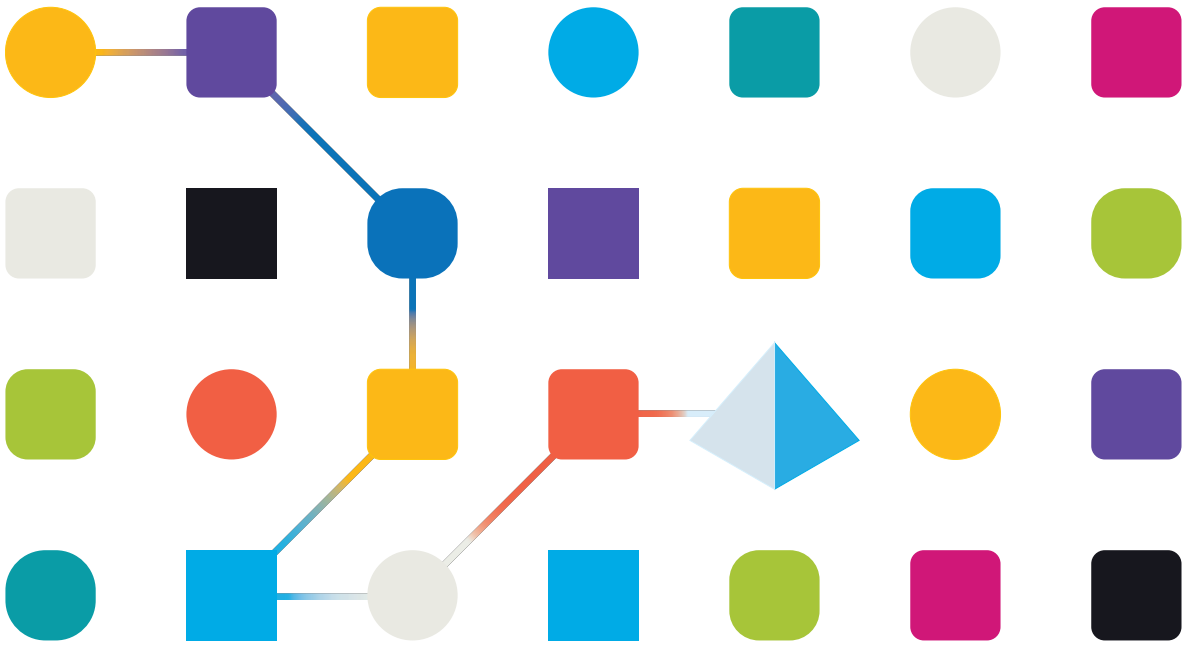
blueprism®

Hub 4.1

Guía de instalación

Revisión del documento: 2.0



Marcas comerciales y derechos de autor

La información que contiene este documento es confidencial y pertenece a Blue Prism Limited y no debe divulgarse a terceros sin el consentimiento por escrito de un representante autorizado de Blue Prism. Ninguna parte de este documento puede reproducirse o transmitirse de ninguna forma ni por ningún medio, ya sea electrónico o mecánico, incluyendo fotocopias, sin el permiso por escrito de Blue Prism Limited.

© 2023 Blue Prism Limited

"Blue Prism", el logotipo de "Blue Prism" y el dispositivo Prism son marcas comerciales o marcas comerciales registradas de Blue Prism Limited y sus filiales. Todos los derechos reservados.

Mediante el presente, se reconocen todas las marcas comerciales y se usan para el beneficio de sus respectivos propietarios.
Blue Prism no es responsable del contenido de sitios web externos a los que este documento hace referencia.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, Reino Unido.
Registrado en Inglaterra: N.º de registro 4260035. Tel.: +44 370 879 3000. Sitio web:
www.blueprism.com

Contenido

Instalación de Hub **4**
Actualización de Hub 4
Orientación relacionada 4
Preparación **5**
Planificación 5
Requisitos previos 6
Lista de descarga de software 8
Requisitos y permisos de software Hub **11**
Requisitos de software 11
Permisos mínimos de SQL 13
Información de aplicación predeterminada 13
Consideraciones de la implementación en varios dispositivos **15**
Puertos de red **16**
Implementación típica de **17**
Descripción general de los pasos comunes de instalación 18
Instalar el servidor de agente de mensajería 19
Instalar y configurar el servidor web 24
Configuración inicial de Hub 48
Solucionar problemas en una instalación de Hub **52**
Conectividad del agente de mensajería 52
Conectividad de la base de datos 52
Servidor web 53
Inicio del sitio web de IMS 53
File Service 53
Autenticación de Windows 53
No se pueden configurar los ajustes de SMTP en Hub 54
Desinstalación de Hub **55**

Instalación de Hub

Esta guía ofrece orientación sobre el proceso a seguir cuando se instala Blue Prism® Hub.

Blue Prism Hub solo es compatible en una implementación de múltiples dispositivos, donde los componentes de Blue Prism se implementan en varios dispositivos. Los motivos de esto son los siguientes:

- Ofrece una implementación extensible de los componentes de Blue Prism adecuada para una amplia variedad de situaciones.
- Las técnicas avanzadas relacionadas con la implementación de servicios adicionales o con la protección y consolidación del entorno en general requerirán este tipo de implementación.

También se incluyen una serie de temas más avanzados dentro de esta guía para ofrecer información sobre la solución de problemas en instalaciones y la configuración de opciones avanzadas. Se supone que la persona que realiza la instalación de Hub tiene conocimientos o experiencia previos en Blue Prism, la configuración de certificados SSL y RabbitMQ.

Si necesita más ayuda cuando consulta este documento, comuníquese con su administrador de cuenta de Blue Prism o con Soporte Técnico. Consulte Contáctenos para obtener más información.

Esta información se relaciona con la versión 4.1 de Blue Prism Hub.

Blue Prism Hub se debe instalar antes de intentar instalar Interact.

Actualización de Hub

Si se actualiza desde una versión anterior de Hub 4, Blue Prism suministra un actualizador. Para obtener más información, consulte Actualización de Hub e Interact.

Orientación relacionada

Los siguientes documentos proporcionan más información sobre aspectos específicos de la implementación de Hub y sus complementos.

Título del documento	Descripción
Guía del usuario de Hub	Es un documento detallado que explica cómo obtener lo mejor de Hub, incluidos el acceso de usuarios, los complementos de licencias y la personalización de Hub.
Guía de instalación 4.7 de la extensión Authentication Server SAML 2.0	Documento que explica cómo instalar la extensión SAML 2.0. Esto es necesario si su organización desea utilizar la autenticación SAML 2.0. Este enlace lo lleva a Digital Exchange, donde se puede acceder a la guía en formato PDF.
Guía del usuario de ALM	Un documento que explica cómo utilizar el complemento Automation Lifecycle Management (ALM). Este es un producto con licencia.
Guía de instalación de Interact	Documento que explica los pasos necesarios para instalar Interact. Este es un producto con licencia.
Guía del usuario de Interact	Documento que explica cómo usar Interact. Este es un producto con licencia.
Guía del usuario de Wireframer	Documento que explica cómo utilizar la opción Wireframer, que forma parte del complemento de ALM. Este es un producto con licencia.

Preparación

Antes de llevar a cabo una instalación de Blue Prism Hub, es importante asegurarse de que la arquitectura esté configurada para admitir la instalación. Se requieren múltiples sistemas para admitir la instalación de Hub.

Planificación

Antes de realizar la instalación, se deben cumplir las siguientes condiciones:

- Debe haber un Servidor SQL disponible para alojar las bases de datos de componentes de Blue Prism, como IMS , Hub, Audit, etc. Durante el proceso de instalación se requiere acceso a nivel de administrador. Consulte Permisos mínimos de SQL en la página 13 para obtener más detalles.
- Debe haber un servidor de agente de mensajería disponible para alojar al agente de mensajería de RabbitMQ. Consulte Instalar el servidor de agente de mensajería en la página 19 para obtener más detalles.
- Un servidor web para la instalación de Hub. Consulte los Requisitos previos en la página siguiente para obtener más información.
- Debe haber disponible acceso de administrador a los dispositivos donde se instalará Blue Prism Hub. Todos los dispositivos deben cumplir las especificaciones mínimas, y los dispositivos deben poder comunicarse unos con otros a través de la red local, incluida la comunicación con su base de datos de Blue Prism. DNS debe estar disponible para todos los componentes.
- La cuenta que realiza la instalación debe tener acceso al archivo hosts. Generalmente se almacena en C:\Windows\System32\drivers\etc\hosts o en %SYSTEMROOT%\System32\drivers\etc\hosts.

Al planificar su implementación, se deben considerar los siguientes puntos:

- ¿Se agregará la base de datos a un servidor de base de datos existente o se pondrá en marcha uno nuevo?

  Blue Prism recomienda que las bases de datos se mantengan en servidores de bases de datos separados.
- ¿Hay suficiente espacio y recursos para alojar las bases de datos agregadas?

  Debe asegurarse de que haya espacio suficiente en el disco y de que los recursos de proceso puedan hacer frente a la carga adicional.
- ¿Qué modo de autenticación se requiere para la base de datos SQL (nativa de SQL o autenticación de Windows)?

  Esta es la decisión de su organización de TI.
- ¿Se configuró el servidor de agente de mensajería para admitir la instalación de Hub?

  Se requiere un servidor de agente de mensajería para completar la instalación de Hub.
- ¿Todos los dispositivos donde se instalará Blue Prism Hub cumplen los requisitos mínimos (incluida la versión 4.7.2 de .NET Framework)?

  Consulte Requisitos y permisos de software Hub en la página 11 para obtener detalles.

Requisitos previos

Consulte Requisitos y permisos de software Hub en la página 11 para obtener detalles sobre los requisitos de software y los permisos mínimos de SQL.

La instalación de Hub requiere los siguientes requisitos previos:

- El servidor SQL debe estar configurado para usar cifrado SSL. Si su organización aún no utiliza cifrado SSL (ha estado ejecutando su entorno sin certificados para servidor SQL o ha estado utilizando un certificado autofirmado), debe obtener un certificado de una autoridad de certificación de confianza e importarlo al servidor SQL para habilitarlo. Para obtener más información, consulte la documentación de Microsoft.

  Para importar un certificado en el servidor SQL:

  1. En la barra de tareas de Windows, abra **Administrador de configuración del servidor SQL**.
  2. En el Administrador de configuración del servidor SQL, expanda **Configuración de red de servidor SQL**, haga clic con el botón derecho en **Protocolos para <SqlServerInstanceName>** y, a continuación, haga clic en **Propiedades**.
  3. En el cuadro de diálogo de propiedades de Protocolos para <SqlServerInstanceName>, seleccione la pestaña **Certificado** y luego seleccione o importe el certificado requerido.
  4. Haga clic en **Aplicar**.

  Los certificados de autoridades de certificación de confianza deben utilizarse para entornos de producción. Sin embargo, se podría utilizar un certificado autofirmado para entornos de prueba de concepto o desarrollo. Es importante que el nombre de dominio completo (FQDN) utilizado por el servidor SQL coincida con el FQDN definido en el certificado. **Si no coinciden, no se establecerá una conexión a la base de datos y su instalación no funcionará correctamente.** Para obtener información sobre el uso y la configuración de certificados autofirmados, consulte Certificados autofirmados.

  Además de las bases de datos instaladas por el instalador de Hub, su base de datos de Blue Prism también debe usar cifrado SSL, utilizando un certificado en el que confíe el servidor de Hub, como una autoridad de certificación de confianza.

- La compilación del servidor de agente de mensajería es una configuración genérica e instalación base de un servicio de agente de mensajería de RabbitMQ. Se recomienda que se cambien las contraseñas predeterminadas y que su departamento de TI complete cualquier requisito de seguridad, como la aplicación de certificaciones SSL.

  Para completar la compilación del agente de mensajería, se debe descargar lo siguiente:

  - Erlang/OTP, consulte: https://www.rabbitmq.com/which-erlang.html
  - RabbitMQ Server (las versiones compatibles son de 3.8.0 a 3.8.8), disponible aquí: https://github.com/rabbitmq/rabbitmq-server/releases/

  Aquí encontrará orientación para la instalación: https://www.rabbitmq.com/install-windows-manual.html

- Blue Prism Hub está instalado en el servidor web y, por lo tanto, requiere que estén instalados el administrador de Internet Information Services (IIS), y los componentes de .Net Core. Estos deben estar preinstalados para permitir una instalación correcta de Blue Prism Hub. Consulte Instalar y configurar el servidor web en la página 24 para obtener más información.

- Certificados: durante el proceso de instalación, se le solicitarán los certificados SSL para los sitios web que se están configurando. Según los requisitos de seguridad de su infraestructura y de la organización de TI, esto podría ser un certificado SSL creado internamente o un certificado adquirido para proteger los sitios web. El instalador se puede ejecutar sin que el certificado esté presente, aunque para que los sitios funcionen, los enlaces en los sitios web de Internet Information Services deberán tener certificados SSL válidos. Para obtener más información, consulte Configurar certificados SSL en la página 24.
- Cuando se utiliza la autenticación de Windows, se requieren cuentas de servicio de Windows definidas para su uso con el entorno de Blue Prism. Esto es para que los servicios de Windows y los grupos de aplicaciones se puedan configurar correctamente para los sitios web creados durante la instalación del Hub.
- De manera predeterminada, se utilizan los grupos de aplicaciones de Internet Information Services. Los grupos de aplicaciones deben tener acceso a los archivos de la aplicación y a certificados que se crean durante la instalación para la protección y autorización de datos. Estos certificados son BluePrismCloud_Data_Protection y BluePrismCloud_IMS_JWT y se encuentran dentro de la carpeta de certificados predeterminada de Windows. Si utiliza la autorización de Windows para acceder al servidor SQL, esta deberá configurarse manualmente. Para obtener más información, consulte Información de aplicación predeterminada en la página 13.
- De manera predeterminada, la cuenta “Sistema local” se utiliza para los servicios. Esta cuenta debe tener acceso a los archivos de la aplicación. Si utiliza la autorización de Windows para acceder al servidor SQL, esta deberá configurarse manualmente.

Lista de descarga de software

Blue Prism Hub

Esto enumera todas las descargas necesarias para instalar Hub. Todas estas se mencionan más adelante en la guía de instalación:

Software y enlace de referencia	Orientación relacionada
RabbitMQ 3.8.0 a 3.8.8 3.9.22 a 3.10.7 Para obtener más información, consulte Descarga e instalación de RabbitMQ.	Instalar el servidor de agente de mensajería en la página 19
Erlang/OTP La versión de Erlang que necesita depende de la versión de RabbitMQ que desea utilizar. Para obtener más información, consulte Requisitos de la versión Erlang de RabbitMQ.	

Software y enlace de referencia	Orientación relacionada
IIS 10.0 Incluido con Windows Server 2016 y Windows Server 2019. Incluido con Windows Server 2016, 2019 y 2022.	Instalar y configurar el servidor web en la página 24
.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 https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **ASP.NET Core Runtime**, seleccione **Paquete de alojamiento**.	
.NET Core 3.1.3 Windows Desktop Runtime https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-desktop-3.1.3-windows-x64-installer https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **.NET Desktop Runtime**, seleccione la descarga adecuada.	
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 Esto se instala de forma predeterminada en Windows Server 2019. Solo necesita instalar .NET Framework si está utilizando Windows Server 2016. .NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 Esto se instala de forma predeterminada en Windows Server 2022. Solo necesita instalar .NET Framework si está utilizando Windows Server 2016 Datacenter o Windows Server 2019.	
Blue Prism Hub 4.1 Descargue Hub desde cualquiera de las siguientes páginas de descarga de productos en el portal de Blue Prism: • Automation Lifecycle Management • Interact	
Extensión de Authentication Server SAML 2.0 Descargar desde Digital Exchange; este es un instalador opcional. Solo se requiere si tiene la intención de usar la autenticación SAML 2.0.	Consulte la guía de instalación en Digital Exchange.

Blue Prism Interact

Blue Prism Interact es un complemento controlado por licencia en Hub y un sitio web adicional para usuarios finales. Si su organización tiene la intención de utilizar Interact, deberá descargar lo siguiente además de las descargas enumeradas en Blue Prism Hub en la página 8.

Software y enlace de referencia	Orientación relacionada
Blue Prism Interact 4.1 Descargue desde el portal de Blue Prism.	Instalar Blue Prism Interact
Archivo API.bprelease remoto de Blue Prism Interact Descargue desde el portal de Blue Prism.	Instalar y configurar el servicio de API web de Interact

Requisitos y permisos de software Hub

Requisitos de software

Las siguientes tecnologías son compatibles con el uso del software:

Sistema operativo

Versión	Servidor web	Agente de mensajería
Centro de datos de Windows Server 2016	✓	✓
Windows Server 2019	✓	✓
Windows Server 2022	✓	✓

Cuando los componentes de Blue Prism están instalados en un sistema operativo de 64 bits, se ejecutará en una aplicación de 32 bits.

Microsoft SQL Server

Se admiten las siguientes versiones de Microsoft SQL Server para ubicar las bases de datos del componente de Blue Prism:

Versión	Express	Standard	Enterprise
Servidor SQL 2016	✓	✓	✓
Servidor SQL 2017	✓	✓	✓
Servidor SQL 2019 (64 bits)	✓	✓	✓

SQL Express solo es adecuado para los entornos de no producción, p. ej., para ejercicios de prueba de concepto.

Nota:

- SQL Express solo es adecuado para los entornos de no producción, p. ej., para ejercicios de prueba de concepto.
- El servidor SQL debe estar configurado para usar cifrado SSL. Si su organización aún no utiliza cifrado SSL (ha estado ejecutando su entorno sin certificados para servidor SQL o ha estado utilizando un certificado autofirmado), debe obtener un certificado de una autoridad de certificación de confianza e importarlo al servidor SQL para habilitarlo. Para obtener más información, consulte la documentación de Microsoft.

  Para conocer los pasos para importar certificados al servidor SQL, consulte Requisitos previos en la página 6.

  Los certificados de autoridades de certificación de confianza deben utilizarse para entornos de producción. Sin embargo, se podría utilizar un certificado autofirmado para entornos de prueba de concepto o desarrollo. Es importante que el nombre de dominio completo (FQDN) utilizado por el servidor SQL coincida con el FQDN definido en el certificado. **Si no coinciden, no se establecerá una conexión a la base de datos y su instalación no funcionará correctamente.** Para obtener información sobre el uso y la configuración de certificados autofirmados, consulte Certificados autofirmados.

También se admite lo siguiente:

- Servidor SQL en máquinas virtuales Azure.
- Instancia administrada SQL de Azure; sin embargo, las bases de datos deben crearse antes de la instalación.

La base de datos SQL de Azure no es compatible actualmente.

Servidor de agente de mensajería

Se requiere el siguiente software en el servidor de agente de mensajería:

- RabbitMQ 3.8.0 a 3.8.8 3.9.22 a 3.10.7
- Erlang/OTP : la versión de Erlang que necesita depende de la versión de RabbitMQ que desea utilizar.

  Para obtener el soporte apropiado de Erlang/OTP, consulte Requisitos de la versión Erlang de RabbitMQ.

  Para obtener el soporte técnico adecuado del sistema operativo, consulte el siguiente enlace: https://www.rabbitmq.com/platforms.html.

Consulte Instalar el servidor de agente de mensajería en la página 19 para obtener más información.

Servidor web

Se requiere el siguiente software en el servidor web:

- .NET Framework 4.7.2: se instala de forma predeterminada en Windows Server 2019.

  .NET Framework 4.8: se instala de forma predeterminada en Windows Server 2022.
- IIS 10.0
- .NET Core Windows Server Hosting 3.1.3

  ASP.NET Core Runtime 6.0.9 o 6.0.10 (paquete de alojamiento de Windows)

- .NET Core Windows Desktop Runtime 3.1.3

  .NET Desktop Runtime 6.0.9 o 6.0.10
- Visual C++ Redistributable 2012 (x64)

⚠ Hub 4.1 solo admite las versiones de ASP.NET Core Runtime y .NET Desktop Runtime que se muestran anteriormente. Si usa una versión posterior, como 7.x.x, puede tener dificultades.

Consulte Instalar y configurar el servidor web en la página 24 para obtener más información.

Permisos mínimos de SQL

Los permisos mínimos de SQL requeridos para que el usuario se conecte a la base de datos durante el proceso de instalación deben tener los privilegios adecuados para crear o configurar las bases de datos desde el producto; por lo tanto, se deberá utilizar una cuenta de administrador adecuada al ejecutar el proceso de instalación:

- Crear base de datos: dbcreator (rol de servidor) o sysadmin (rol de servidor)
- Configurar base de datos: sysadmin (rol de servidor) o db_owner (rol de base de datos)

El usuario de la base de datos requerido para conectarse a las bases de datos durante el funcionamiento normal debe tener los permisos mínimos de SQL para acceder a las bases de datos y a IMS Hub. Los permisos requeridos son los siguientes:

- db_datareader
- db_datawriter

Para obtener más información, consulte Información de aplicación predeterminada abajo.

Información de aplicación predeterminada

La siguiente información muestra las aplicaciones creadas por la instalación utilizando los valores predeterminados. Todas las aplicaciones deben tener acceso completo al certificado BluePrismCloud_Data_Protection ubicado en el almacén de certificados del equipo local. Internet Information Services APPPOOL\Blue Prism – IMS e Internet Information Services APPPOOL\Blue Prism – SignalR también requerirán acceso al certificado BluePrismCloud_IMS_JWT.

Sitios web de Hub

Nombre de aplicación	Nombre de cuenta de servicio de ejemplo para autenticación de SQL Windows	Permisos de Servidor SQL requeridos durante la instalación	Permisos de base de datos requeridos durante la ejecución de la aplicación	Nombre predeterminado de la base de datos
Blue Prism - IMS	Internet Information Services APPPOOL\Blue Prism: IMS	dbcreator/sysadmin	db_datawriter/ db_datareader	ImsDB
Blue Prism - Hub	Internet Information Services APPPOOL\Blue Prism – Hub	dbcreator/sysadmin	Para el primer inicio de sesión y la configuración inicial: dbcreator/sysadmin Inicios de sesión posteriores: db_datawriter/ db_datareader	HubDB
Blue Prism - Email	Internet Information Services APPPOOL\Blue	N/C	N/C	N/C

Nombre de aplicación	Nombre de cuenta de servicio de ejemplo para autenticación de SQL Windows	Permisos de Servidor SQL requeridos durante la instalación	Permisos de base de datos requeridos durante la ejecución de la aplicación	Nombre predeterminado de la base de datos
	Prism – Email			
Blue Prism - Audit Service	Internet Information Services APPPOOL\Blue Prism – Audit Service	dbcreator/sysadmin	db_datawriter/ db_datareader	AuditDB
Blue Prism - File Service	Internet Information Services APPPOOL\Blue Prism – File Service	dbcreator/sysadmin	db_datawriter/ db_datareader	CacheDB

Servicios de Hub

Nombre de aplicación	Nombre de cuenta de servicio de ejemplo para autenticación de SQL Windows	Permisos de Servidor SQL requeridos durante la instalación	Permisos de base de datos requeridos durante la ejecución de la aplicación	Nombre predeterminado de la base de datos
Blue Prism -: oyente del servicio de auditoría	NT AUTHORITY\ SISTEMA	dbcreator/sysadmin	db_datawriter/ db_datareader	AuditDB
Blue Prism -: servicio de registro	NT AUTHORITY\ SISTEMA	N/C	N/C	N/C

Consideraciones de la implementación en varios dispositivos

Cuando se realiza una implementación en varios dispositivos, se deben tener en cuenta los siguientes puntos antes de iniciar la instalación.

Área	Inquietudes del entorno (desarrollo/prueba/preproducción/producción)
Conectividad general	La conectividad entre los diversos dispositivos debe estar configurada adecuadamente. En general, esto requiere que se configure el DNS para permitir que los dispositivos se resuelvan unos a otros en función de su FQDN. Además, las reglas adecuadas de firewall deben estar en vigencia para permitir que los dispositivos se comuniquen en los puertos requeridos.
Servidor de agente de mensajería	Este es un dispositivo único enfocado en proporcionar servicios de gestión de mensajes entre los componentes de Blue Prism. Se recomienda un dispositivo por entorno.
Servidor web	Un solo dispositivo que puede alojar múltiples componentes de Blue Prism. No se recomienda que los entornos se compartan en este dispositivo y que se utilice un dispositivo separado por entorno.
Instancia del servidor de base de datos	Evalúe si la forma en que los recursos están asignados a instancias del Servidor SQL hace que sea adecuado usar una sola instancia compartida para implementaciones de Blue Prism según su importancia y urgencia. (Por ejemplo, los entornos de producción probablemente sean los más críticos para el negocio).
Certificados de trabajador digital	Decida si existe un requisito adicional de aplicar seguridad basada en certificados a las comunicaciones de instrucción que envían los clientes interactivos y los servidores de aplicaciones a trabajador digital; y a las comunicaciones entrantes que reciben los trabajadores digitales si hospedan servicios web. Si se requiere un certificado, este se debe generar manualmente e instalarse en cada trabajador digital aplicable. El nombre común en el certificado se debe alinear con la dirección que se configurará para que utilicen los componentes de Blue Prism cuando se comuniquen con los dispositivos (p. ej., FQDN o nombre corto de equipo). Además, todos los dispositivos que se conectarán a los trabajadores digitales deben confiar en la autoridad de certificación que emitió los certificados generados manualmente.

Puertos de red

Para garantizar la conectividad de red entre dispositivos dentro de la arquitectura, el Firewall de Windows en los servidores correspondientes deberá permitir los siguientes flujos de tráfico:

Servidor de bases de datos	Puerto 1433 para permitir la conectividad del servidor SQL desde el servidor web. Si la instancia del servidor SQL es una instancia con nombre, también requerirá lo siguiente: • El puerto TCP para la instancia con nombre (esto es dinámico de manera predeterminada desde el rango efímero) o el puerto definido si es estático para permitir la conectividad del servidor SQL desde el servidor web. • Puerto UDP 1434 para el servicio de navegador del servidor SQL para permitir la conectividad del servidor SQL desde el servidor web.
Servidor de agente de mensajería	Puerto 5672 para permitir la conectividad de mensajes de RabbitMQ. Puerto 15672 para permitir la conectividad de la consola de administración de RabbitMQ.
Servidor web	Puerto 443 para permitir la conectividad HTTPS.
Digital Workers	Puerto 443 para permitir la conectividad HTTPS.

Se recomienda consultar al experto en infraestructura de red de su organización al configurar los puertos. Puede haber otros puertos que deban configurarse para garantizar la conectividad en su organización.

Implementación típica de

Adecuada para uso en producción y no en producción, una implementación típica contiene todos los componentes de Blue Prism Hub implementados en equipos separados.

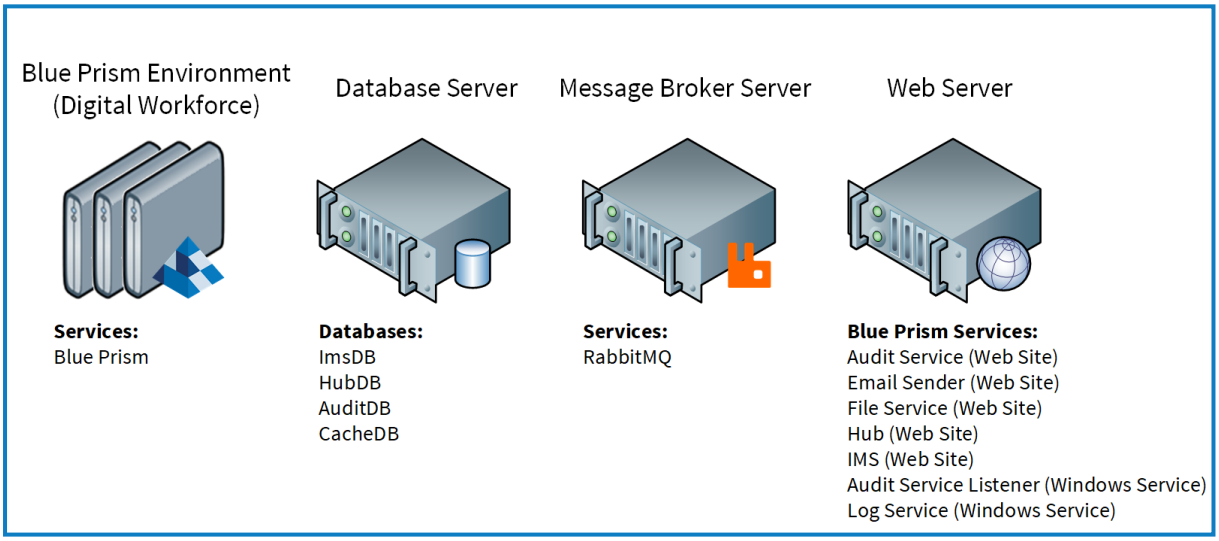
> Antes de seguir esta orientación, asegúrese de haber considerado por completo la información en Preparación en la página 5.

Para entornos de producción, se requiere un mínimo de cuatro recursos:

- Entorno de Blue Prism (fuerza laboral digital)
- Servidor de la base de datos (servidor SQL)
- Servidor de agente de mensajería
- Servidor web

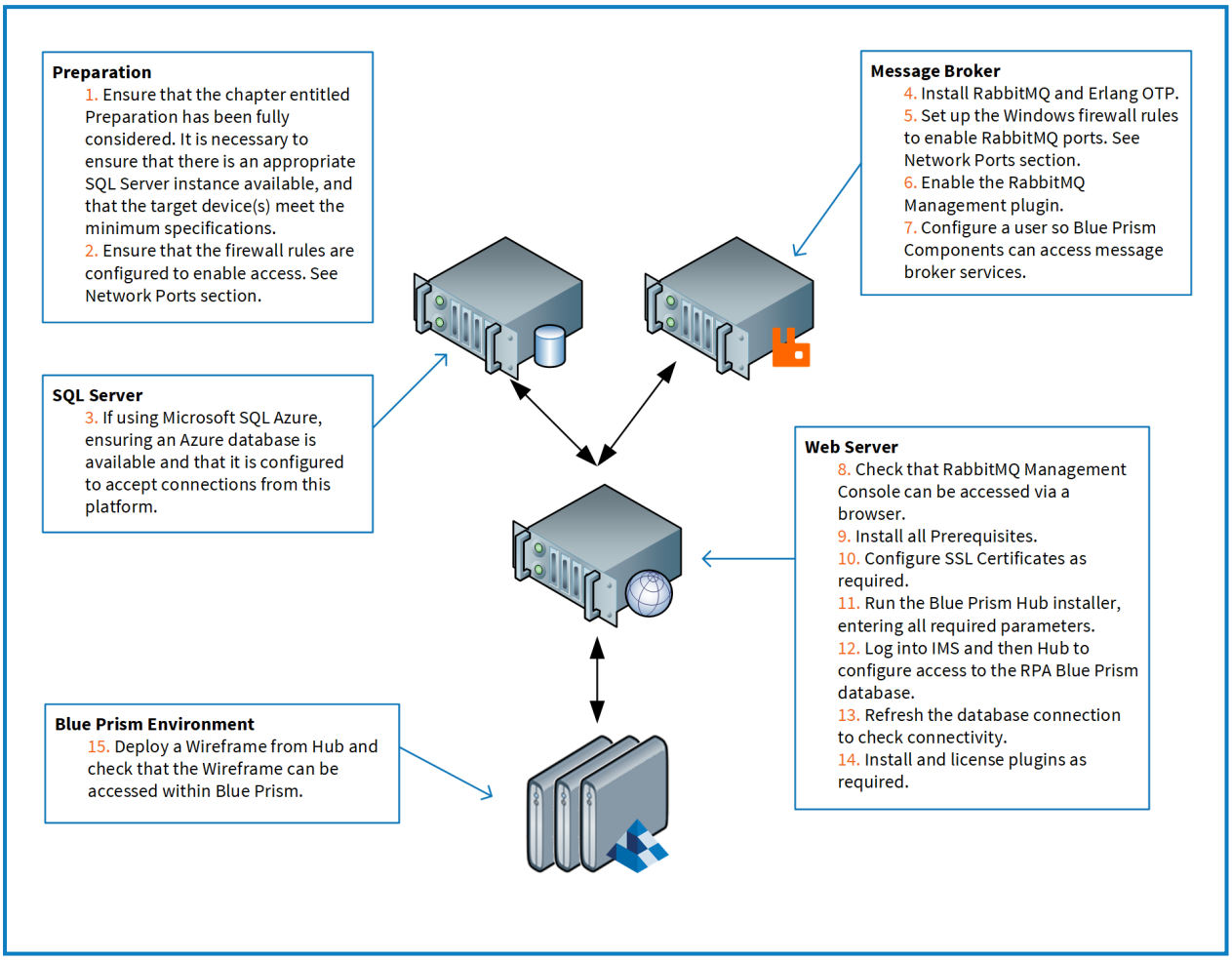
Las instancias de servidor de agente de mensajería y servidor SQL deben estar preconfiguradas antes de la instalación de Blue Prism Hub.

El siguiente diagrama ilustra la arquitectura típica de un entorno.



Descripción general de los pasos comunes de instalación

A continuación se ofrece una descripción general de los pasos necesarios para completar una implementación típica.



Si tiene problemas durante la instalación, consulte Solucionar problemas en una instalación de Hub en la página 52.

Instalar el servidor de agente de mensajería

Instale y configure el servidor de agente de mensajería, incluida la configuración del Firewall de Windows para habilitar la conectividad de red y la consola de administración de RabbitMQ.

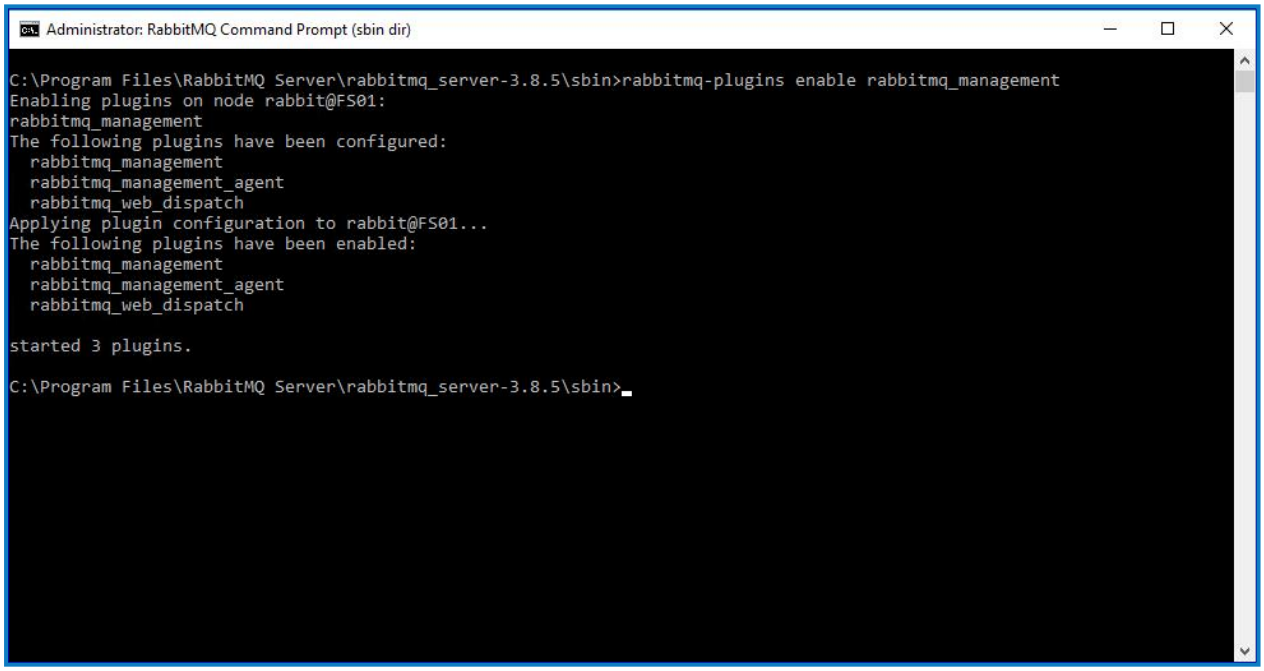
Si el agente de mensajería aún no está instalado y configurado, siga los pasos siguientes:

1. Instalar Erlang/OTP.
2. Descargue e instale RabbitMQ y acepte la configuración predeterminada.

   Para obtener más información, consulte Descarga e instalación de RabbitMQ.

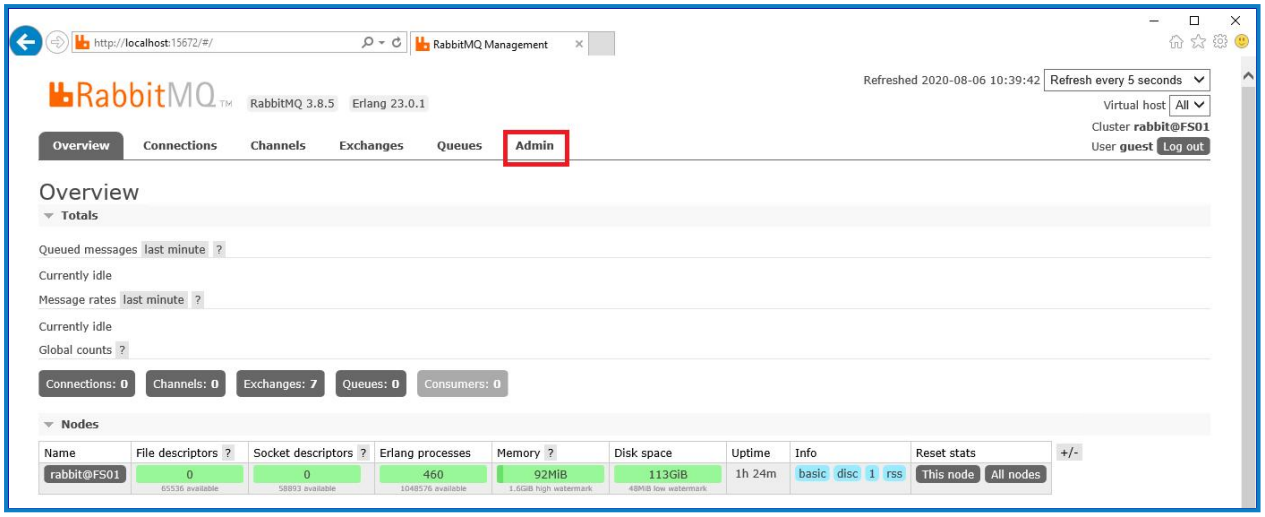
3. Configure el Firewall de Windows para habilitar el tráfico entrante a los puertos 5672 y 15672.
4. En el menú Inicio, en la carpeta Servidor de RabbitMQ, seleccione el símbolo del sistema RabbitMQ (sbin dir).
5. En la ventana del símbolo del sistema de RabbitMQ, escriba el siguiente comando:

```
rabbitmq-plugins enable rabbitmq_management
```

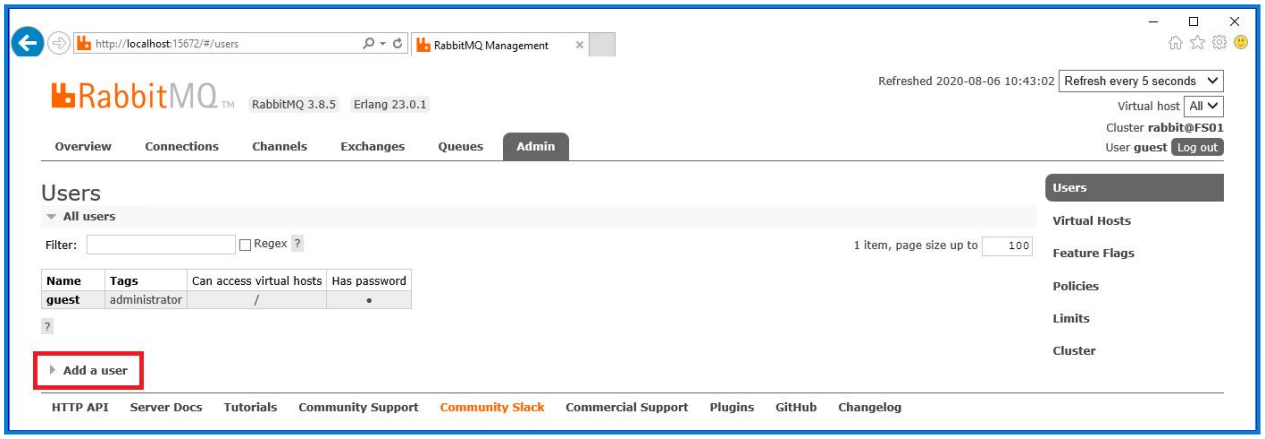


6. Inicie un navegador y navegue a la siguiente URL: http://localhost:15672
7. En la consola de RabbitMQ, inicie sesión con las credenciales predeterminadas de invitado/invitado.

8. En la consola, haga clic en **Admin**.



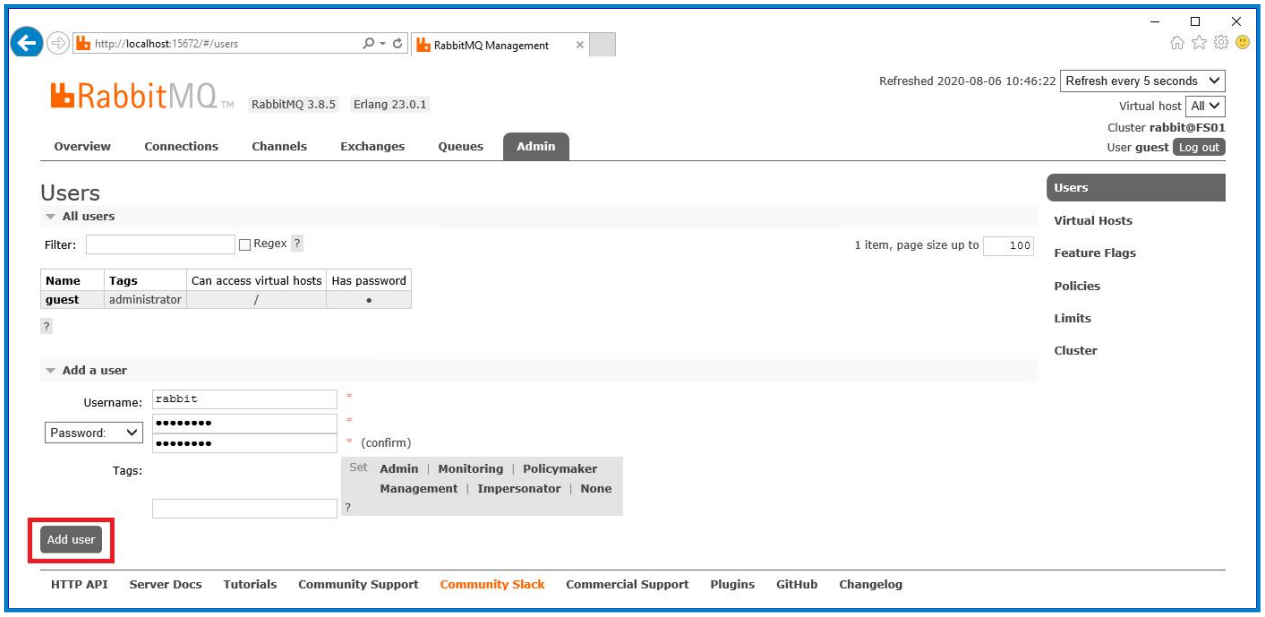
9. Haga clic en **Agregar un usuario**.



10. Ingrese los detalles de un nuevo usuario, proporcionando el nombre de usuario y la contraseña. El usuario no requiere ningún permiso especial y puede dejarse en Ninguno.

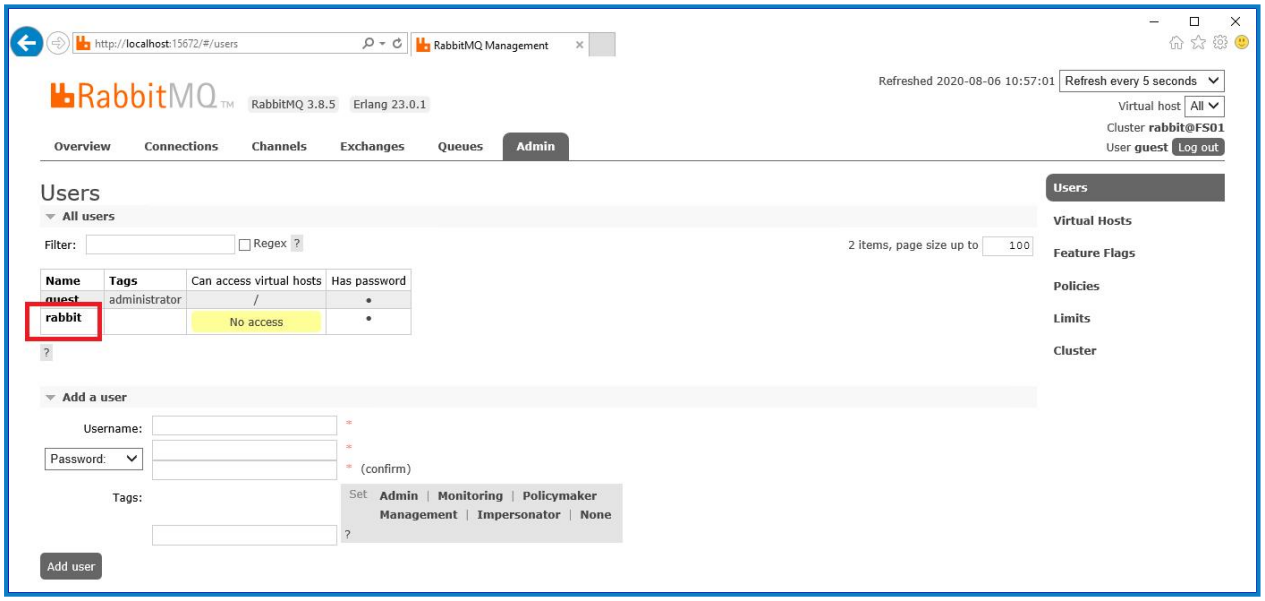
> Los siguientes caracteres no se deben utilizar para la contraseña al crear el usuario de RabbitMQ **# / : ? @ \ ` " $ '**.

11. Haga clic en **Agregar usuario**.

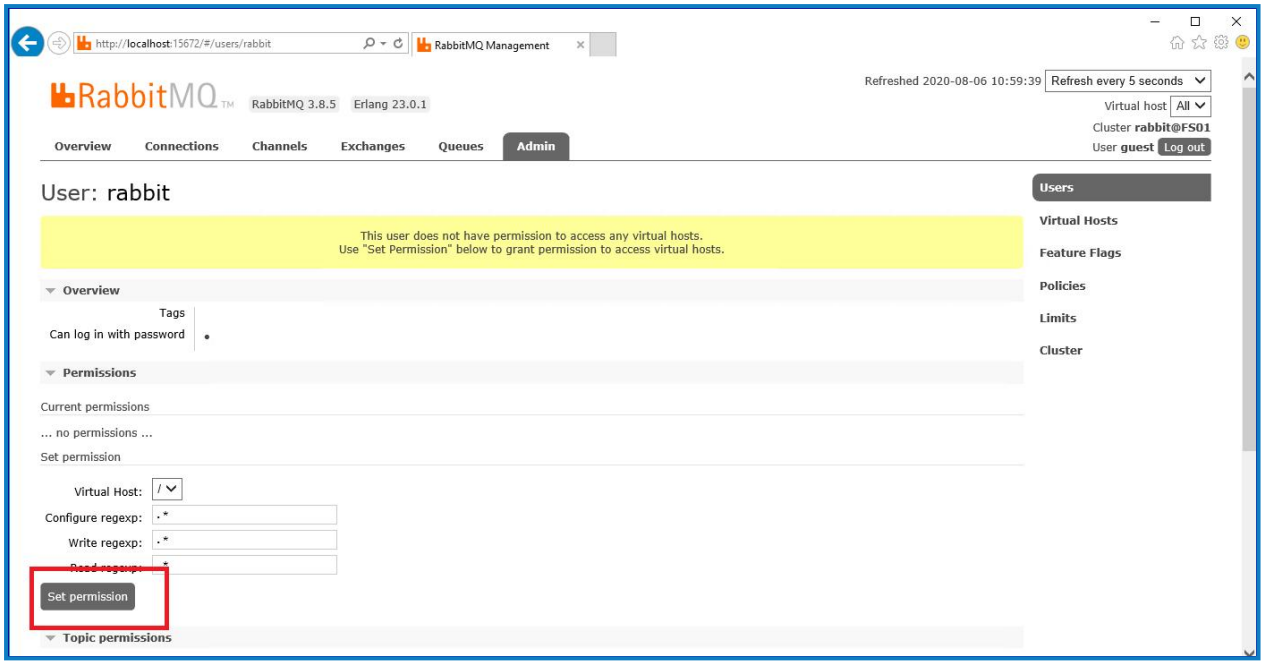


El siguiente paso es establecer los permisos para el usuario.

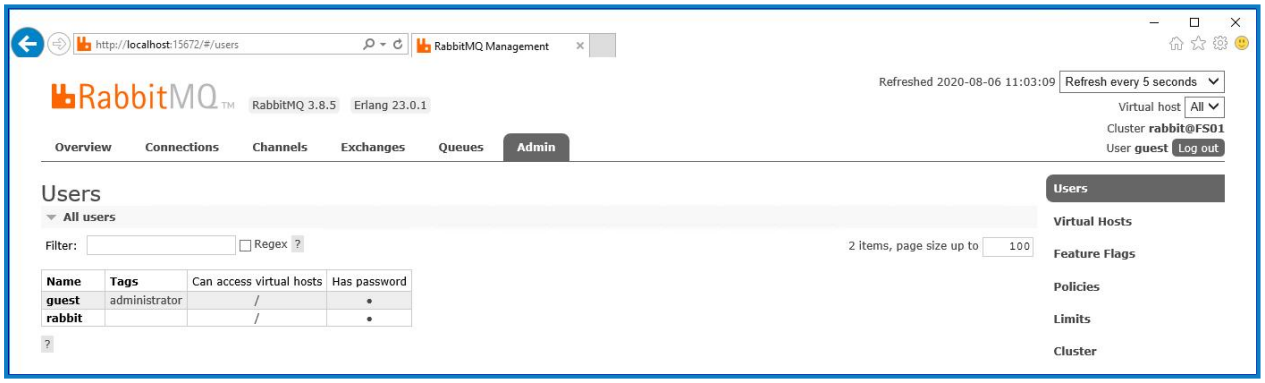
12. Haga clic en el nombre de usuario del usuario que acaba de crear.



13. Haga clic en **Establecer permiso** para asignar los permisos predeterminados.



14. Seleccione la pestaña **Admin** en la parte superior y compruebe que los permisos se hayan configurado correctamente como se muestra a continuación.



Esta cuenta no tiene acceso a la consola de administración, por lo que el uso de las credenciales que acaba de crear no habilitará ningún acceso.

Esta es una configuración genérica e instalación base de un servicio de agente de mensajería RabbitMQ. Se recomienda que se cambien las contraseñas predeterminadas y que su departamento de TI complete cualquier requisito de seguridad, como la aplicación de certificados SSL.

Se recomienda crear una nueva cuenta de administrador y eliminar la cuenta de invitado predeterminada. Dejar la cuenta de invitado predeterminada disponible puede presentar un riesgo de seguridad.

Verificar la conectividad del agente de mensajería RabbitMQ

Inicie un navegador y escriba la siguiente URL: http://<Message Broker Hostname>:15672

Debería aparecer la página de inicio de sesión de la consola de administración de RabbitMQ.

> No podrá iniciar sesión en la consola de administración ya que, de manera predeterminada, la cuenta de invitado está restringida únicamente al acceso local y la cuenta que creó no está autorizada para acceder a la consola de administración.

Si la consola no aparece, reinicie el servicio RabbitMQ. Si aún no apareció la consola, consulte Solucionar problemas en una instalación de Hub en la página 52.

Instalar y configurar el servidor web

Antes de instalar el servidor web de Hub, asegúrese de haber leído la información en Preparación en la página 5.

Instale y configure el servidor web asegurándose de que el sistema se pueda comunicar con el agente de mensajería RabbitMQlos requisitos previos y Blue Prism Hub.

El proceso consta de los siguientes pasos:

1. Instalar IIS
2. Configurar certificados SSL
3. Instalar los componentes de .NET Core
4. Instalar Blue Prism Hub
5. Instalar la extensión Authentication Server SAML 2.0: esto solo se requiere si tiene la intención de usar la autenticación SAML 2.0.

Instalar IIS

El sistema requiere que se instalen el servidor web IIS y los componentes .NET Core.

Es importante que IIS se instale antes de instalar los componentes de .NET Core y Blue Prism Hub. Las funciones y características de IIS se instalan automáticamente como parte de la instalación de Blue Prism Hub. Consulte la ayuda en línea para obtener una lista completa de características y roles.

Instalación por script

Ejecute el comando a continuación utilizando el símbolo del sistema PowerShell:

```
Install-WindowsFeature -name Web-Server -computerName localhost
```

Configurar certificados SSL

Durante el proceso de instalación, se le solicitarán los certificados SSL para los sitios web que se están configurando. Según los requisitos de seguridad de su infraestructura y de la organización de TI, este podría ser un certificado SSL creado internamente o un certificado adquirido para proteger los sitios web.

Al generar un certificado, ingrese el nombre del host en letras minúsculas. Si no utiliza todas las letras en minúscula, puede experimentar una discrepancia de nomenclatura entre el nombre del certificado y el nombre del host cuando utiliza el instalador de Hub. Esto podría provocar que el certificado no se aplique y que el instalador le impida avanzar con la instalación.

El instalador se puede ejecutar sin que el certificado esté presente, aunque para que los sitios funcionen, los enlaces en los sitios web de Internet Information Services deberán tener certificados SSL válidos.

La siguiente tabla detalla los certificados SSL requeridos.

Sitio web en IIS	URL predeterminada (solo a modo de ejemplo)
Sitios web con una interfaz de usuario para que la utilicen usuarios finales	
Blue Prism: Gestión de la información de mercado (Market Information Management, IMS)	https://ims.local
Blue Prism: Hub	https://hub.local
Sitios web para uso exclusivo de la aplicación (servicios)	
Blue Prism: Email Sender	https://email.local
Blue Prism: Audit Service	https://audit.local
Blue Prism: File Service	https://file.local

Certificados autofirmados

Los certificados autofirmados se pueden utilizar, pero solo se recomiendan para entornos de prueba de concepto (POC), prueba de valor (POV) y de desarrollo. Para entornos de producción, utilice certificados de la autoridad de certificación aprobada de su organización. Se recomienda que se comunique con su equipo de Seguridad de TI para verificar cuáles son sus requisitos.

Para generar y aplicar un certificado autofirmado para el servidor SQL:

> Microsoft proporciona un script que se puede utilizar para generar un certificado autofirmado para el servidor SQL. Para obtener más información, consulte la documentación de Microsoft. Es importante que el nombre de dominio completo (FQDN) utilizado por el servidor SQL coincida con el FQDN definido en el certificado. **Si no coinciden, no se establecerá una conexión a la base de datos y su instalación no funcionará correctamente.**

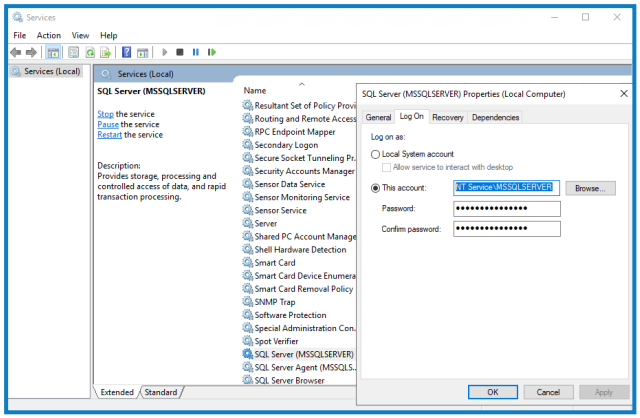
1. Ejecute PowerShell como administrador y ejecute el script de Microsoft con la información para su servidor SQL.

   Esto genera el certificado y lo instala en el servidor SQL.

2. En su servidor SQL:

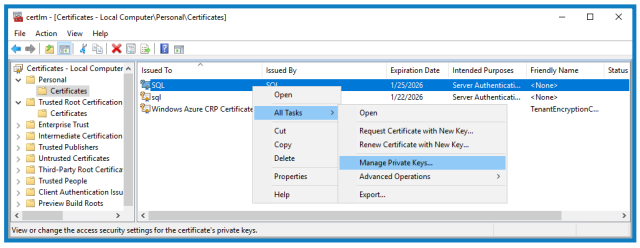
   a. Habilite el acceso a la clave privada del certificado para la cuenta de servicio del servidor SQL. Para hacerlo, siga estos pasos:

i. Si aún no lo sabe, busque el nombre de su cuenta de servicio para el servidor SQL. Esto se muestra en la pestaña Inicio de sesión de Propiedades del servidor SQL, a la que se puede acceder desde Servicios en su servidor SQL.

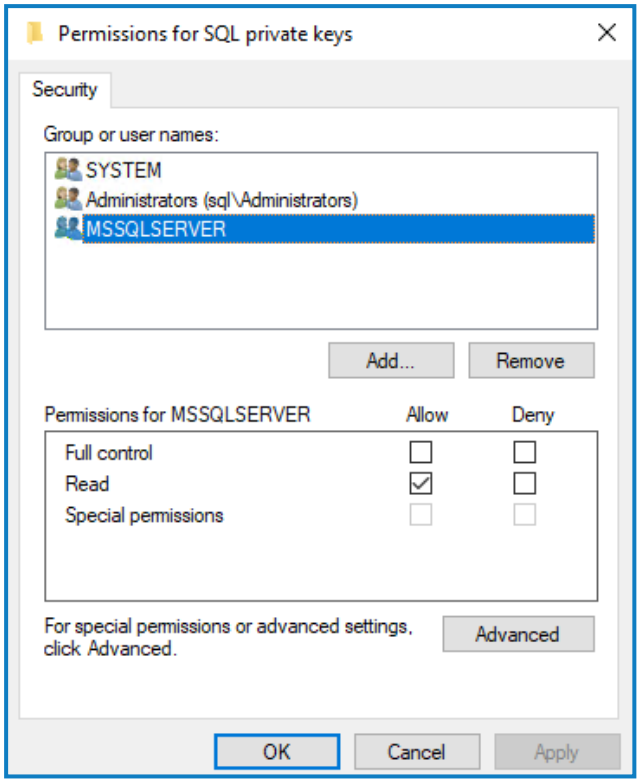


ii. En el servidor SQL, abra Administrador de certificados.

iii. Expanda **Personal**, luego expanda **Certificados**, haga clic con el botón derecho en **SQL**, luego seleccione **Todas las tareas** y, por último, haga clic en **Administrar claves privadas...**



iv. En el cuadro de diálogo Permisos para claves privadas de SQL, agregue su cuenta de servicio de servidor SQL con permisos de lectura. Por ejemplo:



v. Haga clic en **Aceptar** para aplicar los cambios y cerrar el cuadro de diálogo.

b. Habilite SSL en el servidor SQL y especifique el certificado. Para hacerlo, siga estos pasos:

i. En la barra de tareas de Windows, abra **Administrador de configuración del servidor SQL**.

ii. En el Administrador de configuración del servidor SQL, expanda **Configuración de red de servidor SQL**, haga clic con el botón derecho en **Protocolos para <SqlServerInstanceName>** y, a continuación, haga clic en **Propiedades**.

iii. En el cuadro de diálogo de propiedades de Protocolos para <SqlServerInstanceName>, seleccione la pestaña **Certificado** y luego seleccione o importe el certificado requerido.

iv. Haga clic en **Aplicar**.

v. Haga clic en **Aceptar** para cerrar el diálogo de Propiedades.

c. Reinicie el servicio del servidor SQL.

d. Copie el certificado C:\sqlservercert.cer. Deberá agregar esto a los servidores host del sitio web de Hub e Interact.

3. En los servidores host del sitio web:

a. Pegue sqlservercert.cer en los servidores host del sitio web para Hub e Interact.

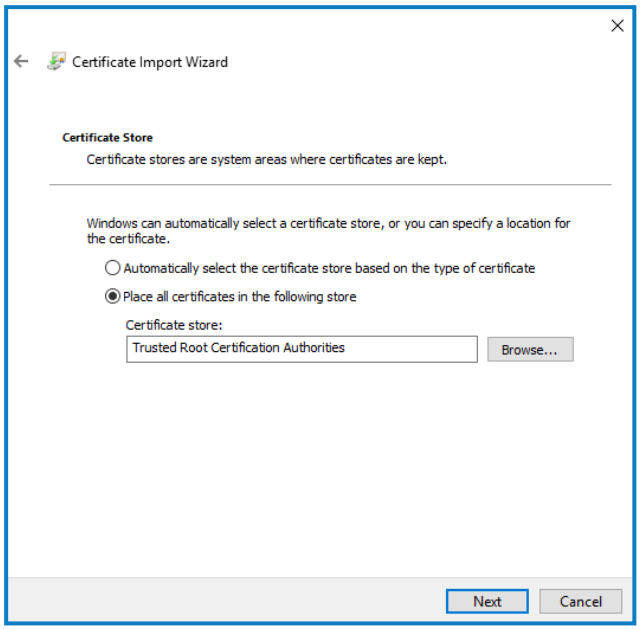
b. Agregue el certificado al almacén de certificados de Autoridades de certificado de confianza del servidor. Para hacerlo, siga estos pasos:

i. Haga doble clic en el certificado y, a continuación, haga clic en **Instalar certificado...**.

Aparece el Asistente de importación de certificados.

ii. En la página de bienvenida, seleccione **Máquina local** en **Ubicación del almacén** y haga clic en **Siguiente**.

iii. En la página Almacén de certificados, seleccione **Colocar todos los certificados en el siguiente almacén** e ingrese **Autoridades de certificado de confianza**.



iv. Haga clic en **Siguiente** y siga al asistente hasta su finalización.

c. Pruebe la conexión desde el servidor host del sitio web al servidor SQL.

Para generar un certificado autofirmado, siga estos pasos:

Para generar un certificado autofirmado para un sitio web:

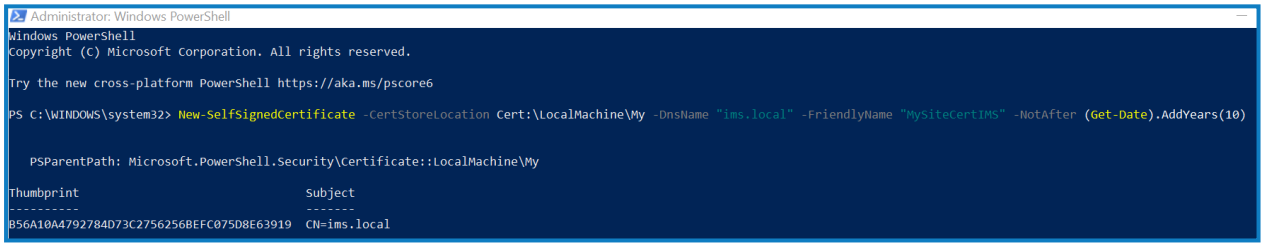
1. Ejecute PowerShell como administrador y utilice el siguiente comando, reemplazando `[Website]` y `[ExpiryYears]` por valores apropiados:

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

   Por ejemplo:

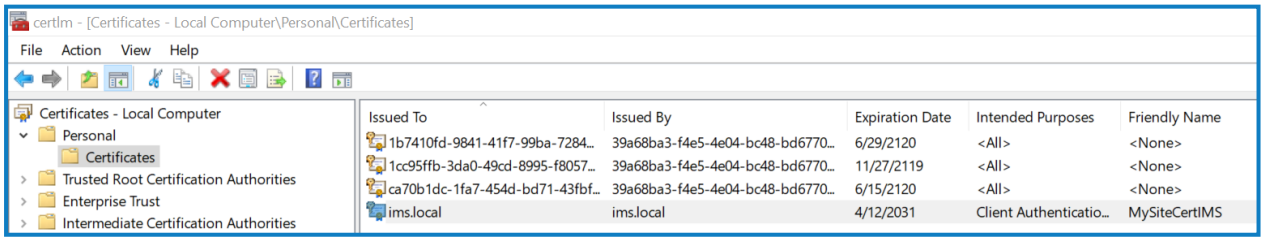
```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName "ims.local" -
FriendlyName "MySiteCertIMS" -NotAfter (Get-Date).AddYears(10)
```

   Este ejemplo crea un certificado autofirmado llamado *MySiteCertIMS* en el almacén de certificados personales, con *ims.local* como asunto y es válido durante 10 años desde el momento de la creación.



> Al generar un certificado, ingrese el nombre de host (`[Website]`) en letras minúsculas. Si no utiliza todas las letras en minúscula, puede experimentar una discrepancia de nomenclatura entre el nombre del certificado y el nombre del host cuando utiliza el instalador de Hub. Esto podría provocar que el certificado no se aplique y que el instalador le impida avanzar con la instalación.

2. Abra la aplicación Administrar certificados del equipo en su servidor web (escriba **administrar equipo** en la barra de búsqueda).
3. Copie y pegue el certificado de Personal > Certificados a Certificado de confianza > Certificados.



4. Repita este proceso para cada sitio web.

Creación de certificados autofirmados con script del sitio web

> Este proceso no se recomienda para entornos de producción.

Ejecute los siguientes comandos de PowerShell:

Para Hub:

```
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)
```

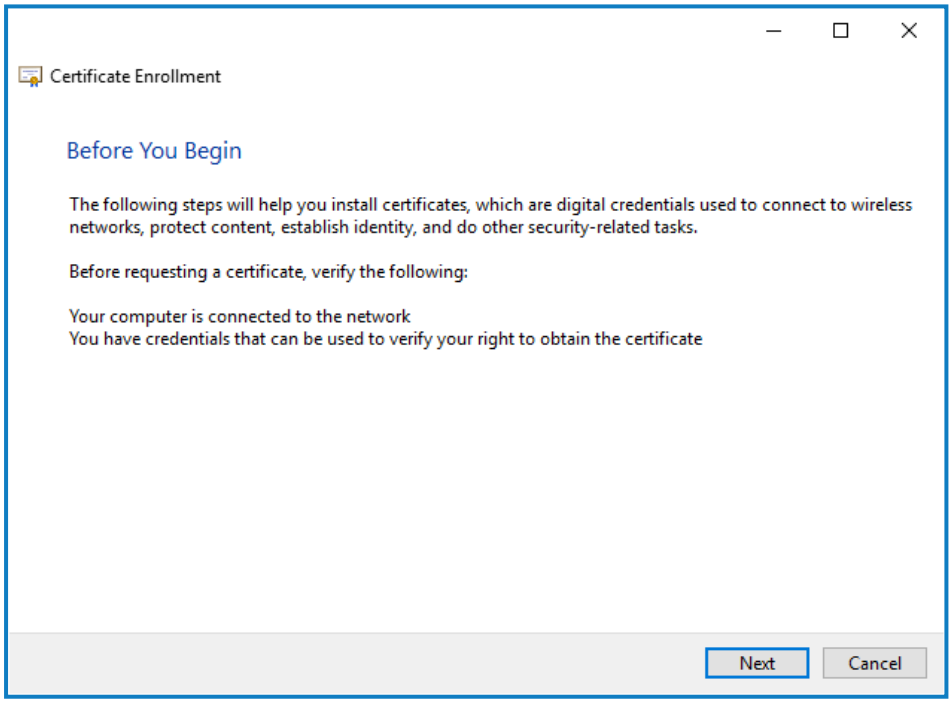
Una vez creados, abra el administrador de certificados del equipo local (certlm), y copie y pegue los certificados en el almacén de certificados de confianza.

Crear una solicitud de certificado sin conexión

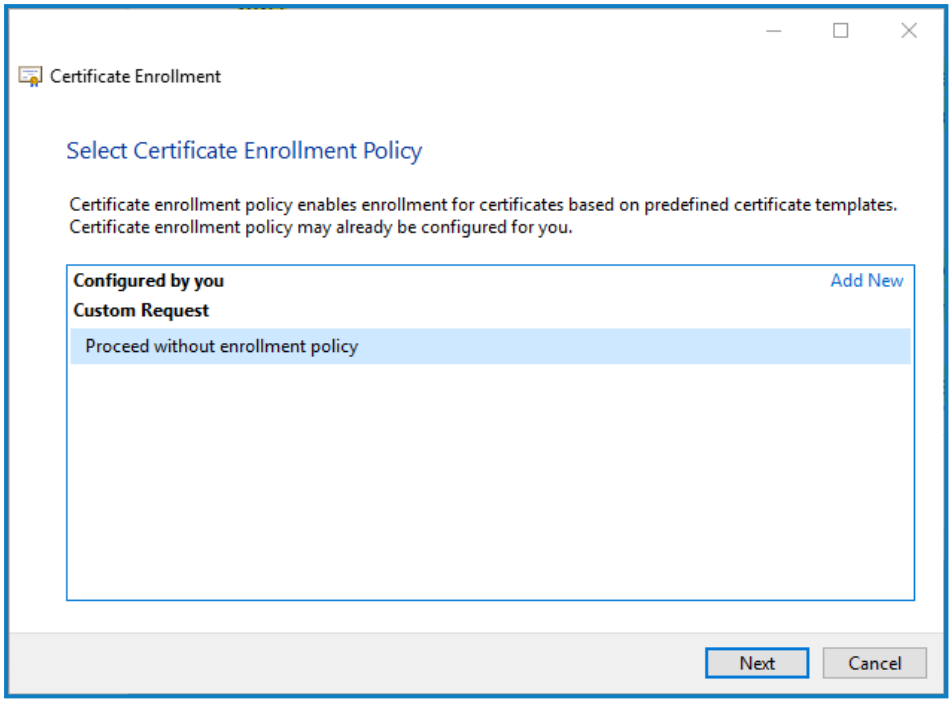
Para crear una solicitud de certificado sin conexión, siga este procedimiento para cada certificado:

1. Abra la aplicación Administrar certificados del equipo en su servidor web (escriba **administrar equipo** en la barra de búsqueda).
2. Haga clic derecho en **Personal** > **Certificados** y seleccione **Todas las tareas** > **Operaciones avanzadas** > **Crear solicitud personalizada** en el menú de acceso directo.

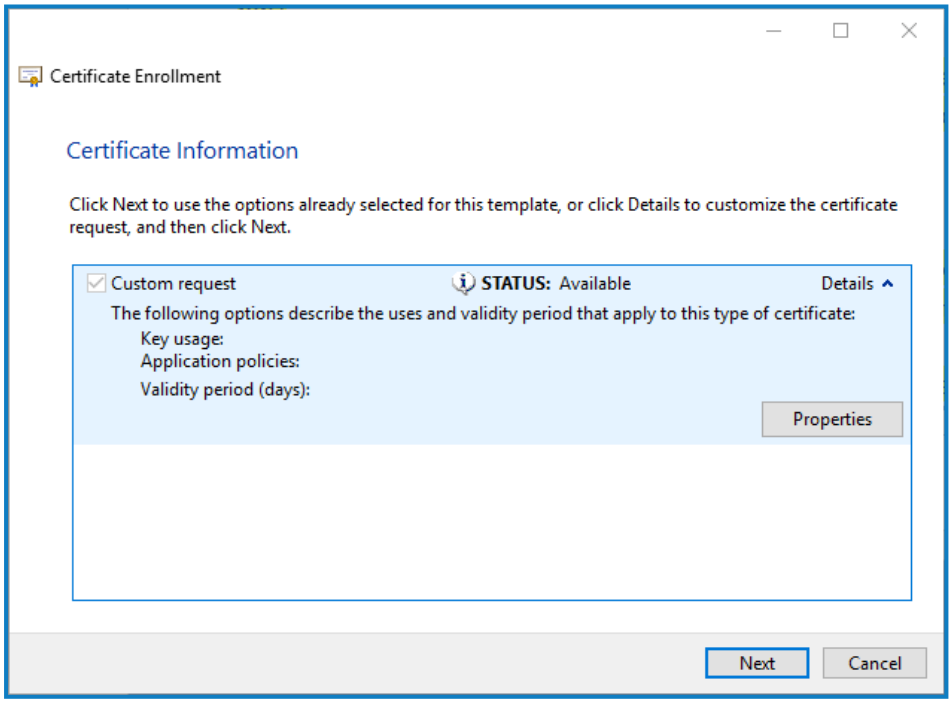
   Aparece el asistente de inscripción del certificado.



3. Haga clic en **Siguiente**.



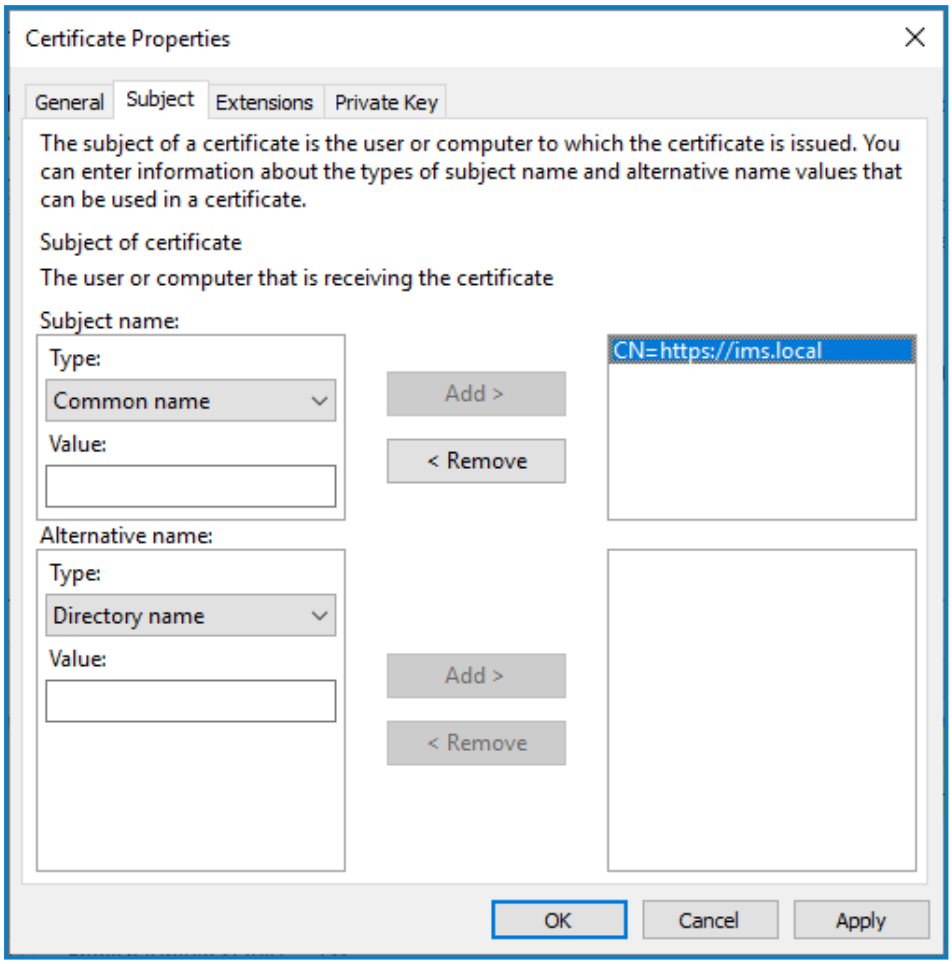
4. Seleccione **Continuar sin política de inscripción** y haga clic en **Siguiente**.
5. En la pantalla Solicitud personalizada, haga clic en **Siguiente**.
6. En la pantalla Información del certificado, haga clic en el menú desplegable **Detalles** y haga clic en **Propiedades**.



7. En la pestaña General del cuadro de diálogo Propiedades del certificado, ingrese un nombre descriptivo y una descripción según el sitio web al que se aplicará este certificado.

8. En la pestaña Asunto, cambie el tipo de nombre del asunto a **Nombre común**, ingrese la URL del sitio web en el campo **Valor** y haga clic en **Agregar**.

   El CN (nombre común) se mostrará en el panel derecho.



9. En la pestaña Extensiones, haga clic en **Uso de clave extendida**, seleccione **Autenticación del servidor** y haga clic en **Agregar**.
10. En la pestaña Clave privada, haga clic en **Opciones de clave**, seleccione el tamaño de clave que desee y seleccione **Hacer que la clave privada sea exportable**.
11. Aún en la pestaña Clave privada, haga clic en **Algoritmo hash** y seleccione un hash adecuado (opcional).
12. Haga clic en **Aceptar**.

    Volverá a la pantalla Inscripción de certificado.
13. Haga clic en **Siguiente**.
14. Agregue un nombre de archivo y una ruta, y haga clic en **Finalizar**.

Después de crear su solicitud de certificado, deberá enviarla a una autoridad de certificación para que puedan procesar su solicitud y emitir un certificado. La solicitud de certificado es un archivo de texto. Por lo general, debe copiar el texto del archivo e ingresarlo en un formulario de presentación en línea en el sitio web de la autoridad de Certificación. Deberá comunicarse directamente con su autoridad de certificación para obtener instrucciones sobre el proceso para enviar su solicitud de certificado.

Instalación de los componentes de .NET Core

Se deben descargar e instalar los siguientes componentes de .NET Core:

- .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

Instalación por script

Para instalar las dependencias .NET, ejecute los siguientes comandos utilizando el símbolo del sistema PowerShell, actualizando C:\temp a la ubicación adecuada según sea necesario:

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

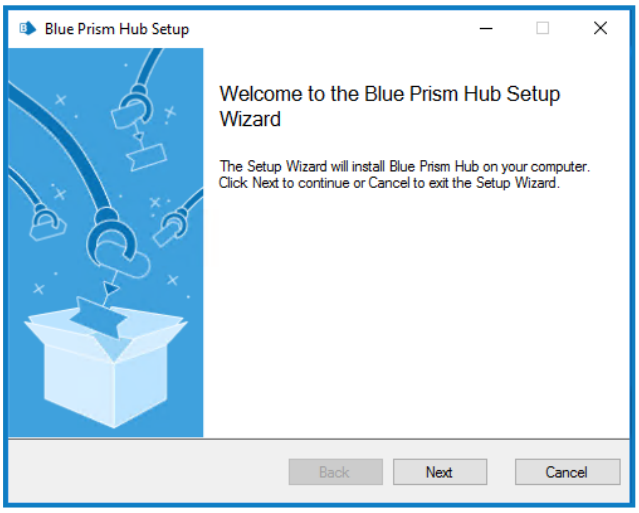
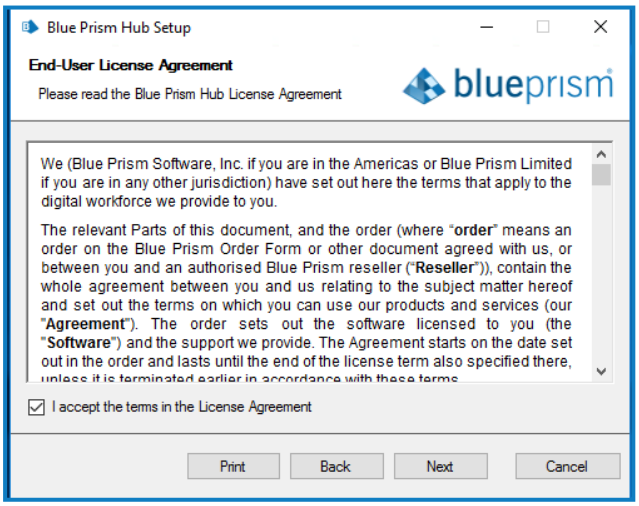
Instalar Blue Prism Hub

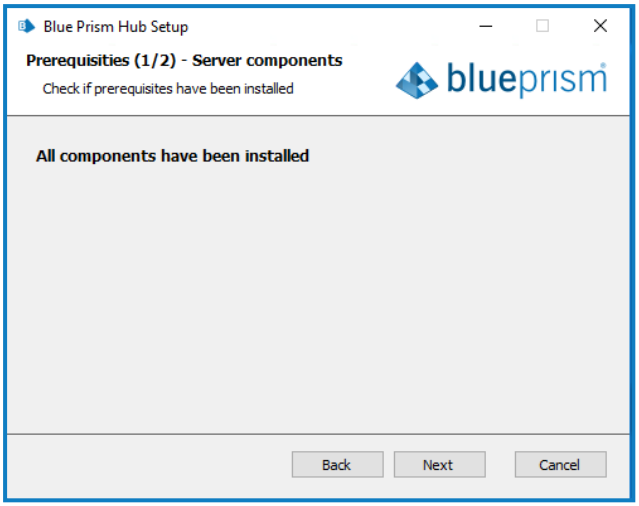
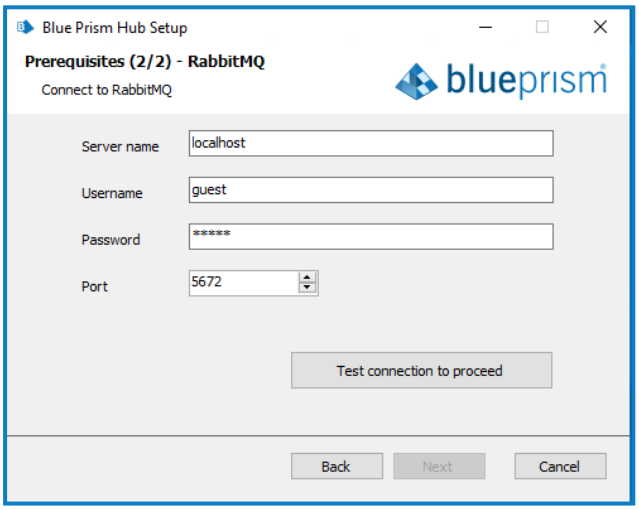
Antes de instalar Blue Prism Hub:

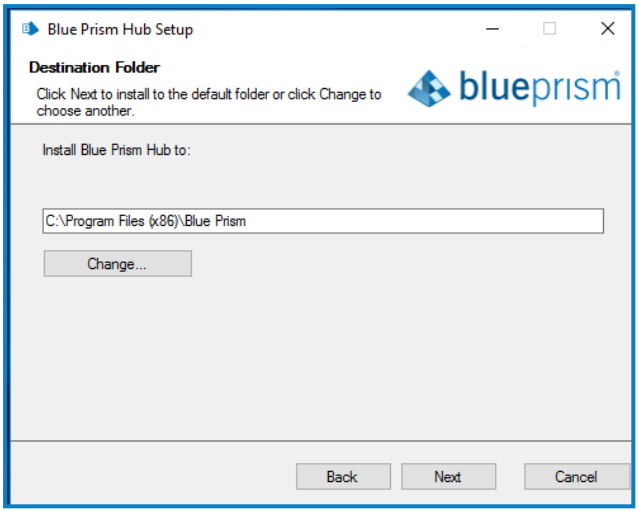
- Si vuelve a instalar Blue Prism Hub después de haberlo usado y eliminado previamente, y se deben usar los mismos nombres de base de datos, se recomienda que las bases de datos se eliminen de los datos antiguos antes de volver a instalarlas.

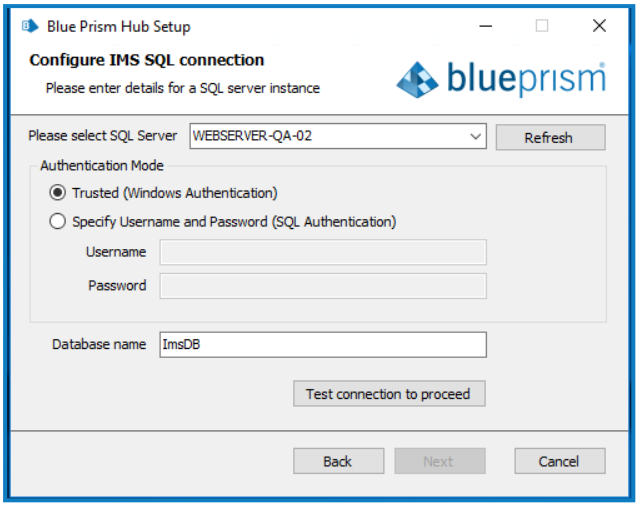
Los pasos a continuación detallan el proceso para instalar el software de Blue Prism Hub. Esto incluye el Authentication Server, Hub y otros servicios asociados. El proceso de instalación creará cualquier base de datos nueva que sea necesaria.

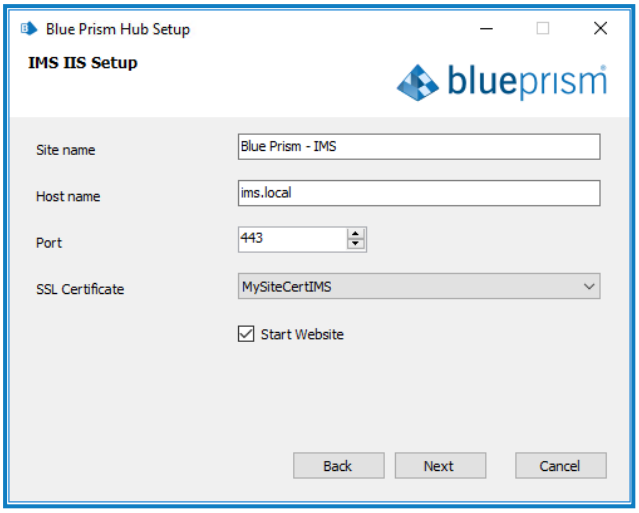
Descargue y ejecute el instalador de Blue Prism Hub, disponible en el portal de Blue Prism, y avance a través del instalador como se muestra a continuación. El instalador se debe ejecutar con derechos de administrador.

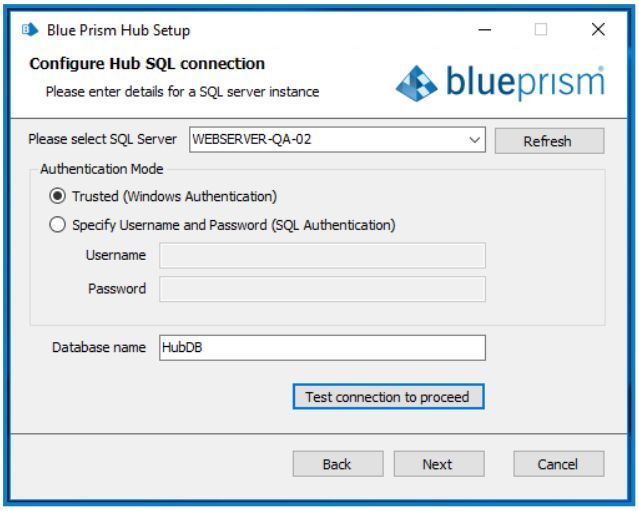
Paso	Página del instalador	Detalles
1		**Bienvenido**
2		**Contrato de licencia** Lea el EULA y, si acepta los términos, seleccione la casilla de verificación.

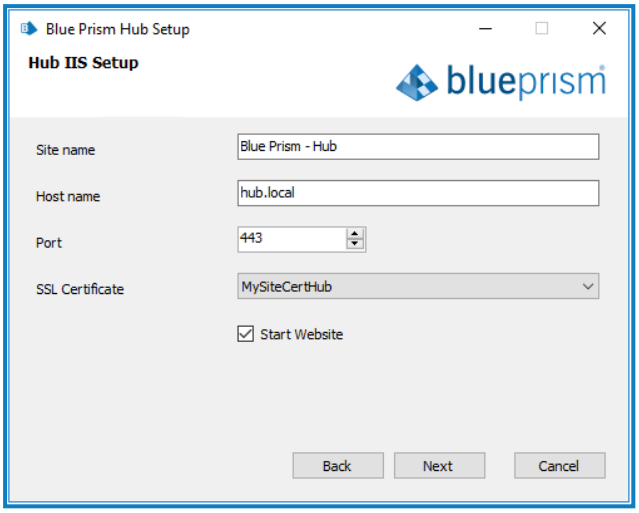
Paso	Página del instalador	Detalles
3		**Requisitos previos 1: Componentes del servidor** El instalador verifica que se hayan instalado los requisitos previos. Se identifican aquellos que no están instalados. No puede continuar hasta que todos los requisitos previos estén instalados. Si hay requisitos previos desinstalados, cancele el instalador e instale los componentes faltantes antes de reiniciar el instalador. De lo contrario, proceda con la instalación.
4		**Requisitos previos 2: RabbitMQ** Ingrese el nombre del servidor o la dirección IP del servidor de agente de mensajería y las credenciales del usuario que creó. El puerto de cola de mensajes predeterminado es 5672. Esto solo debe cambiarse si los puertos predeterminados han sido cambiados por su organización de soporte de TI. Haga clic en **Probar conexión** para verificar la conectividad. Una notificación mostrará el resultado de la prueba. Solo podrá pasar al siguiente paso si la prueba es exitosa. Si la prueba falló, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más detalles.

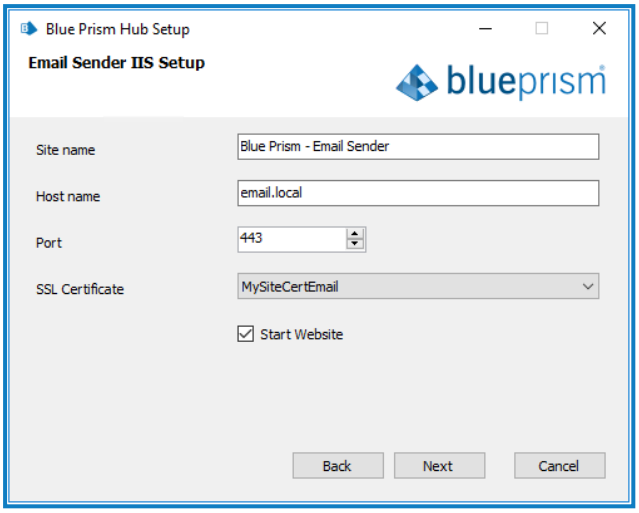
Paso	Página del instalador	Detalles
5		**Carpeta de destino** Especifique la carpeta de instalación requerida. La ubicación predeterminada es C:\Archivos de programa(x86)\Blue Prism, pero puede elegir otra con el botón **Cambiar**.

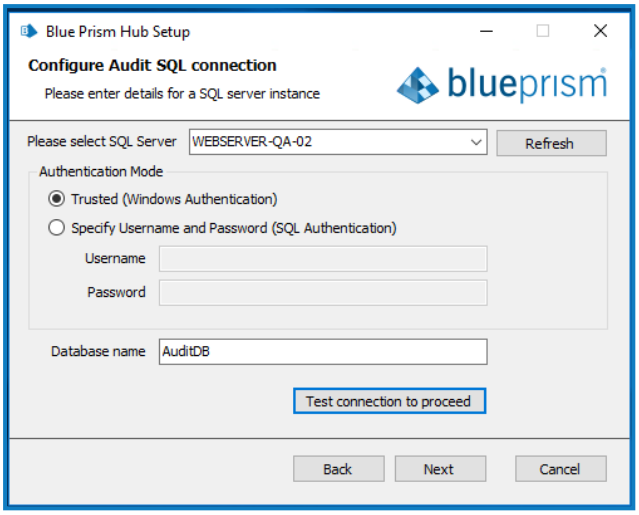
Paso	Página del instalador	Detalles
6		**Conexión SQL de IMS** Configurar los ajustes para la base de datos de IMSal proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Autenticación de Windows en la página 53 para obtener más información. • Si selecciona **Autenticación de SQL**, ingrese el nombre de usuario y la contraseña. Confirme que **Autenticación de SQL** está seleccionado e ingrese el nombre de usuario y la contraseña. ⚠ Debe asegurarse de que la contraseña de su base de datos no contenga un signo igual (=) o un punto y-coma (;). Estos caracteres no son compatibles y provocarán problemas al intentar conectarse a la base de datos. Haga clic en **Probar conexión para continuar** para probar las credenciales SQL y verificar la conectividad. Una notificación mostrará el resultado de la prueba. Solo podrá pasar al siguiente paso si la prueba es exitosa. Si la prueba falla, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más detalles.

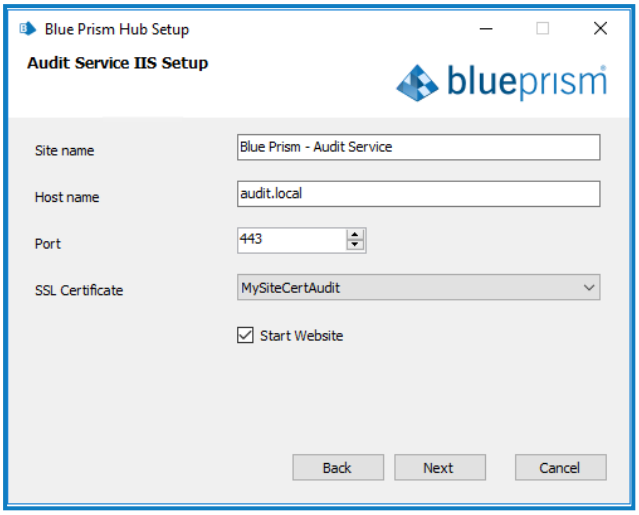
Paso	Página del instalador	Detalles
7		**Configuración de ISS de IMS** Configurar IIS para el sitio web de IMS. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host en minúscula. Esto se utilizará como la URL para el sitio. La primera parte del nombre de host predeterminado no se debe cambiar. Solo puede cambiar la parte *.local* del nombre del host. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. ⚠ No se admite el uso de mayúsculas en las URL. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Seleccione el certificado SSL **The One Cert**. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

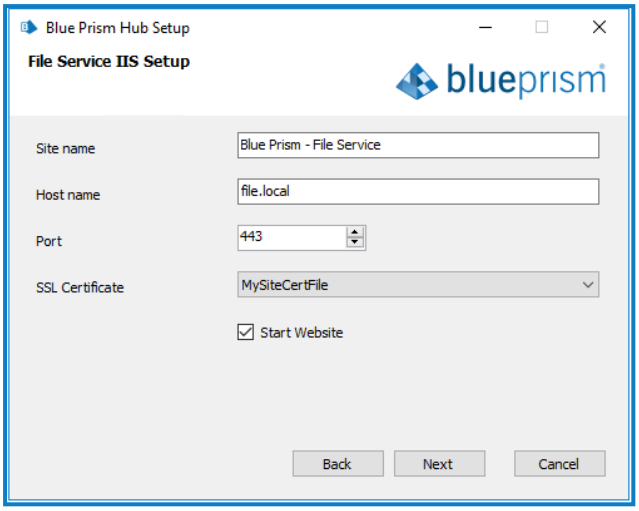
Paso	Página del instalador	Detalles
8		**Conexión SQL de Hub** Configurar los ajustes para la base de datos de Hubal proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Autenticación de Windows en la página 53 para obtener más información. • Si selecciona **Autenticación de SQL**, ingrese el nombre de usuario y la contraseña. Confirme que **Autenticación de SQL** está seleccionado e ingrese el nombre de usuario y la contraseña. ⚠ Debe asegurarse de que la contraseña de su base de datos no contenga un signo igual (=) o un punto y-coma (;). Estos caracteres no son compatibles y provocarán problemas al intentar conectarse a la base de datos. El nombre de la base de datos puede dejarse como valor predeterminado o cambiarse según sea necesario. Haga clic en **Probar conexión para continuar** para probar las credenciales SQL y verificar la conectividad. Una notificación mostrará el resultado de la prueba. Solo podrá pasar al siguiente paso si la prueba es exitosa. Si la prueba falla, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más detalles.

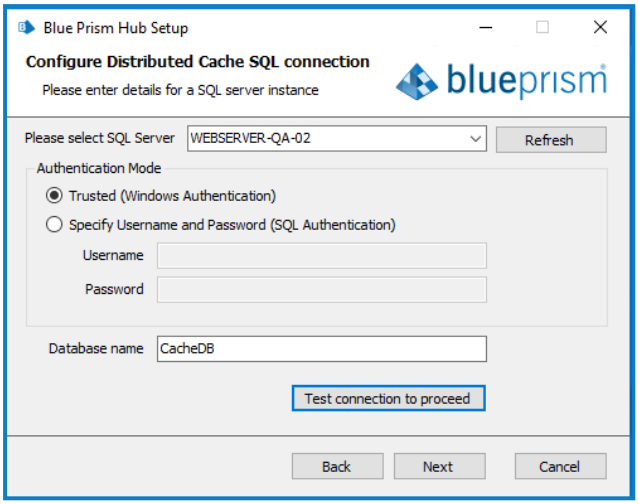
Paso	Página del instalador	Detalles
9		**Configuración de IIS de Hub** Configure el sitio web de Hub. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host en minúscula. Esto se utilizará como la URL para el sitio. La primera parte del nombre de host predeterminado no se debe cambiar. Solo puede cambiar la parte *.local* del nombre del host. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. ⚠ No se admite el uso de mayúsculas en las URL. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Seleccione el certificado SSL **The One Cert**. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

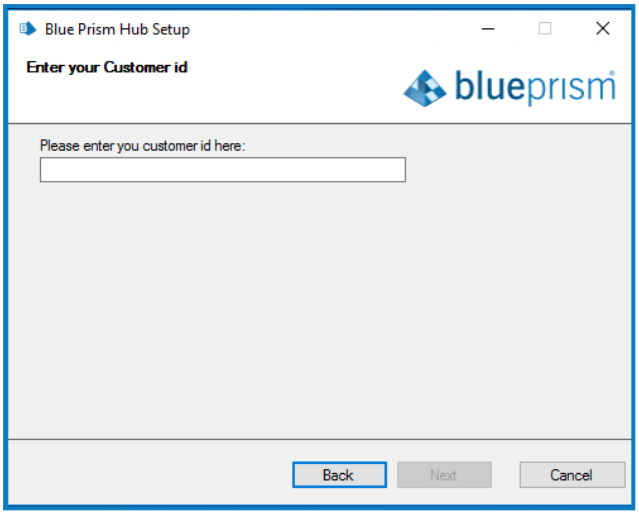
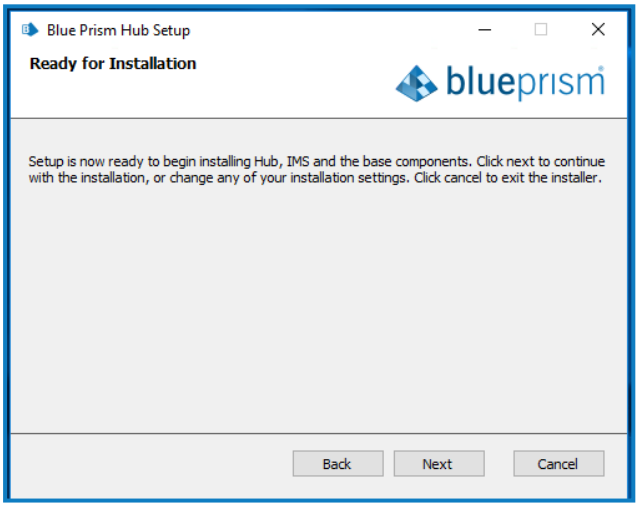
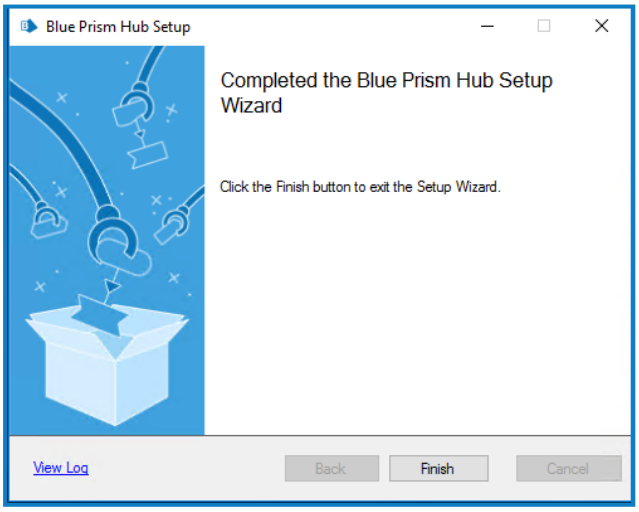
Paso	Página del instalador	Detalles
10		**Email Sender Configuración de IIS** Configurar el sitio web de Email Sender. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host en minúscula. Esto se utilizará como la URL para el sitio. La primera parte del nombre de host predeterminado no se debe cambiar. Solo puede cambiar la parte *.local* del nombre del host. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. ⚠ No se admite el uso de mayúsculas en las URL. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Seleccione el certificado SSL **The One Cert**. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

Paso	Página del instalador	Detalles
11		**Configuración de conexión SQL de Audit** Configurar los ajustes para la base de datos de Audit al proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Autenticación de Windows en la página 53 para obtener más información. • Si selecciona **Autenticación de SQL**, ingrese el nombre de usuario y la contraseña. Confirme que **Autenticación de SQL** está seleccionado e ingrese el nombre de usuario y la contraseña. ⚠ Debe asegurarse de que la contraseña de su base de datos no contenga un signo igual (=) o un punto y-coma (;). Estos caracteres no son compatibles y provocarán problemas al intentar conectarse a la base de datos. El nombre de la base de datos puede dejarse como valor predeterminado o cambiarse según sea necesario. Haga clic en **Probar conexión para continuar** para probar las credenciales SQL y verificar la conectividad. Una notificación mostrará el resultado de la prueba. Solo podrá pasar al siguiente paso si la prueba es exitosa. Si la prueba falla, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más detalles.

Paso	Página del instalador	Detalles
12		**Configuración de IIS de Audit Service** Configurar el sitio web de Audit Service. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host en minúscula. Esto se utilizará como la URL para el sitio. La primera parte del nombre de host predeterminado no se debe cambiar. Solo puede cambiar la parte *.local* del nombre del host. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. ⚠ No se admite el uso de mayúsculas en las URL. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Seleccione el certificado SSL **The One Cert**. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

Paso	Página del instalador	Detalles
13		**Configuración de IIS de File Service** Configure el sitio web de File Service. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host en minúscula. Esto se utilizará como la URL para el sitio. La primera parte del nombre de host predeterminado no se debe cambiar. Solo puede cambiar la parte *.local* del nombre del host. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. ⚠ No se admite el uso de mayúsculas en las URL. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Seleccione el certificado SSL **The One Cert**. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

Paso	Página del instalador	Detalles
14		**Conexión SQL de Distributed Cache** Configurar los ajustes para la base de datos de cacheal proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Autenticación de Windows en la página 53 para obtener más información. • Si selecciona **Autenticación de SQL**, ingrese el nombre de usuario y la contraseña. Confirme que **Autenticación de SQL** está seleccionado e ingrese el nombre de usuario y la contraseña. ⚠ Debe asegurarse de que la contraseña de su base de datos no contenga un signo igual (=) o un punto y-coma (;). Estos caracteres no son compatibles y provocarán problemas al intentar conectarse a la base de datos. El nombre de la base de datos puede dejarse como valor predeterminado o cambiarse según sea necesario. Haga clic en **Probar conexión para continuar** para probar las credenciales SQL y verificar la conectividad. Una notificación mostrará el resultado de la prueba. Solo podrá pasar al siguiente paso si la prueba es exitosa. Si la prueba falla, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más detalles.

Paso	Página del instalador	Detalles
15		**Ingrese su identificación de cliente** Ingrese su identificador de cliente. Blue Prism le proporciona este identificador cuando recibe su licencia de producto para ALM o Interact. Si no ha comprado un complemento con licencia, puede ingresar su propio valor.
16		**Listo para la instalación** Haga clic en **Siguiente** para instalar Hub.
17		**Instalación completa** Si la instalación falla, la opción **Ver registro** le dará detalles del error que se encontró. Para obtener más información, consulte Solucionar problemas en una instalación de Hub en la página 52.

Instalar la extensión Authentication Server SAML 2.0

Si su organización pretende utilizar la autenticación SAML 2.0 para sus usuarios, debe instalar la extensión Authentication Server SAML 2.0 en el servidor web donde están instalados Hub y Authentication Server. Para obtener más información, consulte la guía de instalación 4.7 de la extensión Authentication Server SAML 2.0 en Digital Exchange.

Si su organización no tiene la intención de utilizar la autenticación SAML 2.0 para sus usuarios, no necesita instalar nada más.

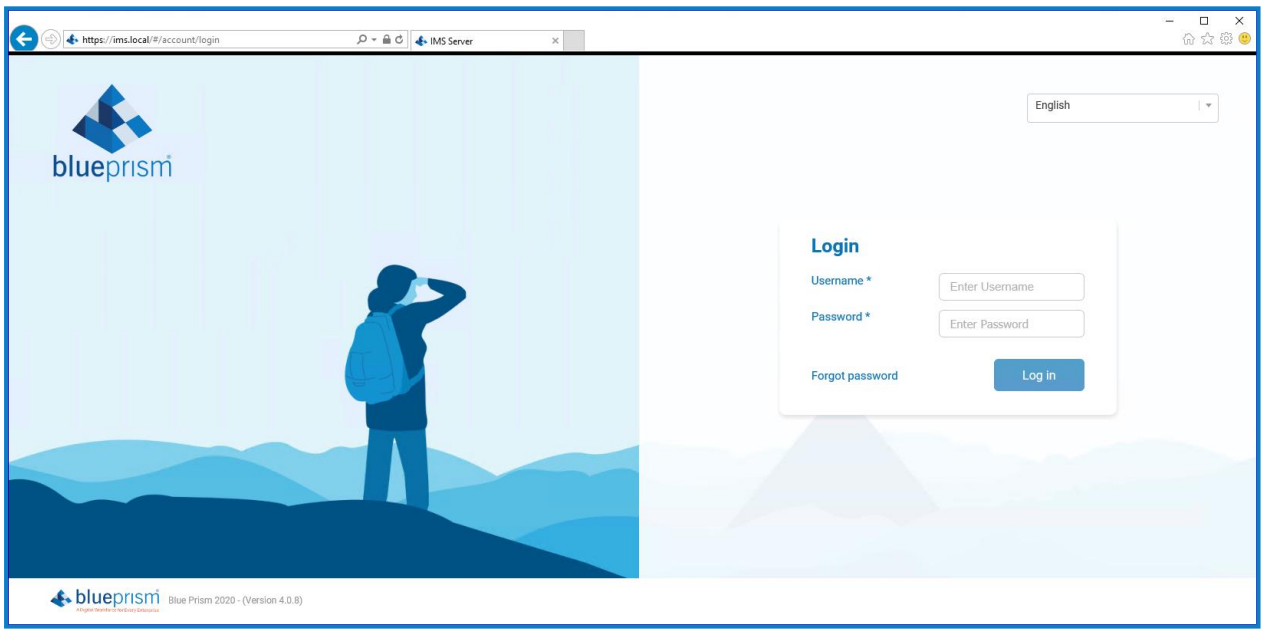
Configuración inicial de Hub

Ahora puede iniciar sesión por primera vez y establecer una configuración determinada para todo el sistema.

Cuando abre la página de inicio de sesión para IMS, la configuración de localización se aplica automáticamente desde su navegador web. La página de inicio de sesión y Hub se muestran en el idioma más compatible con los ajustes de idioma configurados en el navegador. Si el idioma seleccionado en la configuración de su navegador no es compatible, se utiliza el inglés como predeterminado. Si es necesario, puede cambiar manualmente el idioma que desea utilizar desde la lista desplegable en la página de inicio de sesión.

Para ver el proceso de instalación y configuración de Hub, consulte nuestro video de instalación de Blue Prism Hub.

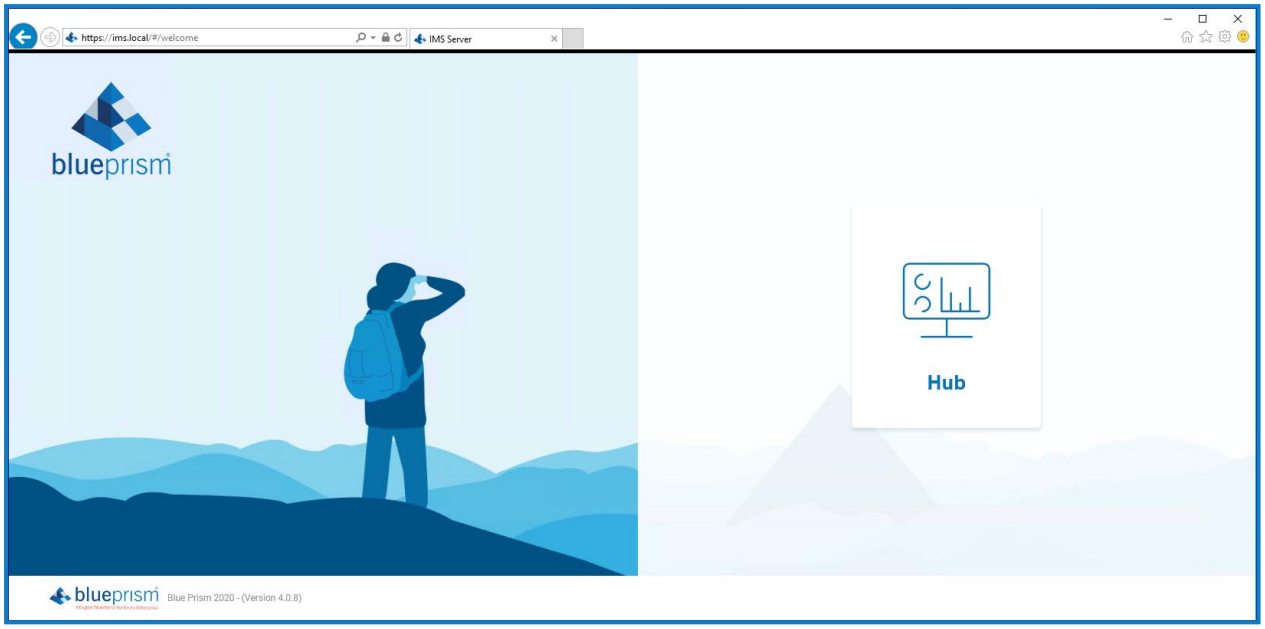
1. Inicie un navegador y vaya al sitio web de IMS , en nuestro ejemplo: https://ims.local



2. Inicie sesión con las credenciales predeterminadas.
   - **Nombre de usuario:** admin
   - **Contraseña**: Qq1234!!

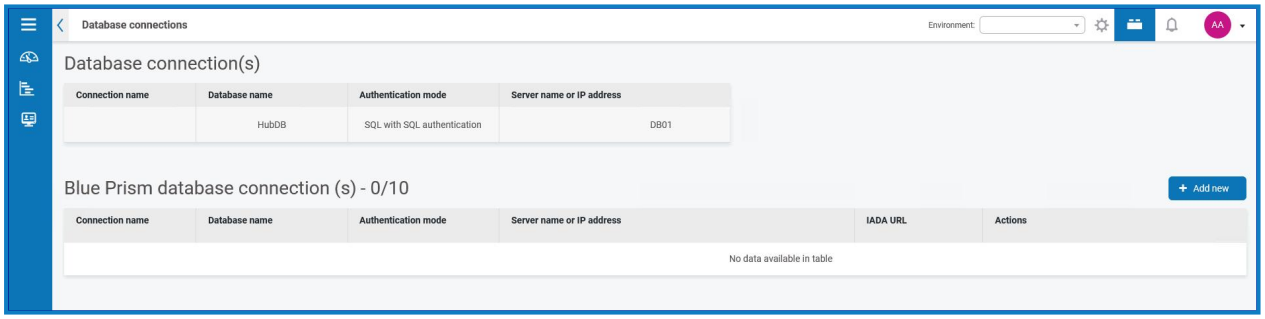
Para obtener información sobre cómo cambiar la contraseña predeterminada y otras configuraciones, consulte la Guía del usuario de Hub.

3. Haga clic en **Hub** para iniciar el sitio web de Hub.

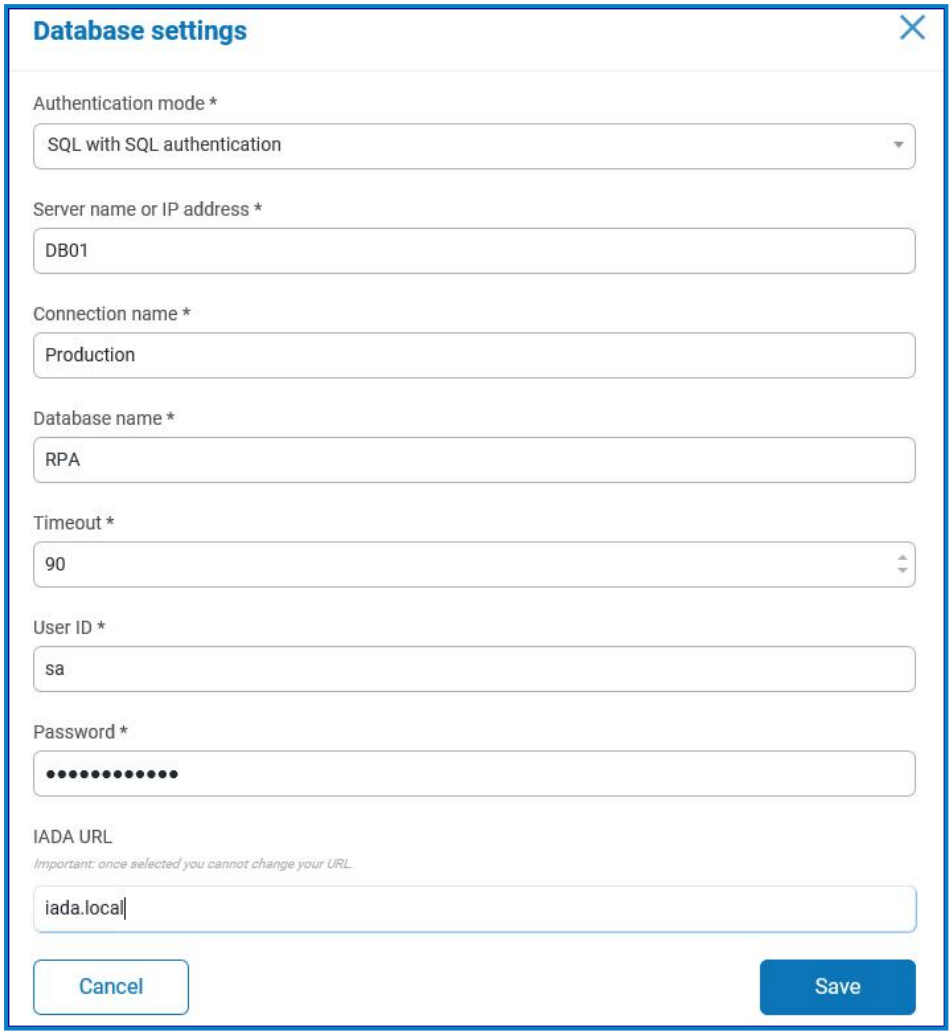


Configuración de base de datos

1. Haga clic en el engranaje de configuración y seleccione **Configuración de base de datos**.



2. Haga clic en **Agregar nuevo** e ingrese los detalles de la base de datos de Blue Prism RPA como se ilustra a continuación.



El valor de tiempo límite es en segundos.

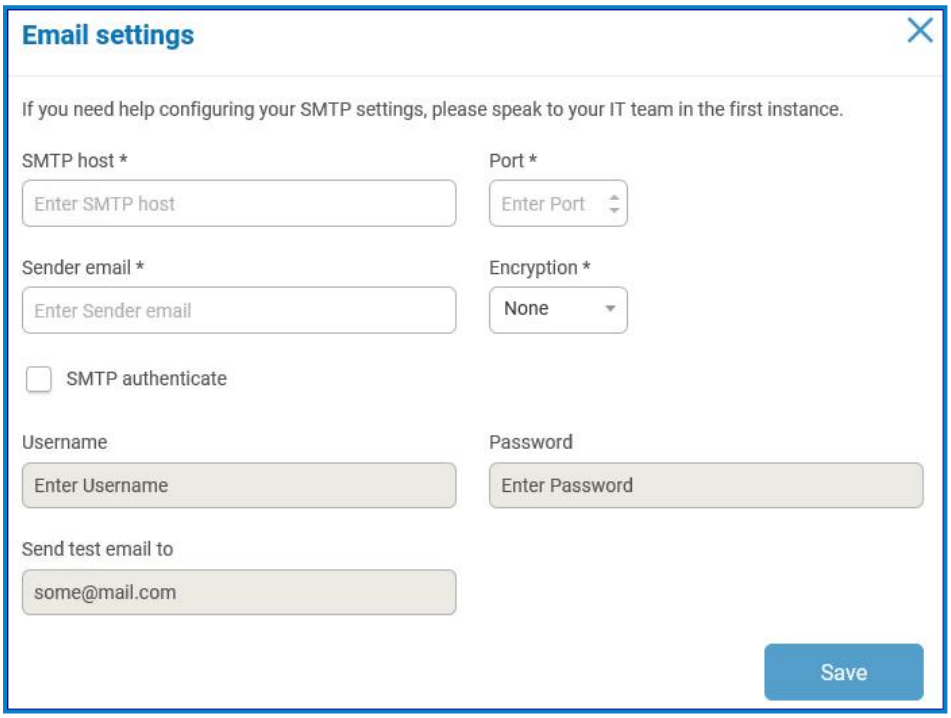
3. Haga clic en **Guardar** para guardar sus datos.
4. Para probar la configuración, vuelva a la configuración de la base de datos y haga clic en el menú de acciones (tres puntos) junto a la base de datos configurada y seleccione **Actualizar**. Si está en funcionamiento, se muestra el siguiente mensaje en la esquina superior derecha de la interfaz de usuario de Hub, que verifica la instalación. Si no se muestra el mensaje, consulte Solucionar problemas en una instalación de Hub en la página 52 para obtener más información.

Configuración de correo electrónico

Se recomienda que se complete la configuración de SMTP. Esto permite enviar correos electrónicos del sistema, como correos electrónicos de contraseña olvidada.

La dirección de correo electrónico utilizada para enviar correos electrónicos se configura al establecer su perfil.

Para verificar la dirección de correo electrónico, haga clic en el engranaje de configuración y seleccione **Configuración de correo electrónico**.



Si los ajustes de correo electrónico no se pueden configurar correctamente, es probable que no se pueda contactar al servidor de agente de mensajería. Consulte Solucionar problemas en una instalación de Hub en la página siguiente para obtener más información.

> Para obtener más información sobre la configuración de correo electrónico, consulte la Guía del usuario de Hub.

Solucionar problemas en una instalación de Hub

Las siguientes secciones buscan ofrecer orientación en caso de que se presenten problemas específicos ya sea durante la instalación o cuando se verifica que la instalación se ha realizado correctamente.

Conectividad del agente de mensajería

Para verificar la conectividad entre el servidor web y el agente de mensajería, compruebe que se pueda acceder a la consola de administración de RabbitMQ a través de un navegador web.

Podría haber varias razones por las que falla la conectividad:

- Verificar la conectividad de la red: asegúrese de que todos los dispositivos relevantes estén conectados a la misma red y puedan comunicarse.
- Firewall: verifique que los firewalls en los servidores o dentro de la red no estén impidiendo la comunicación.

> La consola de administración de RabbitMQ se comunica, de manera predeterminada, en el puerto 15672. Las colas del agente de mensajería utilizan un puerto diferente, 5672, de manera predeterminada. Debe verificarse el acceso TCP del firewall en todos los puertos. Esto se aplica especialmente en el caso de que la organización de TI haya especificado puertos no predeterminados.

Conectividad de la base de datos

El botón **Probar conexión para continuar** dentro del instalador comprueba lo siguiente:

- Si la base de datos existe:
  - Que se puede conectar con esta.
  - Que el Servidor SQL que aloja la base de datos tenga aplicado un certificado válido.
  - Que la cuenta tiene los derechos para leer, escribir y editar la base de datos.
- Si la base de datos no existe:
  - Que la cuenta tiene derecho a crear la base de datos.
  - Que el Servidor SQL tenga aplicado un certificado válido.

Si no se pueden cumplir estos requisitos, la instalación se detendrá.

Hay una serie de verificaciones que se pueden realizar cuando no se puede establecer una conexión con Servidor SQL mediante la LAN:

- Verificar la conectividad de la red: asegúrese de que todos los dispositivos relevantes estén conectados a la misma red y puedan comunicarse.
- Cifrado SSL: asegúrese de que el Servidor SQL tenga un certificado válido. Para obtener más información, consulte Requisitos previos en la página 6.
- Credenciales de SQL: verifique las credenciales de SQL y que el usuario tenga los permisos adecuados en el Servidor SQL.
- Firewall: verifique que los firewalls en los servidores o dentro de la red no estén impidiendo la comunicación.
- Servicio de navegador de SQL: asegúrese de que el servicio de navegador de SQL en el Servidor SQL esté habilitado para permitir que se encuentre una instancia de SQL. Para SQL Server Express, este servicio en general se encuentra deshabilitado de forma predeterminada.

- Habilitar la conectividad de TCP/IP: cuando se requiere conectividad remota para SQL, verifique que la conectividad de TCP/IP esté habilitada para la instancia de SQL. Microsoft ofrece artículos específicos de cada versión de SQL, que proporcionan instrucciones para habilitar el protocolo de red TCP/IP para Servidor SQL.

Si al ejecutar el instalador el proceso de instalación falla con errores en la base de datos, consulte a continuación, luego pruebe que el servidor web tenga una conectividad SQL a la base de datos. Esto podría deberse a cualquiera de los posibles motivos mencionados anteriormente.

```
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.
```

Otro posible motivo de error es que la cuenta utilizada para crear las bases de datos dentro del instalador no tiene privilegios suficientes para crear las bases de datos.

Por último, si la instalación es una reinstalación después de la eliminación del software. Luego, si se utilizaron los mismos nombres de base de datos, deben borrarse los datos antiguos de las bases de datos antes de volver a instalarlas.

Servidor web

Durante el proceso de instalación, el instalador verificará que todos los requisitos previos estén instalados. Se recomienda que, si los requisitos previos no están instalados, se cancele el instalador, se instalen los requisitos previos y se reinicie el proceso del instalador.

Para obtener más información, consulte Requisitos previos en la página 6.

Inicio del sitio web de IMS

Después de completar la instalación, si aparece un mensaje “Error HTTP 500.19 on 0x8007000d” al iniciar el sitio web de IMS, deberá reparar o reinstalar el componente .NET Core 3.1.2 Windows Server Hosting. El archivo para este componente es dotnet-hosting-3.1.2-win.exe.

File Service

Si el File Service no encuentra las imágenes para IMS y Hub, esto se debe a una desinstalación y reinstalación de los productos de Blue Prism. Este problema no ocurrirá para las instalaciones que se hacen por primera vez.

Durante el proceso de eliminación, las bases de datos no se eliminan y, por lo tanto, si la reinstalación utiliza los mismos nombres de base de datos, se seguirán utilizando las rutas originales a los servicios de archivos y URL.

Para superar esto, después de que se haya ejecutado el proceso de eliminación, elimine o limpie las bases de datos para que se hayan eliminado las rutas anteriores o utilice nombres de bases de datos alternativos durante la reinstalación.

Autenticación de Windows

La cuenta que ejecuta la instalación debe tener los permisos del Servidor SQL pertinentes para llevar a cabo la instalación: membresía en los roles de servidor fijos de sysadmin o dbcreator.

Si durante el proceso de instalación se eligió para utilizar la autenticación de Windows, se recomienda establecer una cuenta de servicio de Windows con los permisos necesarios para ejecutar las tareas y operar durante el funcionamiento normal.

Esta cuenta de servicio no solo necesitará la capacidad de realizar el proceso de creación de la base de datos SQL (consulte Permisos mínimos de SQL en la página 13, sino también la propiedad sobre los grupos de aplicaciones de Internet Information Services.

De manera predeterminada, los grupos de aplicaciones se crean con la identidad "ApplicationPoolIdentity". Después de que el instalador haya completado la cuenta de servicio establecida, se deberán asignar permisos para administrar los grupos de aplicaciones.

Si hay problemas con el Audit Service, asegúrese de que la cuenta de servicio de Windows tenga acceso al oyente del servicio de auditoría y a la base de datos de Audit.

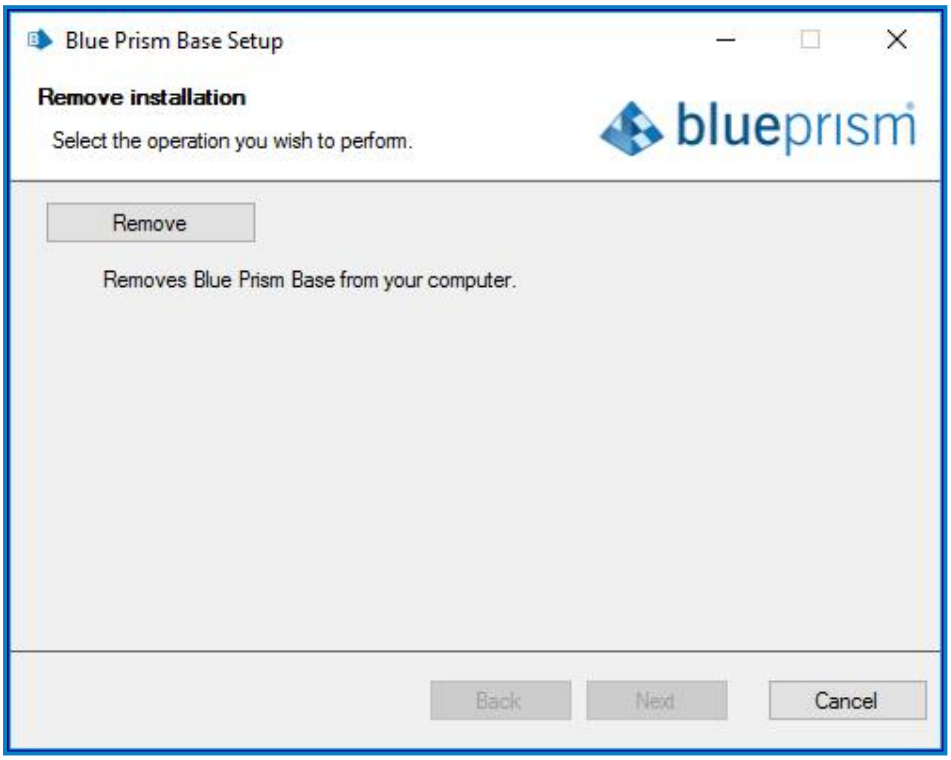
No se pueden configurar los ajustes de SMTP en Hub

Si no puede configurar los ajustes de SMTP en Hub, esto normalmente está relacionado con el orden de inicio de los servicios.

El servidor web debe iniciarse después de que se hayan iniciado todos los servicios de RabbitMQ. Si los servicios del servidor web se inician antes de que el servicio RabbitMQ esté listo, ir a la configuración SMTP en Hub resultará en un mensaje de "algo salió mal".

Desinstalación de Hub

Al hacer clic en el instalador de Blue Prism Hub con los componentes de Blue Prism instalados, se le pedirá que elimine la instalación.



Al retirar la instalación, eliminará los siguientes elementos:

- Grupos de aplicaciones y sitios web de Internet Information Services.
- Servicios.
- Estructura de archivos, excepto para el nivel superior.

Es importante tener en cuenta que las bases de datos no se eliminan. Esto es para permitir el archivo de cualquier dato potencial por parte de la organización o para su uso con fines de auditoría.

> Si la instalación se repite nuevamente después de una eliminación y se utilizan los mismos nombres de base de datos, deben borrarse los datos de las bases de datos antes de la reinstalación.