. • If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>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 58 for further details.</p> |

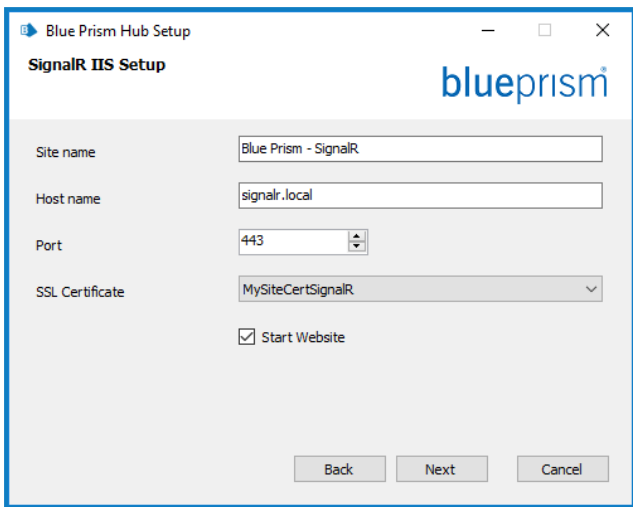

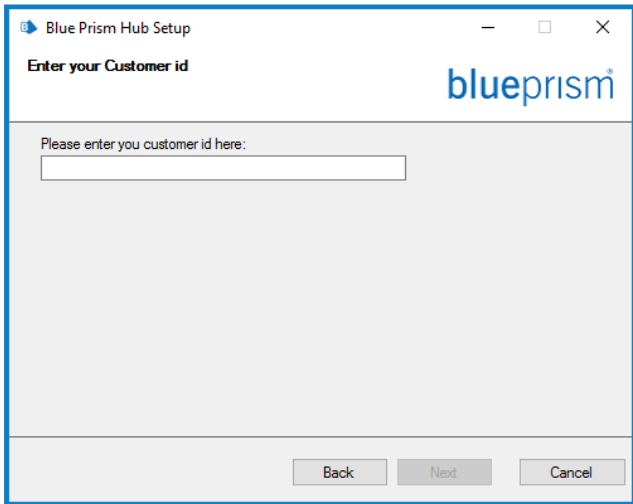
| Step | Installer page | Details |
|------|---|---|
| 12 |  | <h3>Audit Service IIS setup</h3> <p>Configure the Audit Service website. You need to:</p> <ul style="list-style-type: none">• Enter a site name.• Enter a host name in lowercase characters – This will be used as the URL for the site. The first part of the default host name must not be changed. You can only change the <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div> The use of uppercase characters in URLs is not supported.</div> <ul style="list-style-type: none">• 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. |
| 13 |  | <h3>File Service IIS setup</h3> <p>Configure the File Service website. You need to:</p> <ul style="list-style-type: none">• Enter a site name.• Enter a host name in lowercase 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 <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div> The use of uppercase characters in URLs is not supported.</div> <ul style="list-style-type: none">• Enter the port number.• Select the appropriate SSL certificate.• Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

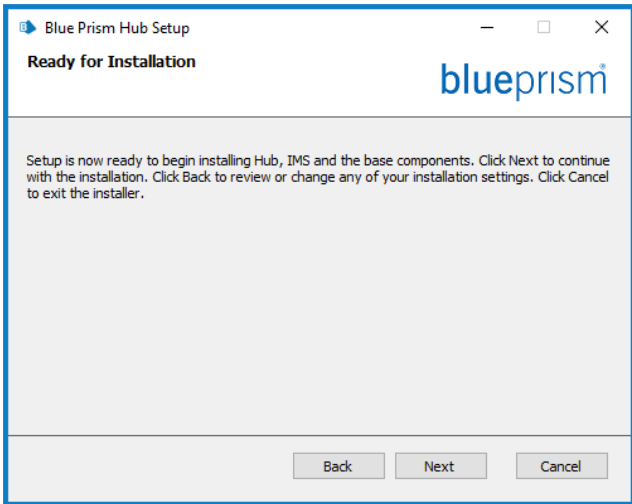
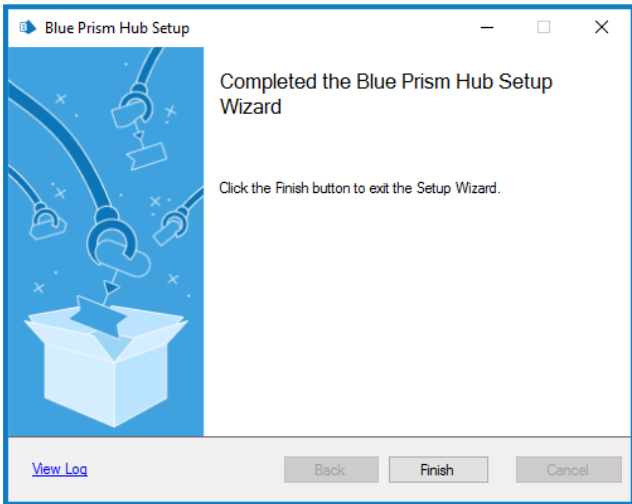
| Step | Installer page | Details |
|------|---|--|
| 14 |  | <h3>Distributed Cache SQL connection</h3> <p>Configure the settings for the Cache database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none">• If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information.• If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>Click Test connection to proceed to test the SQL credentials and verify connectivity.</p> <p>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 58 for further details.</p> |

| Step | Installer page | Details |
|------|---|--|
| 15 |  | <h3>Notification Center SQL connection</h3> <p>Configure the settings for the Notification Center database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none">• If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information.• If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>Click Test connection to proceed to test the SQL credentials and verify connectivity.</p> <p>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 58 for further details.</p> |

| Step | Installer page | Details |
|------|---|--|
| 16 |  | <h3>Notification Center IIS setup</h3> <p>Configure the Notification Center website.</p> <p>You need to:</p> <ul style="list-style-type: none">• Enter a site name.• Enter a host name in lowercase 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 <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div> The use of uppercase characters in URLs is not supported.</div> <ul style="list-style-type: none">• Enter the port number.• Select the appropriate SSL certificate.• Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

| Step | Installer page | Details |
|------|---|--|
| 17 |  | <h3>License Manager SQL connection</h3> <p>Configure the settings for the License Manager database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication on page 59 for further information. • If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>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 58 for further details.</p> |
| 18 |  | <h3>License Manager IIS setup</h3> <p>Configure the License Manager website. You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <code>.local</code> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> <p> The use of uppercase characters in URLs is not supported.</p> </div> <ul style="list-style-type: none"> • Enter the port number. • Select the appropriate SSL certificate. • Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

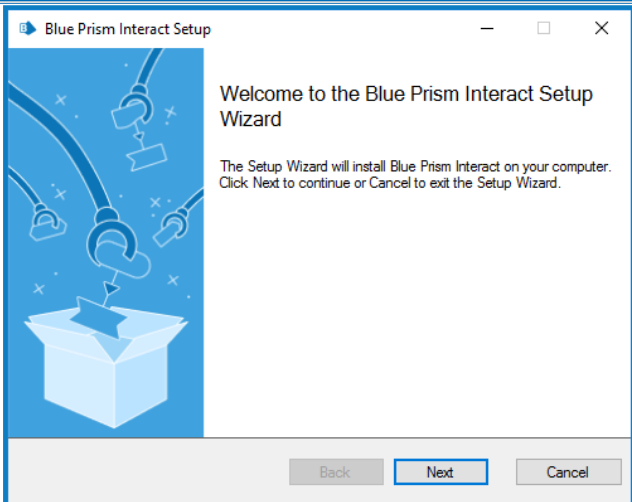
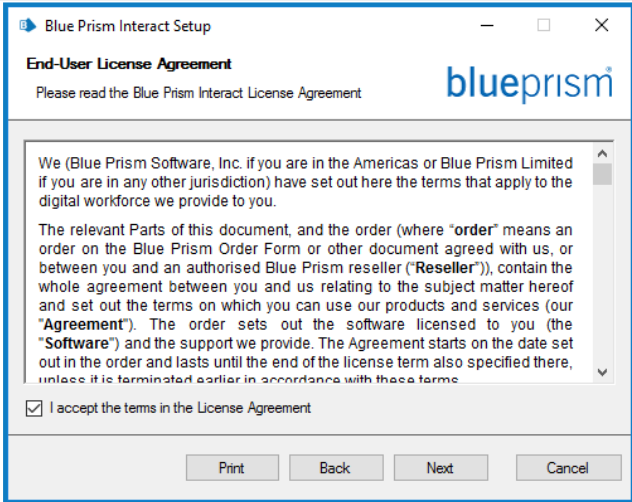
| Step | Installer page | Details |
|------|---|---|
| 19 |  | <h3>SignalR IIS setup</h3> <p>Configure the SignalR website. You need to:</p> <ul style="list-style-type: none">• Enter a site name.• Enter a host name in lowercase characters – This will be used as the URL for the site. The first part of the default host name must not be changed. You can only change the <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div> The use of uppercase characters in URLs is not supported.</div> <ul style="list-style-type: none">• Enter the port number.• Select the appropriate SSL certificate.• Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |
| 20 |  | <h3>Enter your Customer Id</h3> <p>Enter your customer identifier. This identifier is supplied to you by Blue Prism when you receive your product license for ALM or Interact.</p> <p>If you have not purchased a licensed plugin, you can enter your own value.</p> |

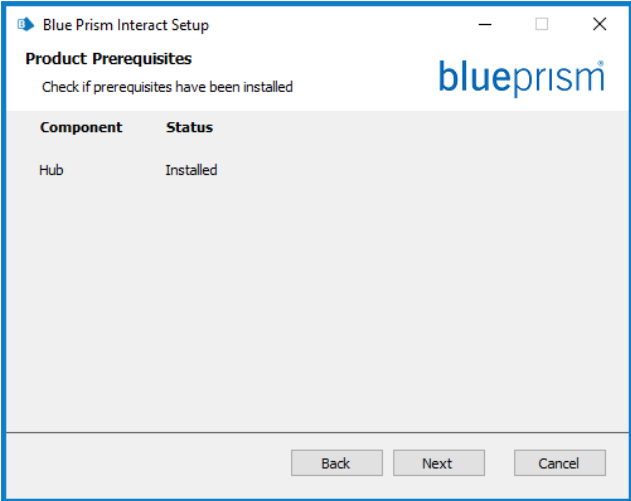

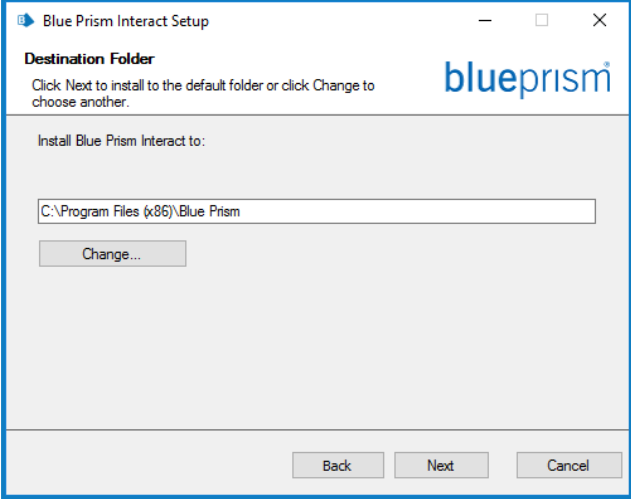
| Step | Installer page | Details |
|------|--|---|
| 21 |  | Ready for Installation Click Next to install Hub. |
| 22 |  | Installation complete If the installation fails, the View Log option gives details of the error that was encountered. For more information, see Troubleshoot a Hub installation on page 58 . |

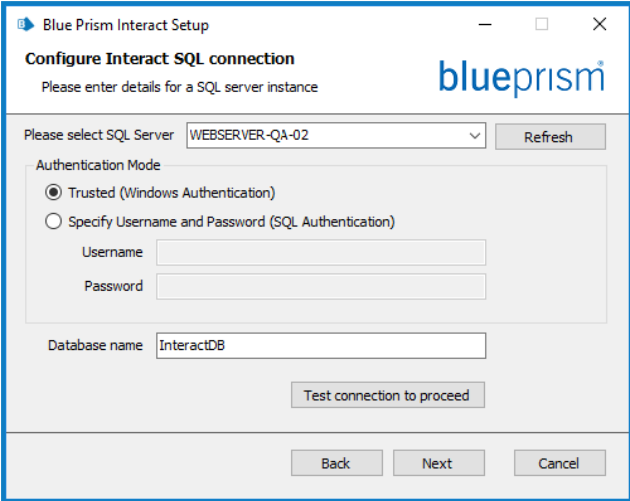
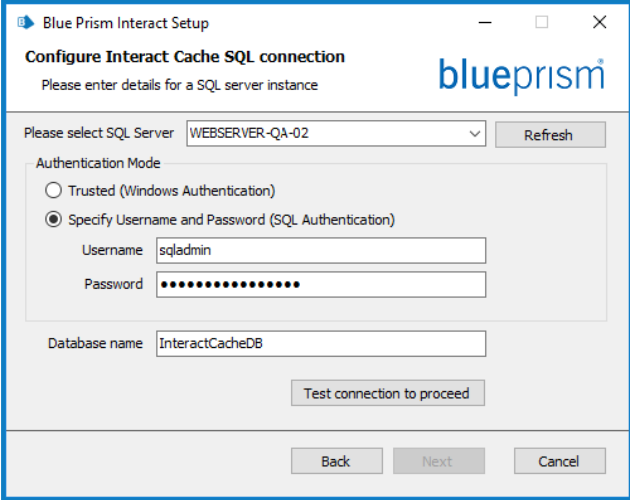
Install Blue Prism Interact

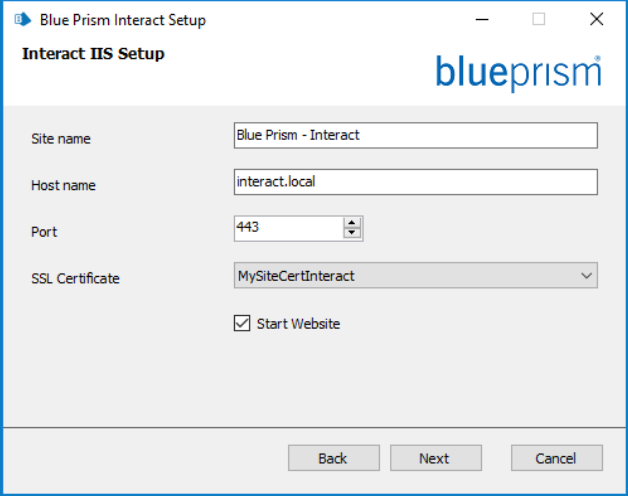

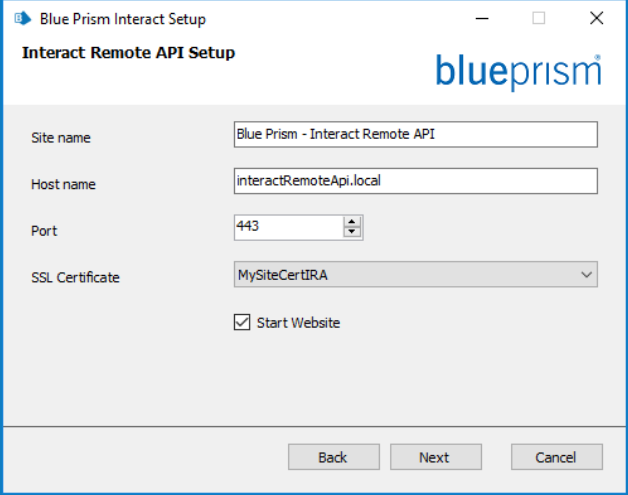

The steps below detail the process for installing the Blue Prism Interact software. This assumes that [Blue Prism Hub](#) has been installed which includes the Identify Management System (IMS), Hub, and other associated services.

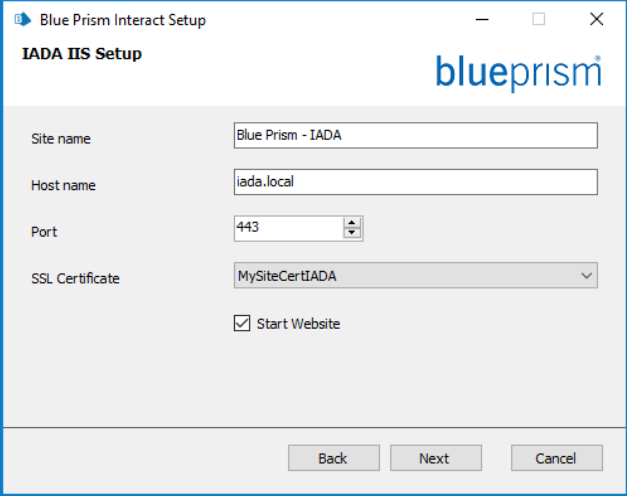

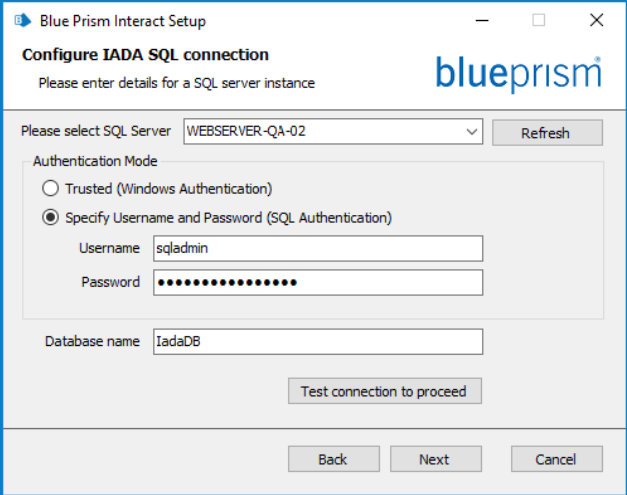
Download and run the Blue Prism Interact installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer must be run with administrator rights.

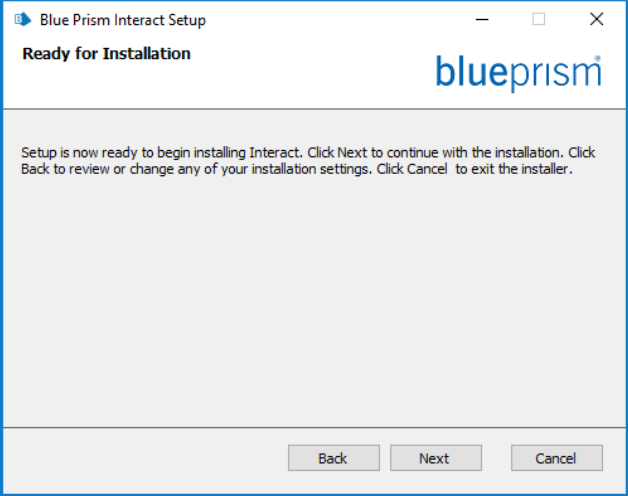
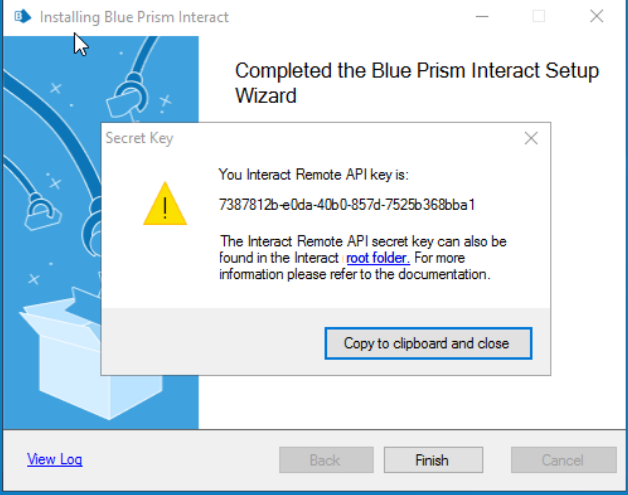

| Step | Installer page | Details |
|------|---|--|
| 1 |  | Welcome Click Next . |
| 2 |  | License agreement Read the End-User License Agreement and if you agree to the terms, select the check box. |

| Step | Installer page | Details |
|------|--|---|
| 3 |  | Product prerequisites <p>The installer checks that the prerequisites have been installed. If the installer finds any prerequisites missing these will be notified to you. Otherwise, continue with the installation.</p> <div> You cannot proceed unless all prerequisites have been installed.</div> |
| 4 |  | Destination folder <p>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.</p> |

| Step | Installer page | Details |
|------|---|--|
| 5 |  | <h3>Configure Interact SQL configuration</h3> <p>Configure the settings for the Interact Database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. • If SQL Authentication is selected, enter the username and password. <p>Click Test connection to proceed to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot an Interact installation on page 56 for further details.</p> |
| 6 |  | <h3>Configure Interact Cache SQL configuration</h3> <p>Configure the settings for the Interact Cache Database by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. • If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>Click Test connection to proceed to test the SQL credentials and verify connectivity. A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot an Interact installation on page 56 for further details.</p> |

| Step | Installer page | Details |
|------|---|---|
| 7 |  | <h3>Interact IIS setup</h3> <p>Configure the Interact website. You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;">  The use of uppercase characters in URLs is not supported. </div> <ul style="list-style-type: none"> • Enter the port number. • Select the appropriate SSL certificate. • Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |
| 8 |  | <h3>Interact Remote API setup</h3> <p>You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <i>.local</i> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;">  The use of uppercase characters in URLs is not supported. </div> <ul style="list-style-type: none"> • Enter the port number. • Select the appropriate SSL certificate. • Leave Start Website selected, unless you do not want the website to automatically start at the end of the installation. |

| Step | Installer page | Details |
|------|---|--|
| 9 |  | <h3>IADA IIS setup</h3> <p>You need to:</p> <ul style="list-style-type: none"> • Enter a site name. • Enter a host name in lowercase 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 <code>.local</code> part of the host name. Ensure that you consider your DNS and Domain structure when choosing a host name. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;">  The use of uppercase characters in URLs is not supported. </div> <ul style="list-style-type: none"> • 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. |
| 10 |  | <h3>Configure IADA SQL configuration</h3> <p>Configure the settings for IADA by providing the SQL Server host name or IP address, and the credentials for the account to create the database:</p> <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. • If SQL Authentication is selected, enter the username and password. <p>The database name can be left as the default value or changed as required.</p> <p>Click Test connection to proceed to test the SQL credentials and verify connectivity.</p> <p>A notification will display the result of the test. You will only be able to move on to the next step if the test is successful. If the test failed, see Troubleshoot an Interact installation on page 56 for further details.</p> |

| Step | Installer page | Details |
|------|--|--|
| 11 |  | Ready for Installation Click Next to install Interact. |
| 12 |  | Installation complete When the installation completes successfully, the Interact Remote API secret key displays and you can copy it to your clipboard. This key is used to set up the Interact APIs in Blue Prism. The key is also stored in the installation root directory, for example, in C:\Program Files (x86)\Blue Prism\Interact Remote API secret key.txt. <div data-bbox="922 1167 1469 1294" style="border: 1px solid #0070c0; padding: 5px; margin-top: 10px;">  It is recommended that you back up the Interact Remote API secret key file. </div> <p>If the installation fails, the View Log option gives details of the error that was encountered.</p> <p>For more information, see Troubleshooting an installation.</p> <p>Click Finish.</p> |

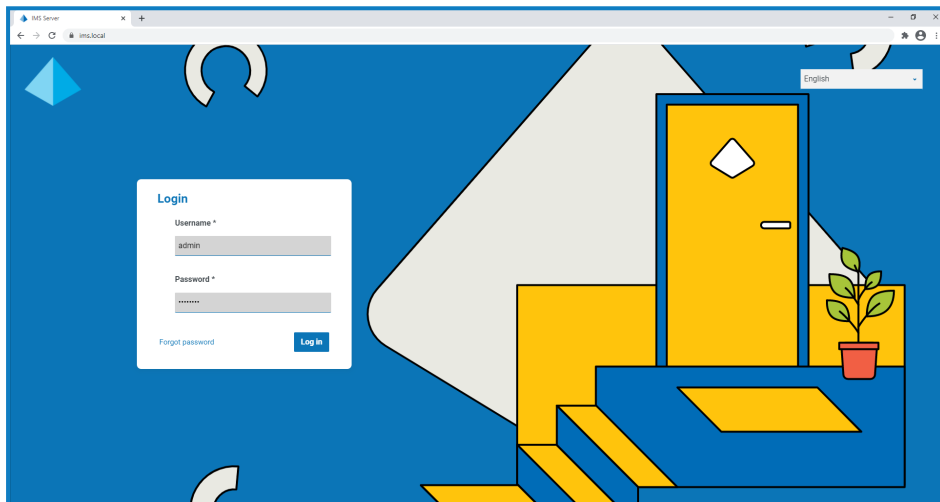
Initial Hub configuration

It is now possible to 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](#).

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

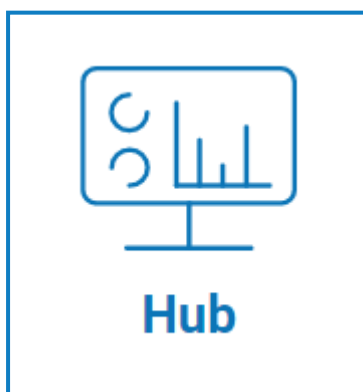


2. Log in using the default credentials.

- **Username:** admin
- **Password:** Qq1234!!

For information about how to change the default password and other settings see the [Hub User Guide](#).

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



Database settings

To configure access to the Blue Prism database:

1. Click your profile icon to open the Settings page, and then click **Environment manager**.
The Environment management page displays.
2. Click **Add connection** and enter the details of the Blue Prism database. An example is shown below:


The screenshot shows a 'Database configuration' form with the following fields and options:

- 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
- Connection name ***
Enter your friendly name for this connection.
Production
- Database name ***
This will be the name of your Blue Prism database.
RPA
- Timeout ***
Enter the seconds for which the system caches the LDAP server response result.
90

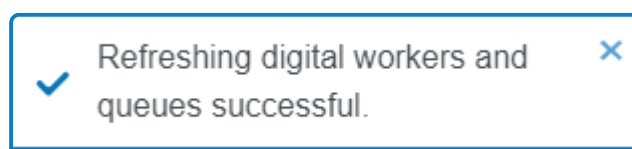
To the right of the configuration fields is a 'Database authentication' section with the following fields:

- User ID ***
sa
- Password ***

An 'Add connection' button is located at the bottom right of the authentication section.

 The Timeout value is in seconds.

3. Click **Add connection** to save the details.
The connection is created and displays in the Environment manager.
4. In the Environment manager, click the refresh icon on your new connection. This updates the information in Hub with the digital workforce and queues held in the database.
If the connection is successful, the following message displays in the top right corner of the Hub user interface, which verifies the installation.



If the message does not display, see [Troubleshoot a Hub installation on page 58](#) for more information.

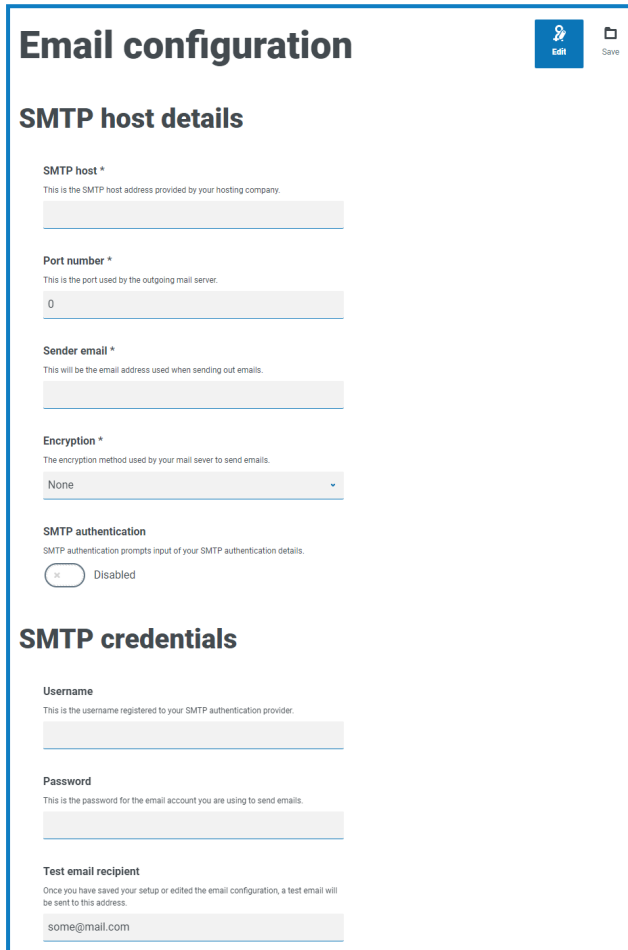
Email settings

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 configure the email settings:

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



The screenshot shows the 'Email configuration' page. At the top right, there are 'Edit' and 'Save' buttons. The page is divided into two main sections: 'SMTP host details' and 'SMTP credentials'.

SMTP host details

- SMTP host ***: A text input field with a placeholder. Below it, a note says: 'This is the SMTP host address provided by your hosting company.'
- Port number ***: A text input field with a placeholder '0'. Below it, a note says: 'This is the port used by the outgoing mail server.'
- Sender email ***: A text input field. Below it, a note says: 'This will be the email address used when sending out emails.'
- Encryption ***: A dropdown menu currently set to 'None'. Below it, a note says: 'The encryption method used by your mail server to send emails.'
- SMTP authentication**: A toggle switch currently set to 'Disabled'. Below it, a note says: 'SMTP authentication prompts input of your SMTP authentication details.'

SMTP credentials

- Username**: A text input field. Below it, a note says: 'This is the username registered to your SMTP authentication provider.'
- Password**: A text input field. Below it, a note says: 'This is the password for the email account you are using to send emails.'
- Test email recipient**: A text input field with the placeholder 'some@mail.com'. Above it, a note says: 'Once you have saved your setup or edited the email configuration, a test email will be sent to this address.'

2. Click **Edit**.
3. Enter the required information.
4. Click **Save**.

If the email settings cannot be successfully configured, it is likely to be an issue where the Message Broker server cannot be reached, see [Troubleshoot a Hub installation on page 58](#) for more information.



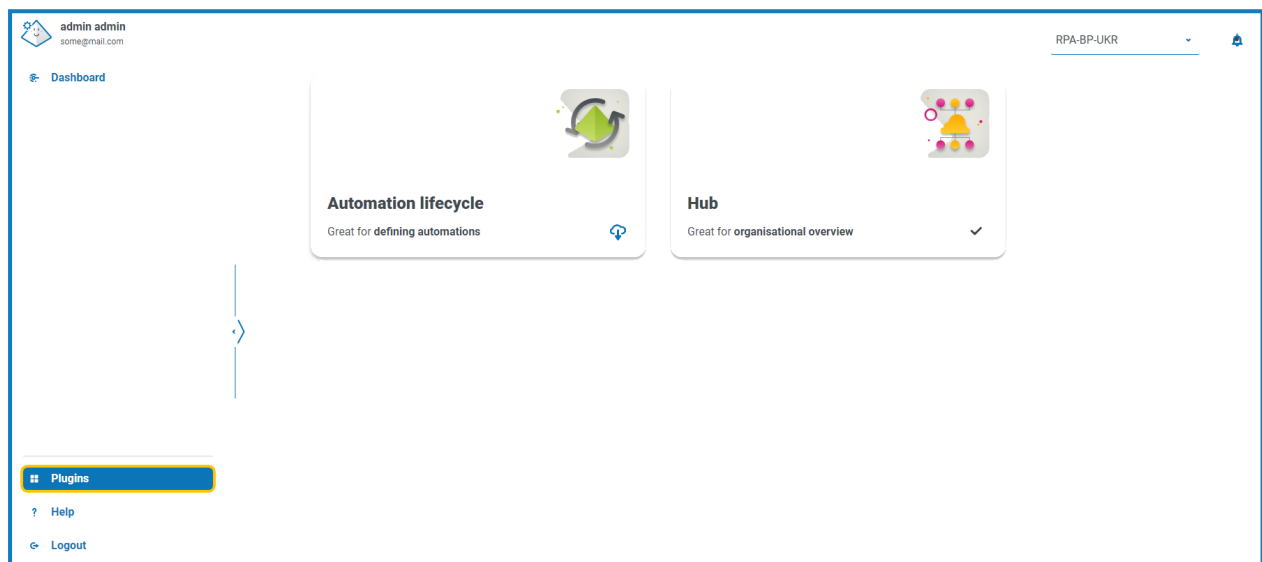
For more information about configuring email settings, see [Hub User Guide](#).

Install Plugins

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

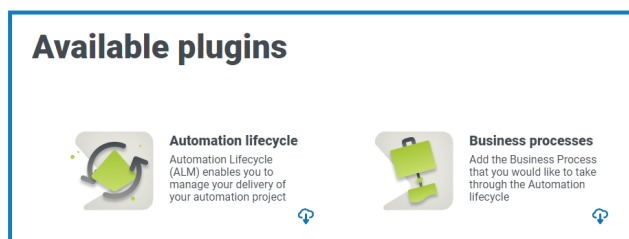
▶ To watch this installation step, see our [Business Processes plugin installation video](#).

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



3. Click **Automation lifecycle**.

The available plugin components display.



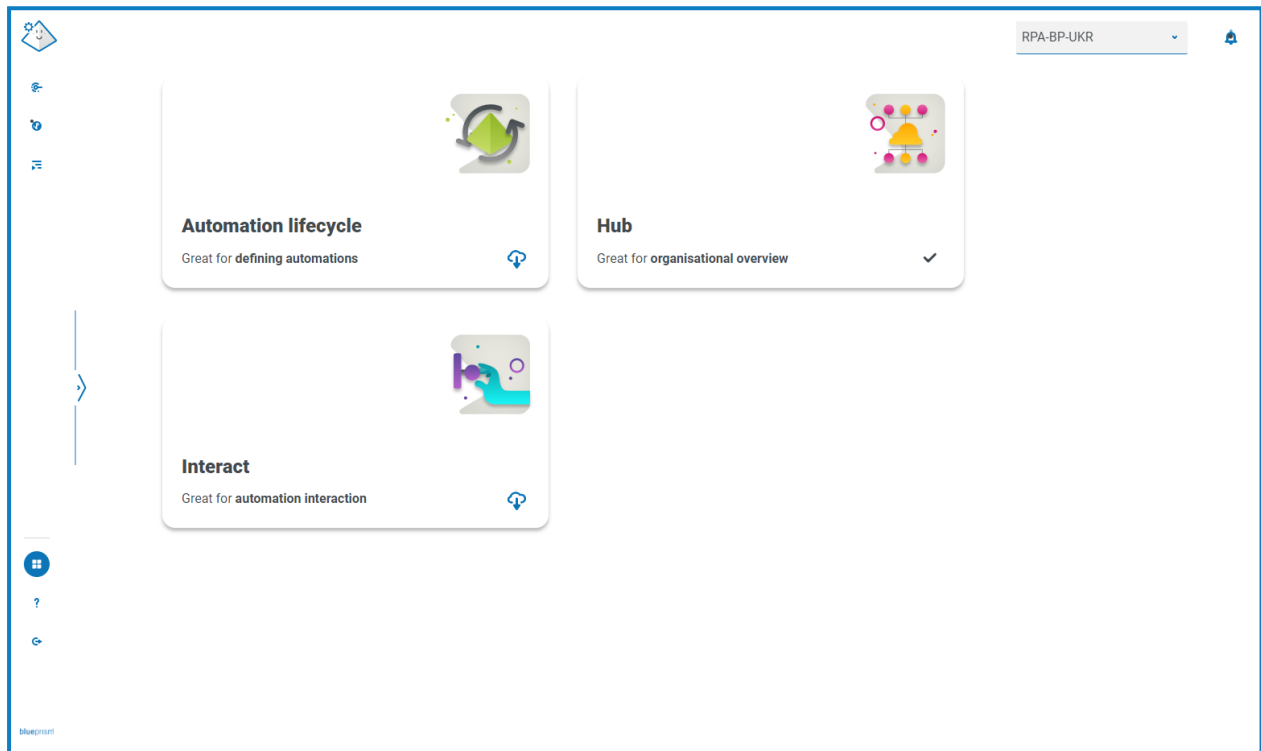
4. Click the download icon in the bottom corner of the **Business processes** tile to initiate the install.
The site restarts.

Install the Interact plugin

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

The Interact plugin must be installed with the associated license.

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



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

The site restarts.

Configure Digital Workers

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


The steps to be completed are:

- [Install SSL certificates](#)
- [Configure the network](#)
- [Install and configure the Interact Web API Service](#)

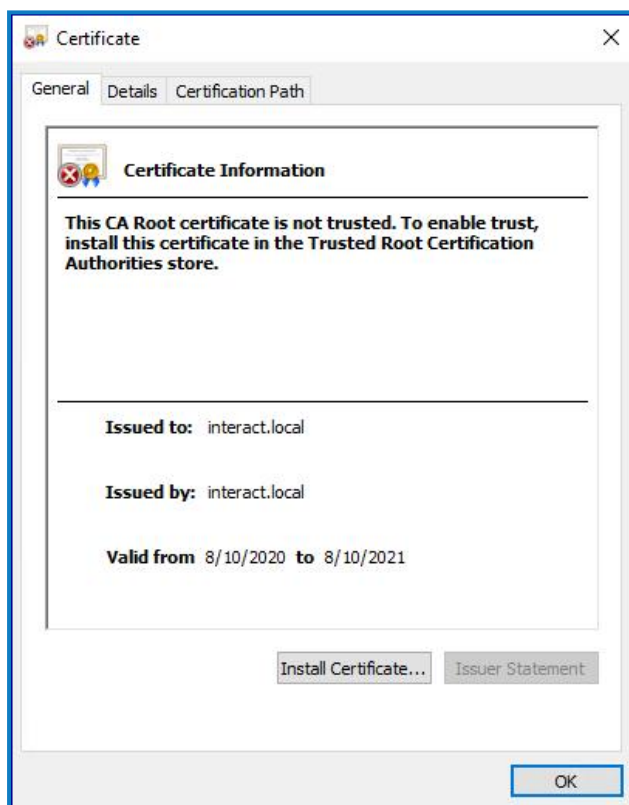
These instructions assume that the user is familiar with Blue Prism.

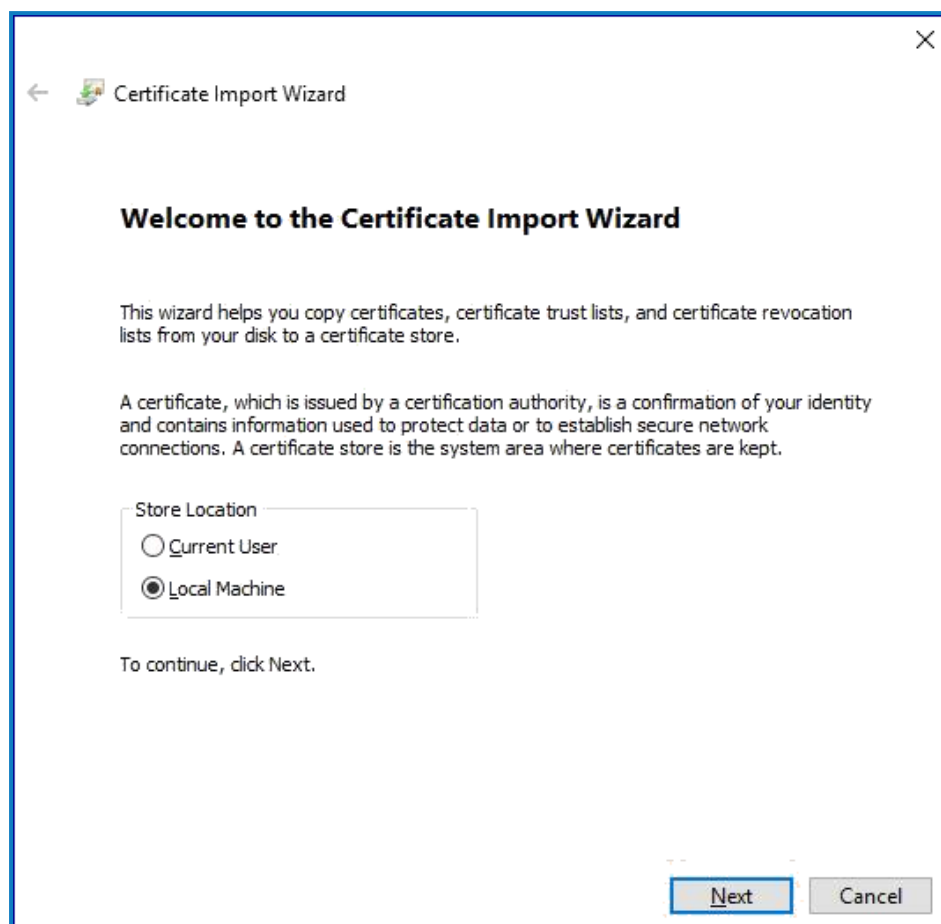
Install SSL certificates

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

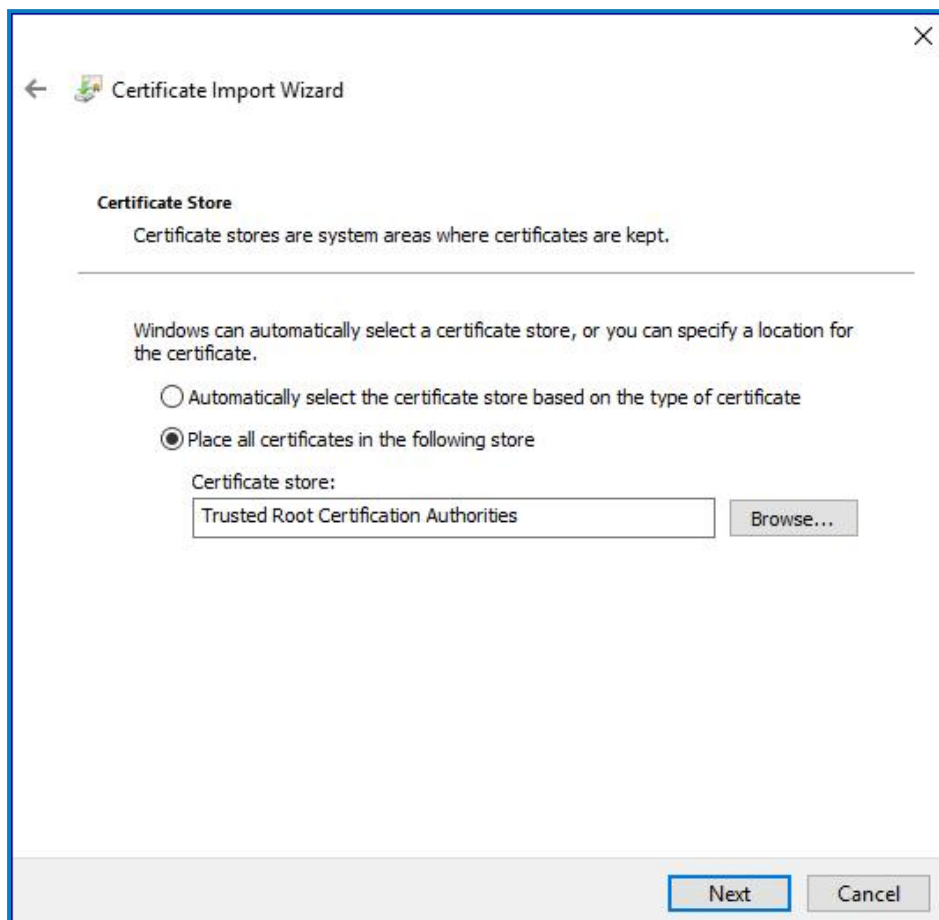
 As this needs to be performed on each Digital Worker the use of third-party tools or GPOs can be used to perform this task at scale.

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

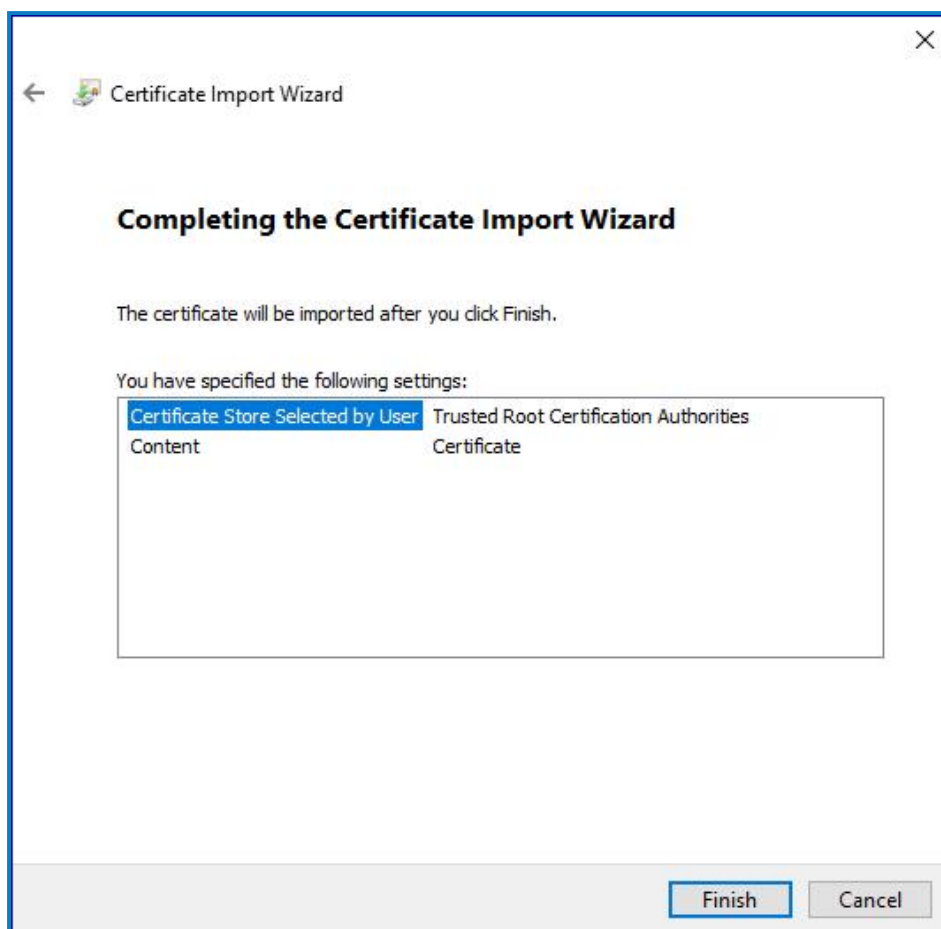


2. Change the Store location to **Local Machine**.

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



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



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


Configure the network

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

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

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

| Website in IIS | Default URL |
|----------------------------------|---------------------------------|
| Blue Prism – Interact | https://interact.local |
| Blue Prism – IMS | https://ims.local |
| Blue Prism – IADA | https://iada.local |
| Blue Prism – Interact Remote API | https://interactremoteapi.local |
| Blue Prism – SignalR | https://signalr.local |

 IMS and SignalR are installed as part of the [Hub installation](#).

Install and configure the Interact Web API service

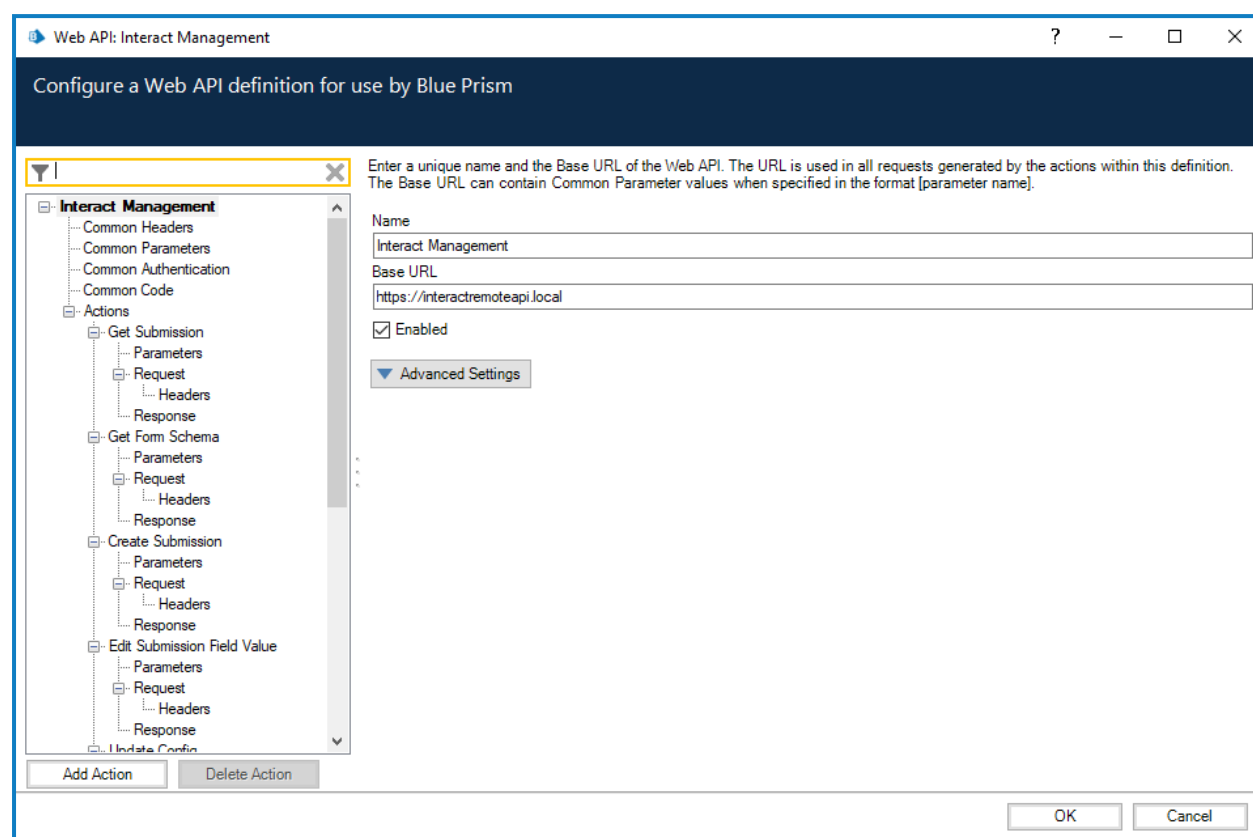
The communication channel back to Interact from Blue Prism is performed by a Blue Prism web service. The web service is available as a release that can be imported into Blue Prism. Once imported it will need to be updated with the appropriate base URL and authorization codes to enable secure communication.

The screenshot displays the Blue Prism System console interface. The left-hand navigation pane shows a tree structure with categories like History, SOAP Web Services, Web API Services, Connection Settings, Exception Types, Environment Variables, Skills, Management, Resources, Pools, Data Gateways, Settings, Configuration, Workflow, Work Queues, Environment Locks, Security, Users, User Roles, Sign-on Settings, Credentials, Encryption Schemes, Audit, Process Logs, Object Logs, Audit Logs, Statistics, Alerts, Design Control, System, Settings, License, Archiving, Scheduler, Calendar, Fonts, Reporting, and Work Queue Snapshots. The 'Web API Services' item is selected. The main pane, titled 'Objects - Web API Services', contains a table with the following data:

| Enabled | Name | Number of Actions | Last Updated | Skills |
|-------------------------------------|---------------------|-------------------|--------------|--------|
| <input checked="" type="checkbox"/> | DecipherCS | 9 | 11/12/2020 | |
| <input checked="" type="checkbox"/> | Interact Management | 8 | 11/24/2020 | |


To the right of the table are four action links: [Add Service](#), [Edit Service](#), [Delete Service\(s\)](#), and [Find References](#). The bottom status bar indicates: 'Sign Out Previous: 11/25/2020 9:13 AM, Current: 11/25/2020 11:38 AM, User: 'Trainee', Connection: 'Sandbox', Connected To: 'SQL Server 2019'.

The image below shows the web API service.



In the main window of the web API service we can see the **Base URL** defined, this will need to be updated to reflect the configuration of your platform setup.

The Common Parameters section is left blank and the Common Authentication section is used. This request a Bearer Token using stored credentials from the Credential store. The default Authorization URL is: <https://ims.local/connect/token>

 To set up the credentials a 'client_secret' must to be configured. This is generated during the installation process and is captured in the Interact Remote API Secret Key file. See [Install Blue Prism Interact on page 38](#) for more details.

Configure credentials for the Interact Web API service

When configuring the credentials for the OAuth 2.0 (Client Credentials) the following four values must be configured in the Blue Prism System Settings ([Security > Credentials](#)):

- **Client ID** – Enter *InteractRemoteClient*.
- **Client Secret** – Enter the code displayed and copied during installation or, if not copied, from the secret key file contents found in: C:\Program Files (x86)\Blue Prism\Interact Remote API secret key.txt.
- **grant_type** – Set the value to *client_credentials*.
- **scope** – Set the value to *interact-remote-api*.

Credential Details

Name: Interact Credentials

Description: Credentials for the Interact Remote API

Type: OAuth 2.0 (Client Credentials)

Application Credentials | Access Rights

Use this credential type for OAuth 2.0 web authentication using client credentials.

Client ID: InteractRemoteClient

Expires: ☒ 2/10/2099

Client Secret:

☐ Marked as invalid

Additional Properties

| Name | Value |
|------------|-------|
| grant_type | |
| scope | |
| | |

OK Cancel

Remember to set up the Access Rights tab in the Credentials Details to ensure it can access the processes for the allowed users.

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

Troubleshoot an Interact installation

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

Database connectivity

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

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

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

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

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

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

Web server

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

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. See [Preparation](#) for details.

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, 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.

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 if the IT organization has specified non-default ports.

Database connectivity

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

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

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

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

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

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

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

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

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

Web server

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

For further information, see [Prerequisites on page 6](#).

Starting the IMS website

After completing the installation, if an 'HTTP Error 500.19 on 0x8007000d' displays when starting the IMS website, you will need to repair or reinstall the .NET Core component .NET Core 3.1.3 Windows Server Hosting. The file for this component is dotnet-hosting-3.1.3-win.exe.

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 9](#), 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.

Updating the Customer ID after installation

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

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

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

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


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

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

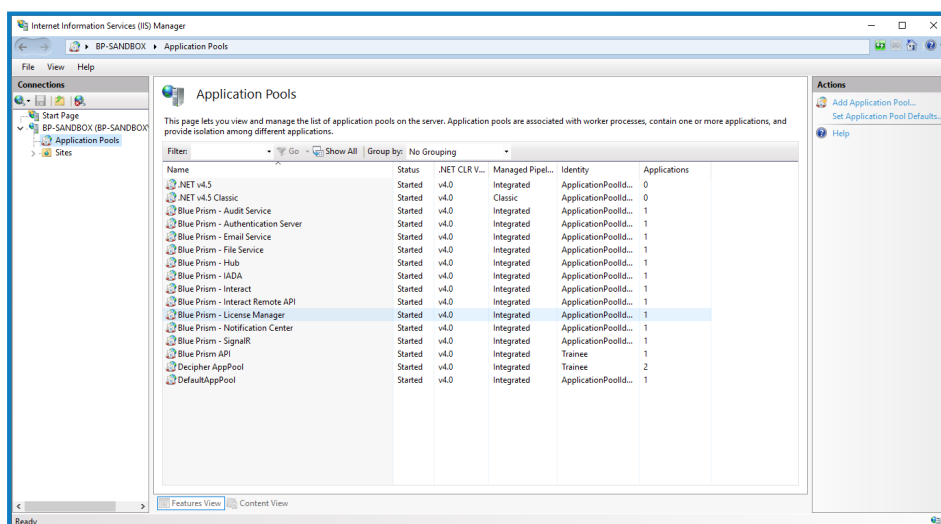
4. Save the file.

To restart License Manager:

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

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

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



The License Manager restarts.

Uninstall Interact

To completely uninstall Interact 4.2, you need to:

1. [Remove Interact using the Programs and Features application.](#)
2. [Remove any remaining files.](#)
3. [Remove the databases.](#)
4. [Remove RabbitMQ data.](#)

Remove Interact using Programs and Features


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

Remove any remaining files

1. In Windows Explorer, open the parent folder for the Interact installation. By default, this is `C:\Program Files (x86)\Blue Prism` but it may have been changed during the [Interact installation](#).
2. Delete the following folders and files:
 - IADA
 - Interact
 - Interact Remote API
 - Submit Form Manager
 - Interact Remote API secret key.txt

Remove the databases

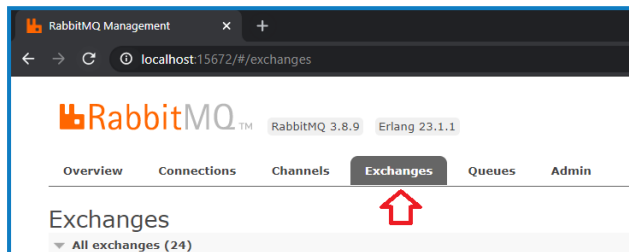
You should only remove databases for test systems. If you are contemplating removing a database for a system that had been in production, you should consider whether the data needs to be archived by your organization or used for audit purposes.

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

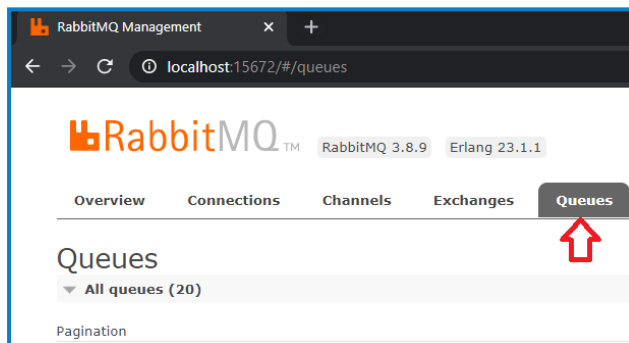
1. Delete, or archive, the database for the Interact application.

Remove RabbitMQ data

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



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



5. Find and remove the following items:
 - EnvironmentChanges
 - Inbox