



Interact 4.0

Install Guide

Document Revision: 1.1



Trademarks and Copyright

The information contained in this guide is the proprietary and confidential information of Blue Prism Cloud Limited and/or its affiliates 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 Cloud Limited or its affiliates.

© Blue Prism Cloud Limited 2001 – 2020

“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 other trademarks are hereby acknowledged and are used to the benefit of their respective owners.

Blue Prism Cloud Limited and its affiliates are not responsible for the content of external websites referenced by this guide.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.

Registered in England: Reg. No. 4260035. Tel: +44 870 879 3000. Web: www.blueprism.com

Contents

Trademarks and Copyright	ii
Contents	iii
Introduction	1
Related documents	1
Preparation	2
Planning	2
Prerequisites	2
Software requirements and permissions	4
Supported software	4
Minimum SQL permissions	4
Multi-device deployment considerations	5
Network ports	6
Typical deployment	7
Overview of typical installation steps	8
Install the Message Broker server	8
Install and configure the web server	13
Install Blue Prism Interact	26
Initial Hub configuration and verification	31
Install the Interact plugin	34
Configure digital workers	34
Verify an installation	41
Troubleshoot an Interact installation	43
Database connectivity	43
Web server	43
Windows Authentication	43
Default application information	44
Troubleshoot a Hub installation	45
Message Broker connectivity	45
Database connectivity	45
Web Server	46
Starting the IMS website	46
File service	46
Windows Authentication	46
Not able to configure SMTP settings in Hub	47
Default application information	47
Uninstall Interact	48

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 4.0 of Blue Prism Interact.

Related documents

The following documents provide further information on specific aspects of the implementation of Hub. These can be provided by your Account Manager or via Technical Support.

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, i.e. IMS, Hub, Audit, Interact, InteractCache etc. 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](#)) 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 will need downloading:
 - Erlang OTP 23.0.1, available here: http://erlang.org/download/otp_versions_tree.html
 - RabbitMQ Server 3.8.5, available here: <https://github.com/rabbitmq/rabbitmq-server/releases/tag/v3.8.5> with installation guidance here: <https://www.rabbitmq.com/install-windows-manual.html>
- Hub is installed on a web server and therefore requires Internet Information Services Manager (IIS), IIS features, and the .Net Core components installed. These need to be pre-installed to enable a successful installation of Blue Prism Hub. These are detailed in the [web server](#) build section.

- The Interact system is a Web Server and therefore requires IIS Web Server, IIS features, 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 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. 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 and located within the default Windows certificate folder. If using Windows Authorization for access to SQL server, it 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, it will need to be configured manually.

Software requirements and permissions

Supported software

The following technologies are supported for use with the software:

Operating system

Version	Web Server	Message Broker
Windows Server 2016 Datacenter	✓	✓

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

Microsoft SQL server

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

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

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

The following are also supported:

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

Azure SQL Database is not currently supported.

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.

Multi-device deployment considerations

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

	Environmental concerns (Development / Test / Pre-Production / Production)
General Connectivity	Connectivity between the various devices must be configured appropriately. Commonly this requires DNS to be configured to allow the devices to resolve each other based on their FQDN; and appropriate firewall rules to be in place to allow the devices to communicate on the required ports.
Message Broker Server	This is a single device focused on providing Message Broking services between Blue Prism components. A device per environment is recommended.
Web Server	A single device which can host multiple Blue Prism components. It is not recommended that environments are shared on this device and that a separate device is used per environment.
Database Server instance	Consider if the way that resources are allocated to SQL Server instances make it appropriate to use a single shared instance for deployments of Blue Prism based on their importance and criticality. (E.g. Dev and Production environments are likely to be most business critical).
Digital Worker Certificates	Decide if there is an additional requirement to apply certificate-based security to the instructional communications from the Interactive Clients and Application Servers to each digital worker; and to inbound communications received by the digital workers if they are hosting web services. If a certificate is required this must be manually generated and installed on each applicable digital worker. The common name on the certificate must align with the address that the Blue Prism components will be configured to use when communicating with the devices (E.g. 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.

Typical deployment

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

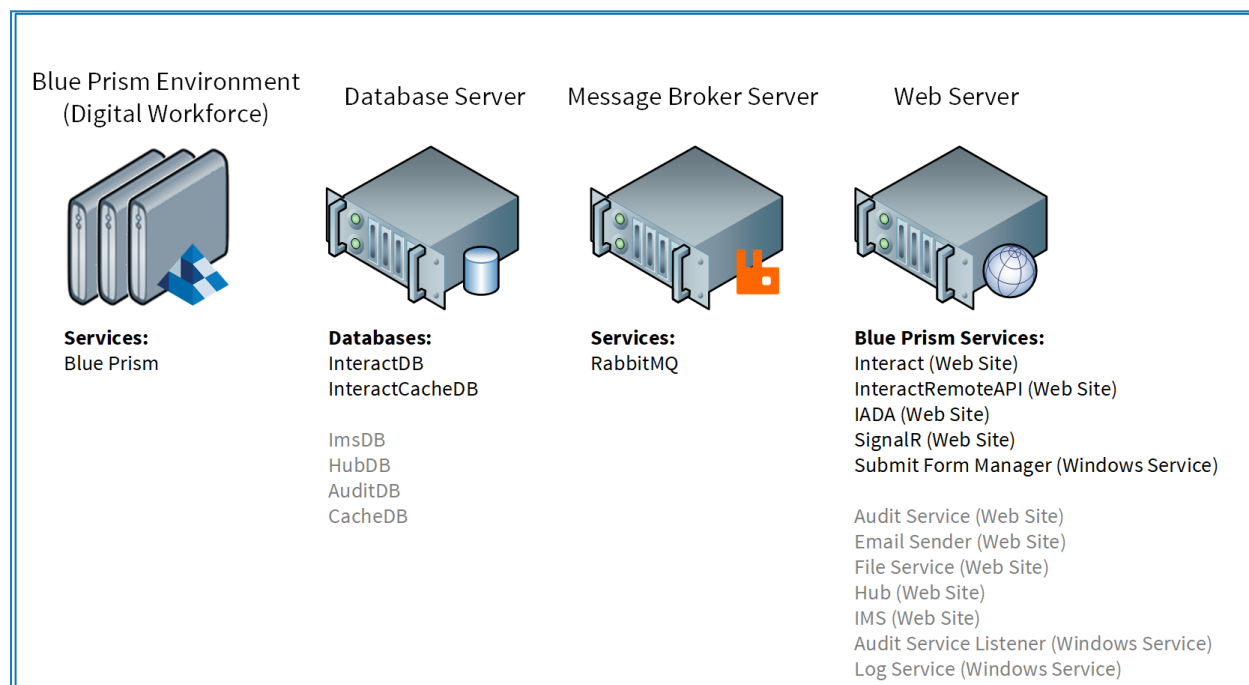
Prior to following this guidance, ensure that you have fully considered the information in [Preparation](#).

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.

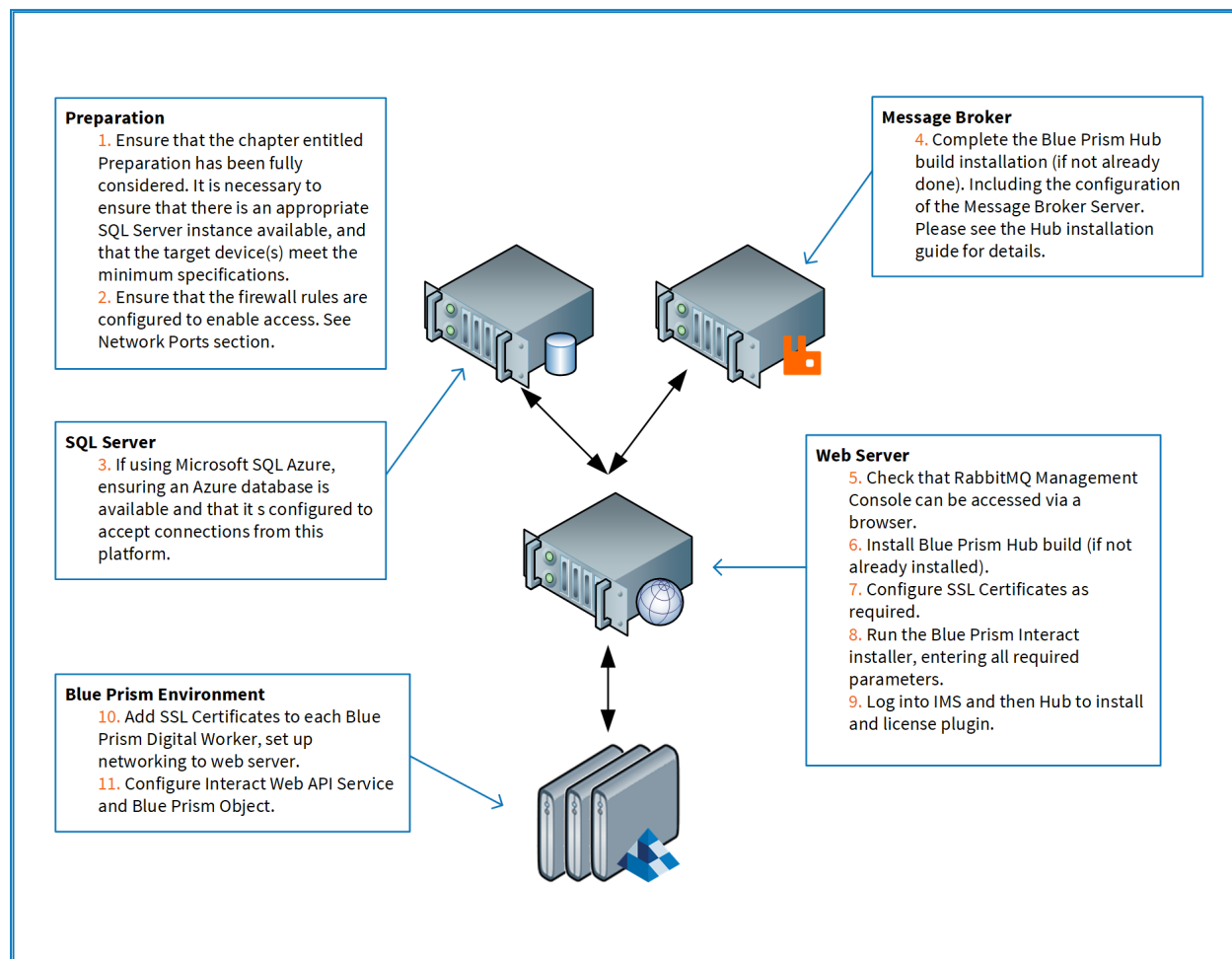
The diagram below illustrates the typical architecture for an environment.



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 23.0.1 (11.0.1).

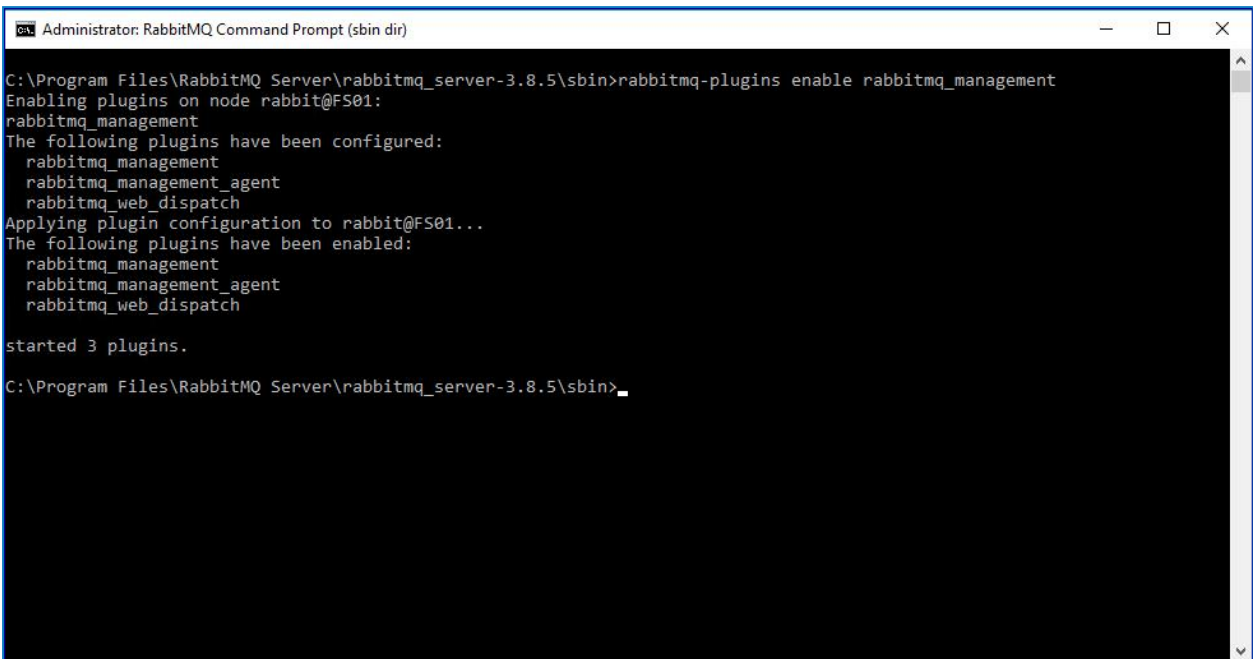
For information see the [Erlang/OTP installation guide](#).

2. Install RabbitMQ Server 3.8.5 and accept the default settings.

For more 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).

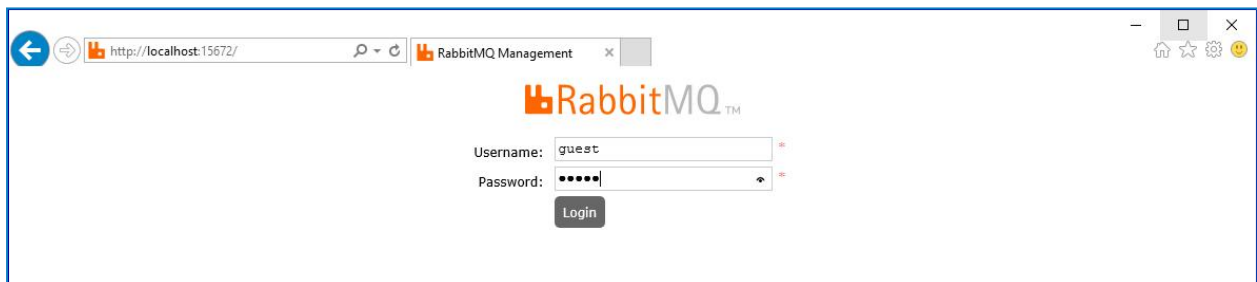
5. In the RabbitMQ Command Prompt window, type the following command: `rabbitmq-plugins enable rabbitmq_management`



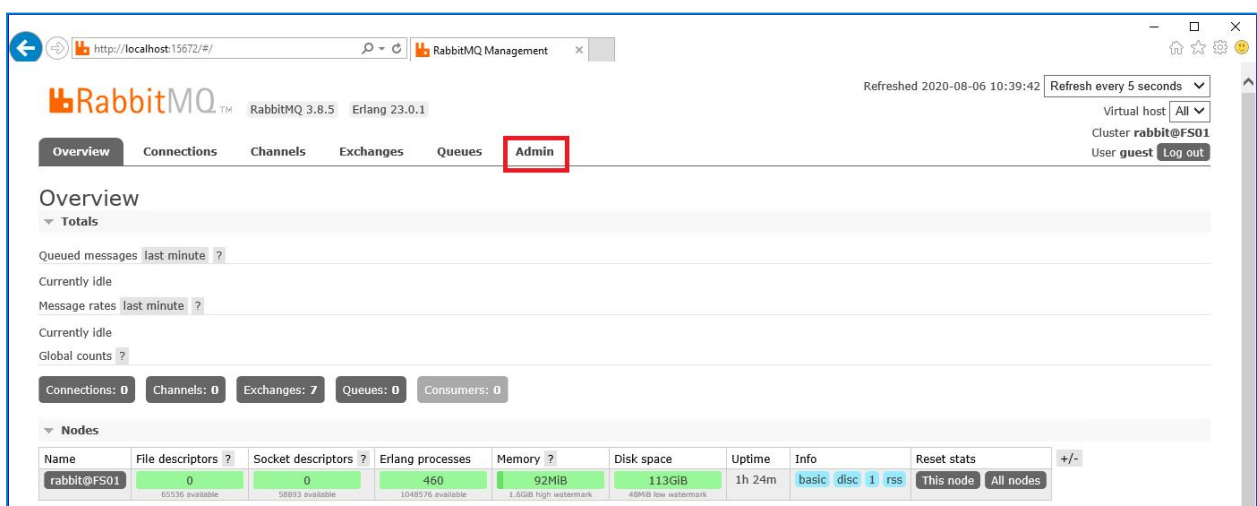
```
Administrator: RabbitMQ Command Prompt (sbin dir)
C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.5\sbin>rabbitmq-plugins enable rabbitmq_management
Enabling plugins on node rabbit@FS01:
rabbitmq_management
The following plugins have been configured:
  rabbitmq_management
  rabbitmq_management_agent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

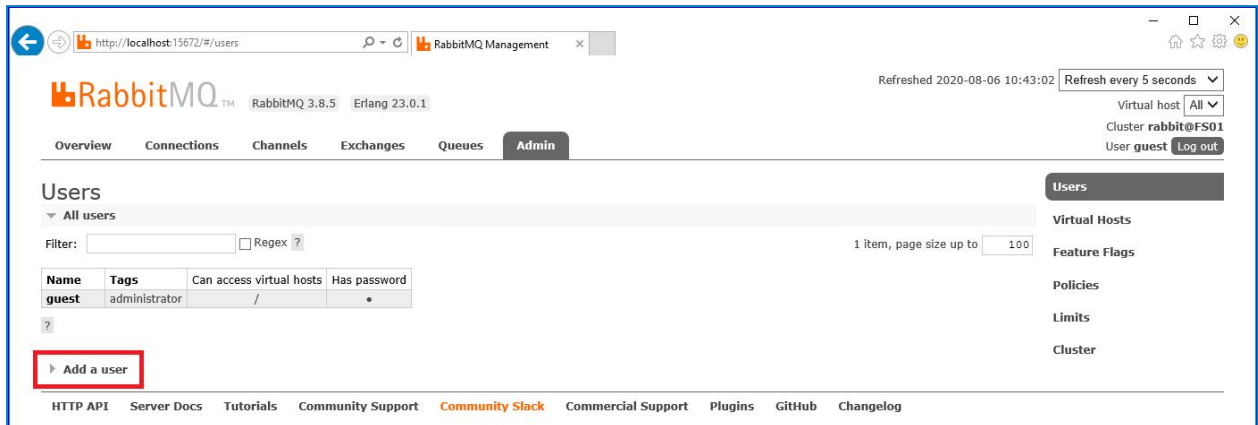
started 3 plugins.
C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.5\sbin>
```

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.



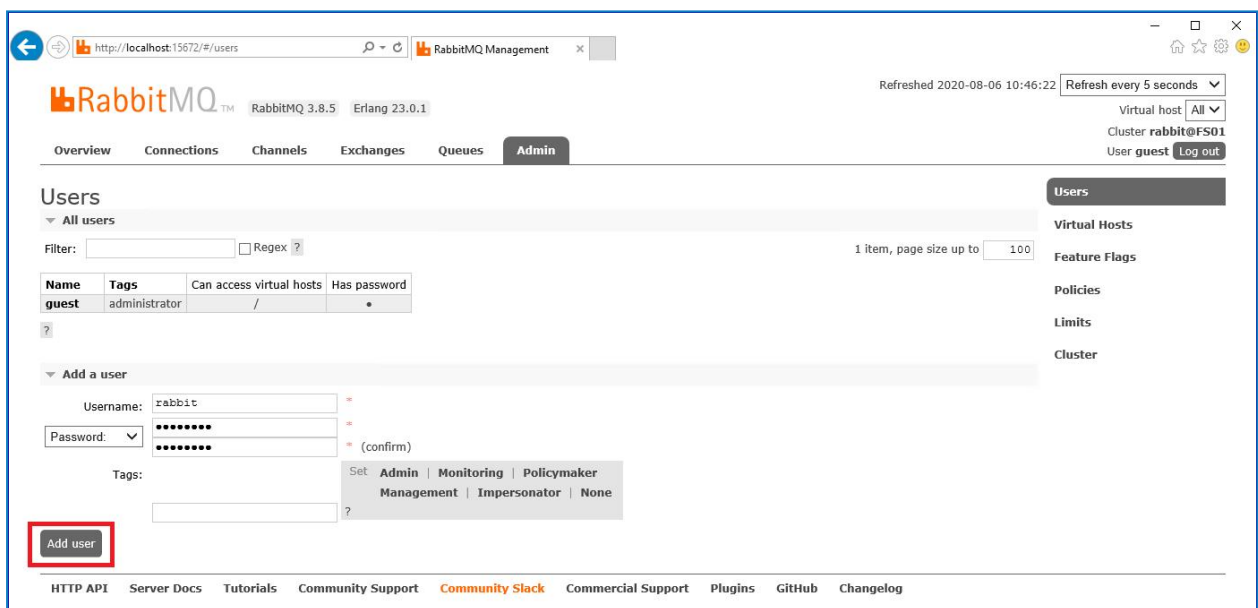
8. In the console, click **Admin**.



9. Click **Add a user**.

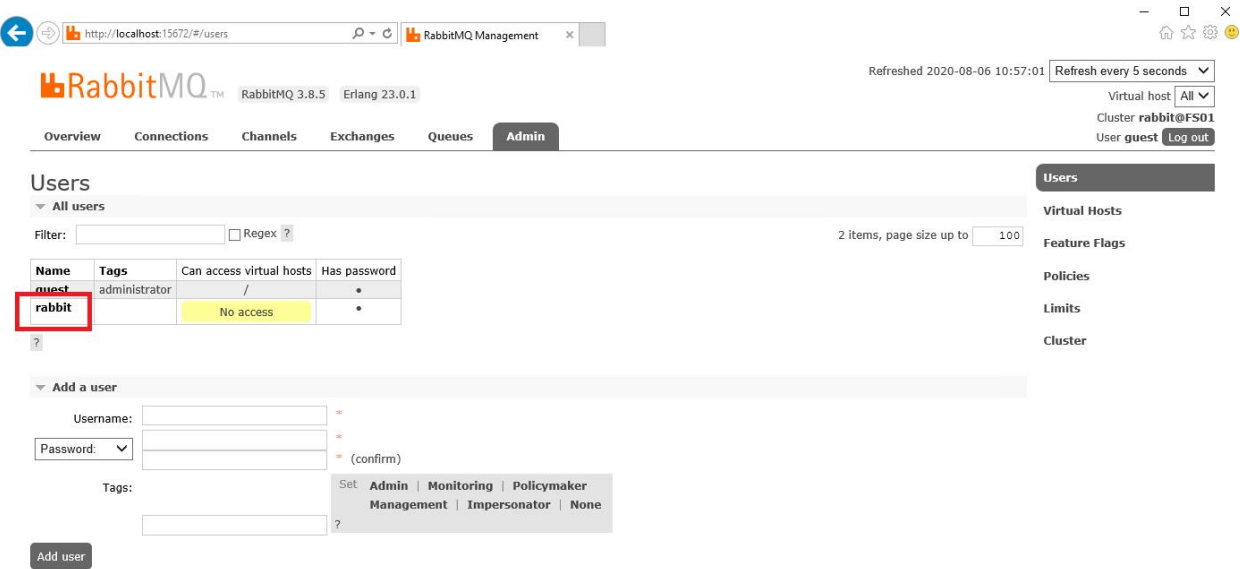
10. Enter the details for a new user, providing the username and password. The user does not require any special permissions and can be left at None.

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

11. Click **Add User**.

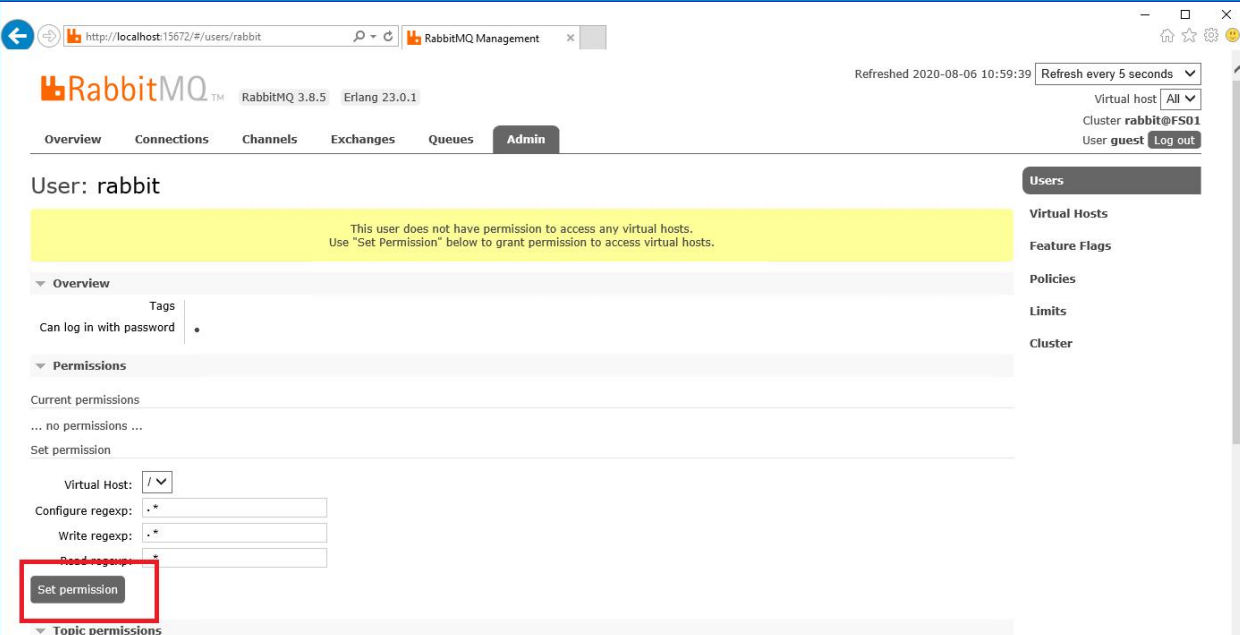
The next step is to set the permissions for the user.

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



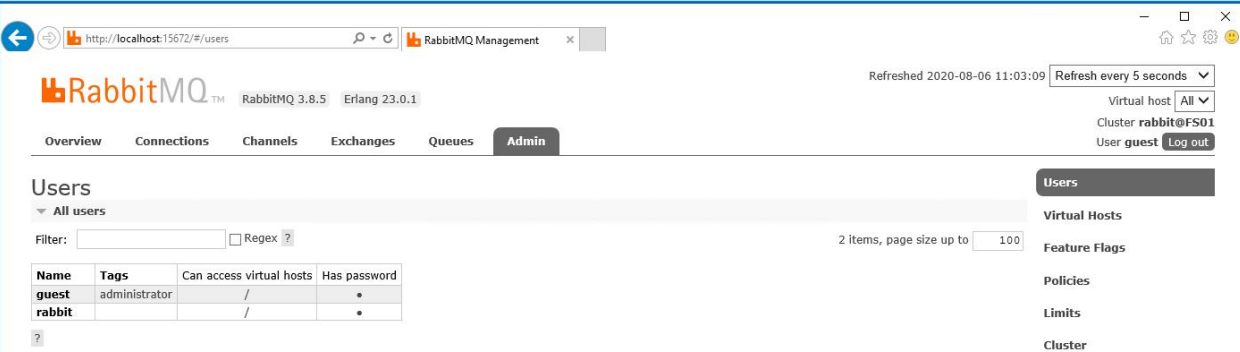
The screenshot shows the RabbitMQ Management interface. The 'Users' tab is active. A table lists users: 'guest' (administrator, can access virtual hosts, has password) and 'rabbit' (No access, no password). The 'rabbit' user is highlighted with a red box. Below the table is a form to 'Add a user' with fields for Username, Password, and Tags. The right sidebar contains links for Users, Virtual Hosts, Feature Flags, Policies, Limits, and Cluster.

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



The screenshot shows the 'User: rabbit' page. A yellow banner states: 'This user does not have permission to access any virtual hosts. Use "Set Permission" below to grant permission to access virtual hosts.' Below this, the 'Permissions' section is visible. The 'Set permission' button is highlighted with a red box. The right sidebar contains links for Users, Virtual Hosts, Feature Flags, Policies, Limits, and Cluster.

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



The screenshot shows the RabbitMQ Management interface. The 'Users' tab is active. A table lists users: 'guest' (administrator, can access virtual hosts, has password) and 'rabbit' (No access, no password). The 'rabbit' user is highlighted with a red box. Below the table is a form to 'Add a user' with fields for Username, Password, and Tags. The right sidebar contains links for Users, Virtual Hosts, Feature Flags, Policies, Limits, and Cluster.

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 certifications 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 logon 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 did not appear, see [Troubleshoot a Hub installation](#).

Install and configure the web server

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

The process consists of the following:

1. [Install the prerequisites](#)
2. [Configure SSL Certificates](#)
3. [Install Blue Prism Hub](#)

Install the prerequisites

The system is a web server and therefore requires IIS Web Server, IIS features and the .Net Core components installed. It is important that IIS is installed before installing the prerequisites below.

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

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

Features

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

Server roles

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

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

Scripted installation

Run the commands below at a PowerShell command prompt:

```
Install-WindowsFeature -Name FS-FileServer -computerName localhost
Install-WindowsFeature -Name FS-Resource-Manager -computerName localhost
Install-WindowsFeature -Name Web-Default-Doc -computerName localhost
Install-WindowsFeature -Name Web-Dir-Browsing -computerName localhost
Install-WindowsFeature -Name Web-Http-Errors -computerName localhost
Install-WindowsFeature -Name Web-Static-Content -computerName localhost
Install-WindowsFeature -Name Web-Http-Redirect -computerName localhost
Install-WindowsFeature -Name Web-Http-Logging -computerName localhost
Install-WindowsFeature -Name Web-Log-Libraries -computerName localhost
Install-WindowsFeature -Name Web-Request-Monitor -computerName localhost
Install-WindowsFeature -Name Web-Http-Tracing -computerName localhost
Install-WindowsFeature -Name Web-Stat-Compression -computerName localhost
Install-WindowsFeature -Name Web-Filtering -computerName localhost
Install-WindowsFeature -Name Web-Client-Auth -computerName localhost
Install-WindowsFeature -Name Web-Cert-Auth -computerName localhost
Install-WindowsFeature -Name Web-Windows-Auth -computerName localhost
Install-WindowsFeature -Name Web-Net-Ext45 -computerName localhost
Install-WindowsFeature -Name Web-AppInit -computerName localhost
Install-WindowsFeature -Name Web-ASP -computerName localhost
Install-WindowsFeature -Name Web-Asp-Net45 -computerName localhost
Install-WindowsFeature -Name Web-ISAPI-Ext -computerName localhost
```

```
Install-WindowsFeature -Name Web-ISAPI-Filter -computerName localhost
Install-WindowsFeature -Name Web-Mgmt-Console -computerName localhost
Install-WindowsFeature -Name Web-Scripting-Tools -computerName localhost
Install-WindowsFeature -Name Web-Mgmt-Service -computerName localhost
Install-WindowsFeature -Name Web-Metabase -computerName localhost
Install-WindowsFeature -Name RSAT-Role-Tools -computerName localhost
Install-WindowsFeature -Name RSAT-File-Services -computerName localhost
Install-WindowsFeature -Name RSAT-FSRM-Mgmt -computerName localhost
Install-WindowsFeature -Name NET-WCF-HTTP-Activation45 -computerName localhost -
Restart
```

.Net core components

- .Net Core 3.1.2 Windows Server Hosting
<https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-3.1.2-windows-hosting-bundle-installer>
- .Net Core 3.1.2 Windows Desktop Runtime
<https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-desktop-3.1.2-windows-x64-installer>
- .Net Core SDK 3.1.300
<https://dotnet.microsoft.com/download/dotnet-core/thank-you/sdk-3.1.300-windows-x64-installer>
- Visual C++ Redistributable 2012 (x64)
https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe
- .Net Framework 4.7.2
<https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer>

Scripted installation

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

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

Configure SSL 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 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

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
Blue Prism – Signal R	https://signalr.local

Self-signed certificates

Self-signed certificates can be used but are only recommended for POC \ POV \ Dev environments, and not Production. It is recommended that you contact your IT Security team to check what their requirements are.

Run the following PowerShell command to create a self-signed certificate:

```
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.

Open the Manage Computer Certificates application on your Web server (type **managed computer** into the search bar), copy and paste the certificate from Personal > Certificates to Trusted Root Certification > Certificates.

This procedure should be followed 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)
```

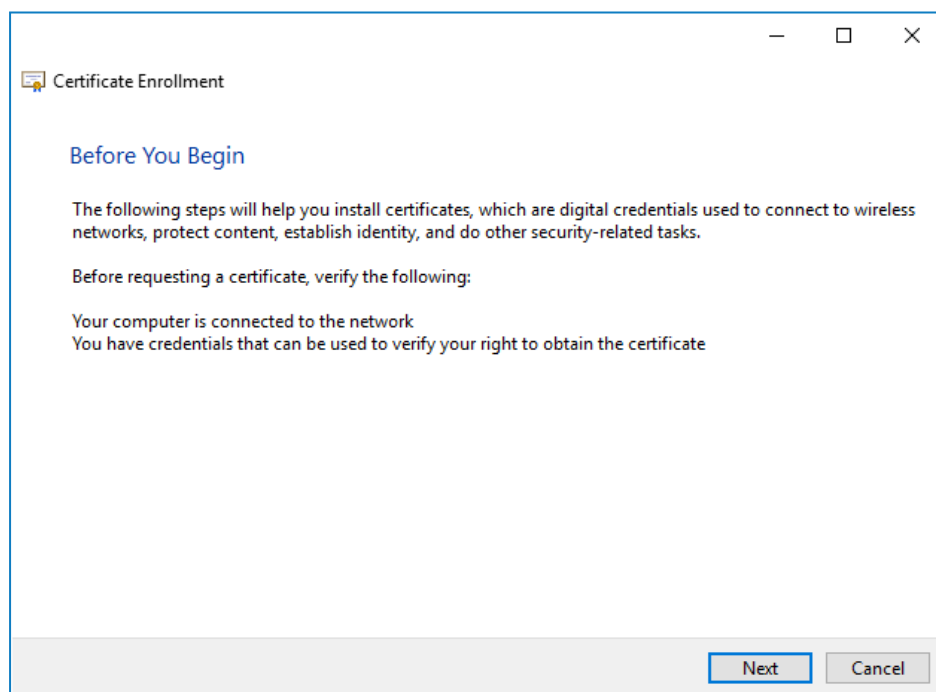
```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
"hub.local" -FriendlyName "MySiteCertHub" -NotAfter (Get-Date).AddYears(10)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
"email.local" -FriendlyName "MySiteCertEmail" -NotAfter (Get-Date).AddYears(10)
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
"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)
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
"signalr.local" -FriendlyName "MySiteCertSignalR" -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.

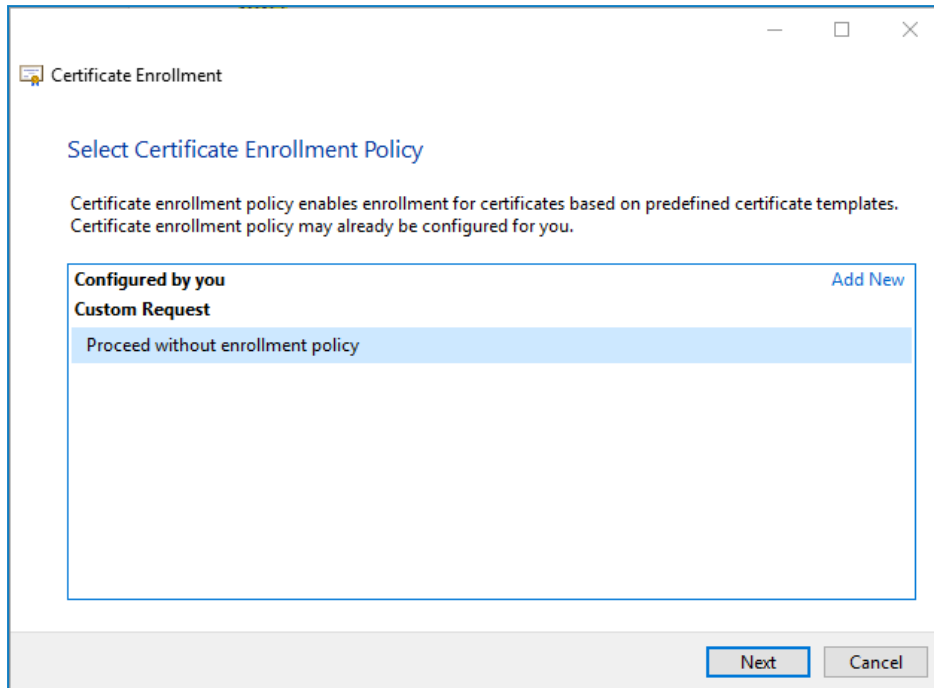
Creating an offline certificate request

To create an Offline Certificate Request, for each certificate follow this procedure:

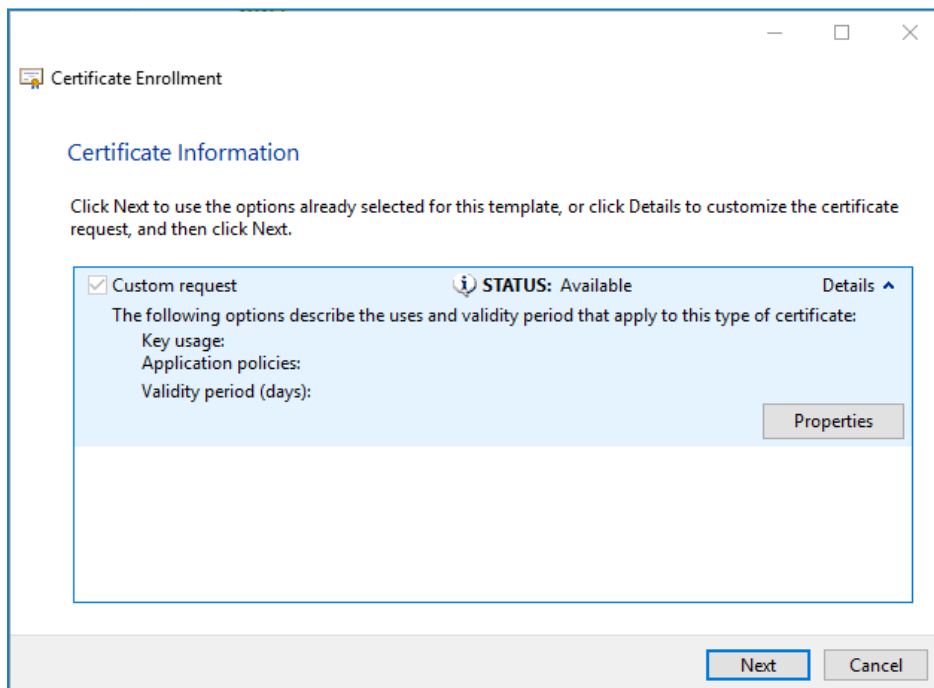
1. Open the Manage Computer Certificates application on your Web server (type **managed computer** into the search bar).
2. Right-click on **Personal > Certificates** and select **All Tasks > Advanced Operations > Create Custom Request** from the shortcut menu. The Certificate Enrollment wizard displays.



3. Click **Next**.



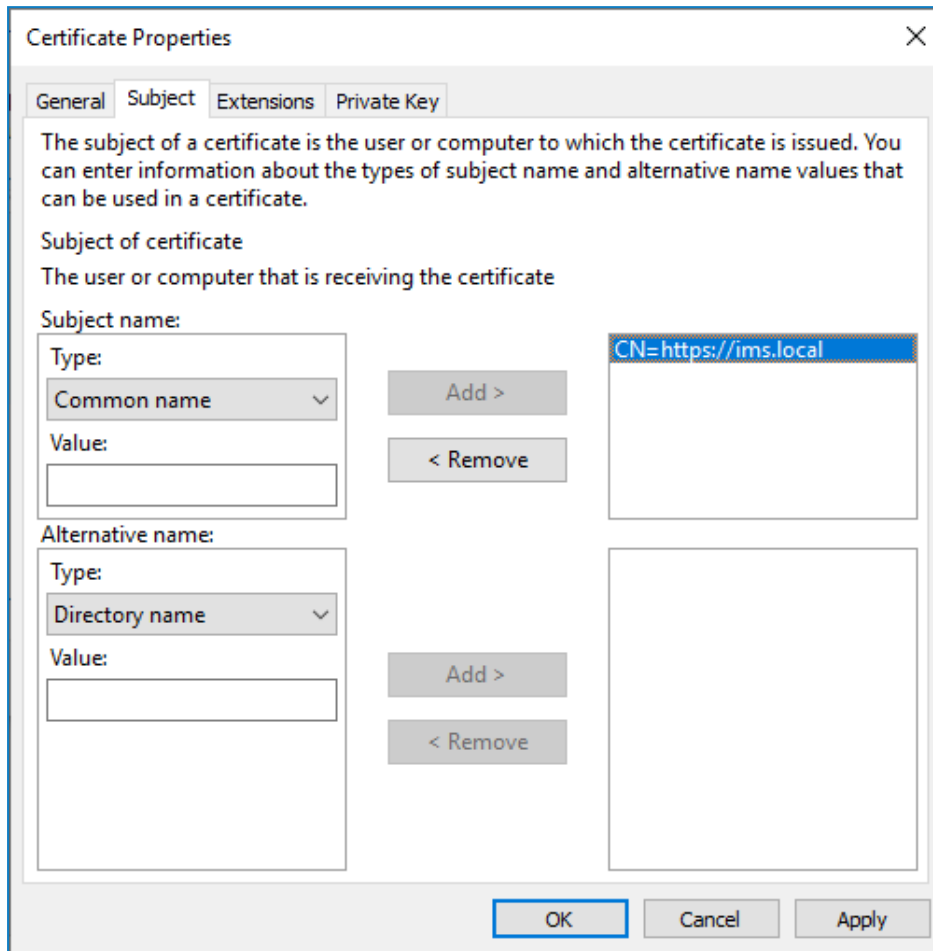
4. Select **Proceed without Enrollment Policy** and click **Next**.
5. On the Custom request screen click **Next**.
6. On the Certificate Information screen click the **Details** drop-down and click **Properties**.



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 Value and click **Add**.

The CN 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 a text box with the following text: '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.' Below this is the label 'Subject of certificate' and the text 'The user or computer that is receiving the certificate'. There are two sections for adding names: 'Subject name:' and 'Alternative name:'. Each section has a 'Type' dropdown menu, a 'Value' text box, and 'Add >' and '< Remove' buttons. In the 'Subject name' section, the 'Type' is set to 'Common name' and the 'Value' is 'https://ims.local'. This entry is displayed in the list on the right. In the 'Alternative name' section, the 'Type' is set to 'Directory name' and the 'Value' is empty. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

9. On Extensions tab click **Extended Key Usage**, select **Server Authentication**, and click **Add**.
10. On the Private Key tab click **Key options**, select a key size of your choice and select **Make private key exportable**.
11. Still on the Private Key tab, click **Hash Algorithm**, and select a suitable Hash (optional).
12. Click **OK**.
- You are returned to the Certificate Enrollment screen.
13. Click **Next**.
14. Add a file name and path and click **Finish**.

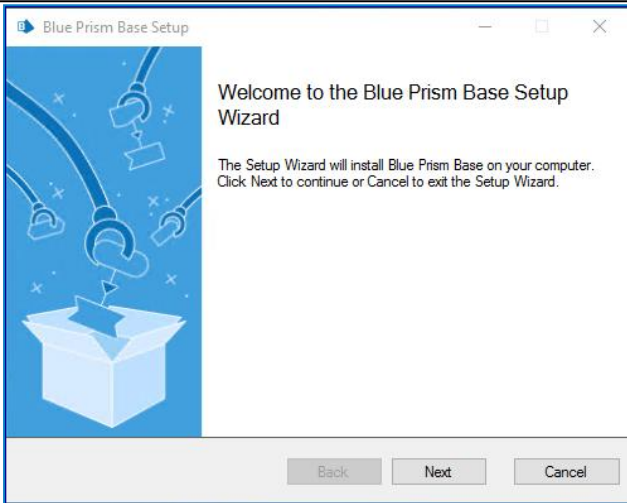
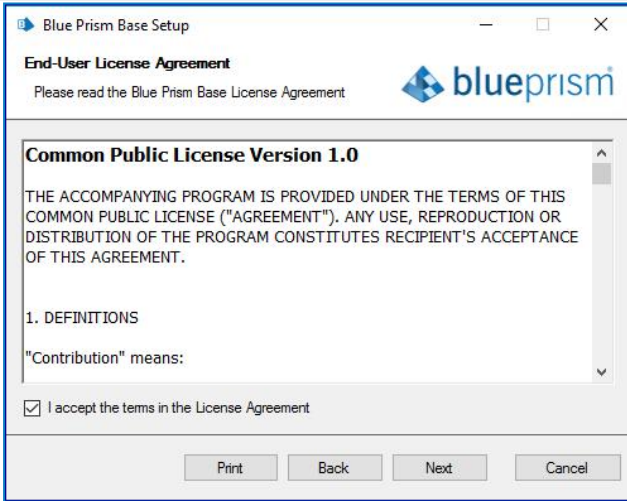
After creating your certificate request, you will need to submit it to a Certificate Authority so they can process your request and issue a certificate. The certificate request is a text file. Usually, you are required to copy the text from the file and enter it into an online submission form on the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

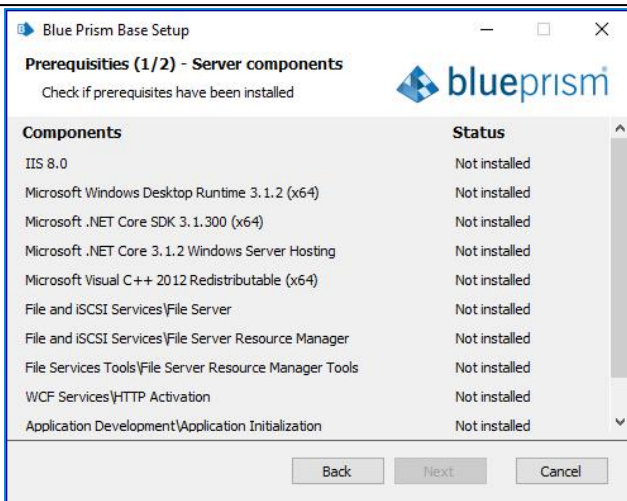
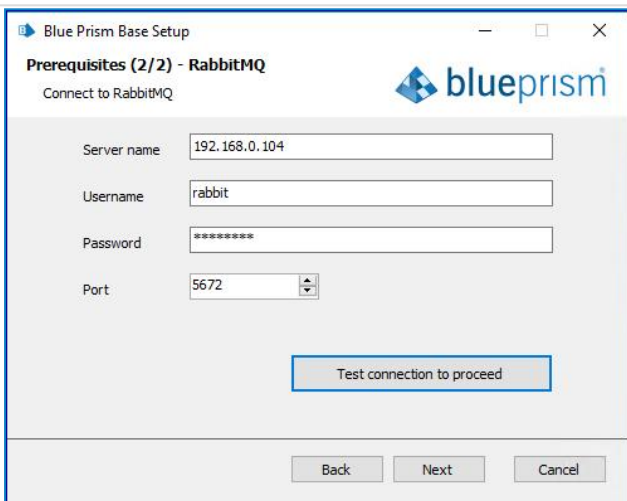
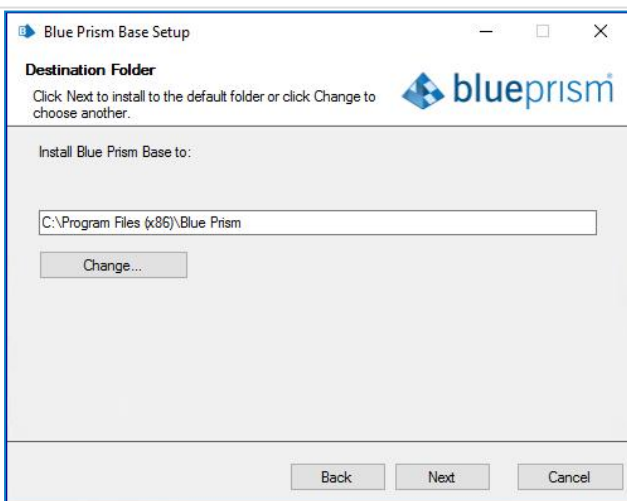
Install Blue Prism Hub

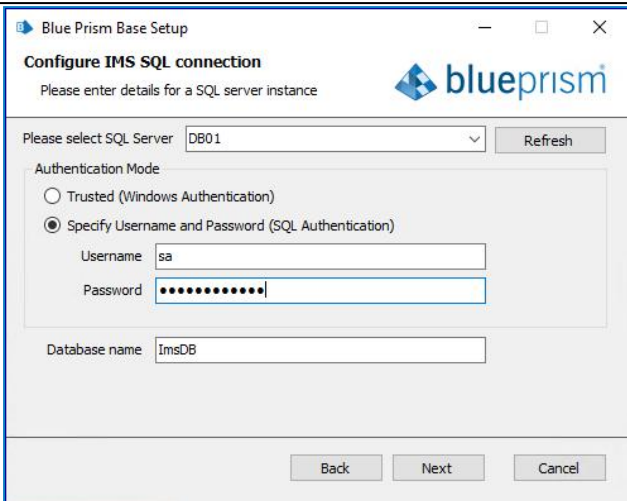
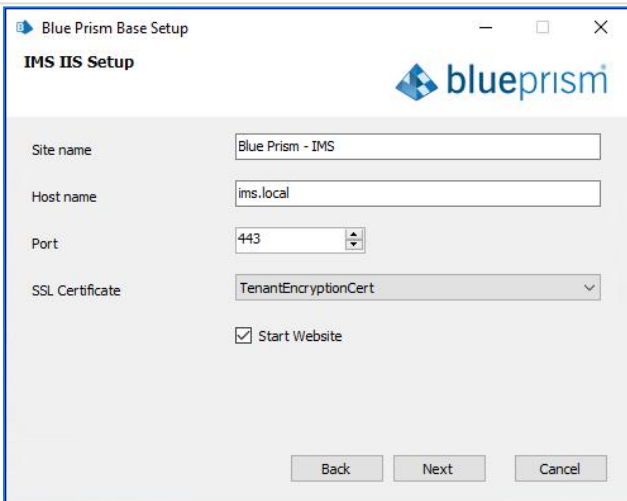
The steps below detail the process for installation of the Blue Prism Hub software. This includes the Identify Management System (IMS), Hub, and other associated services. The installation process will create any new databases that are required.

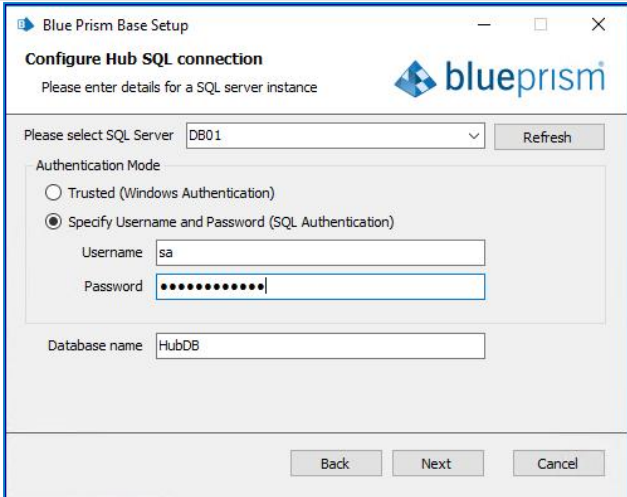
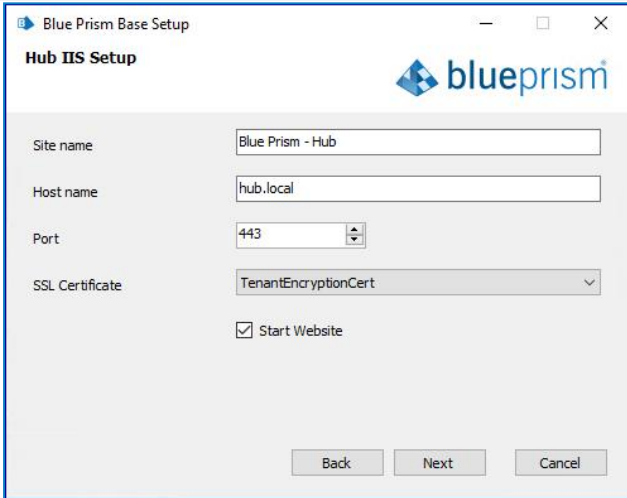
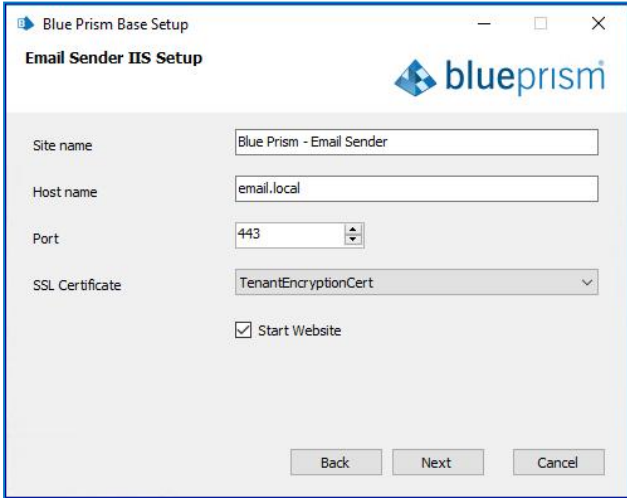
Download and run the Blue Prism Hub installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer should be run with administrator rights.

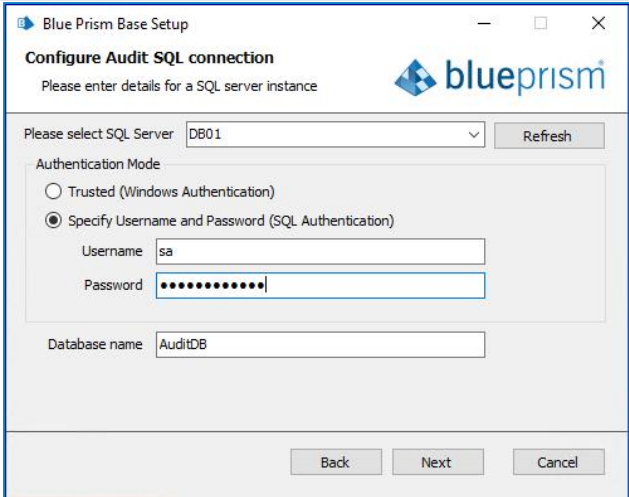
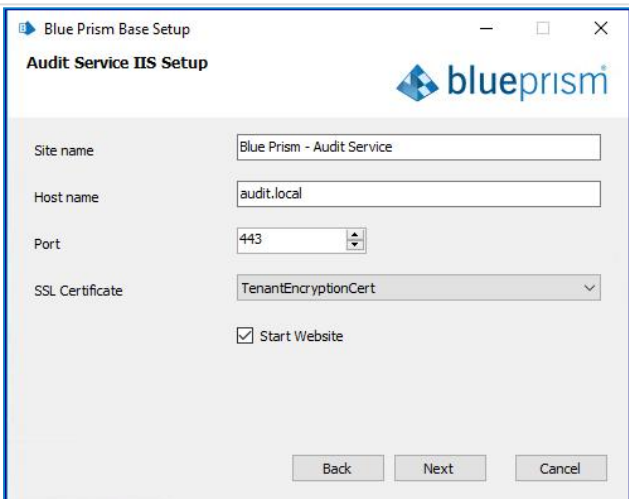
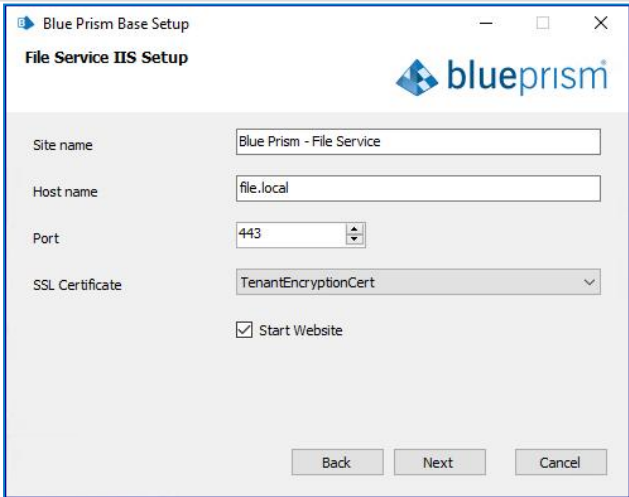
If reinstalling Blue Prism Hub after previously using and removing it, and the same database names are to be used, it is recommended that the databases should be cleared of any old data before re-installing.

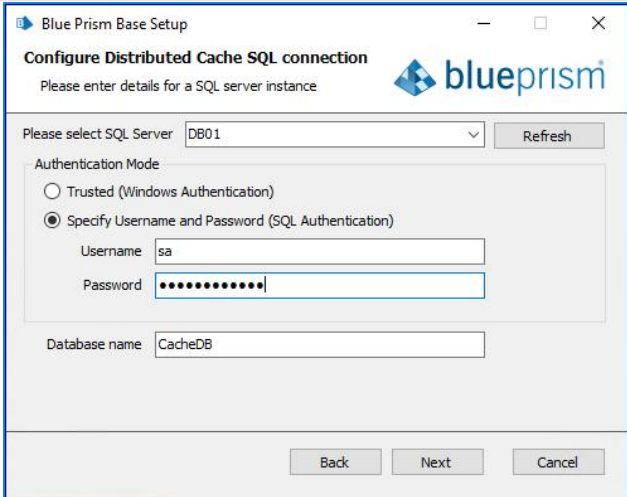
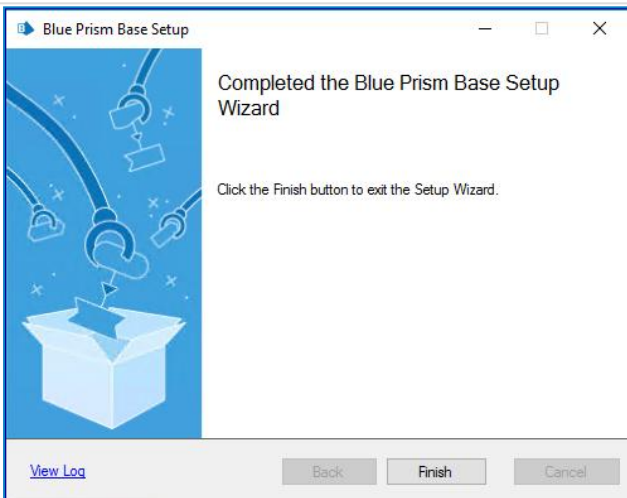
Step	Installer page	Details
1	 <p>The screenshot shows the 'Blue Prism Base Setup' window. On the left is a graphic of puzzle pieces forming a box. The text reads: 'Welcome to the Blue Prism Base Setup Wizard. The Setup Wizard will install Blue Prism Base on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom are 'Back', 'Next', and 'Cancel' buttons.</p>	Welcome
2	 <p>The screenshot shows the 'Blue Prism Base Setup' window with the 'End-User License Agreement' tab selected. It includes the Blue Prism logo and text: 'Please read the Blue Prism Base License Agreement'. A scrollable text area contains the 'Common Public License Version 1.0' terms. Below the text is a checkbox labeled 'I accept the terms in the License Agreement' which is checked. At the bottom are 'Print', 'Back', 'Next', and 'Cancel' buttons.</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		<h3>Prerequisites 1 – Server components</h3> <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		<h3>Prerequisites 2 – RabbitMQ</h3> <p>Enter the server name or IP Address of the Message Broker server and the credentials of the user you created.</p> <div><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. If the test failed see Troubleshoot a Hub installation for further details.</p>
5		<h3>Destination folder</h3> <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		IMS SQL connection Configure the settings for the IMS Database providing the SQL Server hostname or IP Address and the credentials for the account to create the database: <ul style="list-style-type: none"> If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. <div style="border: 1px solid #add8e6; padding: 10px; margin: 10px 0;"> If Windows Authentication is the required method, you need to switch to SQL Authentication and back again to enable the Next button. </div> <ul style="list-style-type: none"> If SQL Authentication is selected, enter the username and password.
7		IMS IIS setup Configure IIS for the IMS website. Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.

Step	Installer page	Details
8	 <p>The screenshot shows the 'Configure Hub SQL connection' window. It includes a dropdown for 'Please select SQL Server' (DB01), a 'Refresh' button, and an 'Authentication Mode' section with two options: 'Trusted (Windows Authentication)' and 'Specify Username and Password (SQL Authentication)'. The latter is selected, with fields for 'Username' (sa) and 'Password' (masked). A 'Database name' field contains 'HubDB'. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.</p>	<h3>Hub SQL connection</h3> <p>Configure the settings for the Hub Database providing the SQL Server hostname 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. Click Next to continue.</p>
9	 <p>The screenshot shows the 'Hub IIS Setup' window. It contains fields for 'Site name' (Blue Prism - Hub), 'Host name' (hub.local), 'Port' (443), and 'SSL Certificate' (TenantEncryptionCert). There is a checkbox for 'Start Website' which is checked. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.</p>	<h3>Hub IIS setup</h3> <p>Configure the Hub website. Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.</p>
10	 <p>The screenshot shows the 'Email Sender IIS Setup' window. It contains fields for 'Site name' (Blue Prism - Email Sender), 'Host name' (email.local), 'Port' (443), and 'SSL Certificate' (TenantEncryptionCert). There is a checkbox for 'Start Website' which is checked. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom.</p>	<h3>Email Sender IIS setup</h3> <p>Configure the Email Sender website. Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.</p>

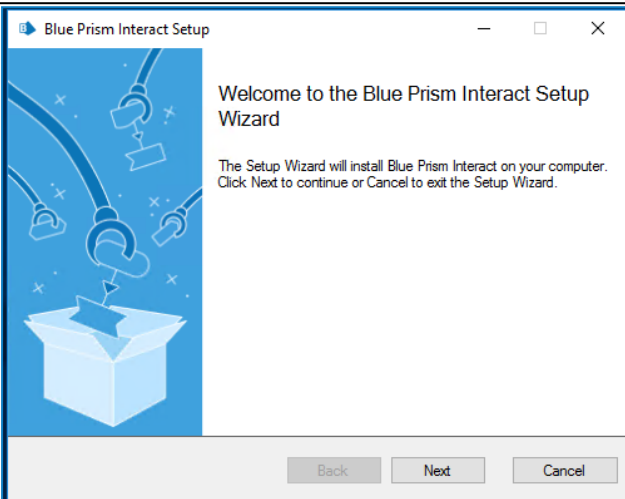
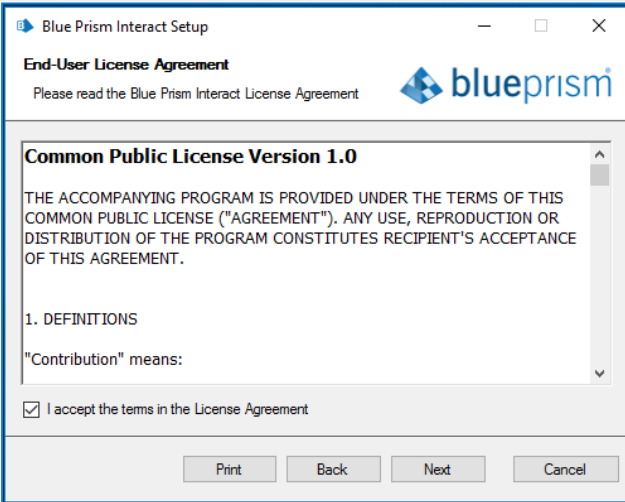
Step	Installer page	Details
11		Audit SQL connection configuration Configure the settings for the Audit Database providing the SQL Server hostname or IP Address and the credentials for the account to create the database: <ul style="list-style-type: none"> If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. If SQL Authentication is selected, enter the username and password. The database name can be left as the default value or changed as required.
12		Audit Service IIS setup Configure the Audit Service website. Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.
13		File Service IIS setup Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.

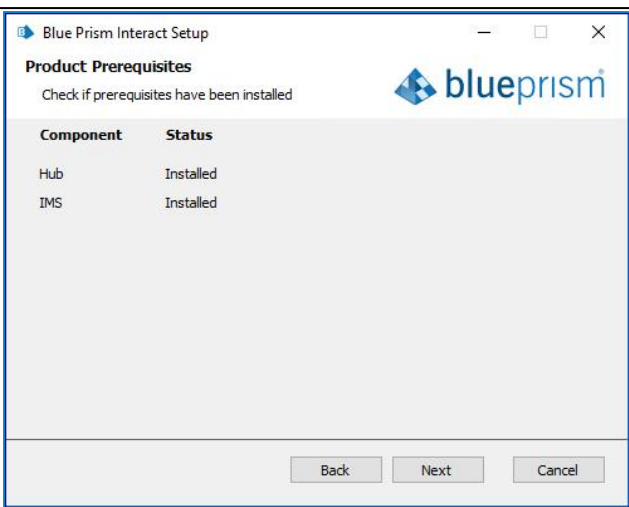
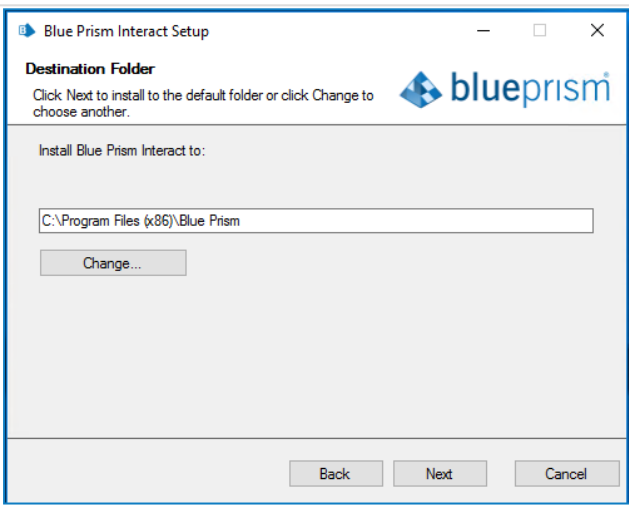
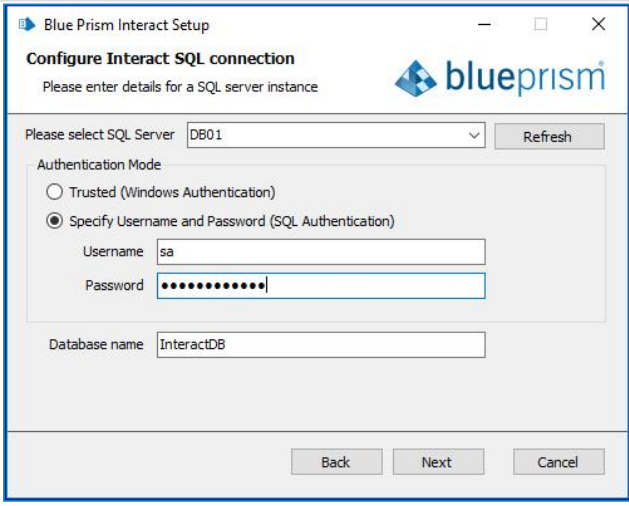
Step	Installer page	Details
14		Distributed Cache SQL connection Configure the settings for the Cache Database providing the SQL Server hostname or IP Address and the credentials for the account to create the database: <ul style="list-style-type: none"> • If Windows Authentication is selected, the account must have the appropriate permissions. See Windows Authentication for further information. • If SQL Authentication is selected, enter the username and password. The database name can be left as the default value or changed as required.
15		Installation complete If the installation failed the View Log option will give you details of the error that was encountered. For more information, see Troubleshoot a Hub installation .

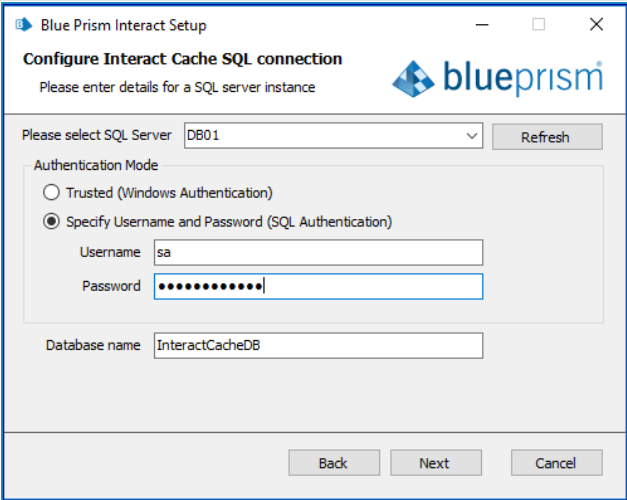
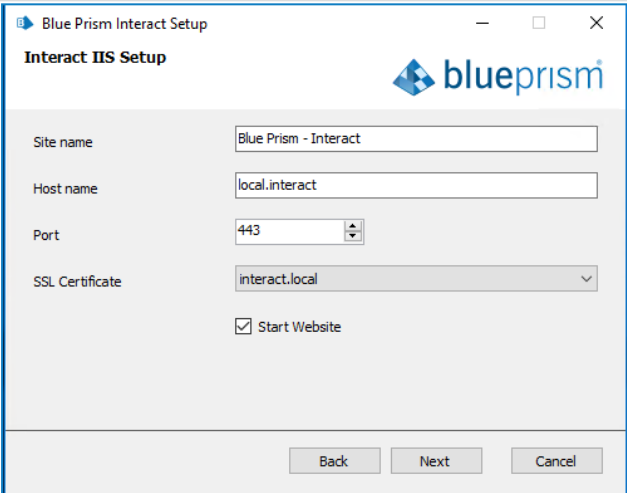
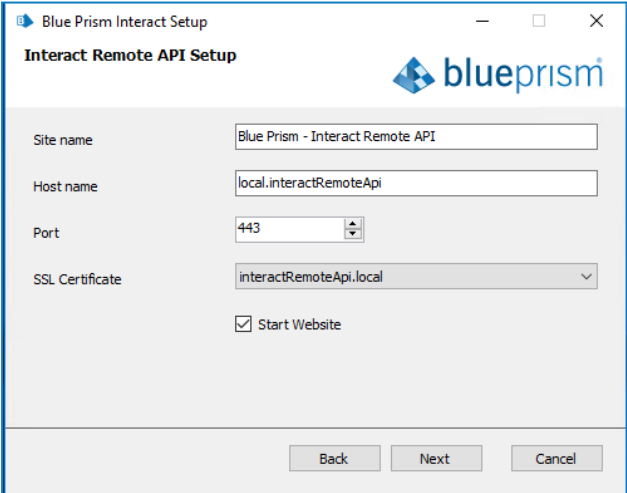
Install Blue Prism Interact

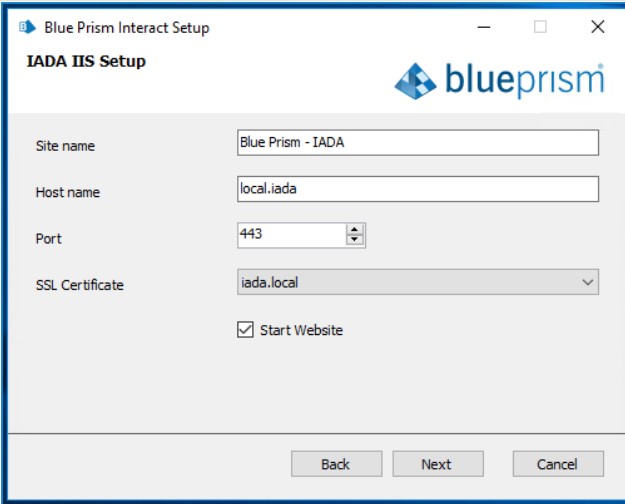
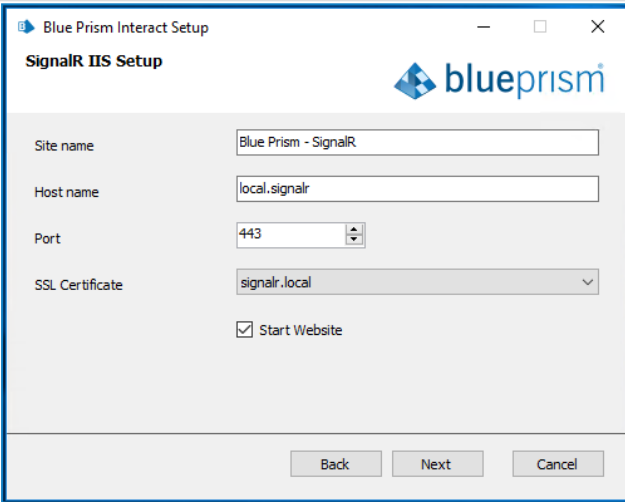
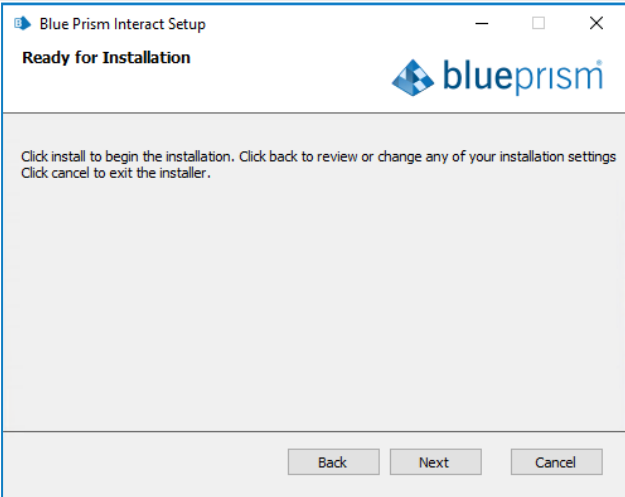
The steps below detail the process for installation of the Blue Prism Interact software. This assumes that the [Blue Prism Hub](#) has been installed which includes the Identify Management System (IMS), Hub, and other associated services.

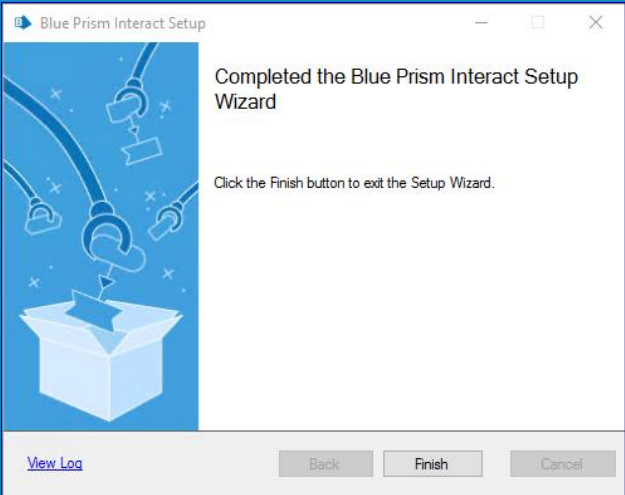
Download and run the Blue Prism Interact installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer should be run with administrator rights.

Step	Installer page	Details
1	 <p>The screenshot shows the 'Blue Prism Interact Setup' window. On the left is a graphic of puzzle pieces forming a box. The text reads: 'Welcome to the Blue Prism Interact Setup Wizard. The Setup Wizard will install Blue Prism Interact on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom are 'Back', 'Next', and 'Cancel' buttons.</p>	Welcome
2	 <p>The screenshot shows the 'Blue Prism Interact Setup' window with the 'End-User License Agreement' tab selected. It includes the Blue Prism logo and the text: 'Please read the Blue Prism Interact License Agreement'. A scrollable text area contains the 'Common Public License Version 1.0' terms. Below the text is a checkbox labeled 'I accept the terms in the License Agreement' which is checked. At the bottom are 'Print', 'Back', 'Next', and 'Cancel' buttons.</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>The screenshot shows the 'Product Prerequisites' window of the Blue Prism Interact Setup. It has a title bar 'Blue Prism Interact Setup' and a close button. Below the title bar is the Blue Prism logo. The main heading is 'Product Prerequisites' with a subtext 'Check if prerequisites have been installed'. There is a table with two columns: 'Component' and 'Status'. The table contains two rows: 'Hub' with status 'Installed' and 'IMS' with status 'Installed'. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.</p>	<h3>Product prerequisites</h3> <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	 <p>The screenshot shows the 'Destination Folder' window of the Blue Prism Interact Setup. It has a title bar 'Blue Prism Interact Setup' and a close button. Below the title bar is the Blue Prism logo. The main heading is 'Destination Folder' with a subtext 'Click Next to install to the default folder or click Change to choose another.' Below this is a text box containing 'C:\Program Files (x86)\Blue Prism' and a 'Change...' button. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.</p>	<h3>Destination folder</h3> <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>
5	 <p>The screenshot shows the 'Configure Interact SQL connection' window of the Blue Prism Interact Setup. It has a title bar 'Blue Prism Interact Setup' and a close button. Below the title bar is the Blue Prism logo. The main heading is 'Configure Interact SQL connection' with a subtext 'Please enter details for a SQL server instance'. Below this is a dropdown menu labeled 'Please select SQL Server' with 'DB01' selected and a 'Refresh' button. Below the dropdown is a section for 'Authentication Mode' with two radio buttons: 'Trusted (Windows Authentication)' and 'Specify Username and Password (SQL Authentication)'. The 'Specify Username and Password' option is selected. Below the radio buttons are two text boxes: 'Username' with 'sa' and 'Password' with masked characters. Below these is a text box for 'Database name' with 'InteractDB'. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.</p>	<h3>Configure Interact SQL configuration</h3> <p>Configure the settings for the Interact Database providing the SQL Server hostname 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. <div>If Windows Authentication is the required method, you need to switch to SQL Authentication and back again to enable the Next button.</div> <ul style="list-style-type: none">If SQL Authentication is selected, enter the username and password.

Step	Installer page	Details
6	 <p>Configure Interact Cache SQL connection Please enter details for a SQL server instance</p> <p>Please select SQL Server: DB01 [Refresh]</p> <p>Authentication Mode:</p> <ul style="list-style-type: none"> <input type="radio"/> Trusted (Windows Authentication) <input checked="" type="radio"/> Specify Username and Password (SQL Authentication) <p>Username: sa</p> <p>Password: [masked]</p> <p>Database name: InteractCacheDB</p> <p>[Back] [Next] [Cancel]</p>	<p>Configure Interact cache SQL configuration</p> <p>Configure the settings for the Interact Cache Database providing the SQL Server hostname 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>
7	 <p>Interact IIS Setup</p> <p>Site name: Blue Prism - Interact</p> <p>Host name: local.interact</p> <p>Port: 443</p> <p>SSL Certificate: interact.local</p> <p><input checked="" type="checkbox"/> Start Website</p> <p>[Back] [Next] [Cancel]</p>	<p>Interact IIS setup</p> <p>Configure the Interact website. Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.</p>
8	 <p>Interact Remote API Setup</p> <p>Site name: Blue Prism - Interact Remote API</p> <p>Host name: local.interactRemoteApi</p> <p>Port: 443</p> <p>SSL Certificate: interactRemoteApi.local</p> <p><input checked="" type="checkbox"/> Start Website</p> <p>[Back] [Next] [Cancel]</p>	<p>Interact remote API setup</p> <p>Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.</p>

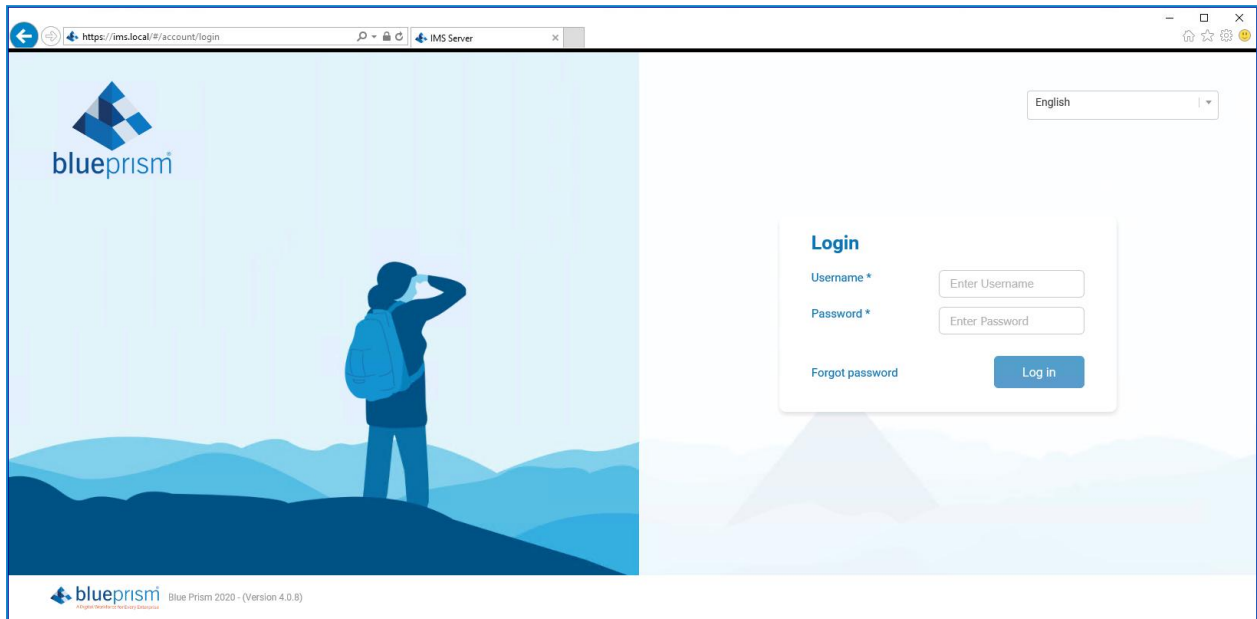
Step	Installer page	Details
9		IADA IIS setup Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.
10		SignalR IIS setup Choose a site name and a Host Name, this is the URL that the site will be accessed over. Define a port to access on and select an SSL certificate as required.
11		Ready for Installation Click Next to install Interact.

Step	Installer page	Details
12		<p>Installation complete</p> <p>If the installation failed, the View Log option will give you details of the error that was encountered.</p> <p>For more information, see Troubleshooting an installation.</p>

Initial Hub configuration and verification

It is now possible to log in for the first time and carry out some system-wide configuration.

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

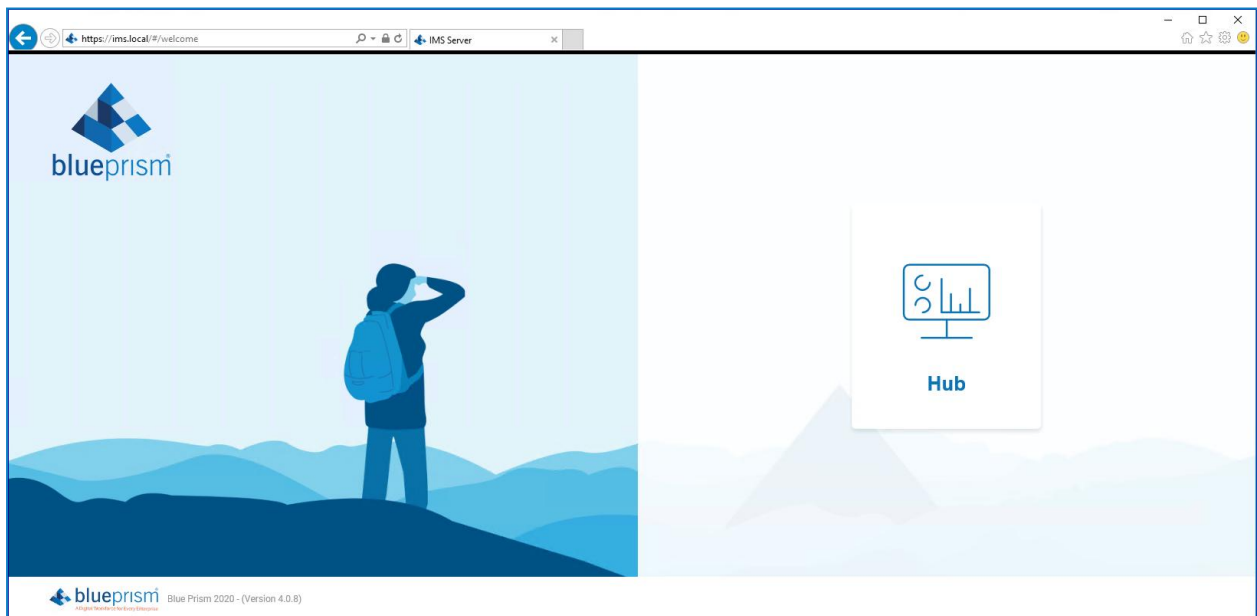


2. Login in using the default credentials.

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

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

3. Click on Hub to launch the Hub website.



Email settings

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

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

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

Email settings

If you need help configuring your SMTP settings, please speak to your IT team in the first instance.

SMTP host *

Enter SMTP host

Port *

Enter Port

Sender email *

Enter Sender email

Encryption *

None

☐ SMTP authenticate

Username

Enter Username

Password

Enter Password

Send test email to

some@mail.com

Save

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

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

Database settings

Configure access to the Blue Prism RPA database.

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

Database connections

Environment:

Database connection(s)

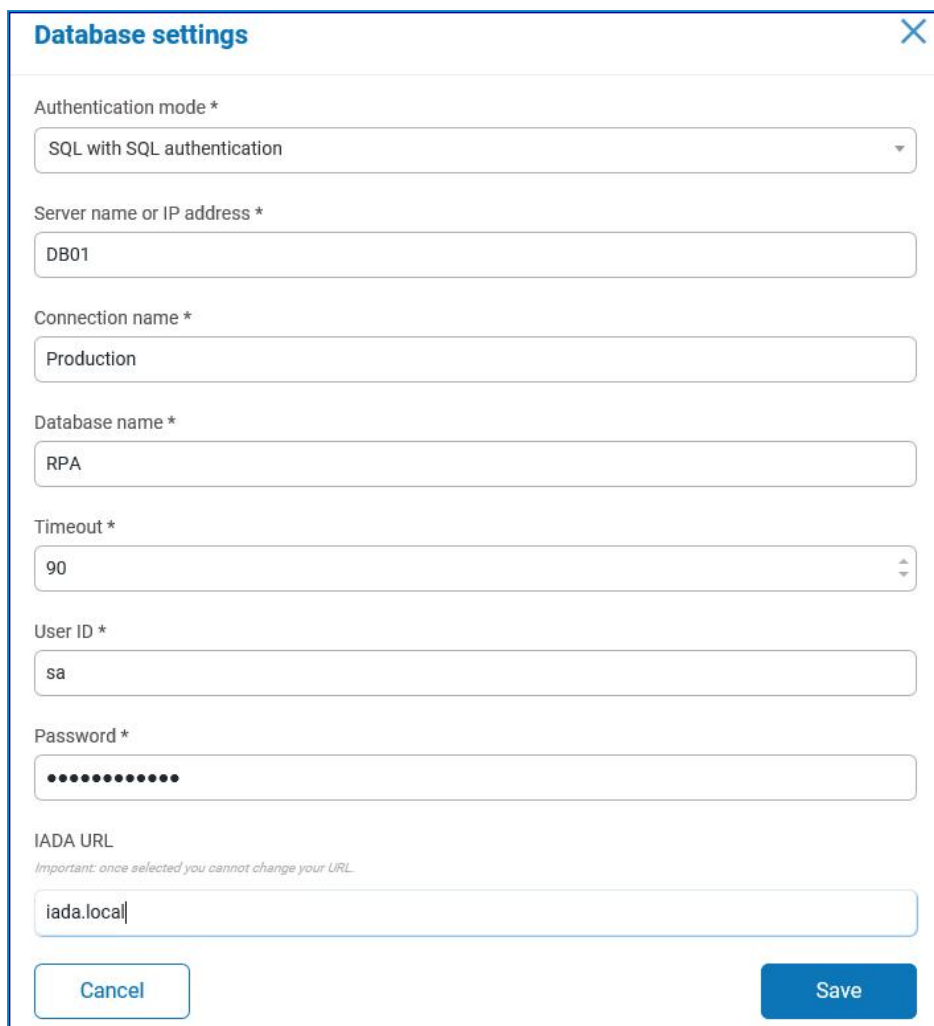
Connection name	Database name	Authentication mode	Server name or IP address
	HubDB	SQL with SQL authentication	DB01

Blue Prism database connection (s) - 0/10

+ Add new

Connection name	Database name	Authentication mode	Server name or IP address	IADA URL	Actions
No data available in table					

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



Database settings [X]

Authentication mode *
SQL with SQL authentication

Server name or IP address *
DB01

Connection name *
Production

Database name *
RPA

Timeout *
90

User ID *
sa

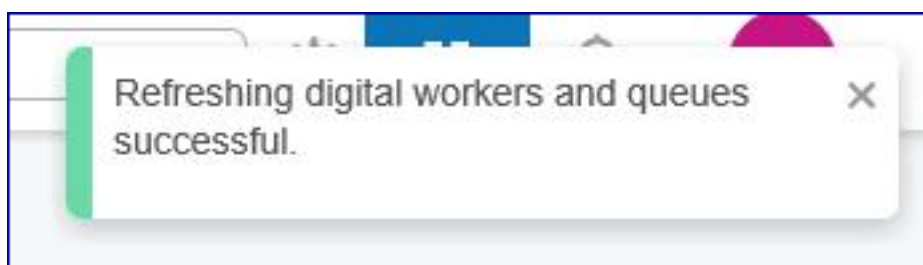
Password *
.....

IADA URL
Important: once selected you cannot change your URL.
iada.local

Cancel Save

The Timeout value is in seconds.

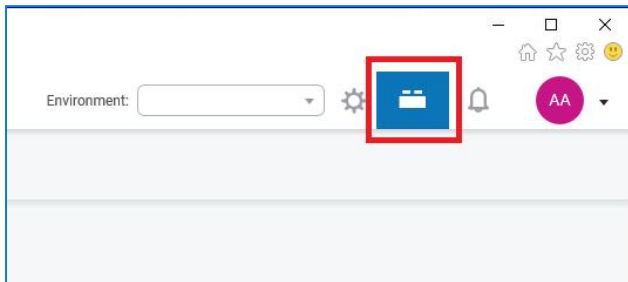
3. Click **Save** to save your data.
4. To test the settings, go back into the Database settings and click on the action menu (three dots) alongside the configured database and select **Refresh**. If operational the following message displays in the top right corner of the Hub user interface, which verifies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



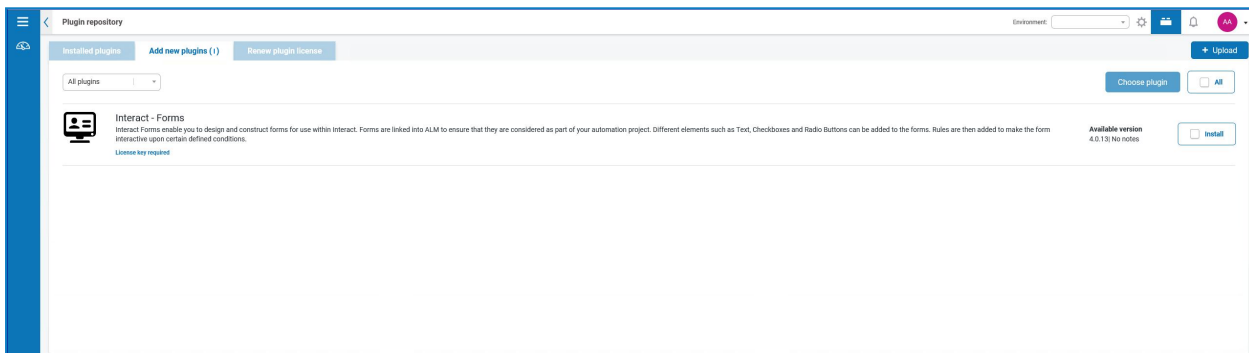
Install the Interact plugin

The Interact plugin must be installed with the associated license.

Click on the Plugin repository, red square in the image below.



In the repository select the Interact Plugin to install and apply the necessary license.



For more information about installing plugins, see the [Hub user guide](#).

Configure digital workers

This section provides the steps required to 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](#)

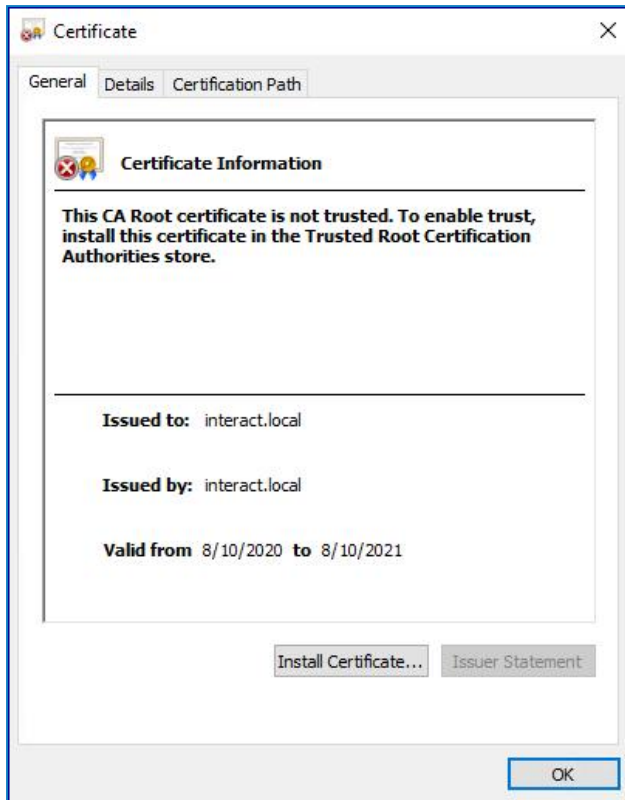
These instructions assume that the user is familiar with Blue Prism.

Install SSL certificates

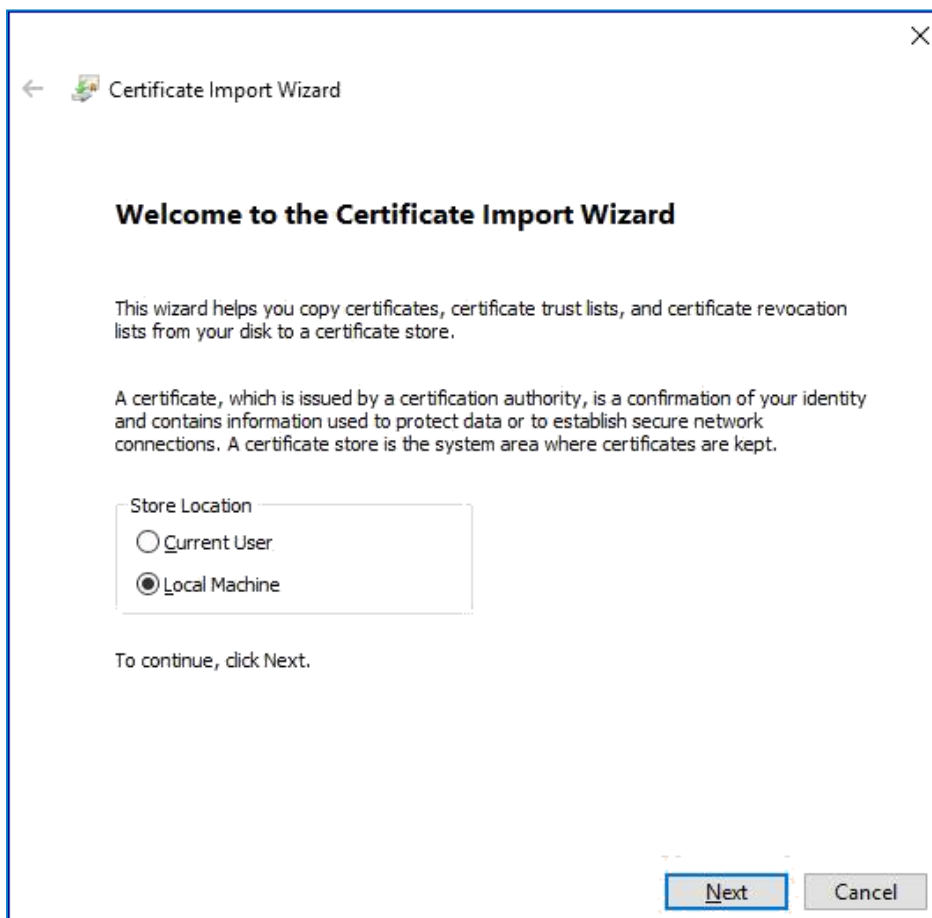
On each Digital Worker, log in and copy across the SSL Certificates for Interact, IADA, Interact Remote API, and Signal R.

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.

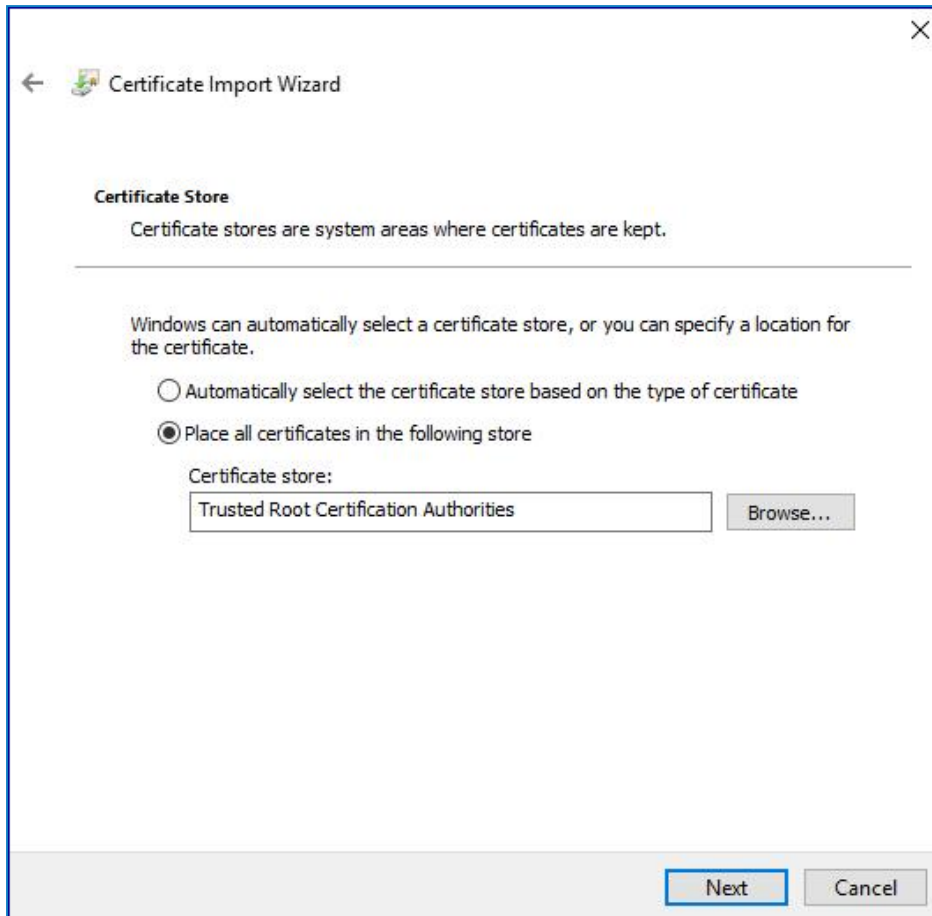
1. Double-click on each SSL Certificate and select to **Install Certificate**.



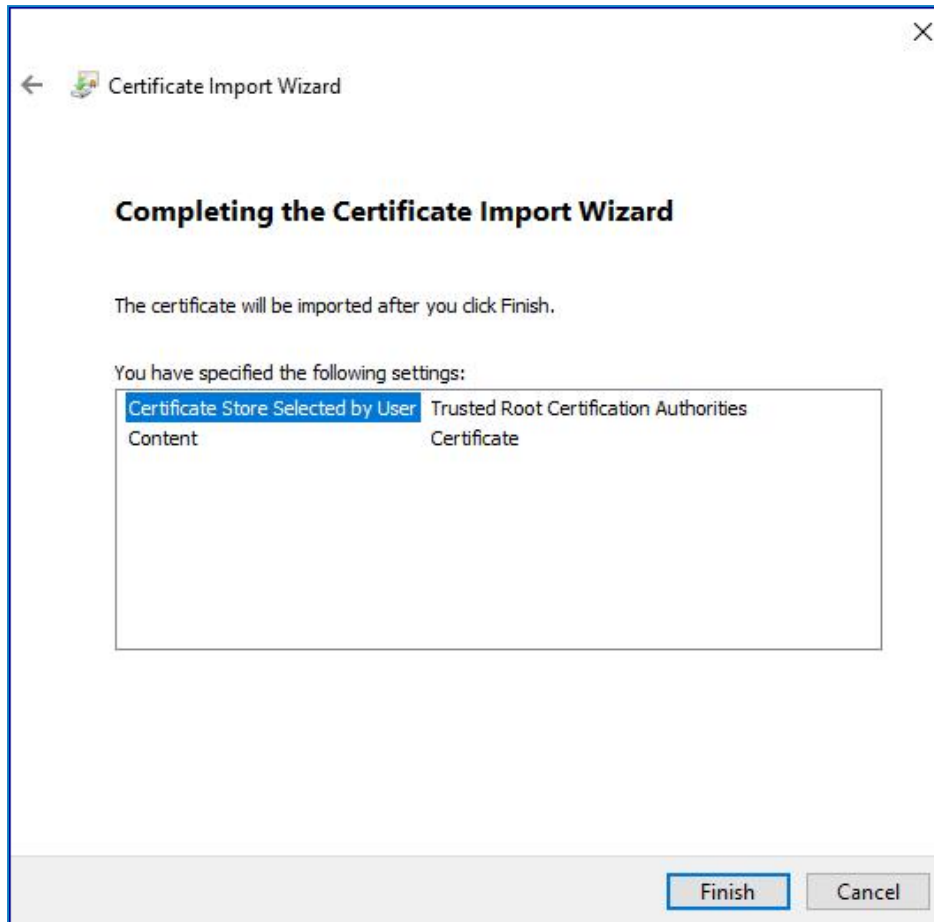
2. Change the Store location to **Local Machine**.



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.

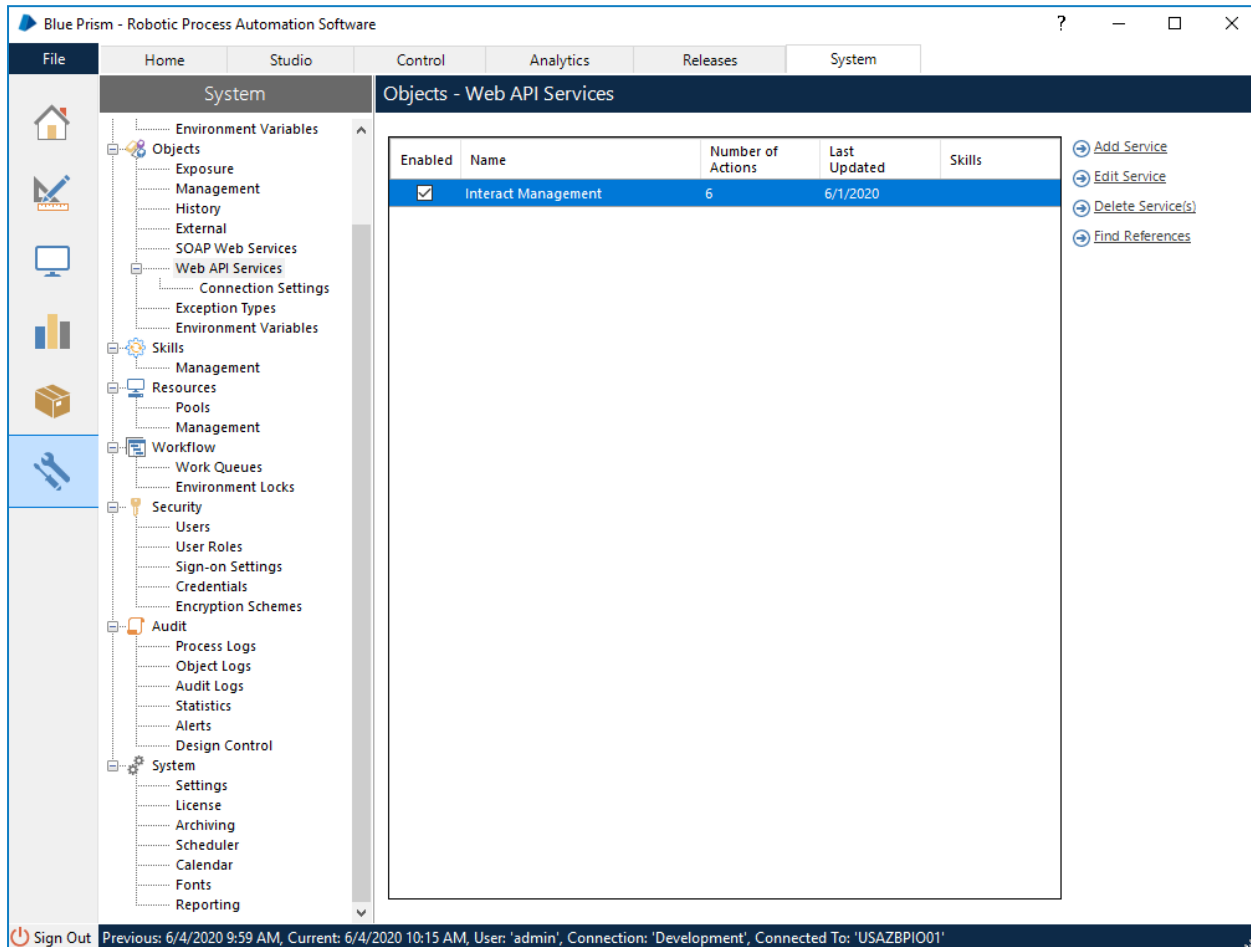
This is dependent on the architecture structure that was deployed, so this could already be established if the systems are domain joined and the IT organization has configured the servers. Alternatively the local hosts file may need to be adjusted to ensure that the sites can be reached.

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 https://IMS.local
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local
Blue Prism – Signal R	https://signalr.local

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.



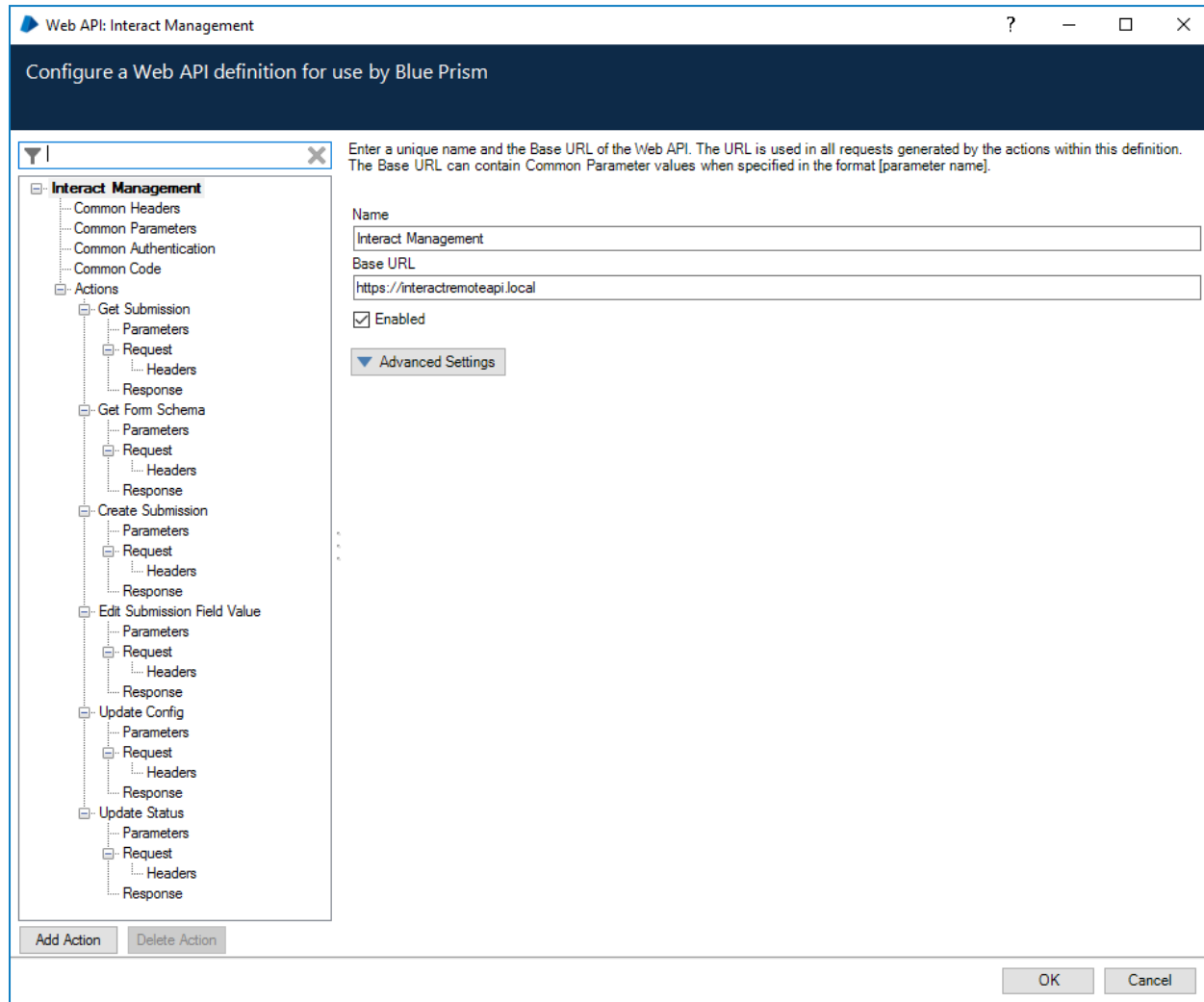
The screenshot shows the Blue Prism - Robotic Process Automation Software interface. The left sidebar contains a tree view of the system structure, including Environment Variables, Objects, Skills, Resources, Workflow, Security, Audit, and System. The main pane displays the 'Objects - Web API Services' table.

Enabled	Name	Number of Actions	Last Updated	Skills
<input checked="" type="checkbox"/>	Interact Management	6	6/1/2020	

On the right side of the table, there are four action links: [Add Service](#), [Edit Service](#), [Delete Service\(s\)](#), and [Find References](#).

The status bar at the bottom indicates: **Sign Out** Previous: 6/4/2020 9:59 AM, Current: 6/4/2020 10:15 AM, User: 'admin', Connection: 'Development', Connected To: 'USAZBPIO01'

The image below shows the web API service.



Web API: Interact Management

Configure a Web API definition for use by Blue Prism

Enter a unique name and the Base URL of the Web API. The URL is used in all requests generated by the actions within this definition. The Base URL can contain Common Parameter values when specified in the format [parameter name].

Interact Management

- Common Headers
- Common Parameters
- Common Authentication
- Common Code
- Actions
 - Get Submission
 - Parameters
 - Request
 - Headers
 - Response
 - Get Form Schema
 - Parameters
 - Request
 - Headers
 - Response
 - Create Submission
 - Parameters
 - Request
 - Headers
 - Response
 - Edit Submission Field Value
 - Parameters
 - Request
 - Headers
 - Response
 - Update Config
 - Parameters
 - Request
 - Headers
 - Response
 - Update Status
 - Parameters
 - Request
 - Headers
 - Response

Name: Interact Management

Base URL: https://interactremoteapi.local

☒ Enabled

Advanced Settings

Add Action Delete Action

OK Cancel

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 URI 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.

Configure credentials for the Interact Web API service

When configuring the credentials for the OAuth 2.0 (Client Credentials) the following four values need to be configured as indicated below:

- Username = InteractRemoteClient
- Password = Client Secret (from secret key file contents)

Additional Properties:

- grant_type set value to client_credentials
- scope set value to interact-remote-api

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 six defined actions:

- Get Submission
- Get Form Schema
- Create Submission
- Edit Submission Field Value

- Update Config
- Update Status

These actions are called from a supplied Blue Prism Object so after the initial configuration of the URL and authorization codes the Web Service does not need to be amended. In the next section we will go through each of the actions within the Blue Prism Object and explain how they are used.

Verify an installation

This section provides a simple scenario to test that the basic components of the Blue Prism installation are operating as expected.

The verification steps include:

- [Creating a business process inside Hub.](#)
- [Creating an Interact Form.](#)
- [Adding the Form to a role.](#)
- [Submitting the Form and ensuring that it appears in a queue within Blue Prism.](#)

These instructions assume that the user is familiar with Blue Prism and that there is a queue already in existence in Blue Prism.

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

Once the business process is created it cannot be deleted.

Creating a business process inside Hub

1. Log into IMS and select Hub (login with an administrator role).
2. Refresh the queues and digital workers in Hub:
 - a. Click the settings cog and select the database settings.
 - b. Go to the RPA database environment that you will be submitting to and click **Refresh** from the action menu (three dots).
3. Select **Business Processes** from the left navigational bar.
4. Click **Add New**.
5. Enter in a unique identifier and a name from the Business Process, optionally add in a description, then click **Next**.
6. Select and add any additional users if required then click **Next**.
7. Enter any additional notes if required and click **Save**.

Creating an Interact Form

1. Select **Forms** from the left Navigational bar.
2. Select **Add New** to create a new Interact Form.
3. Select the business process from the drop-down if not already selected.
4. Enter a name for the Interact Form and a description.
5. Select the **Queue** box to indicate that we want to submit the Interact Form to a Blue Prism Queue.
6. Select the environment from the drop-down and then select the required queue name.

If the database settings have not been refreshed, the Queue in Blue Prism won't be seen.

7. Leave the Priority and SLA blank, do not tick the Email check box.
8. Leave the Default approval type at **None**.
9. Enter a Category. For example if you were creating a New Starter Form, you may group the Forms in a Human Resource category.
10. Select an Icon to represent the Form in Interact.
11. Click **Save**.
12. In the new display, select **Add page** and in the new form type a name and click **Save**.
13. Click the **+** corresponding to the page that you just created.
14. In the Create capture field dialog, leave everything as the default and in the **Label** field enter **First Name**.
15. Click **Save**.
16. Click the **+** again and in the Create capture field dialog, leave everything as the default and enter in the **Label** field enter **Last Name**.
17. Click **Save**.
18. Click **Save** in the main window and in the Increase minor dialog, enter an update note and click **Save**.

Adding the form to a role

1. Click the settings cog and select **Users, roles and registration approval**.
2. Click on the **Roles** tab and then select **Add New**.
3. Change the Role type to **Interact**.
4. Enter a role name and an optional description, then click **Next**.
5. Select the user(s) who you want to have access to the Form that you have created and click **Next**.
6. Select from Form you have just created from the drop-down and click **Save**.

Submitting the form to a queue in Blue Prism

1. Log into Interact via IMS with the user you just allowed access to the created Form.
2. Click on the Form that you just created and click **Select** on the expanded view.
3. Enter your first and last names and then click the **Select** button.
4. Log into Blue Prism and check whether there is an item in the work queue specified when creating the Form.

This completes the verification of the installation.

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

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.

Default application information

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

Interact websites

Application Name	Default service account name for SQL Windows Authentication	Database permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - Interact	IIS APPPOOL\ Blue Prism – Interact	dbowner (create / alter tables)	Read / Write	InteractDB, InteractCacheDB
Blue Prism - Interact Remote API	IIS APPPOOL\ Blue Prism – Interact Remote API	Read / Write	Read / Write	ImsDB, InteractDB
Blue Prism - IADA	IIS APPPOOL\ Blue Prism – IADA			
Blue Prism - SignalR	IIS APPPOOL\ Blue Prism – SignalR			

Interact services

Application Name	Default service account name for SQL Windows Authentication	Database permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - Submit Form Manager	NT AUTHORITY\SYSTEM	Read / Write	Read / Write	InteractDB

Troubleshoot a Hub installation

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

Message Broker connectivity

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

There could be several reasons that connectivity fails:

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

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

Database connectivity

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

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

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

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

Web Server

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

Starting the IMS website

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

If the Windows features were not installed in their entirety before the .Net Core Component, then the .Net Core 3.1.2 Windows Server Hosting will need to be repaired or reinstalled.

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

File service

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

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

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

Windows Authentication

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

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

This service account will need not only the ability to perform the SQL database creation process, see Minimum SQL permissions, 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, i.e. IIS start before the RabbitMQ service is ready then going into the SMTP settings in Hub will result in a 'something went wrong' message.

Default application information

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

Hub websites

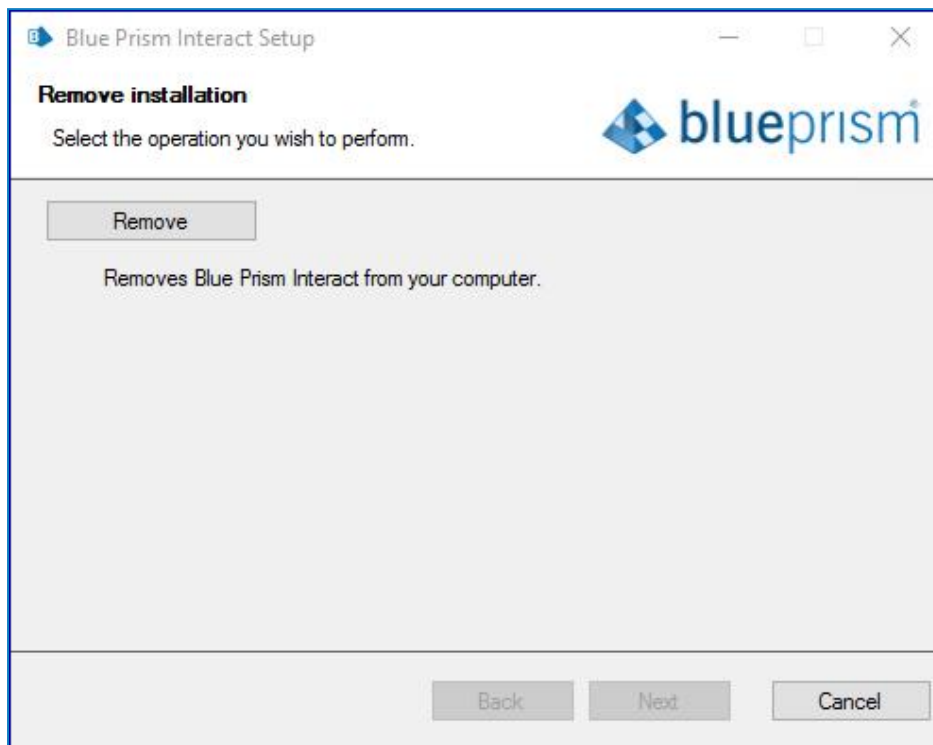
Application Name	Default service account name for SQL Windows Authentication	Database permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - IMS	IIS APPPOOL\ Blue Prism – IMS	dbowner (create / alter tables)	Read / Write	ImsDB
Blue Prism - Hub	IIS APPPOOL\ Blue Prism – Hub	dbowner (create / alter tables)	dbowner (create / alter tables)	HubDB
Blue Prism - Email	IIS APPPOOL\ Blue Prism – Email			
Blue Prism - Audit Service	IIS APPPOOL\ Blue Prism – Audit Service	dbowner (create / alter tables)	Read / Write	AuditDB
Blue Prism - File Service	IIS APPPOOL\ Blue Prism – File Service	dbowner (create / alter tables)	Read / Write	CacheDB

Hub services

Application Name	Default service account name for SQL Windows Authentication	Database permissions required during installation	Database permissions required during application running	Default database name
Blue Prism - Audit Service Listener	NT AUTHORITY\SYSTEM	dbowner (create / alter tables)	Read / Write	AuditDB
Blue Prism - Log Service	NT AUTHORITY\SYSTEM			

Uninstall Interact

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



When removing the installation it will remove the following items:

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

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

If the installation is repeated again after removing Interact, the existing database should be backed-up and the connection dropped prior to installation.