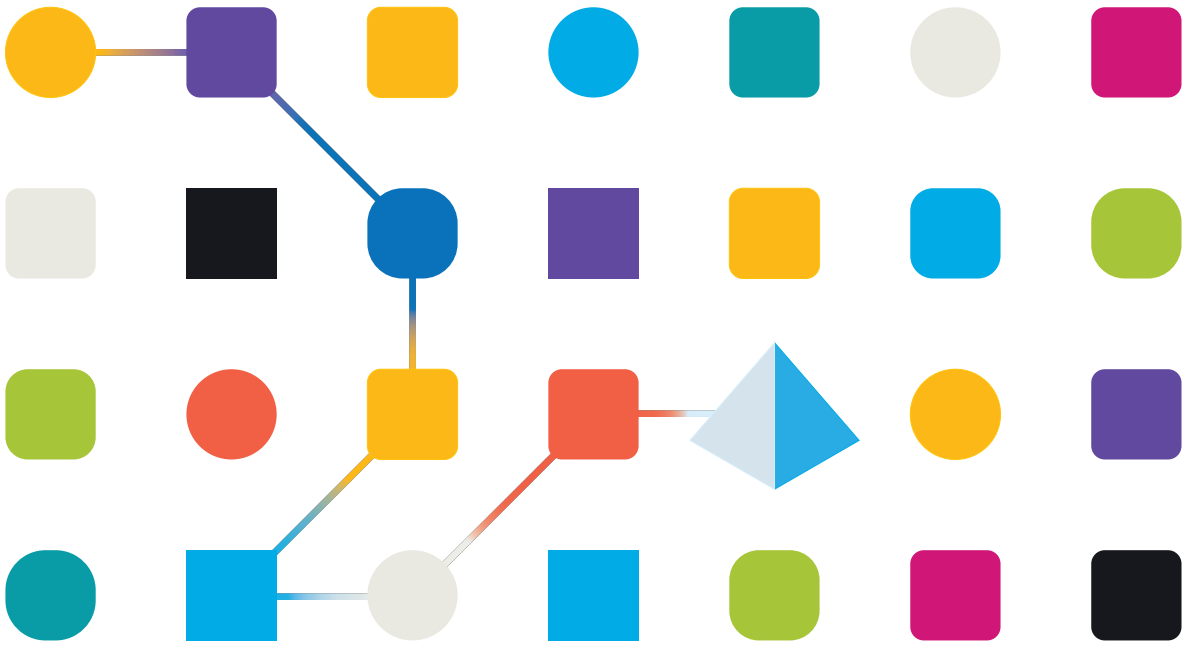
blueprism®

Interact 4.7

Guía de instalación

Revisión del documento: 4.0



Marcas comerciales y derechos de autor

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

Introducción

Esta guía ofrece orientación sobre el proceso a seguir cuando se instala Blue Prism® Interact y contiene información sobre cómo probar que la instalación se realizó correctamente.

Blue Prism Interact solo es compatible con una implementación de múltiples dispositivos. Aquí es donde se implementan los componentes de Blue Prism 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.

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 únicamente con la versión 4.7 de Blue Prism Interact.

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

Actualización de Interact

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

Videos

Además de esta guía de instalación, puede ver nuestros videos que demuestran el proceso de instalación. Haga clic aquí para ver los videos de instalación de Interact.

Documentos relacionados

Los siguientes documentos proporcionan más información sobre aspectos específicos de la implementación de Hub e Interact.

Título del documento	Descripción
Guía del usuario de Hub	Documento dirigido a los usuarios de Hub que explica cómo aprovechar al máximo Hub.
Guía del administrador de Hub	Documento detallado, dirigido a administradores de Hub, que explica cómo aprovechar al máximo Hub, incluidos el acceso de usuarios, las licencias de complementos y la personalización de Hub.
Guía de usuario de complementos de Interact	Es un documento detallado que explica cómo obtener lo mejor de Interact, incluidas la creación de formularios y la asignación de roles.
Guía del usuario de Interact	Documento detallado que explica cómo usar Interact para enviar y aprobar formularios.
Guía del usuario del servicio de API web de Interact	Es un documento que proporciona información detallada sobre cómo utilizar el servicio de API web de Interact y el objeto de Blue Prism relacionado.

Preparación

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

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 Authentication Server , Hub, Audit, Interact, InteractCache, etc. Durante el proceso de instalación se requiere acceso a nivel de administrador. Consulte Permisos mínimos de SQL para obtener más detalles.
- Debe haber un servidor de agente de mensajería disponible para alojar al agente de mensajería de RabbitMQ.
- Un servidor web para las instalaciones coexistentes de Hub (consulte los Requisitos previos en la página siguiente) e Interact
- Debe haber acceso de administrador disponible a los dispositivos donde se instalará Blue Prism Interact. 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.
- 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?

  Para obtener detalles, consulte Requisitos y permisos de software.

Requisitos previos

Consulte Requisitos y permisos de software para obtener detalles sobre los requisitos de software y los permisos mínimos de SQL.

La instalación de Interact 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 en la guía de instalación de Blue Prism Hub.
  >
  > 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.

- Blue Prism Hub requiere que se instale y configure un servidor de agente de mensajería.
- 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 25 para obtener más información.

- El sistema Interact es un servidor web y, por lo tanto, requiere que se instale un servidor web de Internet Information Services y los componentes de .NET Core. Todos estos se instalan como parte de una instalación correcta de Blue Prism Interact utilizando los medios de instalación de Blue Prism Hub y Blue Prism Interact.
- Creará los siguientes sitios web con el instalador de Interact; debe definir las URL en función del dominio de su organización:

Sitio web en IIS	URL predeterminada
Sitios web con una interfaz de usuario para utilización de los usuarios finales	
Blue Prism: Interact	https://interact.local
Sitios web para uso exclusivo de la aplicación (servicios)	
Blue Prism: IADA	https://iada.local
Blue Prism: Remote API de Interact	https://interactremoteapi.local

⚠ Las URL predeterminadas que se muestran arriba son adecuadas para un entorno independiente, como un entorno de prueba. Las estructuras de DNS y dominio de su organización deben tenerse en cuenta al elegir nombres de host para su instalación.

Esto es de forma adicional a los sitios web creados por el instalador de Hub; consulte Configurar certificados SSL en la página 26 para obtener una lista.

- 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. Consulte Configurar certificados SSL para obtener detalles.
- 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 14.
- 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 3.9.22 a 3.10.7, o 3.11.9 a 3.11.10 Para obtener más información, consulte Descarga e instalación de RabbitMQ.	Instalar el servidor de agente de mensajería en la página 20
Erlang/OTP 24.x o 25.x 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.	
IIS 10.0 Incluido con Windows Server 2016, 2019 y 2022.	Instalar y configurar el servidor web en la página 25
ASP.NET Core Runtime 6.0.9 o 6.0.10 (paquete de alojamiento de Windows) https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **ASP.NET Core Runtime**, seleccione **Paquete de alojamiento**.	
.NET Desktop Runtime 6.0.9 o 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **.NET Desktop Runtime**, seleccione la descarga adecuada.	
.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 4.7 Descargue Hub desde cualquiera de las siguientes páginas de descarga de productos en el portal de Blue Prism: • Automation Lifecycle Management • Decision • 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 anterior.

Software y enlace de referencia	Orientación relacionada
Blue Prism Interact 4.7 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 mínimos de hardware

La siguiente información detalla los requisitos mínimos de hardware recomendados para instalar y ejecutar de manera efectiva Hub e Interact 4.7. Para conocer los requisitos de software, consulte Requisitos y permisos de software en la página siguiente.

Recurso de tiempo de ejecución

Consulte los requisitos mínimos en la guía de instalación para conocer la versión de Blue Prism que tiene instalada. Visite la ayuda de Blue Prism para obtener más información.

Servidor de bases de datos

- Procesador Intel Quad Xeon
- 8 GB de RAM
- Servidor SQL:
  - 2016, 2017 o 2019 (64 bits): ediciones Express, estándar o empresarial

    > Las ediciones de SQL Express solo son adecuadas para los entornos de no producción, p. ej., para ejercicios de prueba de concepto.

  - Base de datos SQL de Azure: se requiere un mínimo de 100 eDTU durante la instalación. Esto puede reducirse a 50 eDTU después de la instalación.
  - Servidor SQL en máquinas virtuales Azure
  - Instancia administrada SQL de Azure
- Para obtener el soporte técnico adecuado para el sistema operativo, consulte los siguientes documentos:
  - Servidor SQL 2016 o 2017: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver15
  - Servidor SQL 2019: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

Servidor de agente de mensajería

- Procesador Intel Dual Xeon
- 8 GB de RAM
- Windows Server 2016 Datacenter o 2019 o 2022

Servidor web

- Procesador Intel Dual Xeon
- 8 GB de RAM
- Windows Server 2016 Datacenter o 2019 o 2022
- Requisitos previos según se detalla en Preparación en la página 6

Requisitos y permisos de software

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)	✓	✓	✓

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 7.

  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:

- Base de datos SQL de Azure: se requiere un mínimo de 100 eDTU durante la instalación. Esto puede reducirse a 50 eDTU después de la instalación.
- Servidor SQL en máquinas virtuales Azure.
- Instancia administrada SQL de Azure; sin embargo, las bases de datos deben crearse antes de la instalación.

Servidor de agente de mensajería

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

- RabbitMQ 3.9.22 a 3.10.7, o 3.11.9 a 3.11.10
- Erlang/OTP 24.xo 25.x: 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 20 para obtener más información.

El objetivo de Blue Prism es probar por completo todas las nuevas versiones de RabbitMQ con la última versión de Hub en un plazo de dos meses a partir de la disponibilidad general de ese software. Si se requiere algún desarrollo posterior de Hub para admitir una nueva versión de RabbitMQ, se incorporarán actualizaciones a un lanzamiento futuro de Hub según lo determine nuestro ciclo de lanzamiento.

Servidor web

Se requiere el siguiente software en el servidor web:

- .NET Framework 4.8: se instala de forma predeterminada en Windows Server 2022.
- IIS 10.0
- ASP.NET Core Runtime 6.0.9 o 6.0.10 (paquete de alojamiento de Windows)
- .NET Desktop Runtime 6.0.9 o 6.0.10

Interact 4.7 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 25 para obtener más información.

Navegador web en máquinas cliente

Las versiones más recientes de los siguientes navegadores web son compatibles con Interact:

- Google Chrome
- Microsoft Edge (basado en Chromium)

Para permitir que los usuarios de Directorio Activo inicien sesión en Interact con un navegador Chrome o Edge, los navegadores deben configurarse para la autenticación de Windows integrada.

Microsoft Internet Explorer y Mozilla Firefox no son compatibles.

Blue Prism

Se requiere Blue Prism 6.4.0 o posterior para usar con Interact.

Permisos mínimos de SQL

Los permisos mínimos de SQL 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 la base 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 de Interact e Interact Cache. Los permisos requeridos son los siguientes:

- db_datareader
- db_datawriter

Se debe utilizar un usuario con acceso db_owner a la base de datos durante el proceso de instalación y en la primera ejecución de la aplicación. Una vez completado, el acceso a la base de datos para este usuario se puede cambiar a db_datareader y 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 de Interact, 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 – IADA también requerirá acceso al certificado BPC_SQL_CERTIFICATE.

> Para obtener información sobre las aplicaciones de Hub, consulte Requisitos y permisos del software Hub.

Sitios web de Interact

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 - Interact	Internet Information Services APPPOOL\Blue Prism – Interact	dbcreator/sysadmin	db_datawriter/ db_datareader	InteractDB, InteractCacheDB
Blue Prism - Remote API de Interact	Internet Information Services APPPOOL\Blue Prism – Interact Remote API	dbcreator/sysadmin	db_datawriter/ db_datareader	AuthenticationServerDB, InteractDB
Blue Prism - IADA	Internet Information Services APPPOOL\Blue Prism – IADA	dbcreator/sysadmin	db_datawriter/ db_datareader	IadaDB

Servicios Interact

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 - Submit Form Manager	NT AUTHORITY\ SISTEMA	N/C	db_datawriter/ db_datareader	InteractDB

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). Se recomienda que los diferentes tipos de entornos, como los entornos de desarrollo, UAT y producción, tengan su propia instancia de Servidor SQL dedicado. Sin embargo, puede ejecutar varios entornos de desarrollo en la misma instancia de Servidor SQL.
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

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

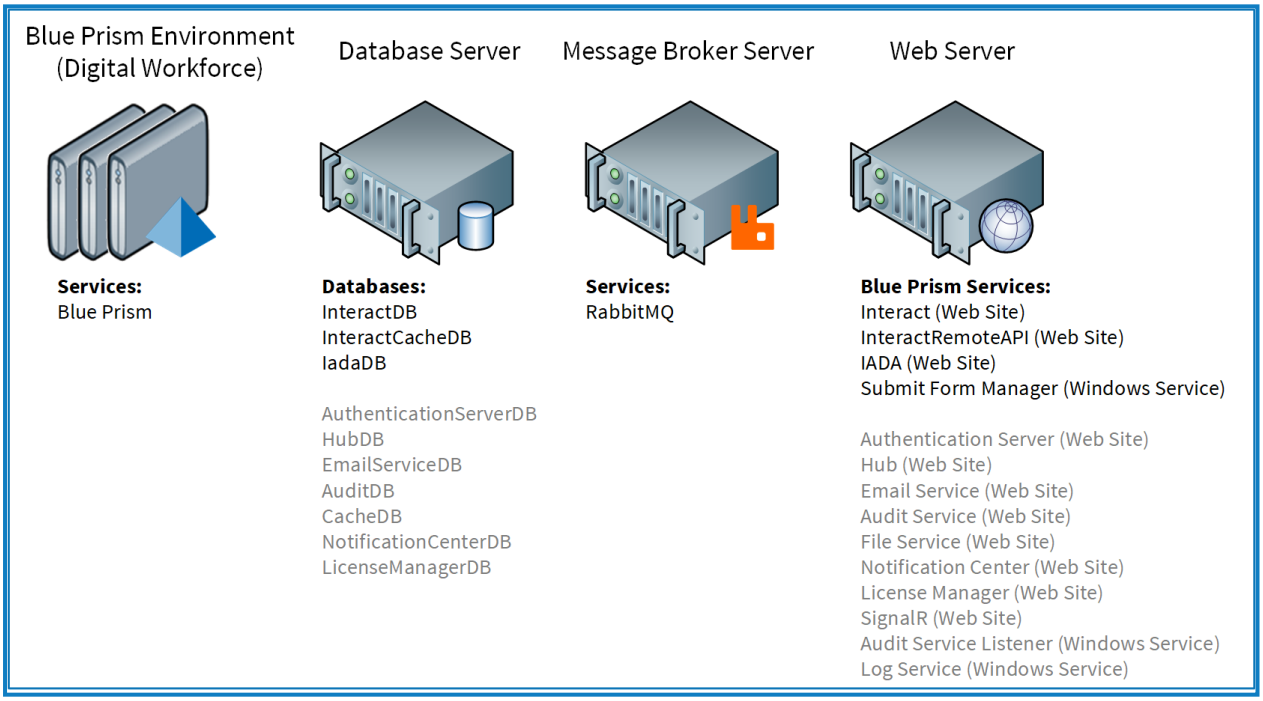
Antes de seguir esta orientación, asegúrese de haber considerado por completo la información en Preparación.

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

- Servidor web
- Servidor de agente de mensajería
- Trabajadores digitales
- Servidor SQL

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

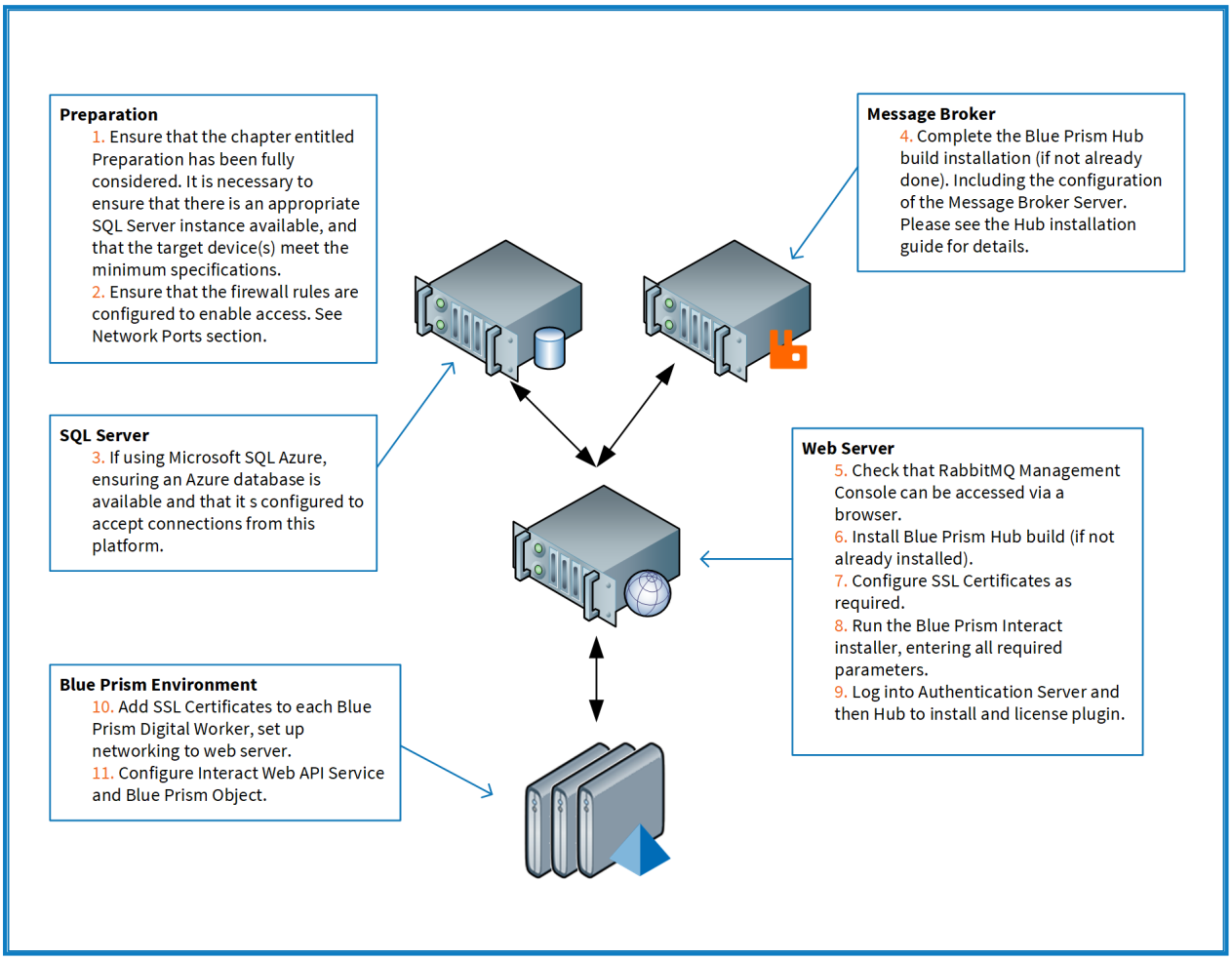
El siguiente diagrama ilustra la arquitectura típica de un entorno.



Los elementos en gris se implementan como parte de la instalación de Blue Prism Hub.

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.

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.

Hay videos instructivos disponibles sobre cómo instalar el software para el servidor de agente de mensajería en: https://bpdocs.blueprism.com/video/installation.htm.

Para ver las versiones de software, consulte Requisitos de software en la página 12.

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

1. Descargue e instale Erlang, y acepte la configuración predeterminada en el asistente de instalación.

   La versión de Erlang que necesita depende de la versión de RabbitMQ que desea utilizar. Para:
   - Versión y soporte de Erlang/OTP, consulte Requisitos de la versión Erlang de RabbitMQ.
   - Información de instalación, consulte la Guía de instalación de Erlang/OTP.
   - Descargas, consulte Descargar Erlang/OTP.

   Para ver este paso de instalación, vea nuestro video de instalación de Erlang.

2. Descargue e instale RabbitMQ y acepte la configuración predeterminada.

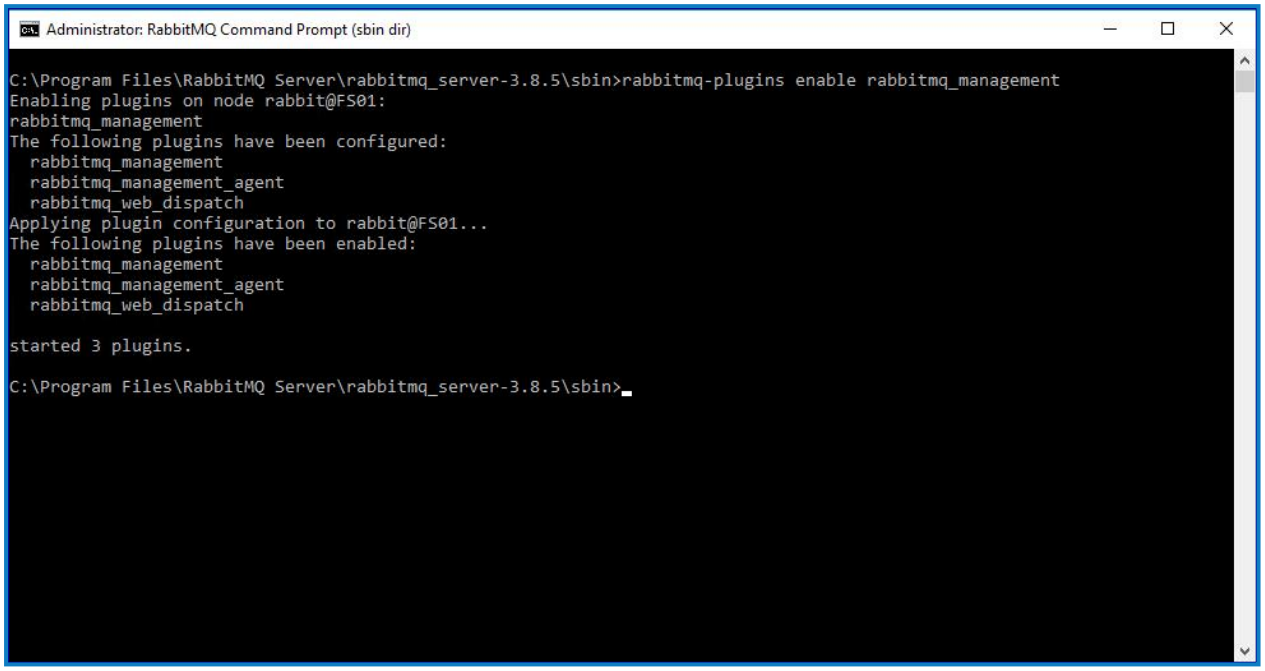
   Para obtener más información, consulte Descarga e instalación de RabbitMQ.

   Para ver este paso de instalación, vea nuestro video de 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).

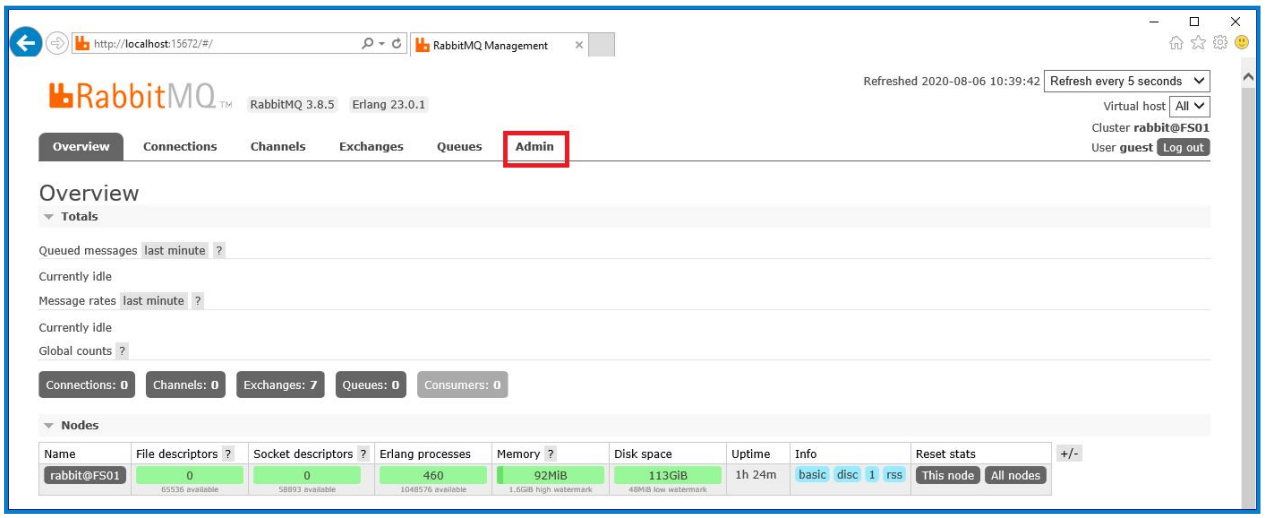
5. En la ventana del símbolo del sistema de RabbitMQ, escriba el siguiente comando:

```
rabbitmq-plugins enable rabbitmq_management
```

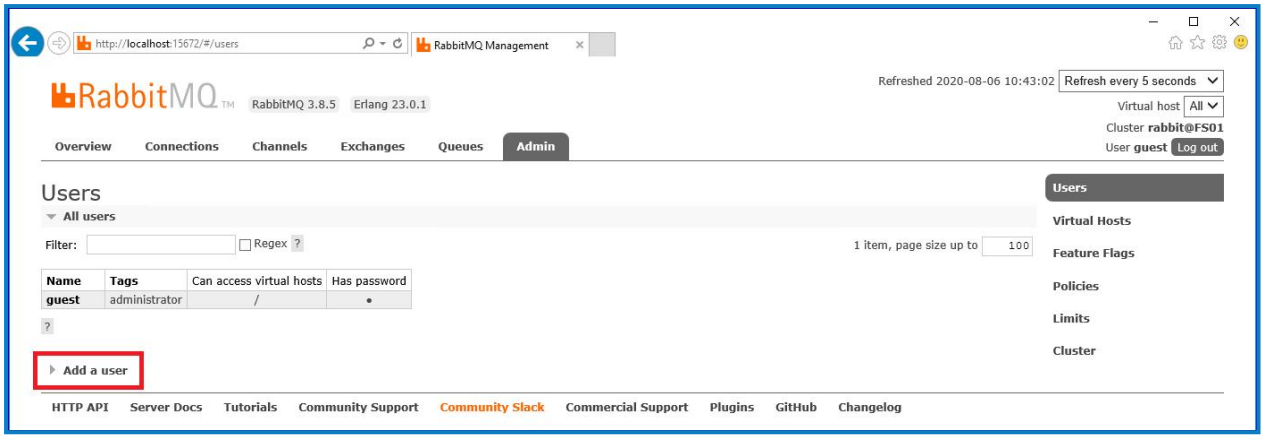


6. Inicie un navegador y navegue a la siguiente URL: http://localhost:15672
7. En la consola de RabbitMQ, inicie sesión con las credenciales predeterminadas de invitado/invitado.

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



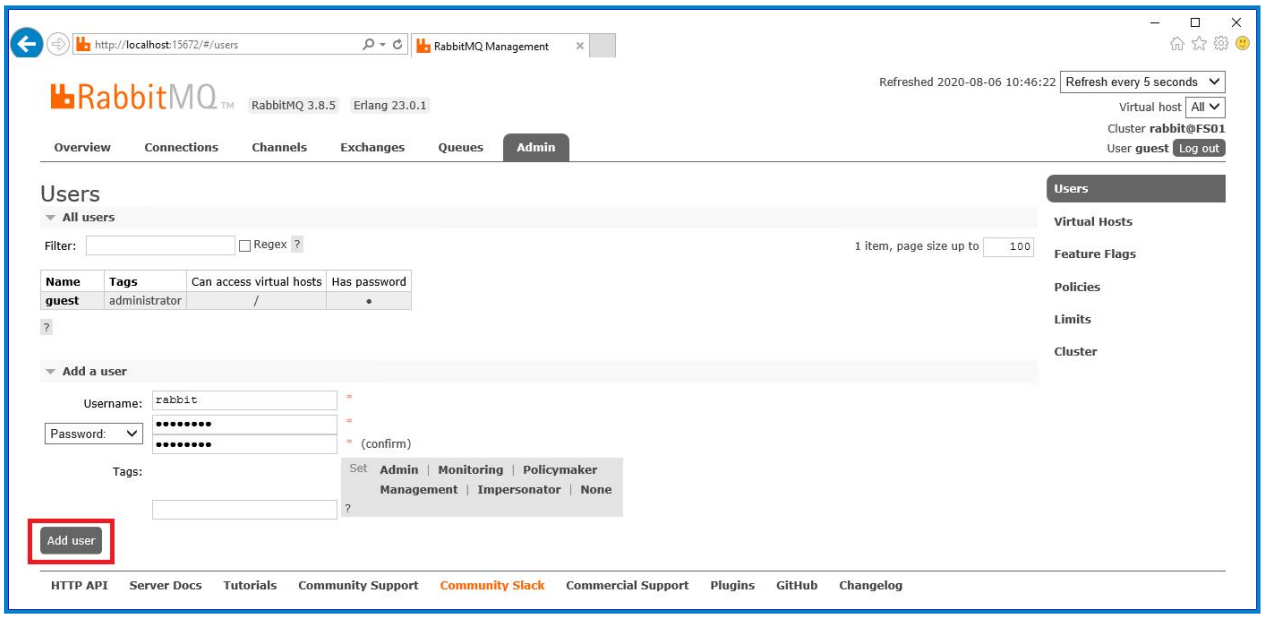
9. Haga clic en **Agregar un usuario**.



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.

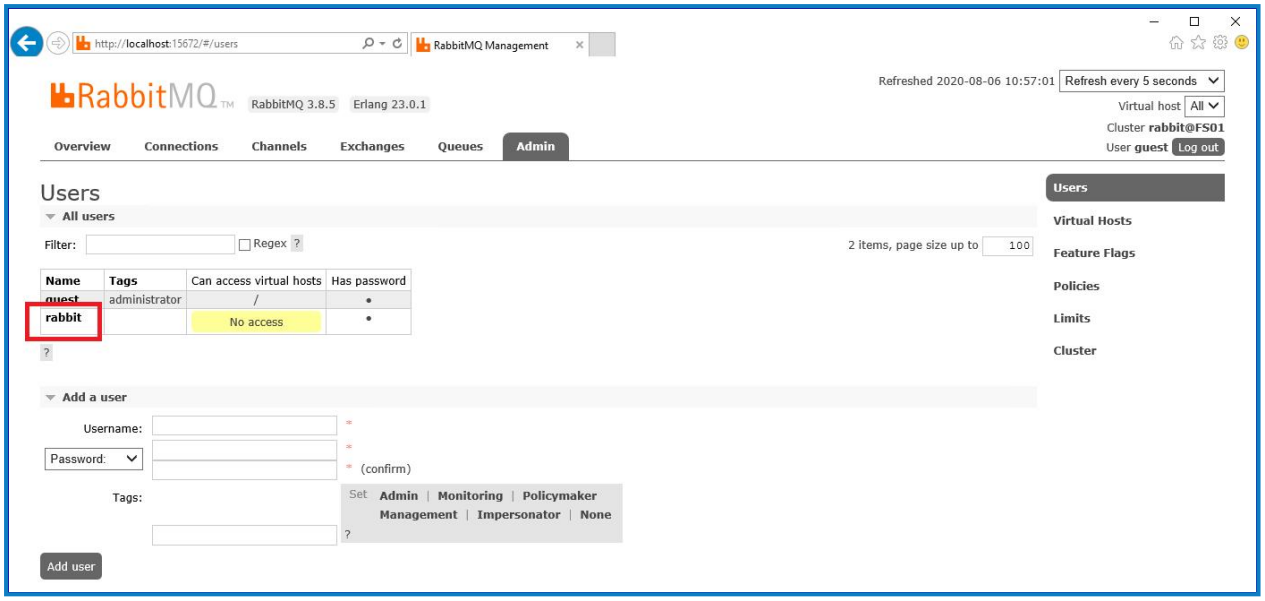
> Los siguientes caracteres no se deben utilizar para la contraseña al crear el usuario de RabbitMQ **# / : ? @ \ ` " $ '**.

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

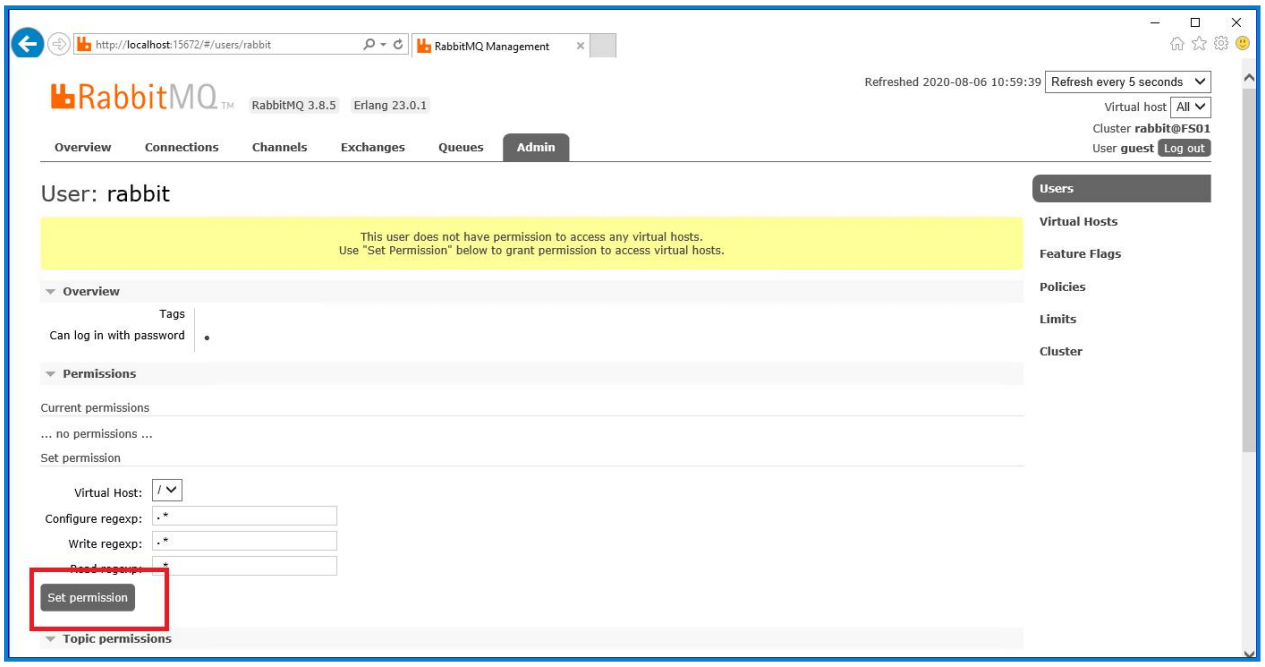


El siguiente paso es establecer los permisos para el usuario.

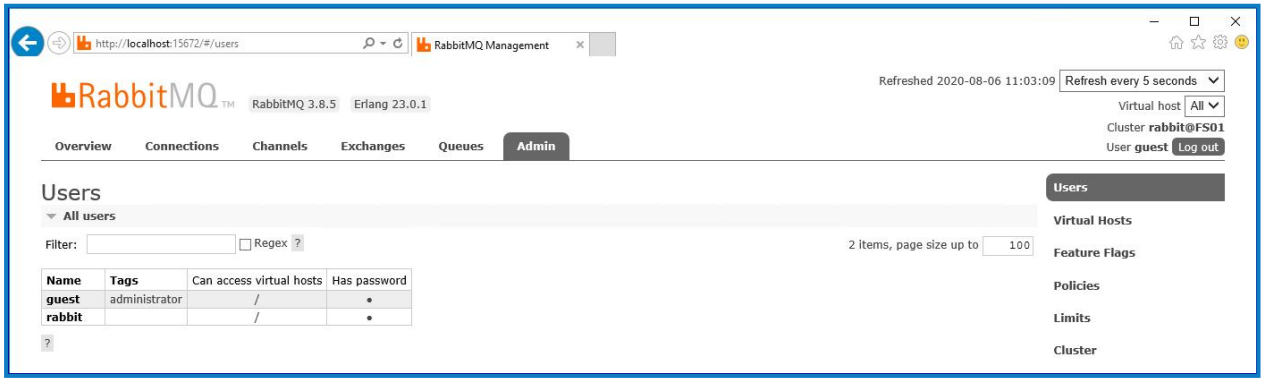
12. Haga clic en el nombre de usuario del usuario que acaba de crear.



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 98.

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 6.

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.

Los nombres de host predeterminados proporcionados en los procedimientos a continuación solo son adecuados para un entorno independiente, como un entorno de prueba. Las estructuras de DNS y dominio de su organización deben tenerse en cuenta al elegir nombres de host en su instalación.

Hay videos instructivos disponibles sobre cómo instalar el software de requisito previo y Blue Prism Hub en: https://bpdocs.blueprism.com/es-la/video/installation.htm.

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.

Instalación por script

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

```
Install-WindowsFeature -name Web-Server, Web-Windows-Auth -IncludeManagementTools
```

Para ver este paso de instalación, vea nuestro video de instalación de IIS.

De manera predeterminada, IIS se instala con la configuración **Autenticación anónima** habilitada. Hub y sus sitios relacionados requieren esta configuración. Si deshabilitó **Autenticación anónima**, debe habilitarla antes de ejecutar el instalador de Hub. Para obtener más información sobre la autenticación anónima, consulte la página Autenticación anónima de Microsoft.

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.

Las tablas a continuación detallan los certificados SSL requeridos.

Sitios web de Hub:

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: Authentication Server	https://authentication.local
Blue Prism: Hub	https://hub.local
Sitios web para uso exclusivo de la aplicación (servicios)	
Blue Prism: Email Service	https://email.local
Blue Prism: Audit Service	https://audit.local
Blue Prism: File Service	https://file.local
Blue Prism: Notification Center	https://notification.local
Blue Prism: License Manager	https://license.local
Blue Prism: SignalR	https://signalr.local

Sitios web de Interact:

Sitio web en IIS	URL predeterminada
Sitios web con una interfaz de usuario para utilización de los usuarios finales	
Blue Prism: Interact	https://interact.local
Sitios web para uso exclusivo de la aplicación (servicios)	
Blue Prism: IADA	https://iada.local
Blue Prism: Remote API de Interact	https://interactremoteapi.local

> Las URL predeterminadas que se muestran arriba son adecuadas para un entorno independiente, como un entorno de prueba. Las estructuras de DNS y dominio de su organización deben tenerse en cuenta al elegir nombres de host para su instalación.

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.

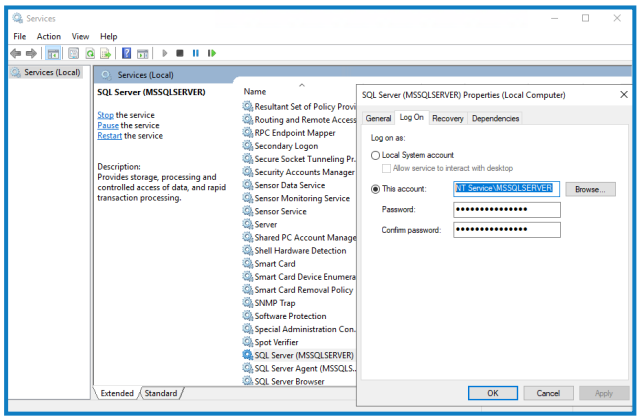
Para generar y aplicar un certificado autofirmado para el servidor SQL:

> 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.**

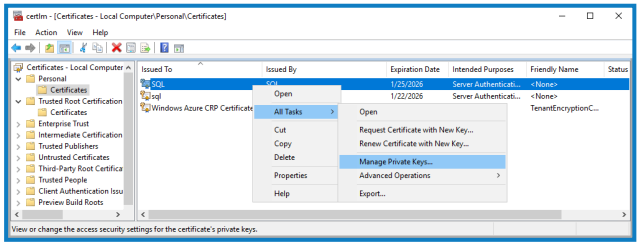
1. Ejecute PowerShell como administrador y ejecute el script de Microsoft con la información para su servidor SQL.

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

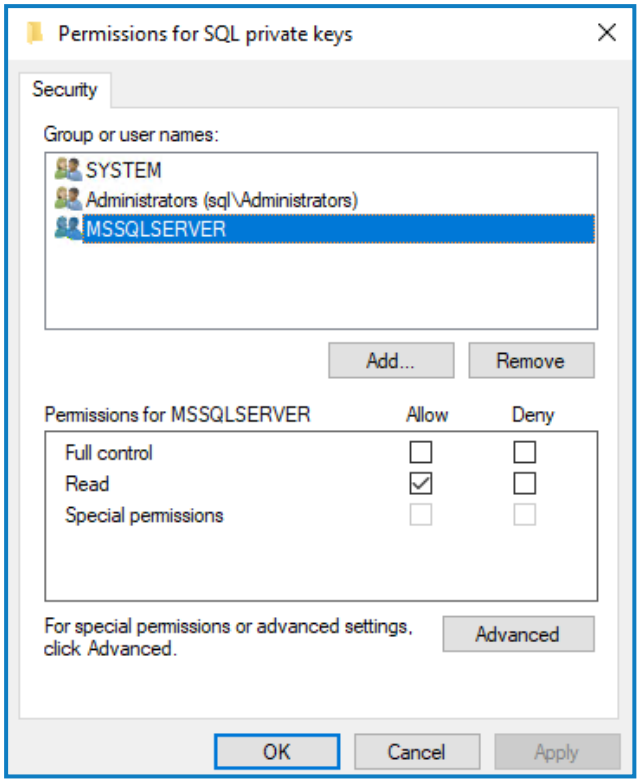
2. En su servidor SQL:
   a. Habilite el acceso a la clave privada del certificado para la cuenta de servicio del servidor SQL. Para hacerlo, siga estos pasos:
      i. Si aún no lo sabe, busque el nombre de su cuenta de servicio para el servidor SQL. Esto se muestra en la pestaña Inicio de sesión de 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.

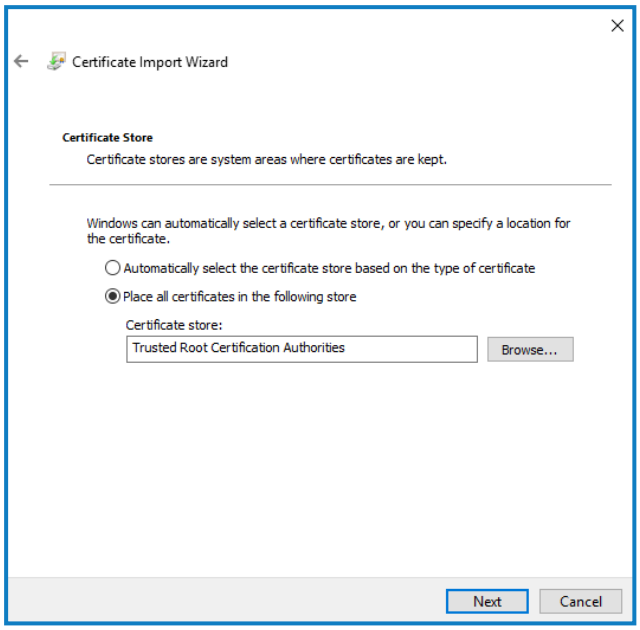
b. Agregue el certificado al almacén de certificados de Autoridades de certificado de confianza del servidor. Para hacerlo, siga estos pasos:

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 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
"authentication.local" -FriendlyName "MySiteCertAuthentication" -NotAfter (Get-
Date).AddYears(10)
```

Este ejemplo crea un certificado autofirmado llamado *MySiteCertAuthentication* en el almacén de certificados personales, con *authentication.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. Este proceso creará un único certificado que se puede aplicar a cada sitio web.

Ejecute los siguientes comandos de PowerShell:

```
New-SelfSignedCertificate -CertStoreLocation Cert:\LocalMachine\My -DnsName
XXXXXXXXXX,authentication.local,hub.local,email.local,audit.local,file.local,signalr.local,notifi
cation.local,license.local,interact.local,iada.local,interactremoteapi.local -FriendlyName
"TheOneCert" -NotAfter (Get-Date).AddYears(10)
```

> XXXXXXXXXX debe reemplazarse por el nombre del servidor host.

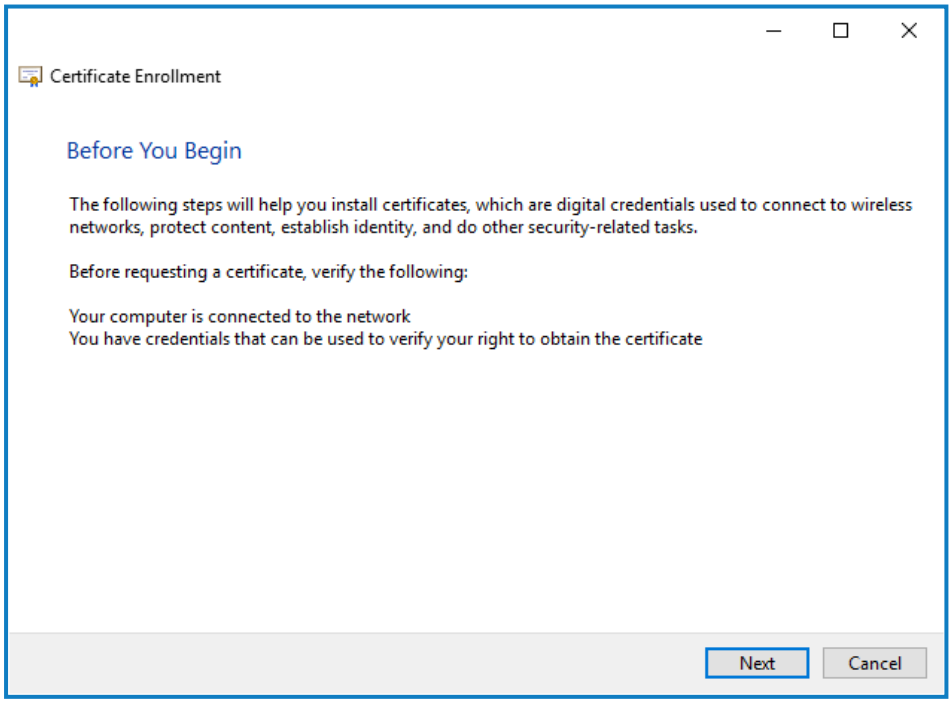
Una vez creados, abra el administrador de certificados del equipo local (certlm), y copie y pegue los certificado en el almacén de certificados de confianza.

Crear una solicitud de certificado sin conexión

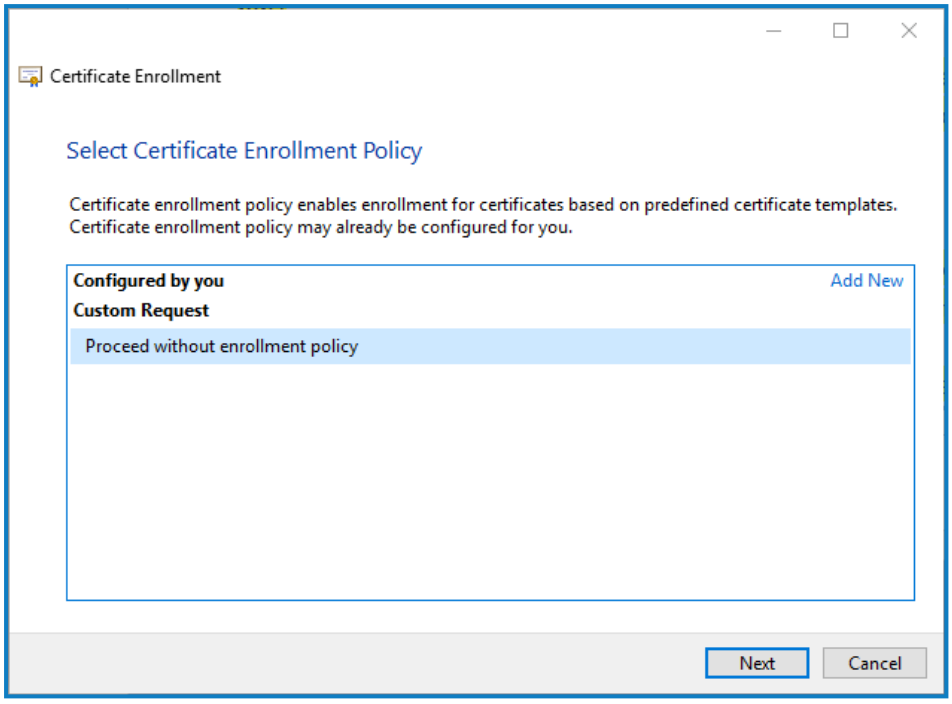
Para crear una solicitud de certificado sin conexión, siga este procedimiento para cada certificado:

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.

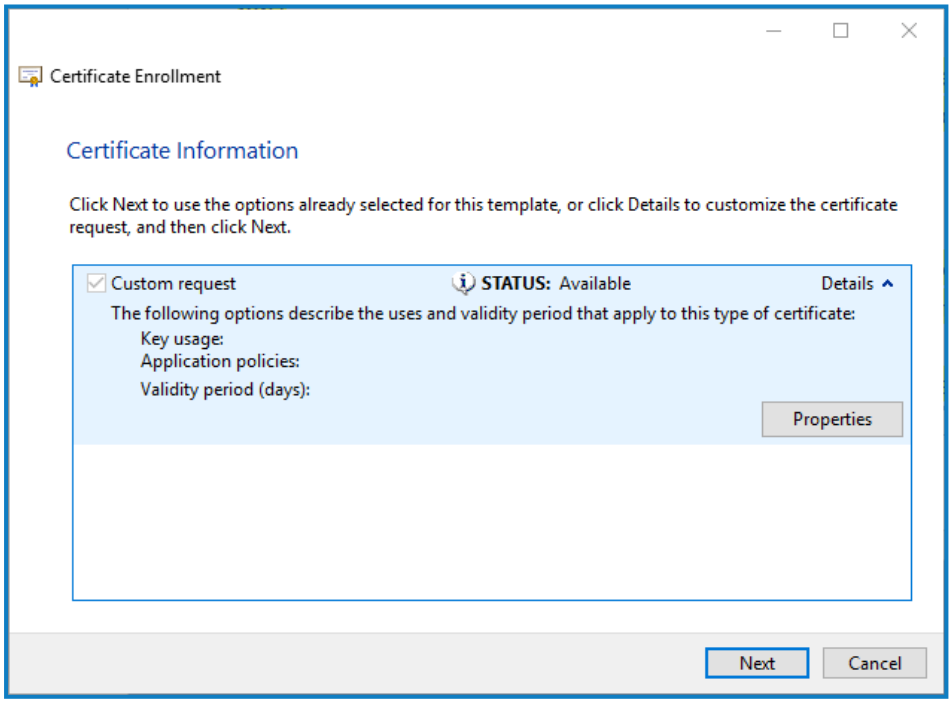
   Aparece el asistente de inscripción del certificado.



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 componentes de .NET Core.

Paso	Detalles
1	Descargue los siguientes componentes y almacénelos en una ubicación temporal, por ejemplo, C:\temp: • ASP.NET Core Runtime 6.0.9 o 6.0.10 (paquete de alojamiento de Windows) https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **ASP.NET Core Runtime**, seleccione **Paquete de alojamiento**. • .NET Desktop Runtime 6.0.9 o 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0: seleccione la versión que requiere. En **.NET Desktop Runtime**, seleccione la descarga adecuada. • .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.

2	Para instalar las dependencias .NET, ejecute cada uno de los siguientes comandos con el símbolo del sistema PowerShell, y espere hasta que cada uno de ellos finalice, antes de ejecutar el siguiente comando:
	Para Windows Server 2016 y Windows Server 2019:
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	`start-process "C:\temp\ndp48-x86-x64-allos-enu.exe" /q -wait`
	Para Windows Server 2022:
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	Asegúrese de que el nombre y la ruta del archivo coincidan con los archivos que se almacenaron en el paso 1.

3	Reinicie el servidor antes de instalar Blue Prism Hub para asegurarse de que los componentes estén completamente instalados y registrados.

Para ver este paso de instalación, vea nuestro video de instalación de .NET.

Instalar Blue Prism Hub

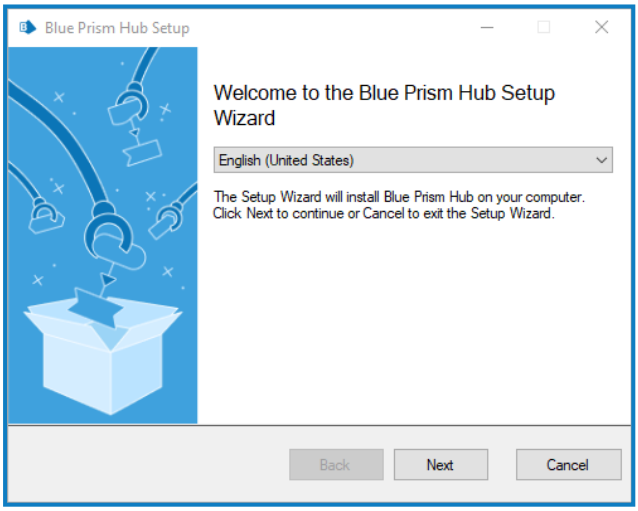
Antes de instalar Blue Prism Hub:

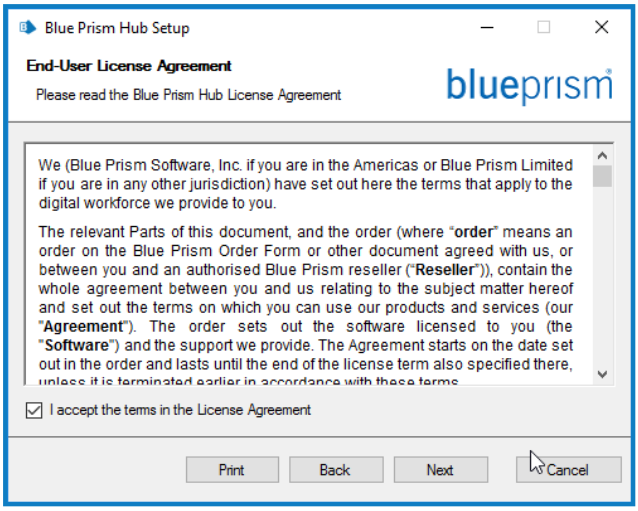
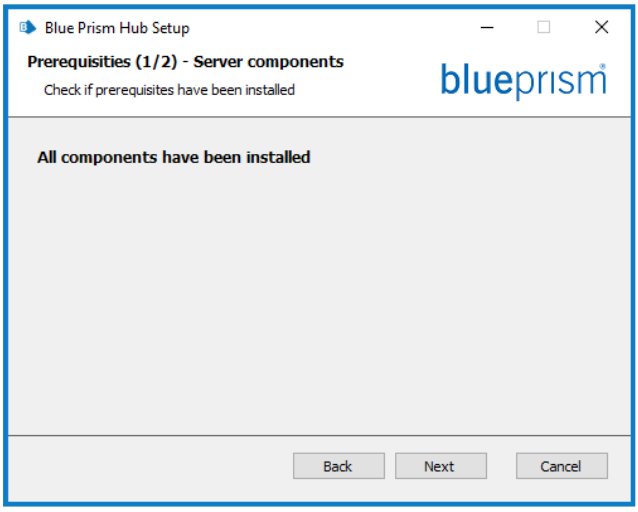
- Si ha comprado ALM, Decision o Interact, necesitará su identificación de cliente durante la instalación de Hub. Esto se puede encontrar en el correo electrónico que se le envió cuando compró ALM, Decision o Interact.
- Si desea utilizar el complemento Blue Prism Decision en Hub, deberá instalar el contenedor del servicio del modelo de Blue Prism Decision en un host de Docker antes de ejecutar el asistente de instalación de Hub. Para obtener más información, consulte Instalar Blue Prism Decision.
- 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.

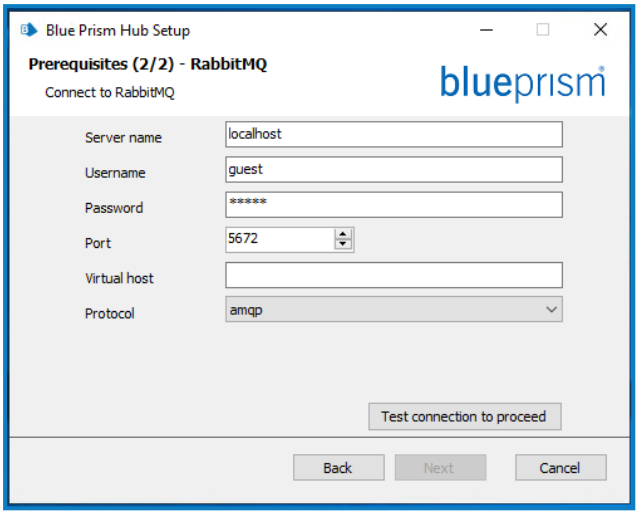
Para ver el proceso de instalación y configuración de Hub, consulte nuestro video de instalación de Blue Prism Hub.

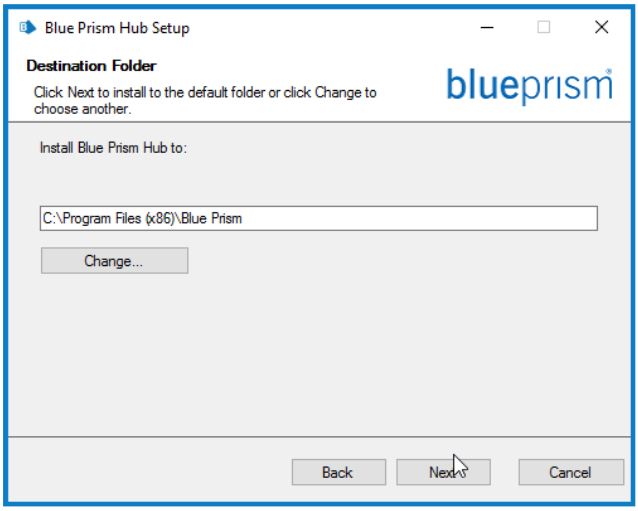
Los pasos a continuación detallan el proceso para instalar el software de Blue Prism Hub. Esto incluye el Identify Management System (IMS), Hub y otros servicios asociados. El proceso de instalación creará cualquier base de datos nueva que sea necesaria.

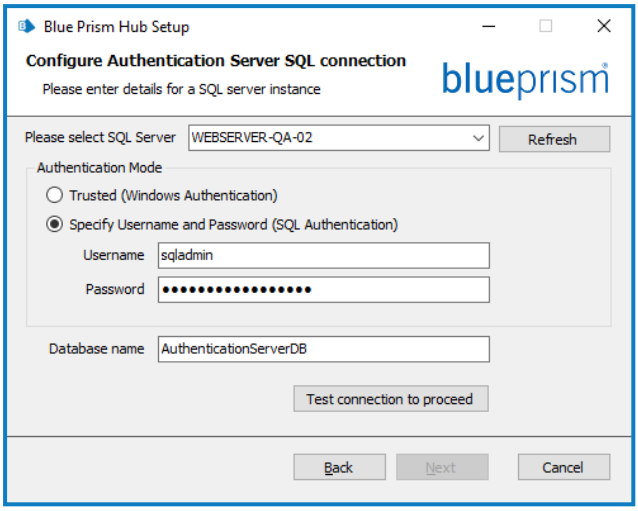
Descargue y ejecute el instalador de Blue Prism Hub, disponible en el portal de Blue Prism, y avance a través del instalador como se muestra a continuación. El instalador se debe ejecutar con derechos de administrador.

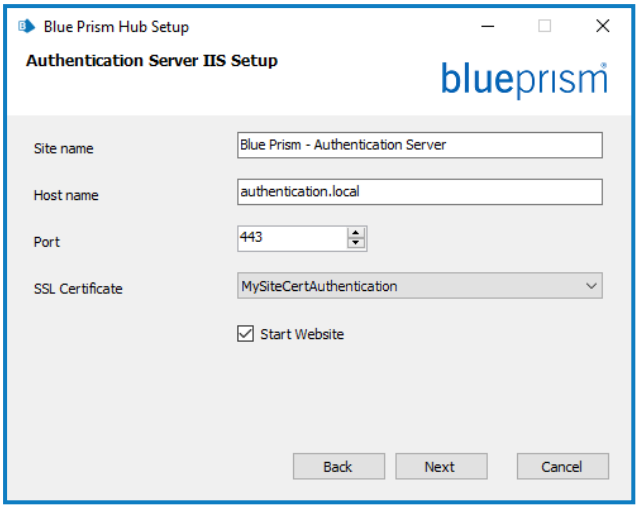
Paso	Página del instalador	Detalles
1		**Bienvenido** Si es necesario, seleccione otro idioma para el instalador de la lista desplegable. El idioma predeterminado es el inglés (Estados Unidos). Haga clic en **Siguiente**.

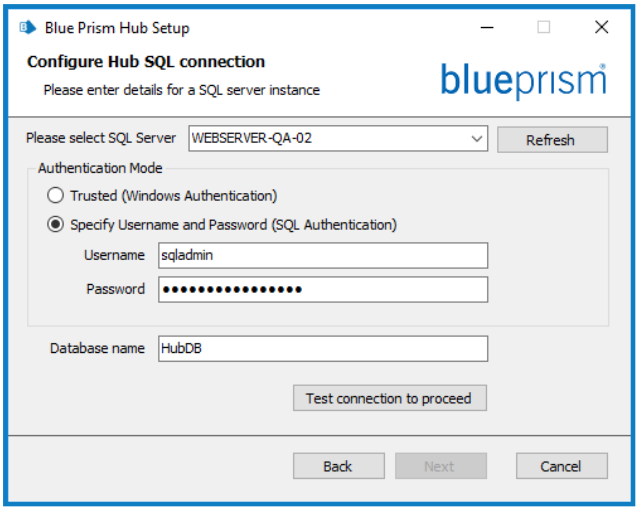
Paso	Página del instalador	Detalles
2		**Contrato de licencia** Lea el EULA y, si acepta los términos, seleccione la casilla de verificación.
3		**Requisitos previos 1: Componentes del servidor** El instalador verifica que se hayan instalado los requisitos previos. Se identifican aquellos que no están 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.

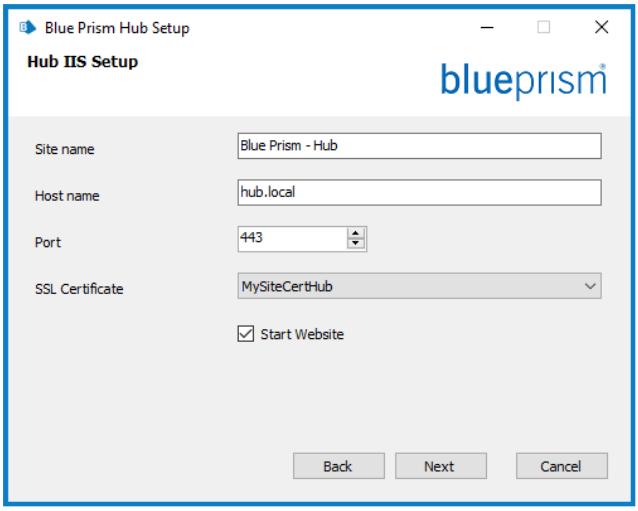
Paso	Página del instalador	Detalles
4		**Requisitos previos 2: RabbitMQ** Ingrese el nombre del servidor o la dirección IP del servidor de agente de mensajería y las credenciales del usuario que creó. El puerto de cola de mensajes predeterminado es 5672. Esto solo debe cambiarse si los puertos predeterminados han sido cambiados por su organización de soporte de TI. De manera predeterminada, el campo **Virtual host** está en blanco. Puede dejarlo en blanco; la conexión se realizará a la raíz de RabbitMQ. Como alternativa, si tiene hosts virtuales configurados en RabbitMQ, puede conectarse a un host específico. En **Host virtual**, ingrese el nombre del host virtual en RabbitMQ al que desea conectarse. El host virtual ya debe existir en RabbitMQ. No puede ingresar un nuevo nombre, ya que este instalador no creará un nuevo host virtual. Puede encontrar más información sobre los hosts virtuales en el sitio web de RabbitMQ - Hosts virtuales. En la lista desplegable **Protocolo**, seleccione el protocolo que desea utilizar. Puede seleccionar AMQP o AMQPS. Si selecciona AMQPS, se muestra un campo adicional para que ingrese el certificado que debe utilizarse para la conexión. Puede encontrar más información sobre la configuración y los certificados de TLS en el sitio web de RabbitMQ - Soporte técnico de TLS. Si utiliza AMQPS, deberá dar el control total del certificado RabbitMQ a los grupos de aplicaciones de Blue Prism IIS. Para obtener más información, consulte Solucionar problemas en una instalación de Hub en la página 98. 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

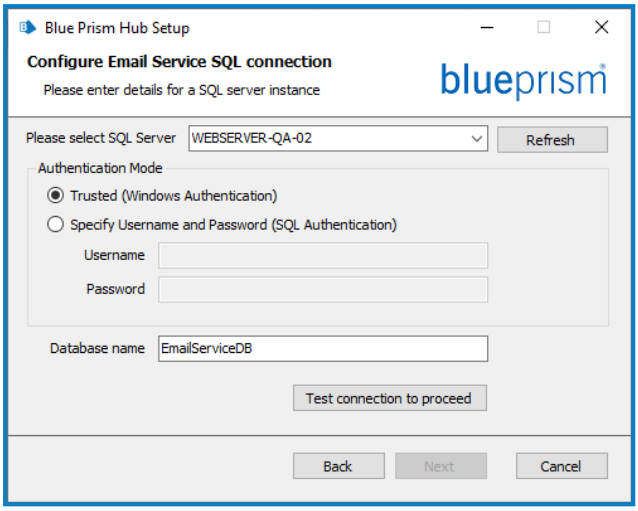
Paso	Página del instalador	Detalles
		es exitosa. Si la prueba falló, consulte Solucionar problemas en una instalación de Hub en la página 98 para obtener más detalles.
5		**Carpeta de destino** Especifique la carpeta de instalación requerida. La ubicación predeterminada es C:\Archivos de programa(x86)\Blue Prism, pero puede elegir otra con el botón **Cambiar**.

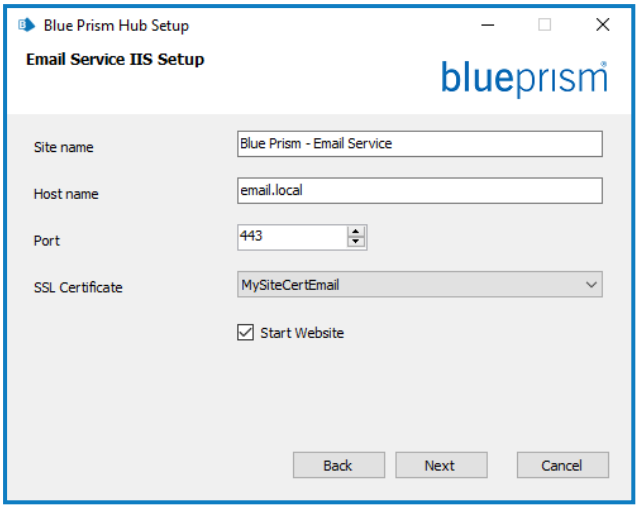
Paso	Página del instalador	Detalles
6		**Conexión SQL de Authentication Server** Configurar los ajustes para la base de datos del Authentication Serveral proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

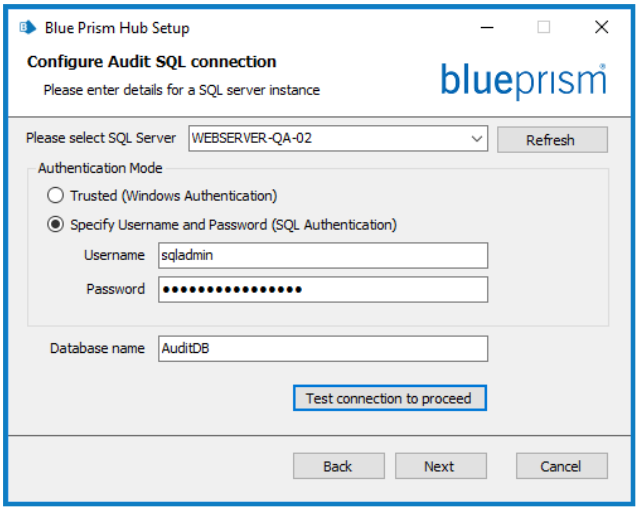
Paso	Página del instalador	Detalles
7		**Configuración de IIS de Authentication Server** Configure IIS para el sitio web de Authentication Server. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación. Una vez finalizada la instalación, se habilita la función **Autenticación de Windows** de IIS en el sitio web de Authentication Server.

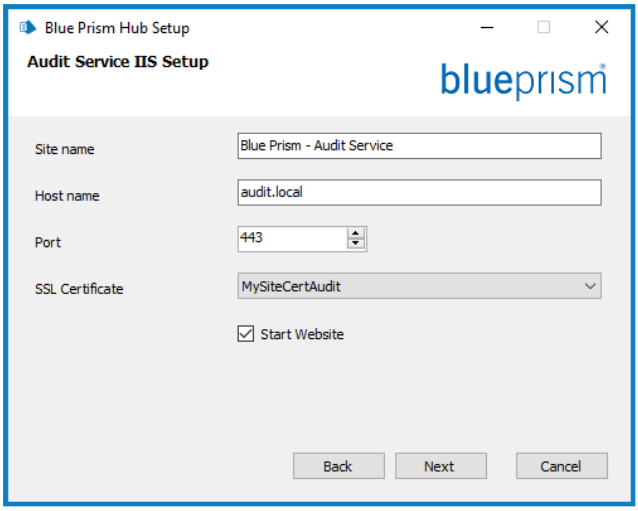
Paso	Página del instalador	Detalles
8		**Conexión SQL de Hub** Configurar los ajustes para la base de datos de Hubal proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

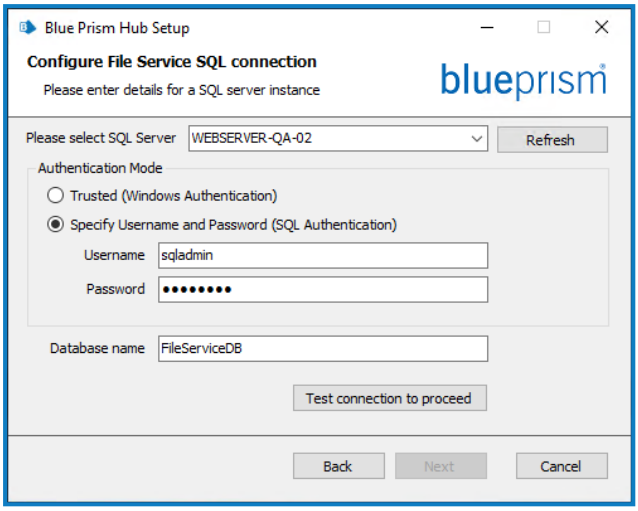
Paso	Página del instalador	Detalles
9		**Configuración de IIS de Hub** Configure el sitio web de Hub. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

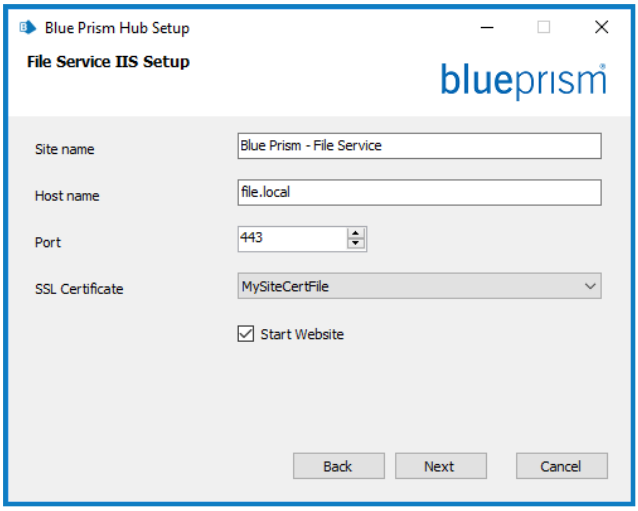
Paso	Página del instalador	Detalles
10		**Conexión SQL de Email Service** Configurar los ajustes para la base de datos de Email Service al proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

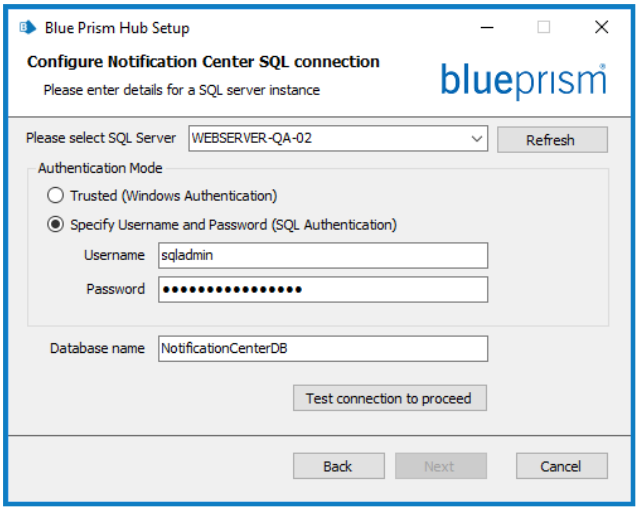
Paso	Página del instalador	Detalles
11		**Email Service Configuración de IIS** Configurar el sitio web de Email Service. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

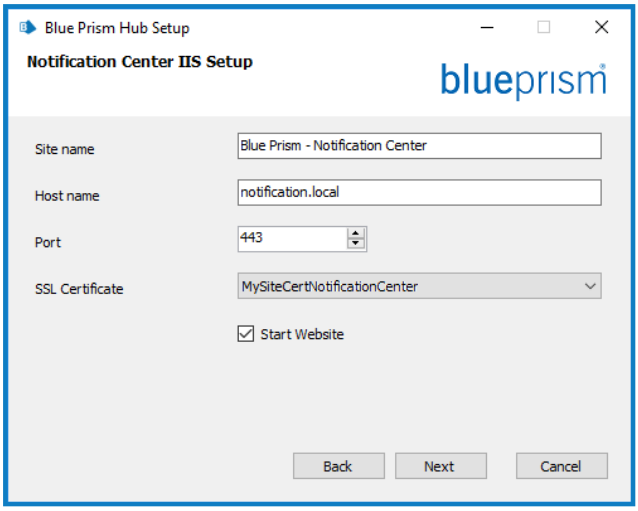
Paso	Página del instalador	Detalles
12		**Configuración de conexión SQL de Audit** Configurar los ajustes para la base de datos de Audit al proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

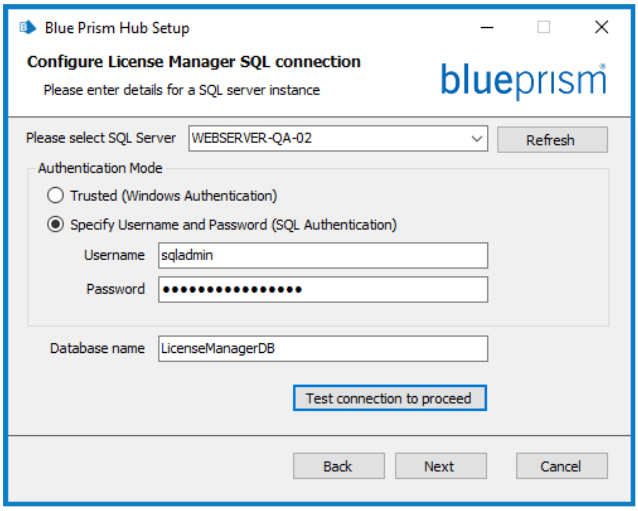
Paso	Página del instalador	Detalles
13		**Configuración de IIS de Audit Service** Configurar el sitio web de Audit Service. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

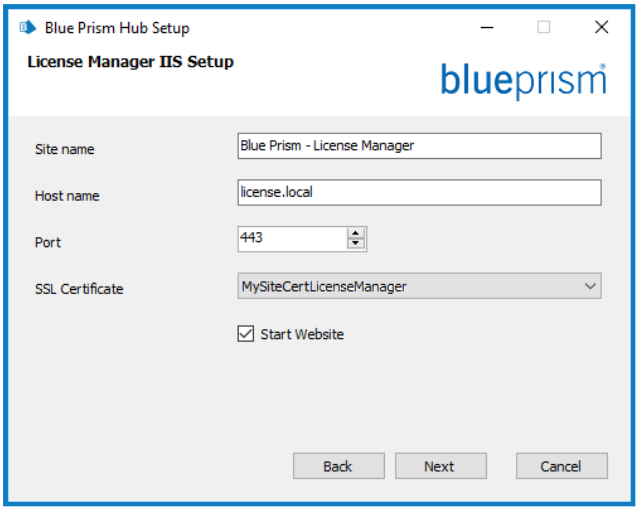
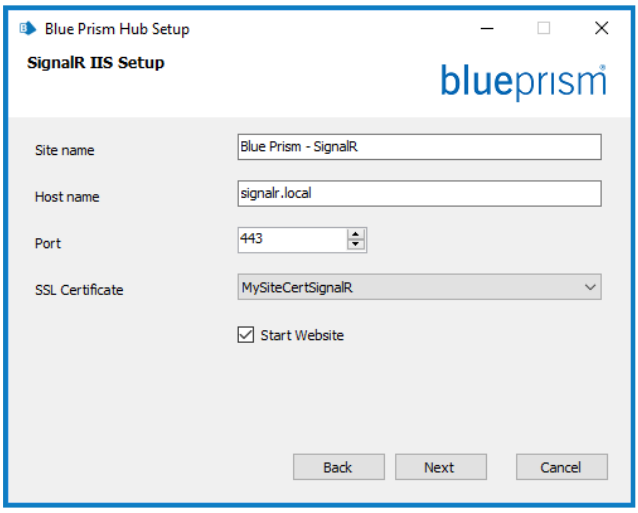
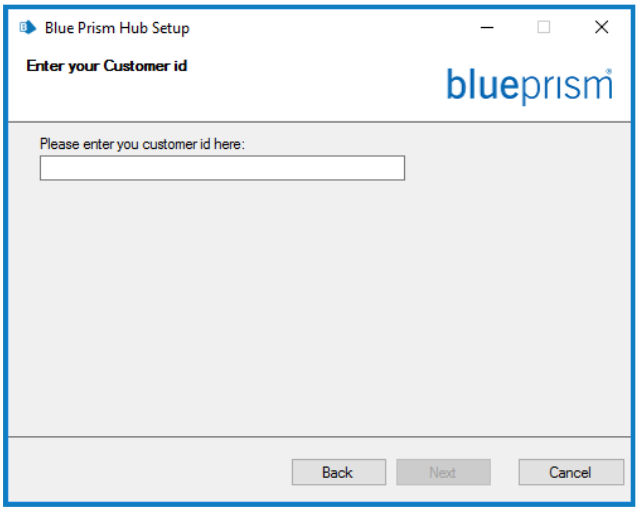
Paso	Página del instalador	Detalles
14		**Configuración de la conexión SQL de File Service** Configurar los ajustes para la base de datos de File Service al proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

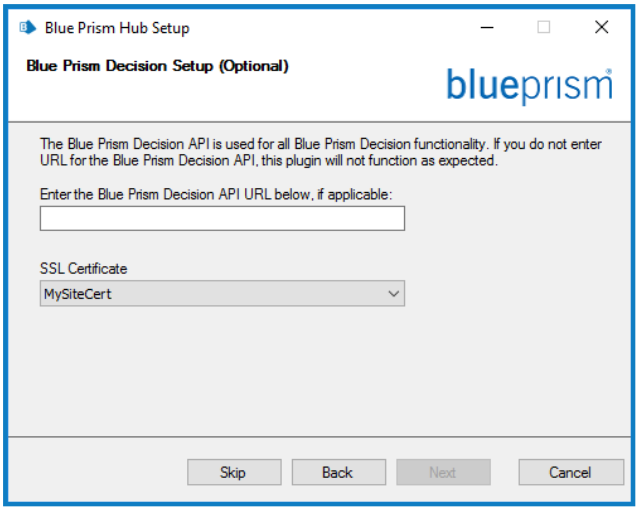
Paso	Página del instalador	Detalles
15		**Configuración de IIS de File Service** Configure el sitio web de File Service. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.

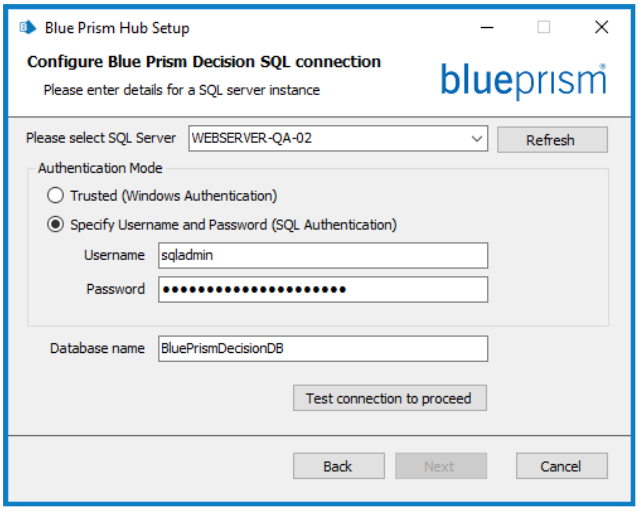
Paso	Página del instalador	Detalles
16		**Conexión SQL de Notification Center** Configurar los ajustes para la base de datos de Notification Centeral proporcionar el nombre de host o la dirección IP del Servidor SQL y las credenciales de la cuenta para crear la base de datos: • Si selecciona **Autenticación de Windows**, la cuenta debe tener los permisos correspondientes. Consulte Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

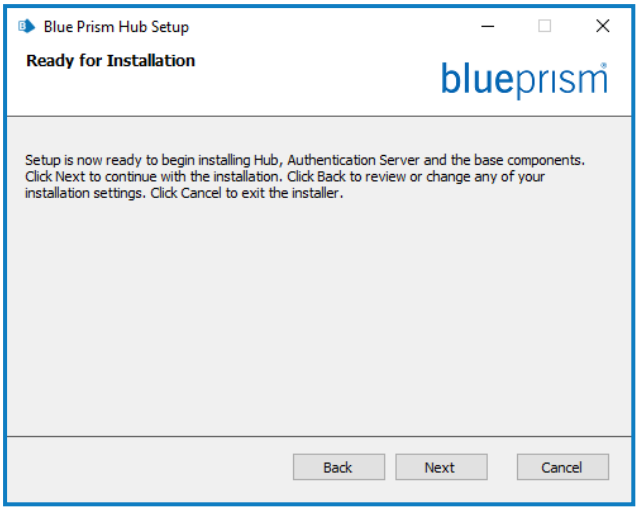
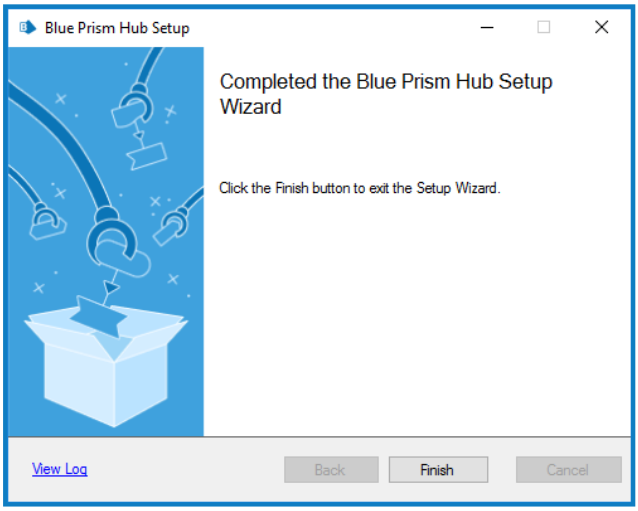
Paso	Página del instalador	Detalles
17		**Configuración de IIS de Notification Center** Configure el sitio web de Notification Center. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • 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
18		**Conexión SQL de License Manager** Configurar los ajustes para la base de datos del License Manageral 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 Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

Paso	Página del instalador	Detalles
19		**Configuración de IIS de License Manager** Configure el sitio web de License Manager. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.
20		**Configuración de SignalR IIS** Configure el sitio web de SignalR. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.
21		**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. Si más adelante compra un complemento con licencia, su Id. de cliente deberá cambiarse dentro del archivo de configuración. Para obtener más información, consulte Solucionar problemas en una instalación de Hub en la página 98.

Paso	Página del instalador	Detalles
22		**Configuración de Blue Prism Decision (opcional)** Si desea usar Blue Prism Decision, debe hacer lo siguiente: • Ingrese la URL para el contenedor del servicio del modelo de Blue Prism Decision seguido del número de puerto. La URL debe tener el formato https://<FQDN>:<port number>, por ejemplo, https://decision.blueprism.com:50051. La URL debe coincidir con el FQDN que se especificó en el certificado. El número de puerto debe coincidir con el puerto que se definió cuando el contenedor se configuró para ejecutarse. Para obtener más información, consulte Instalar Blue Prism Decision. • Seleccione el certificado SSL adecuado. Si no desea utilizar Blue Prism Decision, haga clic en **Omitir**. Aparece la pantalla Listo para la instalación.

Paso	Página del instalador	Detalles
23		**Configurar la conexión SQL de Blue Prism Decision** Configurar los ajustes para la base de datos de Blue Prism Decisional 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 Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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 98 para obtener más detalles.

Paso	Página del instalador	Detalles
24		**Listo para la instalación** Haga clic en **Siguiente** para instalar Hub.
25		**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 98.

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.

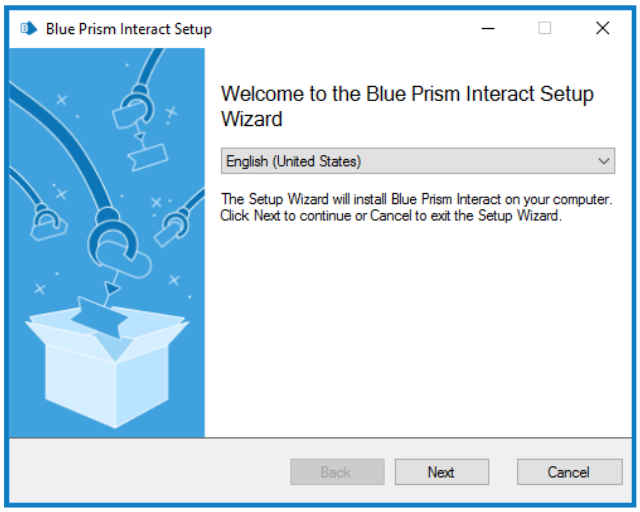
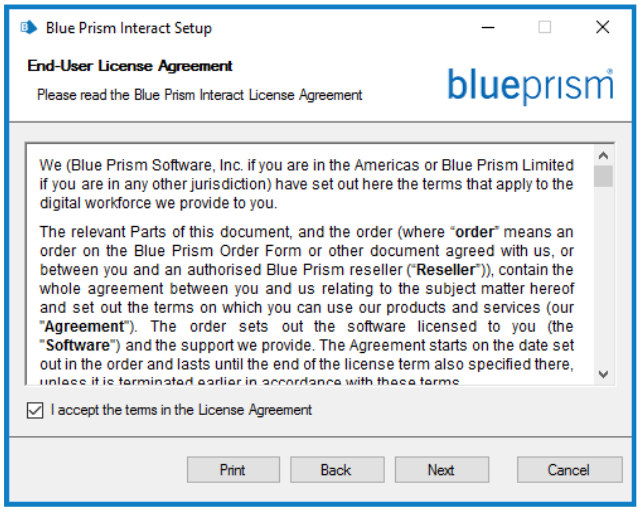
Si su organización no tiene la intención de utilizar la autenticación SAML 2.0 para sus usuarios, no necesita instalar nada más.

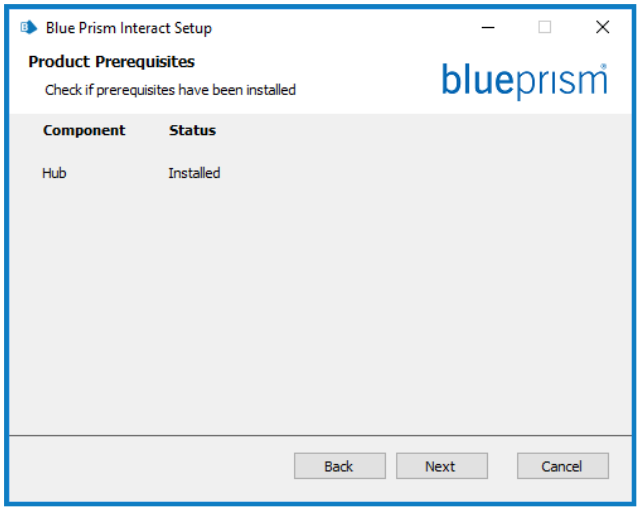
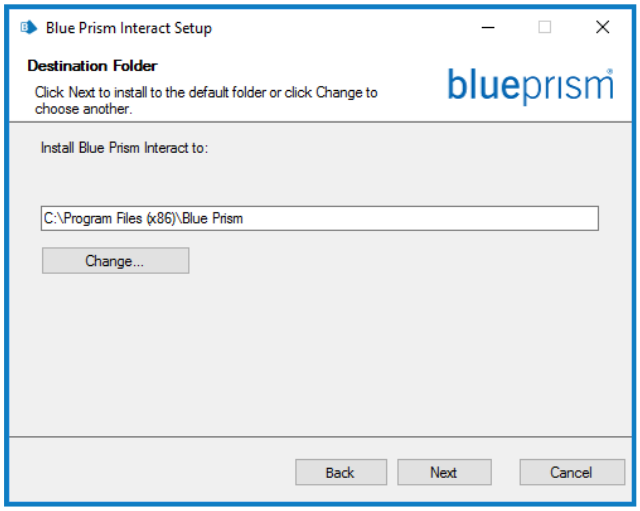
Instalar Blue Prism Interact

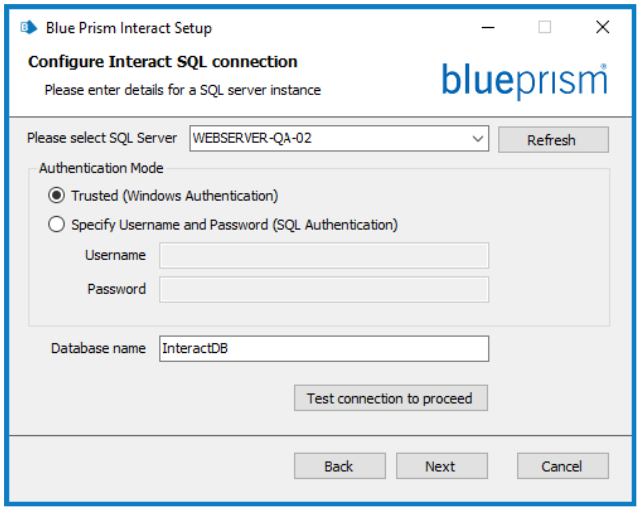
Los siguientes pasos detallan el proceso para instalar el software de Blue Prism Interact. Esto supone que se instaló Blue Prism Hub se ha instalado, lo que incluye el Authentication Server, Hub y otros servicios asociados.

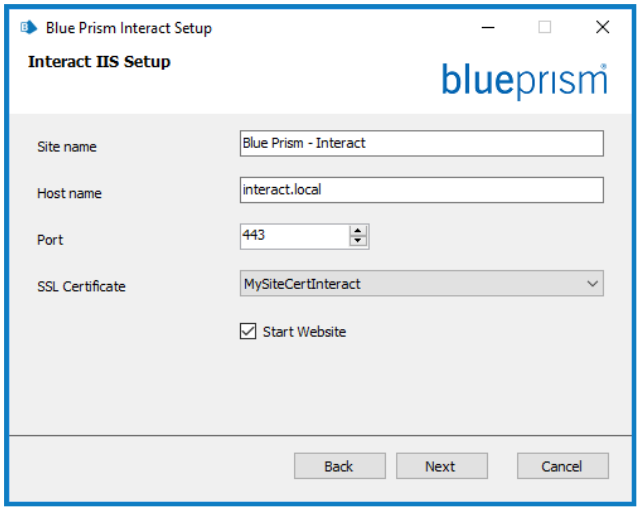
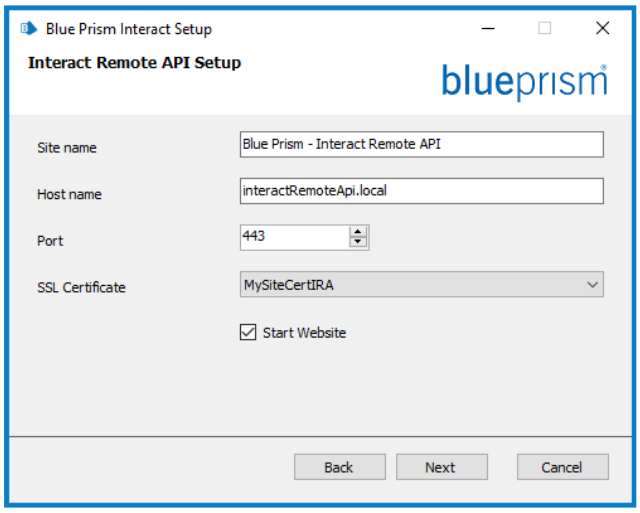
Descargue y ejecute el instalador de Blue Prism Interact, disponible en el portal de Blue Prism, y avance a través del instalador como se muestra a continuación. El instalador se debe ejecutar con derechos de administrador.

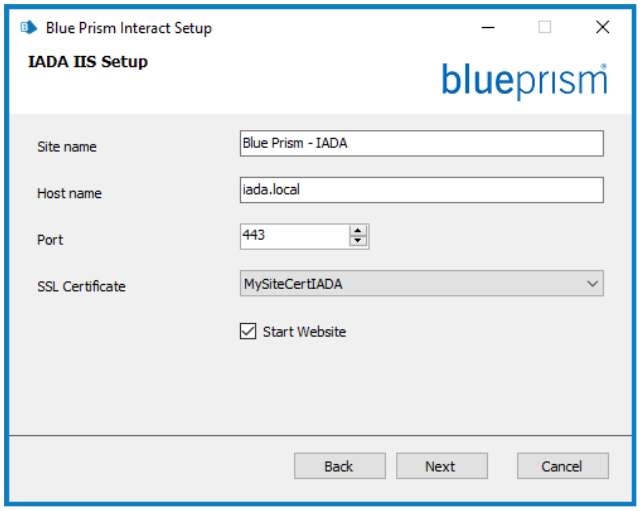
Para ver el proceso de instalación y configuración de Interact, consulte nuestro video de instalación de Blue Prism Interact.

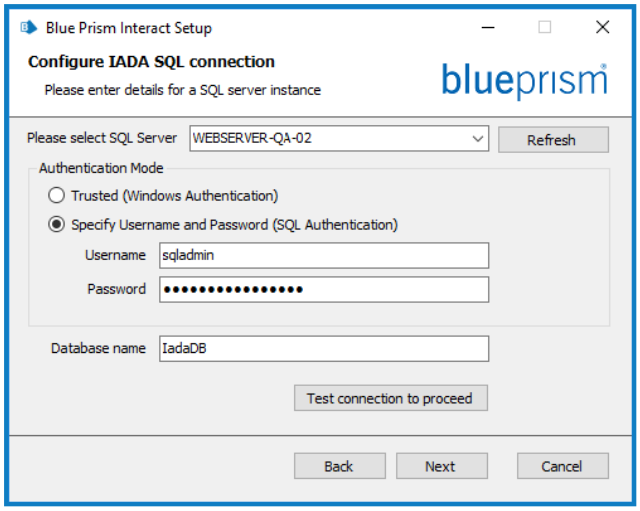
Paso	Página del instalador	Detalles
1		**Bienvenido** Si es necesario, seleccione otro idioma para el instalador de la lista desplegable. El idioma predeterminado es el inglés (Estados Unidos). Haga clic en **Siguiente**.
2		**Contrato de licencia** Lea el EULA y, si acepta los términos, seleccione la casilla de verificación.

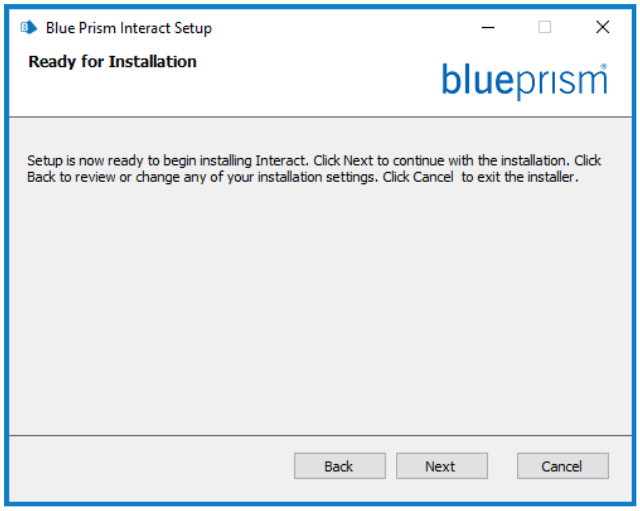
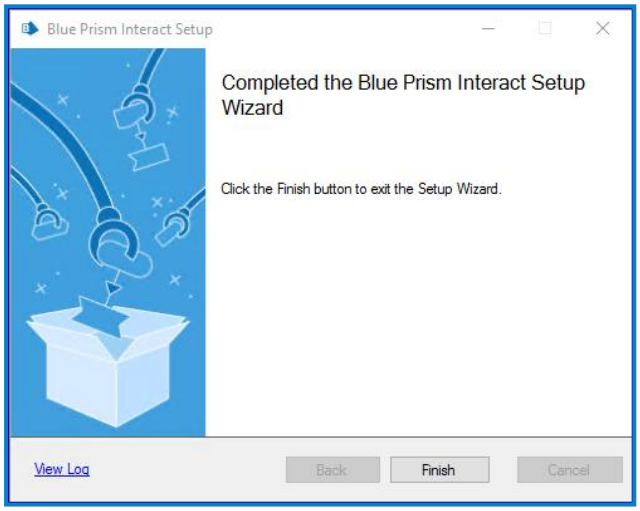
Paso	Página del instalador	Detalles
3		**Requisitos previos del producto** El instalador verifica que se hayan instalado los requisitos previos. Si el instalador determina que falta algún requisito previo, se le notificará. De lo contrario, continúe con la instalación. No puede continuar a menos que se hayan instalado todos los requisitos previos.
4		**Carpeta de destino** Especifique la carpeta de instalación requerida. La ubicación predeterminada es C:\Archivos de programa(x86)\Blue Prism, pero puede elegir otra ubicación con el botón **Cambiar**.

Paso	Página del instalador	Detalles
5		**Ajustar la configuración SQL de Interact** Configurar los ajustes para la base de datos de Interactal 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 Instalación de mediante autenticación de Windows en la página 61 para obtener más información. • Si selecciona **Autenticación de SQL**, 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** a fin de 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 Interact en la página 91 para obtener más detalles.

Paso	Página del instalador	Detalles
6		**Configuración de IIS de Interact** Configure el sitio web de Interact. Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • Deje seleccionado **Iniciar sitio web**, a menos que no desee que el sitio web se inicie automáticamente al final de la instalación.
7		**Configuración de Remote API de Interact** Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • 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		**Configuración de IIS de IADA** Debe hacer lo siguiente: • Ingrese un nombre de sitio. • Ingrese un nombre de host. Esto se utilizará como la URL para el sitio. Asegúrese de considerar su estructura de DNS y de dominio al elegir un nombre de host. • Ingrese el número de puerto. • Seleccione el certificado SSL adecuado. • 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
9		**Ajuste la configuración SQL de IADA** Configurar los ajustes para IADAal 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 Instalación de mediante autenticación de Windows en la página siguiente para obtener más información. • Si selecciona **Autenticación de SQL**, 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** a fin de 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 Interact en la página 91 para obtener más detalles.

Paso	Página del instalador	Detalles
10		**Listo para la instalación** Haga clic en **Siguiente** para instalar Interact.
11		**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. Haga clic en **Finalizar**.

Instalación de mediante autenticación de Windows

La cuenta que se utiliza para ejecutar la instalación debe tener los permisos del Servidor SQL pertinentes para llevar a cabo la instalación; es decir, membresía en los roles de servidor fijos de sysadmin o dbcreator.

Si se eligió la autenticación de Windows durante el proceso de instalación, se debe utilizar una cuenta de servicio de Windows para los grupos de aplicaciones y los servicios con los permisos necesarios para ejecutar las tareas y los procesos durante el funcionamiento normal. La cuenta de servicio de Windows necesitará lo siguiente:

- La capacidad de realizar los procesos de la base de datos SQL, consulte Permisos mínimos de SQL en la página 14.
- Permisos para los certificados requeridos.
- Propiedad sobre grupo de aplicaciones de IIS.
- Propiedad sobre los servicios de Windows instalados por Hub e Interact.

⚠ Debe asignar los grupos de aplicaciones y los servicios para usar las cuentas de Windows antes de crear un entorno en Hub. Si asigna las cuentas después de crear un entorno, puede experimentar problemas de rendimiento; por ejemplo, los formularios creados con el complemento Interact pueden no mostrarse a los usuarios en Interact.

Asignación de la cuenta de servicio de Windows como propietaria en certificados

Se deben otorgar permisos a la cuenta de servicio de Windows para los certificados de BluePrismCloud. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el Administrador de certificados. Para hacerlo, escriba *Certificados* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrar certificados del equipo**.
2. En el panel de navegación, amplíe **Personal** y haga clic en **Certificados**.
3. Siga los pasos a continuación para los certificados BluePrismCloud_Data_Protection y BluePrismCloud_IMS_JWT:
    a. Haga clic con el botón derecho en el certificado y seleccione **Todas las tareas** y haga clic en **Administrar claves privadas...**.

    Aparece el diálogo Permisos para el certificado.

    b. Haga clic en **Agregar** y luego ingrese la cuenta de servicio y haga clic en **Aceptar**.
    c. Con la cuenta de servicio seleccionada en la lista **Nombres de grupo o usuario**, asegúrese de que la opción **Control completo** esté seleccionada en la lista **Permisos para {account name}**.
    d. Haga clic en **Aceptar**.

    La cuenta de servicio ahora tiene acceso al certificado.

Asignación de una cuenta de servicio de Windows al grupo de aplicaciones

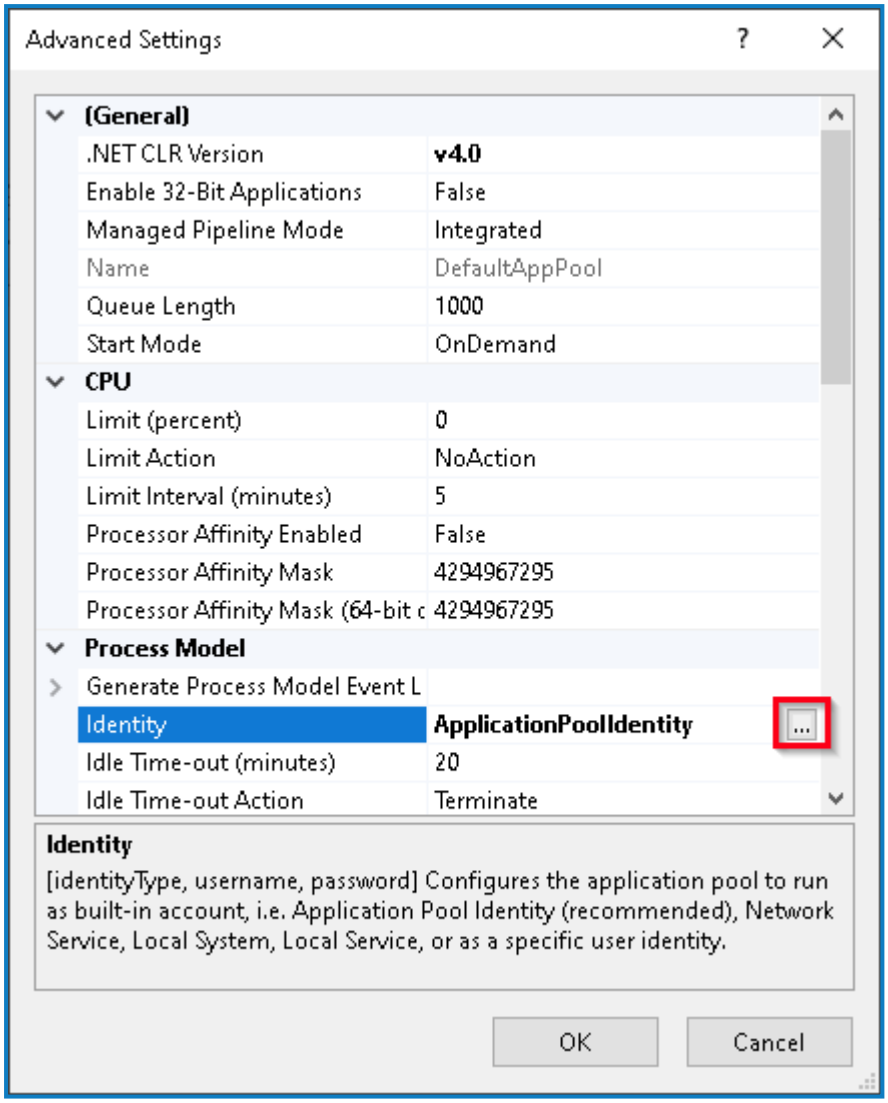
De manera predeterminada, los grupos de aplicaciones se crean con la identidad "ApplicationPoolIdentity". Después de que el instalador haya finalizado, se deberá asignar la cuenta de servicio de Windows para administrar los grupos de aplicaciones. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el administrador de Internet Information Services (IIS).
2. En el panel Conexiones, expanda el host y seleccione **Grupos de aplicaciones**.
3. Revise los valores de la columna **Identidad**.

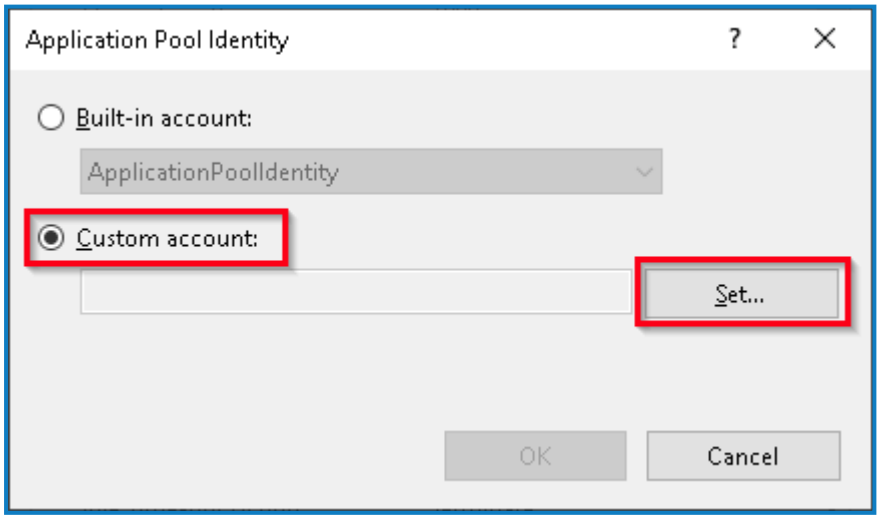
    La identidad de un grupo de aplicaciones debe coincidir con la cuenta de servicio de Windows específica.
4. Para cualquier grupo de aplicaciones que tenga *ApplicationPoolIdentity* en la columna **Identidad**, haga clic con el botón derecho en la fila y seleccione **Configuración avanzada...**.

    Aparece el diálogo Configuración avanzada.

5. Seleccione la configuración **Identidad** y luego haga clic en el botón **...** (elipsis):



6. En el diálogo Identidad del grupo de aplicaciones, seleccione la opción **Cuenta personalizada** y haga clic en **Establecer...**.



Aparece el diálogo Establecer credenciales.

7. Ingrese las credenciales para la cuenta de servicio de Windows requerida y haga clic en **Aceptar**.

8. Repita el procedimiento para cualquier grupo de aplicaciones que necesite cambiar.
9. Reinicie el servicio de RabbitMQ.
10. Reinicie todos los grupos de aplicaciones.
11. Reinicie Internet Information Services.

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.

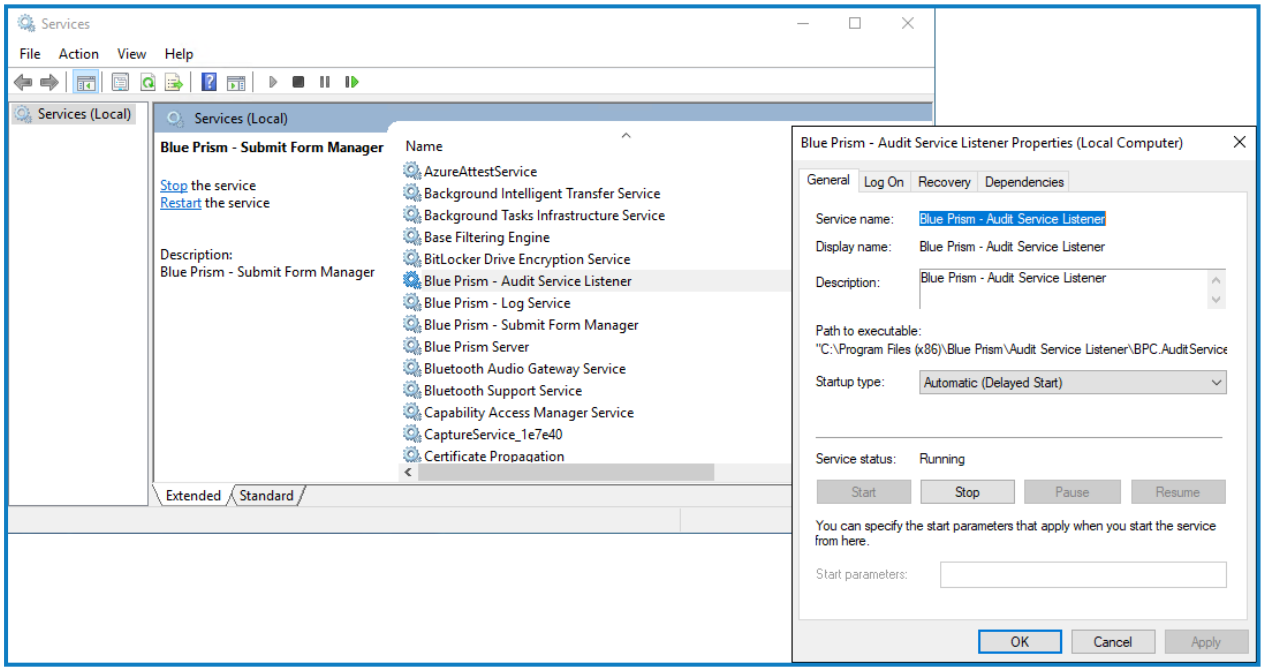
Asignación de una cuenta de servicio de Windows a un servicio

La cuenta de servicio de Windows debe asignarse para administrar los siguientes servicios:

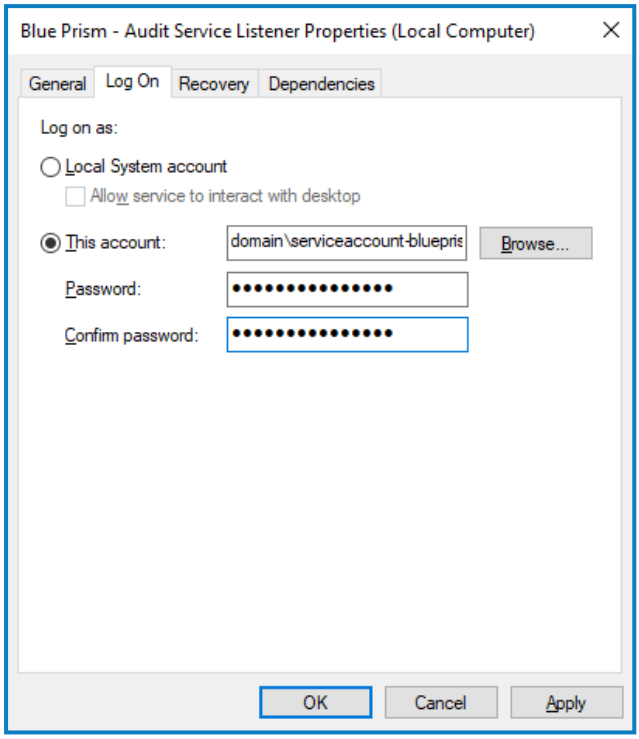
- Blue Prism: oyente del servicio de auditoría
- Blue Prism: servicio de registro
- Blue Prism: Submit Form Manager

Para hacerlo, siga estos pasos:

1. En el servidor web, abra Servicios.
2. Haga clic derecho en el servicio y, a continuación, haga clic en **Propiedades**.



3. En la pestaña Iniciar sesión, seleccione **Esta cuenta** y luego ingrese el nombre de la cuenta o haga clic en **Examinar** para encontrar la cuenta que desea usar.



4. Ingrese la contraseña de la cuenta y haga clic en **Aceptar**.
5. En la ventana Servicios, haga clic derecho en el servicio y, a continuación, haga clic en **Reiniciar**.
6. Repita este procedimiento para los otros servicios de Blue Prism.

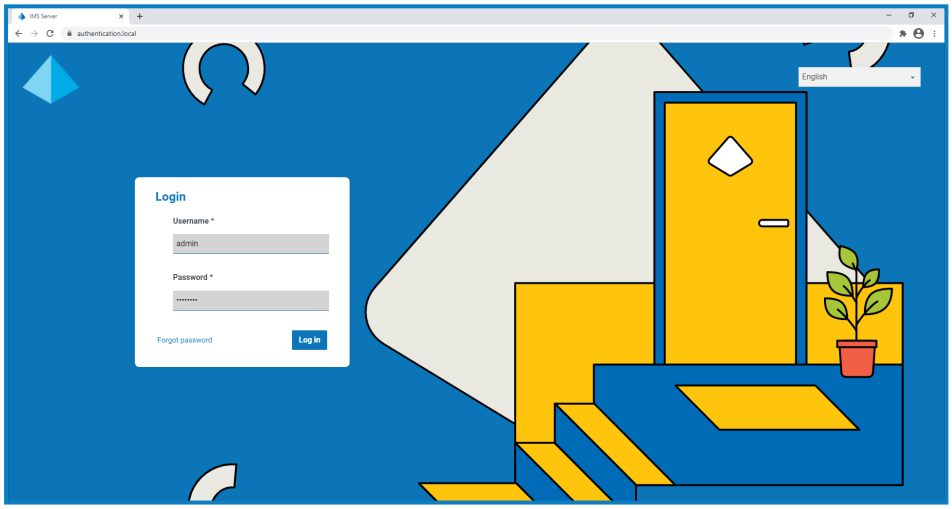
Configuración inicial de Hub

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

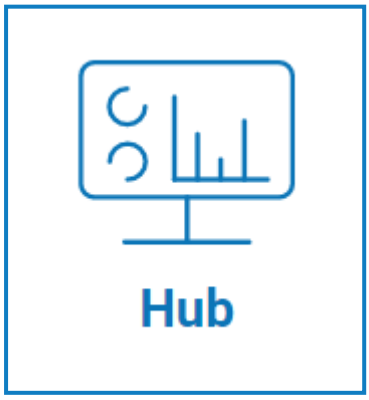
Cuando abre la página de inicio de sesión para Authentication Server, la configuración de localización se aplica automáticamente desde su navegador web. La página de inicio de sesión y Hub se muestran en el idioma más compatible con los ajustes de idioma configurados en el navegador. Si el idioma seleccionado 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 Authentication Server, en nuestro ejemplo: https://authentication.local



2. Inicie sesión con las credenciales predeterminadas.
   - **Nombre de usuario:** admin
   - **Contraseña**: Qq1234!!
3. Haga clic en **Hub** para iniciar el sitio web de Hub.



4. Cambie la contraseña predeterminada por una nueva contraseña segura.
   a. En Hub, haga clic en el ícono de perfil para abrir la página Configuración y luego haga clic en **Perfil**.
   b. Haga clic en **Actualizar contraseña**.

      Aparece el cuadro de diálogo Actualice su contraseña.
   c. Ingrese la contraseña de administrador actual, luego ingrese y repita una nueva contraseña.
   d. Haga clic en **Actualizar**.

      Se cambia la contraseña del administrador.

Configuración de base de datos

⚠ Si instaló su entorno para usar la autenticación de Windows, debe asignar los grupos de aplicaciones y los servicios para usar las cuentas de Windows antes de crear un entorno en Hub. De lo contrario, es posible que experimente problemas de rendimiento; por ejemplo, los formularios creados con el complemento Interact pueden no mostrarse a los usuarios en Interact. Para obtener más información, consulte Instalación de mediante autenticación de Windows en la página 61.

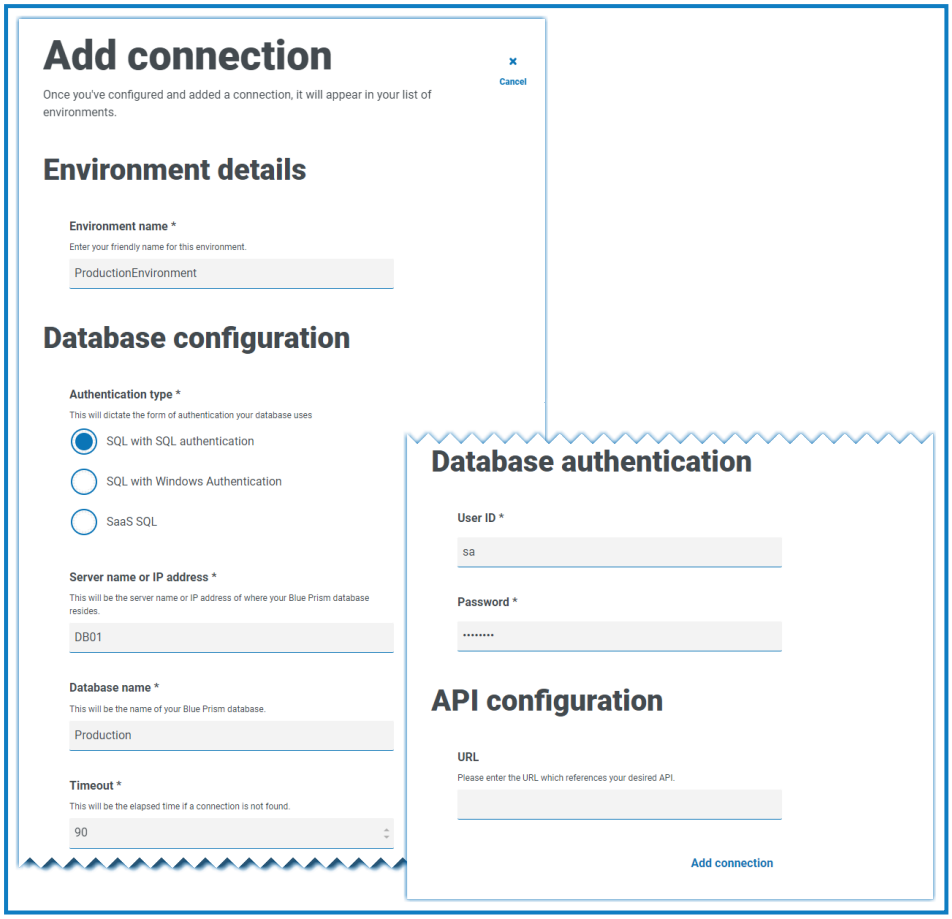
Todas las bases de datos instaladas como parte del instalador de Hub utilizan el cifrado SSL. Para que Hub se conecte correctamente a la base de datos de Blue Prism, la base de datos de Blue Prism también debe configurarse para usar cifrado SSL. Para obtener más información, consulte Requisitos previos en la página 7.

Para configurar el acceso a la base de datos de Blue Prism, haga lo siguiente:

1. Haga clic en el ícono de su perfil para abrir la página Configuración y luego haga clic en **Administrador de entorno**.

   Aparece la página Administración del entorno.

2. Haga clic en **Agregar conexión** e ingrese los detalles de la base de datos de Blue Prism. A continuación se muestra un ejemplo:



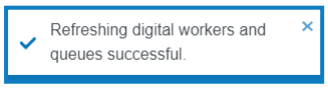
El valor de tiempo límite es en segundos.

3. Haga clic en **Agregar conexión** para guardar los detalles.

   La conexión se crea y se muestra en el administrador de entorno.

4. En el administrador de entorno, haga clic en el ícono de actualización en su nueva conexión. Esto actualiza la información en Hub con la fuerza laboral digital y las colas guardadas en la base de datos.

   Si la conexión se realiza correctamente, aparece 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 98 para obtener más información.

Crear un administrador

Deberá crear una cuenta de administrador con información válida para finalizar la configuración de Hub. No debe usar la cuenta de administrador genérica para completar la configuración, esto se debe a lo siguiente:

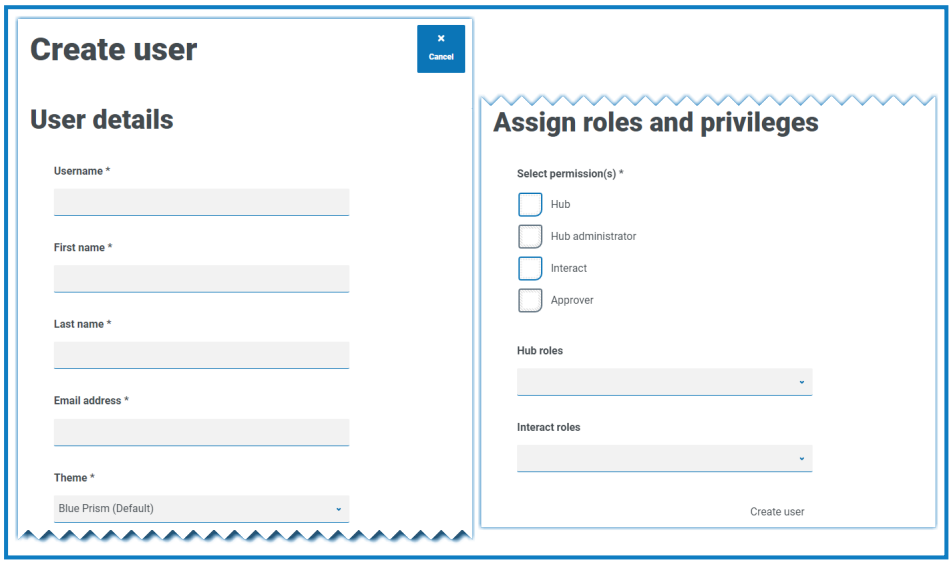
- Se necesita una dirección de correo electrónico real para probar la configuración de correo electrónico.

- Para un registro de auditoría completo, se debe utilizar un usuario designado para realizar cambios de configuración, en lugar de la cuenta genérica.

Para crear un nuevo administrador, haga lo siguiente:

1. Haga clic en el ícono de su perfil para abrir la página Configuración y luego haga clic en **Usuarios**.
2. En la página Usuarios, haga clic en **Agregar usuario**.

   Aparece la sección Crear usuario.



3. Ingrese los siguientes detalles:
   - Nombre de usuario
   - Nombre
   - Apellido
   - Dirección de correo electrónico
4. Seleccione los permisos de **Hub** y **Administrador de Hub**.
5. Haga clic en **Crear usuario**.

   Aparece el diálogo Crear contraseña.
6. Seleccione **Actualizar la contraseña del usuario de forma manual**.

   Las contraseñas deben obedecer las restricciones dentro de Hub.
7. Haga clic en **Continuar** y siga las instrucciones en pantalla.
8. Finalmente, haga clic en **Crear** para crear el usuario.

   El nuevo usuario aparece en la lista de usuarios.
9. Cierre sesión en Hub y vuelva a iniciar sesión con su nueva cuenta.

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 configurar los ajustes de correo electrónico, debe iniciar sesión con el usuario que creó en Crear un administrador en la página 68. Esto se debe a que el proceso de configuración envía un correo electrónico de prueba y, por lo tanto, requiere un usuario con una dirección de correo electrónico activa.

Puede configurar sus ajustes de correo electrónico mediante uno de los siguientes métodos de autenticación:

- **Nombre de usuario y contraseña:** este método de autenticación requiere la siguiente información:
  - **Host SMTP:** la dirección de su host SMTP.
  - **Número de puerto:** el número de puerto utilizado por el servidor de correo saliente.
  - **Correo electrónico del remitente:** la dirección de correo electrónico que se utiliza al enviar correos electrónicos. Los destinatarios de correo electrónico verán esto como la dirección de origen.
  - **Cifrado:** el método de cifrado utilizado por el servidor de correo electrónico para enviar los correos electrónicos.
  - **Nombre de usuario:** el nombre de usuario para la autenticación SMTP.
  - **Contraseña:** la contraseña de la cuenta.
  - **Destinatario de correo electrónico de prueba:** el correo electrónico de prueba se enviará a esta dirección de correo electrónico. Esto se predetermina a la dirección de correo electrónico del usuario que realiza los cambios y no se puede cambiar.
- **Microsoft OAuth 2.0:** este método de autenticación requiere la siguiente información:
  - **Correo electrónico del remitente:** la dirección de correo electrónico que se utiliza al enviar correos electrónicos. Los destinatarios de correo electrónico verán esto como la dirección de origen.
  - **Id. de la aplicación:** esta información es la id. de la aplicación (cliente) definida en Azure AD y se la proporcionará su equipo de soporte de TI.
  - **Id. del directorio**: esta información es la id. del directorio (suscriptor) definida en Azure AD y se la proporcionará su equipo de soporte de TI.
  - **Secreto del cliente:** este es el secreto del cliente generado por Azure AD, se lo proporcionará su equipo de soporte de TI y controla el proceso de autenticación

    > Para obtener información sobre cómo encontrar estos detalles en Azure AD, consulte la documentación de Microsoft.
  - **Destinatario de correo electrónico de prueba:** el correo electrónico de prueba se enviará a esta dirección de correo electrónico. Esto se predetermina a la dirección de correo electrónico del usuario que realiza los cambios y no se puede cambiar.

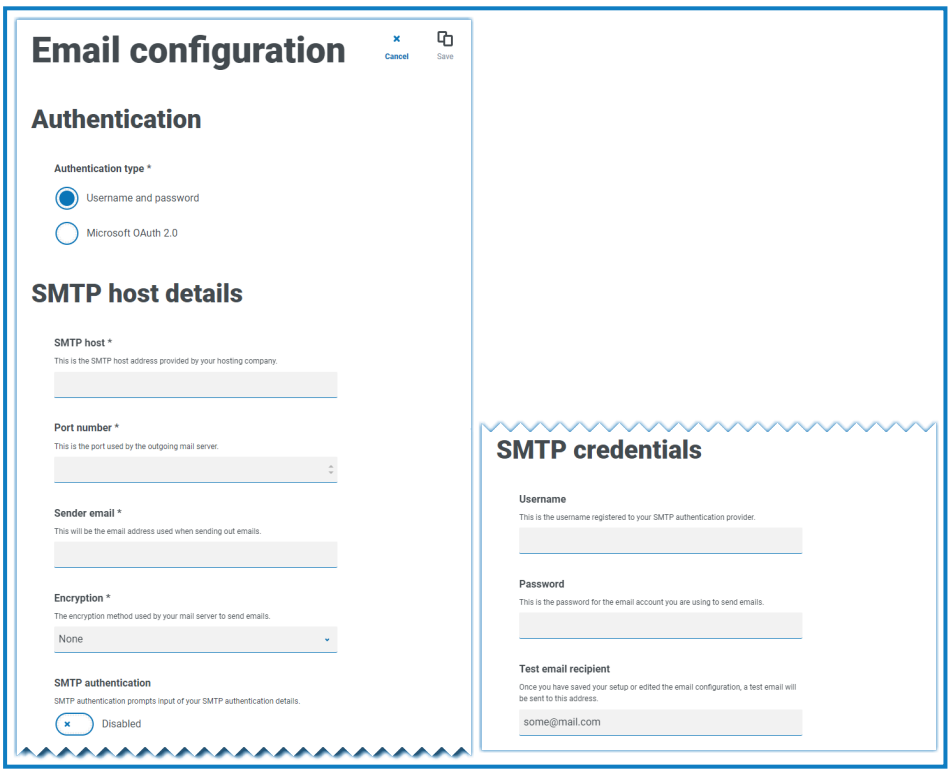
> Si está utilizando Microsoft OAuth 2.0, el permiso Mail.Send en Directorio Activo de Azure debe estar habilitado. Esto se encuentra en la pestaña Permiso de API en las propiedades de la aplicación en Directorio Activo de Azure. Para obtener más información, consulte Solucionar problemas en una instalación de Hub en la página 98.

Para configurar los ajustes de correo electrónico, haga lo siguiente:

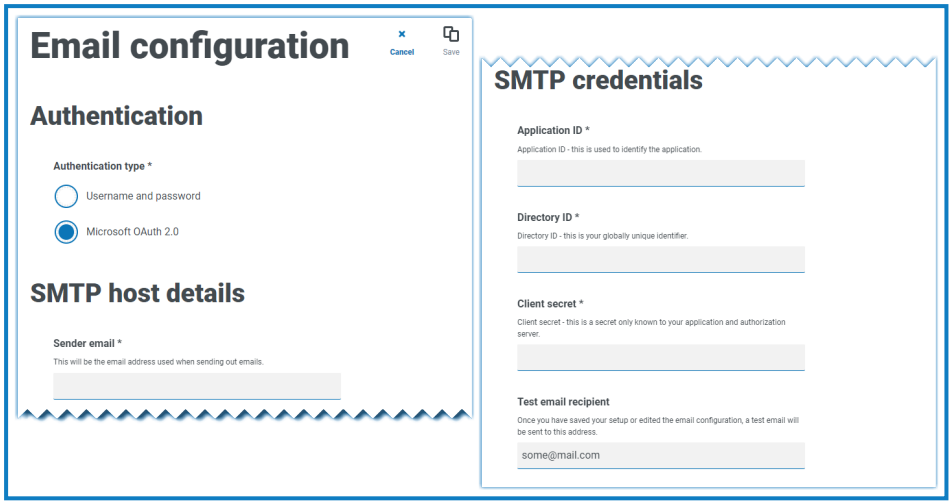
1. Haga clic en el ícono de su perfil para abrir la página Configuración y luego haga clic en **Configuración de correo electrónico**.
2. Haga clic en **Editar**.
3. Seleccione el tipo de autenticación que desea utilizar.

   Los campos de la página dependen de su selección, como se detalla anteriormente. Si selecciona:

   - **Nombre de usuario y contraseña**, la página Configuración de correo electrónico se muestra de la siguiente manera:



- **Microsoft OAuth 2.0**, la página Configuración de correo electrónico se muestra de la siguiente manera:



4. Ingrese la información requerida.
5. Haga clic en **Guardar**.

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 98 para obtener más información.

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

Configurar Authentication Server

Authentication Server permite a los usuarios iniciar sesión en Blue Prism, Hub e Interact con las mismas credenciales. Authentication Server es compatible con Blue Prism 7.0 y posterior.

Con Blue Prism 6

Si su organización utiliza Blue Prism 6:

- Authentication Server no se puede usar para autenticar usuarios entre Blue Prism y Hub. Los usuarios pueden iniciar sesión en Blue Prism y Authentication Server con cuentas independientes.
- Debe configurar los ajustes de autenticación en Hub. Consulte Configuración de la autenticación en la página siguiente.

Con Blue Prism 7

Si su organización utiliza Blue Prism 7, debe considerar si su organización desea que los usuarios utilicen la misma cuenta para las aplicaciones de Blue Prism.

- Si su organización desea utilizar las mismas cuentas de usuario:
  1. Configure Authentication Server; consulte la Guía de configuración de Authentication Server.
  2. Configure los ajustes de autenticación en Hub. Consulte Configuración de la autenticación en la página siguiente.
- Si su organización no desea utilizar las mismas cuentas de usuario, solo configure los ajustes de autenticación en Hub. Consulte Configuración de la autenticación en la página siguiente.

Para ver los pasos de configuración, mire nuestro video Configurar Authentication Server.

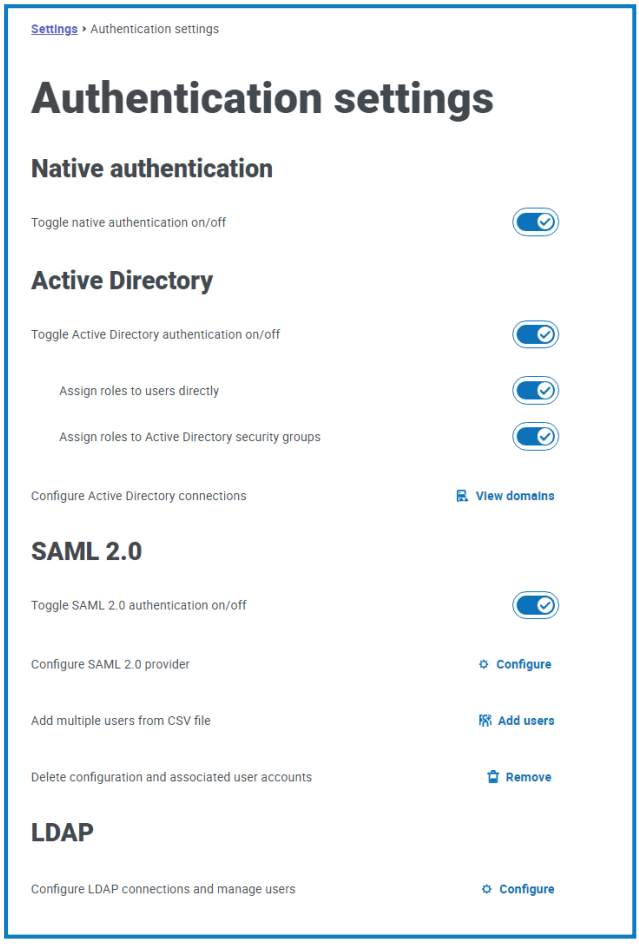
Configuración de la autenticación

La configuración de autenticación para un entorno de Hub se puede definir en la página Configuración de autenticación.

Para definir la configuración de autenticación:

1. Haga clic en el ícono de su perfil para abrir la página Configuración y luego haga clic en **Configuración de autenticación**.

   Aparece la página Configuración de autenticación.



2. Seleccione los tipos de autenticación que desee usar y las opciones relacionadas si es necesario.
   - **Autenticación nativa**: está habilitada de forma predeterminada en nuevos entornos o al actualizar Hub.
   - **Directorio Activo**: esto solo se puede habilitar si el servidor que aloja Authentication Server es miembro de un dominio de Directorio Activo. Si está habilitado, también se pueden configurar dominios de Directorio Activo y administración de roles de usuario.
   - **SAML 2.0**: esta opción solo es visible en la página Configuración de autenticación si la extensión de Authentication Server SAML 2.0 se ha instalado en el servidor web host donde está instalado Authentication Server.
   - **LDAP**: para habilitar la autenticación de LDAP, se debe crear al menos una conexión de LDAP.

Según los requisitos de su organización, tiene las siguientes opciones:

- Habilitar todos los tipos de autenticación.
- Desactive uno o varios tipos de autenticación; esto solo puede hacerse mientras haya al menos un usuario administrador en el sistema que esté configurado para iniciar sesión con un tipo de autenticación diferente a los tipos que se están deshabilitando.

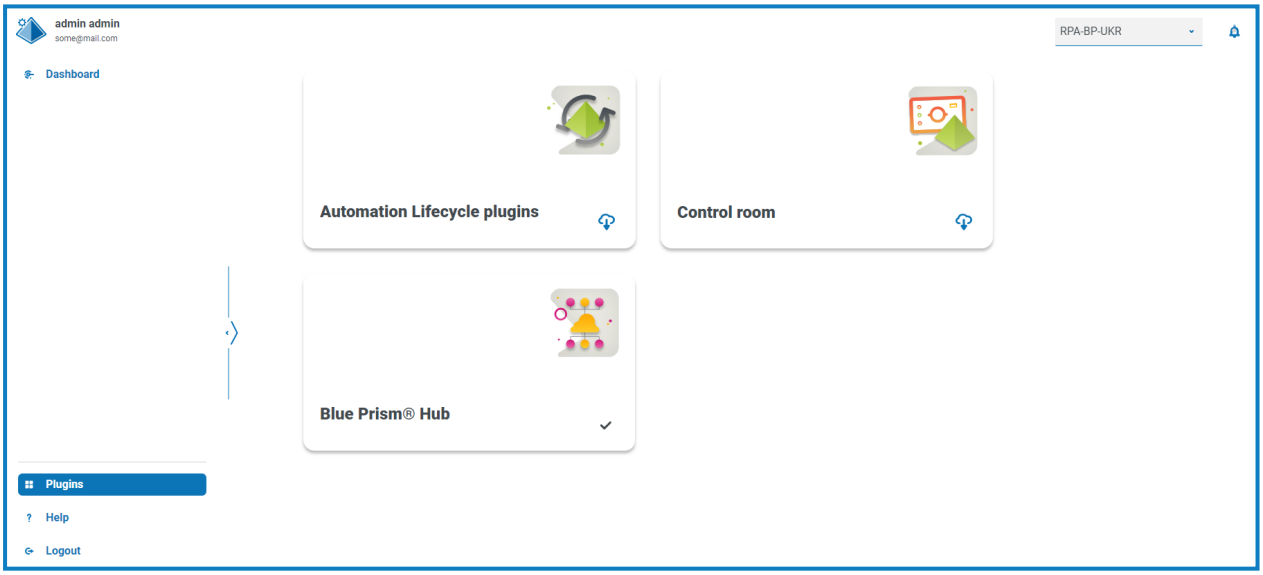
Para obtener más información sobre la forma de configurar los ajustes de autenticación, consulte la Guía del administrador de Hub.

Instalar complementos

Como parte de la instalación, Hub instala automáticamente los complementos de Hub. Sin embargo, si desea utilizar ALM o Interact, primero deberá instalar el complemento de procesos empresariales disponible en forma gratuita.

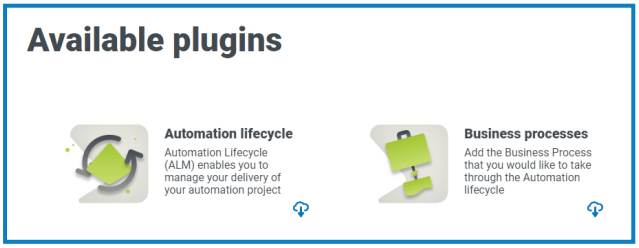
Para ver este paso de instalación, vea nuestro video de instalación del complemento de procesos empresariales.

1. Inicie sesión en Hub.
2. Haga clic en **Complementos** para abrir el repositorio de complementos.



3. Haga clic en **Ciclo de vida de la automatización**.

   Aparecen los componentes del complemento disponibles.



4. Haga clic en el ícono de descarga en la esquina inferior del mosaico **Procesos empresariales** para iniciar la instalación.

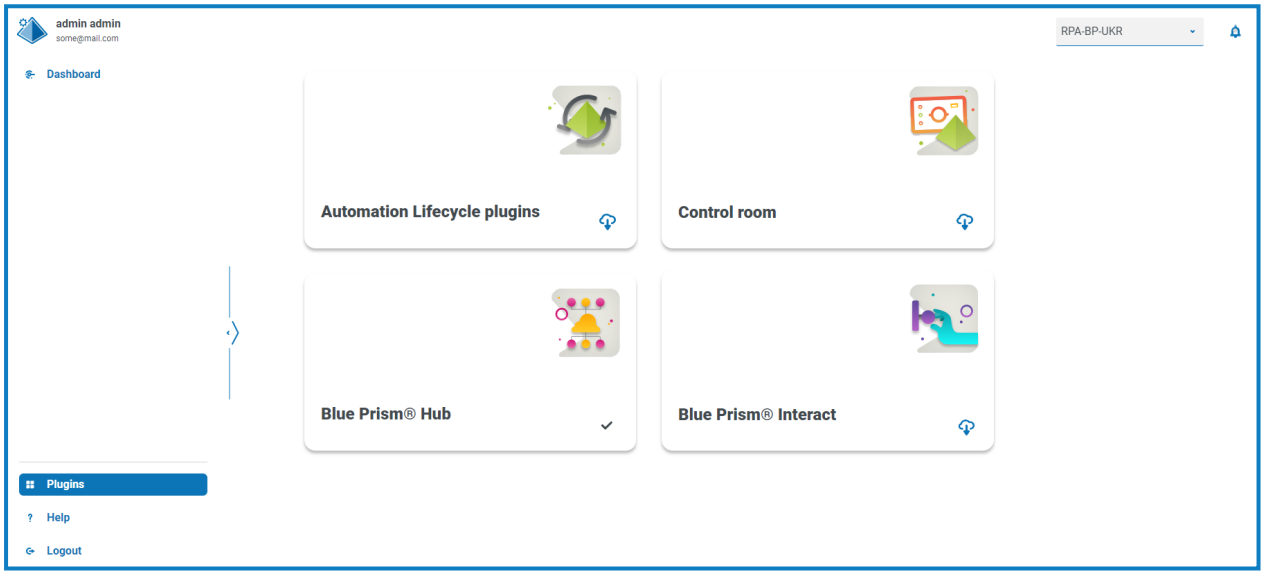
   El sitio se reinicia.

Instalar el complemento Interact

El complemento Interact depende del complemento de procesos empresariales, ya que no puede crear un formulario sin un proceso empresarial. El complemento de procesos empresariales se proporciona gratis dentro del repositorio de complementos y se puede encontrar en Automation Lifecycle Management (ALM). Asegúrese de haber instalado el complemento de procesos empresariales antes de instalar Interact. Para obtener más información, consulte Instalar complementos en la página anterior.

El complemento Interact debe instalarse con la licencia asociada.

1. Inicie sesión en Hub.
2. Haga clic en **Complementos** para abrir el repositorio de complementos.



3. En el tile **Interact**, haga clic en el ícono de descarga en la esquina inferior para iniciar la instalación y aplicar la licencia necesaria.

   El sitio se reinicia.

Configurar Digital Workers

Esta sección proporciona los pasos que se deben realizar con cada Digital Worker para permitirle conectarse a Interact.

Los pasos que se deben completar son los siguientes:

- Instalar certificados SSL
- Configurar la red
- Instalar y configurar el servicio de API web de Interact

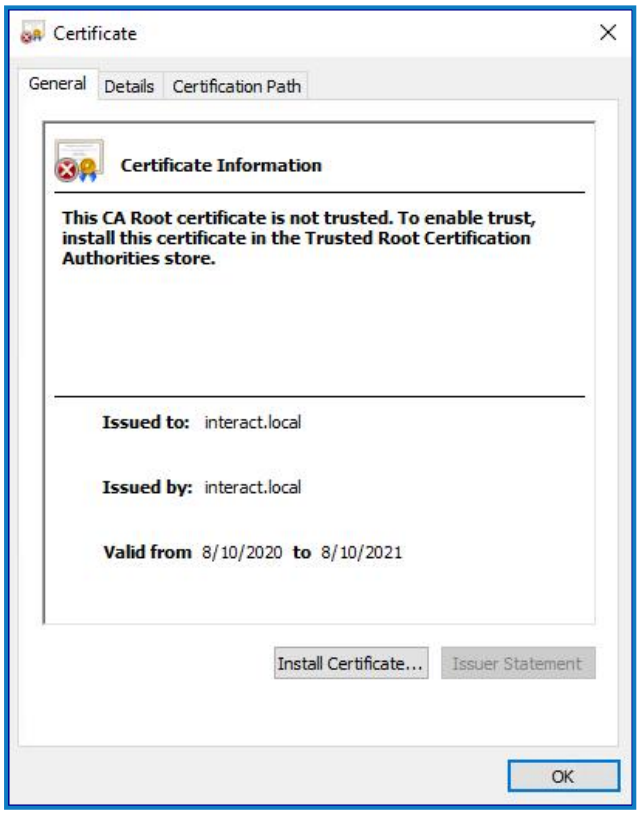
Estas instrucciones suponen que el usuario está familiarizado con Blue Prism.

Instalar certificados SSL

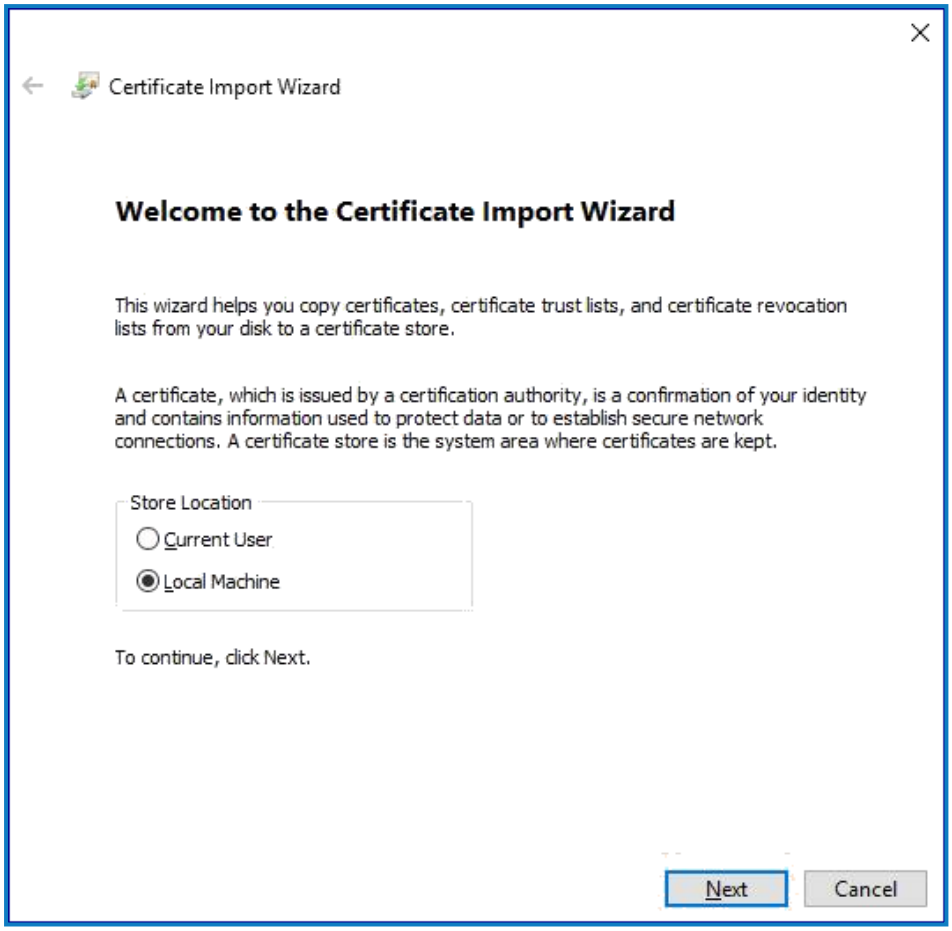
En cada Digital Worker, inicie sesión y copie los certificados SSL para Interact, IADA, Remote API de Interact, Authentication Server y SignalR.

> Como esto se debe realizar en cada Digital Worker, se pueden utilizar herramientas de terceros o GPO para realizar esta tarea a escala.

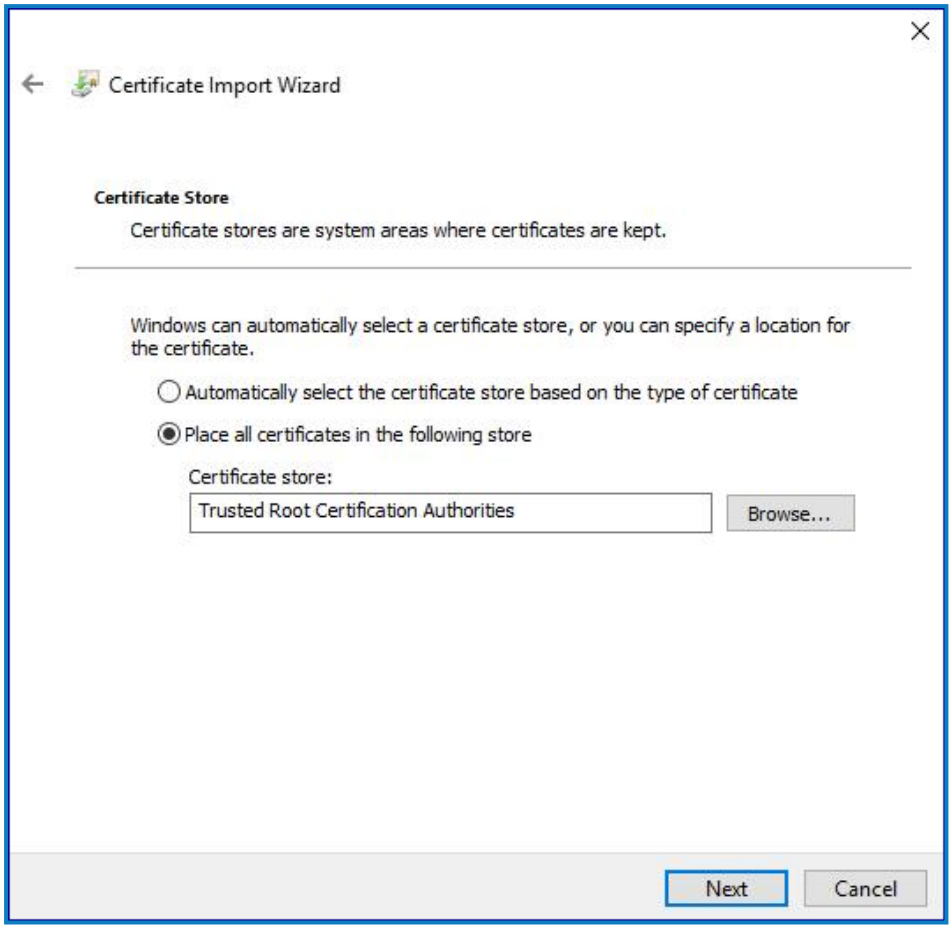
1. Haga doble clic en cada certificado SSL y seleccione **Instalar certificado**.



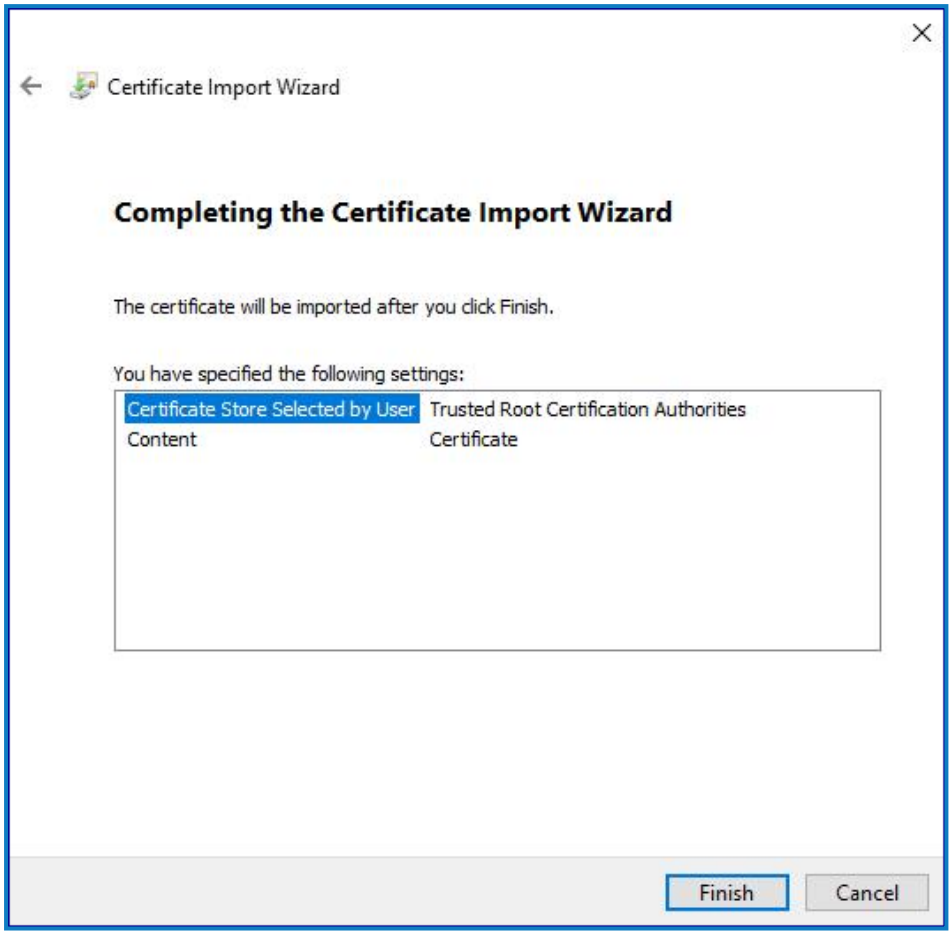
2. Cambie la ubicación de almacenamiento a **equipo local**.



3. Seleccione **Colocar todos los certificados en el siguiente almacén**, haga clic en **Examinar** y seleccione **Almacén de Autoridades de certificados de confianza**.



4. Compruebe que el certificado SSL esté asignado en el almacén correcto y luego haga clic en **Finalizar**.



5. Reconozca el mensaje para confirmar que la tarea se realizó correctamente.
6. Repita los pasos para todos los certificados SSL.

Configurar la red

Es importante que se pueda acceder al sitio web de Interact y, en particular, al sitio de Remote API de Interact.

Esto depende de la estructura de arquitectura que se implementó, por lo que ya podría establecerse si los sistemas se unen al dominio y la organización de TI configuró los servidores. Como alternativa, es posible que se deba ajustar el archivo de hosts locales para garantizar que se pueda acceder a los sitios.

Los sitios que deben ser accesibles desde cada Digital Worker son los siguientes:

Sitio web en IIS	URL predeterminada
Blue Prism: Interact	https://interact.local
Blue Prism: Authentication Server	https://authentication.local
Blue Prism: IADA	https://iada.local
Blue Prism: Remote API de Interact	https://interactremoteapi.local
Blue Prism: SignalR	https://signalr.local

Authentication Server y SignalR se instalan como parte de la instalación de Hub.

Instalar y configurar el servicio de API web de Interact

Blue Prism e Interact se comunican a través de la Remote API de Blue Prism Interact. Para usar esta API, el archivo de lanzamiento del servicio de API de Interact debe importarse a Blue Prism; esto incluye un servicio de API web y VBO. Una vez importado, deberá actualizarse con la URL base y los códigos de autorización adecuados para permitir la comunicación segura.

En el servicio web hay una serie de acciones definidas; consulte la Guía del usuario del servicio de API web de Interact para obtener más información.

Si desea configurar Blue Prism para usar Interact, debe:

1. Configurar una cuenta de servicio en Hub y generar una clave secreta.
2. Importar el VBO del servicio de API de Interact a Blue Prism.
3. Configurar las credenciales para la cuenta del servicio de API web de Interact en Blue Prism.
4. Configurar el servicio API de Interact para permitir que Blue Prism se comunique con Interact.

Configurar una cuenta de servicio

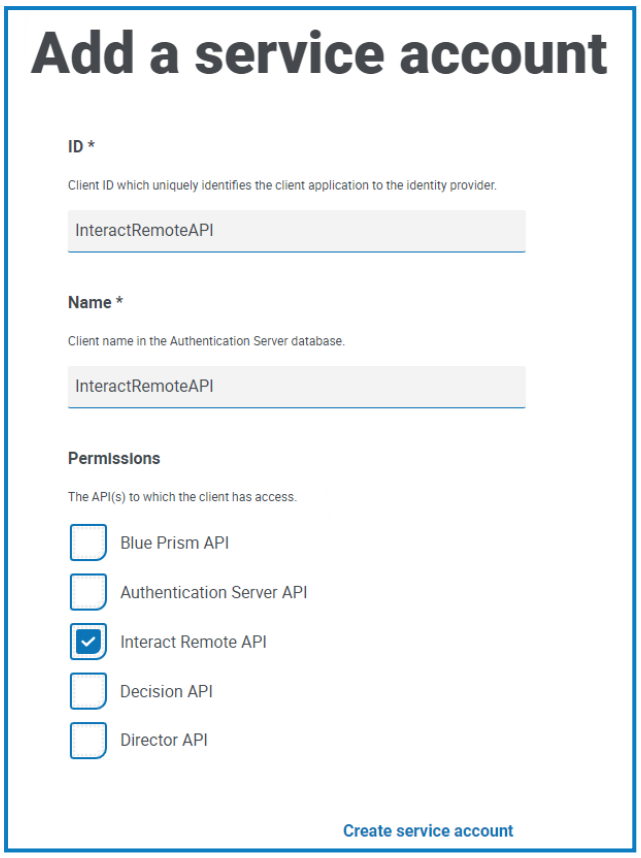
Para configurar las credenciales de Remote API de Interact en Blue Prism, se requiere una clave secreta. Esta se genera a partir de la cuenta de servicio asociada en Hub para su uso con Remote API de Interact. Si pierde la clave, puede volver a generar otra desde la cuenta de servicio. Para obtener más información, consulte Cuentas de servicio.

Para crear una cuenta de servicio, haga lo siguiente:

1. En Blue Prism Hub, en la página Cuentas de servicio, haga clic en **Agregar cuenta**.
2. Ingrese una id. única y un nombre descriptivo, por ejemplo, *InteractRemoteAPI*.

> No utilice *InteractRemoteClient*. Este nombre se asigna internamente en el sistema.

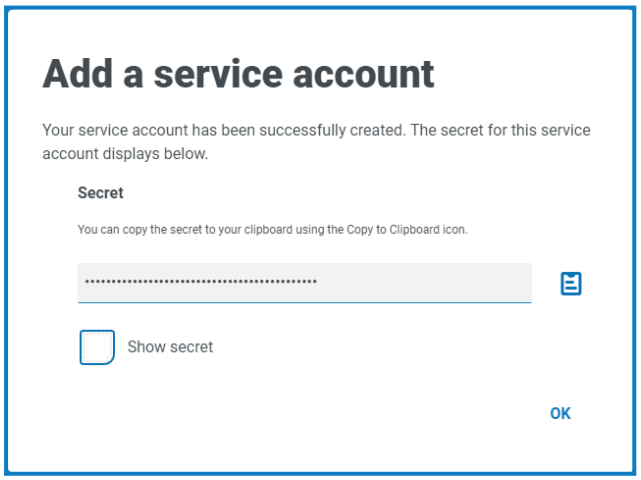
3. En **Permisos**, seleccione **Remote API de Interact**.



4. Haga clic en **Crear cuenta de servicio**.

   Aparece el diálogo Agregar una cuenta de servicio con una clave secreta generada. Deberá ingresar esta clave en el cliente interactivo de Blue Prism al configurar la credencial asociada.

5. Copie la clave secreta generada en su portapapeles para pegarla en el cliente interactivo de Blue Prism.



6. Haga clic en **Aceptar** para cerrar el diálogo.

   Aparece la página Cuentas de servicio con la cuenta recién creada que se muestra.

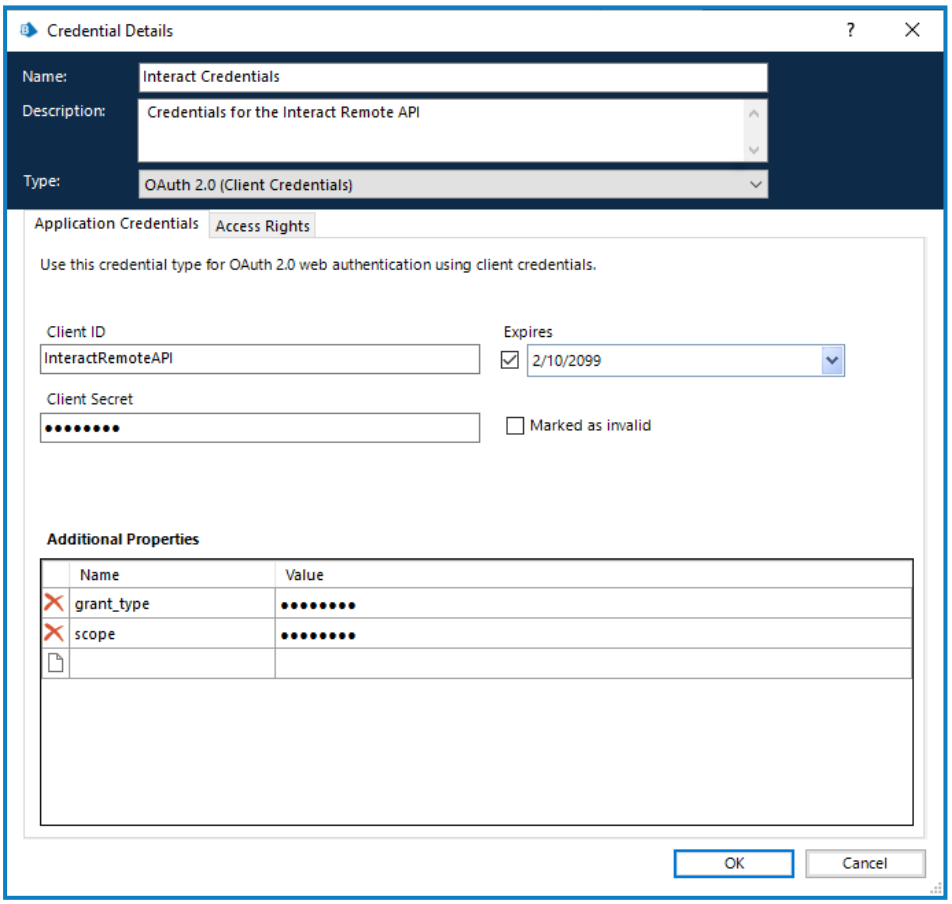
Importar el VBO

1. Descargue el archivo de lanzamiento del servicio API de Interact del portal de Blue Prism.
2. En Blue Prism, seleccione **Archivo** y haga clic en **Importar** > **Lanzamiento/Habilidad** y siga las indicaciones para importar el archivo de lanzamiento a Blue Prism. Para obtener más información, consulte Importar un archivo.

Configurar credenciales en Blue Prism

1. Inicie sesión en el cliente interactivo de Blue Prism, seleccione **Sistema** y haga clic en **Seguridad** > **Credenciales**. Consulte Seguridad > Credenciales para obtener información adicional.
2. Haga clic en **Nueva**.

   Se muestra el diálogo Detalles de la credencial.
3. En la pestaña Credenciales de la aplicación del diálogo Detalles de la credencial:
   a. Ingrese un nombre.
   b. Cambie el **Tipo** a **OAuth 2.0 (Credenciales del cliente)**.
   c. En **Id. de cliente**, ingrese la Id. que utilizó para crear la cuenta de servicio anterior en Configurar Digital Workers en la página 76, por ejemplo, *InteractRemoteAPI*.
   d. En **Secreto del cliente** ingrese la clave secreta generada para la cuenta de servicio.

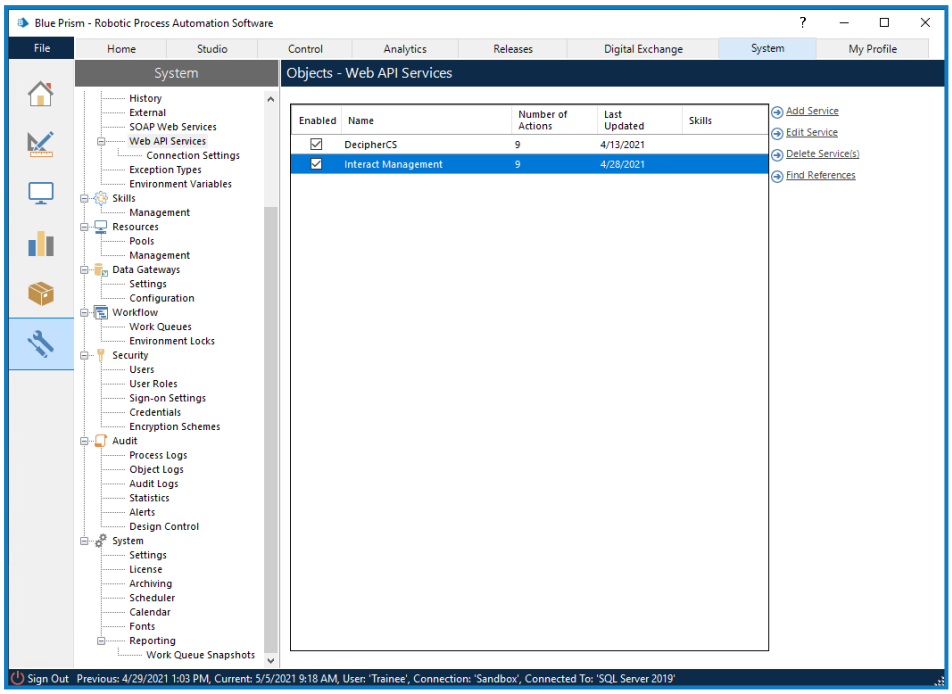


4. En la pestaña Derechos de acceso del diálogo Detalles de la credencial, configure los permisos de acceso requeridos.
5. Haga clic en **Aceptar**.

Configurar el servicio web

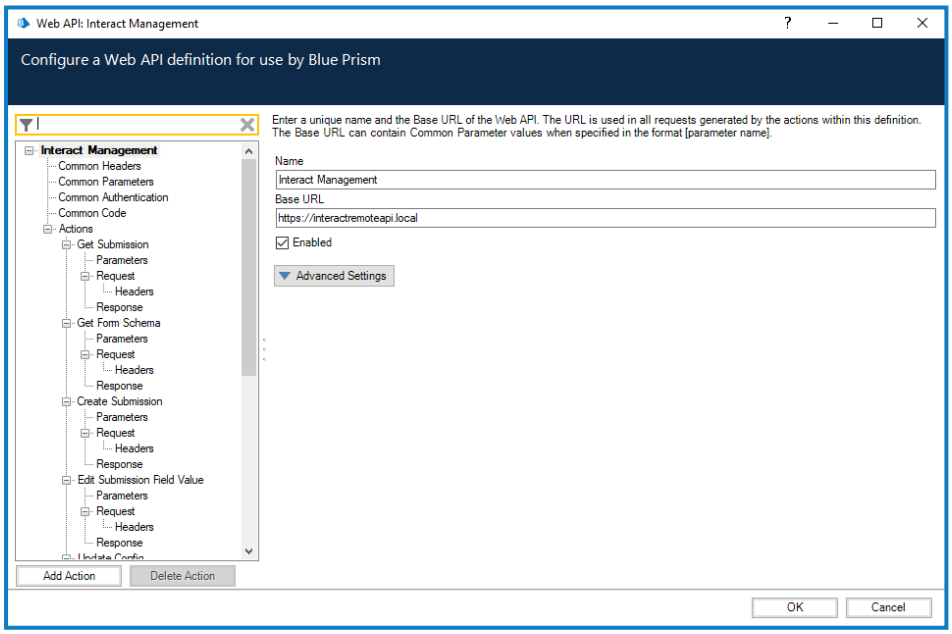
1. En Blue Prism, seleccione **Sistema** y luego haga clic en **Objetos** > **Servicios de API web**.

   Aparece la pantalla Objetos: servicios de API web. Por ejemplo:



2. Seleccione **Administración de Interact** y haga clic en **Editar servicio**.

   Aparece la pantalla API web: administración de Interact.



3. En la pantalla de apertura de API web: administración de Interact, en **URL base**, ingrese la URL para el servicio API de Interact de su organización. Esto se definió durante la instalación de Interact.
4. Seleccione **Autenticación común** en el árbol de navegación y luego complete lo siguiente:
   a. Asegúrese de que el **Tipo de autenticación** esté configurado como **OAuth 2.0 (credenciales del cliente)**

b. En **URI de autorización**, ingrese la URL del Authentication Server en el formato:

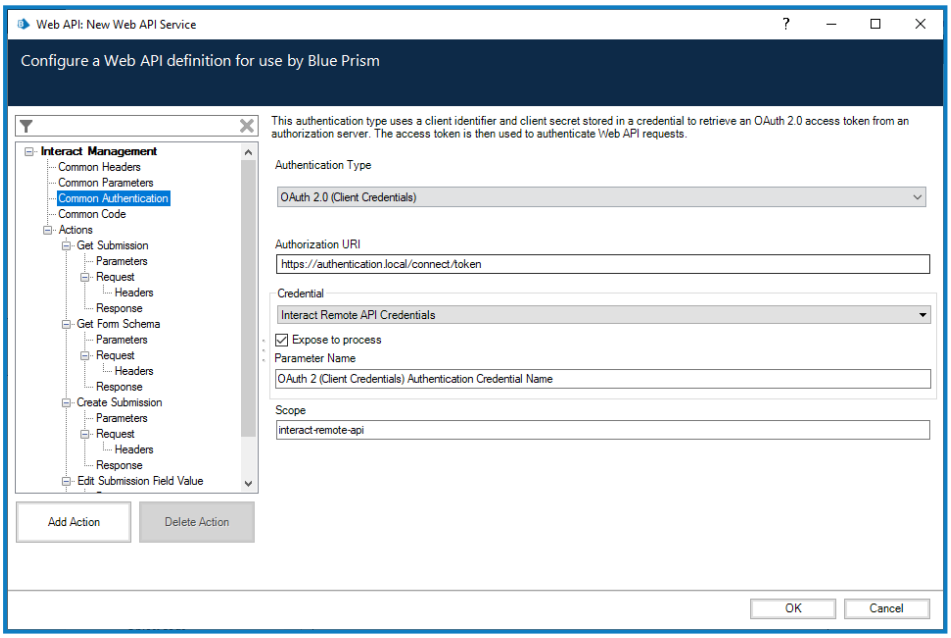
`<Authentication Server URL>:<port if specified during install>/connect/token`

Por ejemplo, `https://authentication.blueprism.com:5000/connect/token`

O bien, si se utilizó el puerto predeterminado, `https://authentication.blueprism.com/connect/token`.

> Si ha actualizado desde una versión anterior a 4.3, su sistema seguirá usando IMS. En este caso, debe ingresar la información en el formato:
>
> `<IMS URL>:<port if specified>/connect/token`
>
> Por ejemplo, `https://ims.blueprism.com:5000/connect/token`.

c. En **Credencial**, seleccione la credencial que creó en Configurar credenciales en Blue Prism en la página 82.



5. Haga clic en **Aceptar** para guardar y completar la configuración del servicio de API web.

Verificar una instalación de

En esta sección se ofrece un escenario simple para evaluar el funcionamiento, según lo previsto, de los componentes básicos de la instalación de Interact. Este proceso de verificación requiere que:

- Se haya configurado una conexión a una base de datos de Blue Prism en Hub; consulte Configuración de base de datos en la página 67 para obtener más información.
- Exista una cola de trabajo válida en el entorno de Blue Prism que se puede utilizar para esta prueba.
- El servicio de API de Interact esté instalado y configurado en Blue Prism; consulte Configurar Digital Workers en la página 76 para obtener más información.

Los pasos de verificación incluyen:

- Verificar que Interact puede enviar información a una cola de trabajo en Blue Prism:
  - Crear un proceso empresarial dentro de Hub: cada formulario está vinculado a un proceso empresarial.
  - Crear un formulario de Interact: cree un nuevo formulario con una página y un campo para usar en la prueba de verificación.
  - Agregar el formulario a un rol: proporcione a un usuario acceso al formulario en Interact.
  - Enviar el formulario y asegurarse de que aparezca en una cola dentro de Blue Prism.
- Verificar que Blue Prism pueda proporcionar información a Interact:
  - Crear un proceso simple de Blue Prism.

Estas instrucciones suponen que el usuario está familiarizado con Blue Prism.

Si experimenta problemas durante la verificación de la instalación, consulte Solucionar problemas en una instalación.

⚠ Si instaló su entorno para usar la autenticación de Windows, debe asignar los grupos de aplicaciones y servicios para usar las cuentas de Windows y luego crear un entorno en Hub antes de llevar a cabo esta verificación. Si no lo hace, los formularios creados en el complemento de Interact no se mostrarán a los usuarios en Interact. Para obtener más información, consulte Instalación de mediante autenticación de Windows en la página 61 y Configuración inicial de Hub en la página 66.

Crear un proceso empresarial dentro de Hub

1. Inicie sesión en Authentication Server con una cuenta de usuario administrador y seleccione **Hub**.
2. En la barra de navegación izquierda, seleccione **Automation Lifecycle** y haga clic en **Procesos empresariales**.
3. Haga clic en **Agregar nueva**.
4. Ingrese un identificador único y un nombre para el proceso empresarial. También puede ingresar una descripción.
5. Si es necesario, ingrese una nota adicional y haga clic en **Crear proceso empresarial**.

Para obtener más información sobre la creación de procesos empresariales, consulte la guía del usuario de Automation Lifecycle Management.

Crear un formulario de Interact

Debe crear un formulario que tenga, como mínimo, una página con un campo.

1. En Hub, en la barra de navegación izquierda, seleccione **Interact** y haga clic en **Formularios**.
2. Seleccione **Crear formulario** para crear un nuevo formulario de Interact.
3. Seleccione el proceso empresarial que creó en la lista desplegable si aún no está seleccionado.
4. Ingrese un nombre para el formulario de Interact y una descripción, por ejemplo, *Formulario de prueba*.
5. En **Método de entrega**, seleccione **Cola**.
6. Seleccione el entorno de la lista desplegable y luego seleccione el nombre de cola requerido.

   Si la cola requerida no se muestra en la lista, haga clic en el ícono Actualizar para actualizar las colas.
7. Deje en blanco **Prioridad**, **ANS**, **Correo electrónico** y **Rol de Interact**.
8. Deje el **Tipo de aprobación predeterminado** con el valor **Ninguno**.
9. En **Categoría**, ingrese un nombre para la categoría. Por ejemplo, *TestCategory*.
10. Seleccione un ícono entre los predefinidos para representar el formulario en Interact.
11. Haga clic en **Crear formulario**.

    Aparece la página Editar formulario.
12. Haga clic en **Crear página**.

    Aparece el panel Crear página.
13. Ingrese un nombre y una descripción para la nueva página y haga clic en **Guardar**.

    En la página Editar formulario se muestra la página que creó.
14. Haga clic en los puntos suspensivos (**...**) en la página que acaba de crear y, a continuación, haga clic en **Crear campo**.

    Aparece el diálogo Elegir tipo de captura.
15. Haga clic en **Texto**.
16. En la página Crear texto, ingrese *TestTextField* en el campo **Etiqueta** y deje todo lo demás con los valores predeterminados.
17. Haga clic en **Crear campo**.
18. En la página Editar formulario, haga clic en **Guardar**.
19. En el panel Aumentar versión secundaria, ingrese una nota de actualización y haga clic en **Guardar**.

Para obtener más información sobre cómo crear un proceso empresarial, consulte la guía del usuario del complemento de Interact.

Agregar el formulario a un rol

1. En Hub, haga clic en el ícono de su perfil para abrir la página Configuración y luego haga clic en **Roles y permisos**.

   Aparece la página Roles y permisos.
2. Haga clic en **Crear rol**.

   Aparece la sección Crear rol.
3. Ingrese un nombre de función, como *Rol de prueba de Interact*. También puede ingresar una descripción.
4. Cambie el **Tipo de rol** a **Interact**.
5. En **Agregar formulario**, seleccione el formulario que acaba de crear de la lista desplegable. Si ha utilizado el nombre de ejemplo elegido en Crear un formulario de Interact en la página anterior, será **Formulario de prueba**.
6. En **Agregar usuario**, seleccione los usuarios que podrán acceder al formulario que ha creado. Agregue el usuario administrador que está utilizando como mínimo.
7. Haga clic en **Guardar**.
8. Cierre sesión en Hub.

Para obtener más información sobre cómo implementar un proceso empresarial, consulte la guía del usuario del complemento de Interact.

Enviar el formulario a una cola de trabajo en Blue Prism

1. Inicie sesión en Authentication Server con las credenciales de un miembro en el rol que asignó al formulario y seleccione **Interact**.

   Para los fines de la prueba, puede utilizar el administrador asignado al rol o un usuario. Solo los miembros del rol pueden ver el formulario en Interact, independientemente de sus privilegios administrativos.
2. Haga clic en el formulario que acaba de crear (**Formulario de prueba**).

   El formulario se muestra con el campo de texto único.
3. Ingrese texto en el campo y luego haga clic en **Enviar**.
4. Inicie sesión en Blue Prism y verifique si hay un elemento en la cola de trabajo especificada al crear el formulario.

Para obtener más información sobre el uso de Interact como usuario final, consulte la guía del usuario de Interact .

Esto completa la verificación de la instalación y demuestra que Interact puede comunicarse con Blue Prism. El siguiente paso es verificar que Blue Prism pueda proporcionar información a Interact.

Crear un proceso simple de Blue Prism

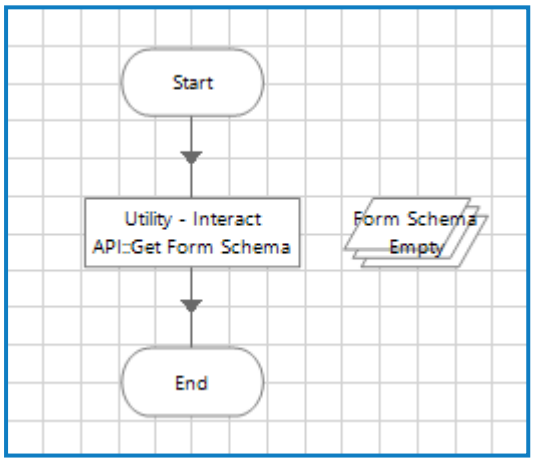
Puede utilizar uno de estos dos procesos. Ambos demuestran comunicación entre Blue Prism e Interact. Estos procesos muestran:

- Opción 1: Blue Prism puede consultar y recibir una respuesta de Interact, en este caso, el nombre del formulario.
- Opción 2: Blue Prism puede cambiar un valor en un formulario y el cambio se muestra en Interact.

Opción 1: Recuperar el nombre del formulario

1. Cree un proceso en Blue Prism.
2. Agregue una acción a su proceso y configure las siguientes propiedades:
   a. Configure el **Objeto de negocio** en **Utilidad - API de Interact**.
   b. Configure la **Acción** como **Obtener esquema de formulario**.
   c. En la pestaña Entrada, en **Valor del nombre del formulario**, ingrese el nombre del formulario que creó entre comillas dobles, por ejemplo, "*Formulario de prueba*".
   d. En la pestaña Salida, genere la colección predeterminada del Esquema de formulario.
3. Conecte la fase de acción con las fases Inicio y Fin.

   Su proceso debe ser similar a este:



4. Ejecute el proceso.
5. Una vez completado, abra la colección Esquema de formulario y seleccione la pestaña **Valores actuales**. Esto debe reflejar el contenido del formulario; en este caso, solo un campo de texto TestTextField.

Opción 2: Cambiar un valor de campo

Este proceso requiere que haya un elemento en la cola de trabajo; uno se envió como parte de Enviar el formulario a una cola de trabajo en Blue Prism en la página anterior.

1. Cree un proceso en Blue Prism.
2. Agregue tres acciones a su proceso y configure las siguientes propiedades:

   Acción 1:

   a. Configure el **Objeto de negocio** como **Colas de trabajo**.
   b. Configure la **Acción** como **Obtener elemento siguiente**.
   c. En la pestaña Entrada, en el **Valor de cola**, ingrese el nombre de la cola a la que envió el formulario. Esto se especificó en Crear un formulario de Interact en la página 86 en el paso 6. El nombre de la cola debe ingresarse entre comillas dobles, por ejemplo, "*InteractQueue*".

d. En la pestaña Salida, genere el campo predeterminado Recopilación de datos e Id. de elemento.

Acción 2:

a. Configure el **Objeto de negocio** en **Utilidad - API de Interact**.

b. Configure la **Acción** como **Editar valor del campo de texto**.

c. En la pestaña Entrada, introduzca los siguientes valores:

- Para **Id. de envío**, ingrese *[Data._requestId]*.
- Para **Nombre de campo**, ingrese el nombre del campo entre comillas dobles, por ejemplo, "*TestTextField*".
- Para **Valor de campo**, ingrese la fase entre comillas dobles que desea volver a pasar a Interact, por ejemplo, "*un texto de muestra en el campo*".

Acción 3:

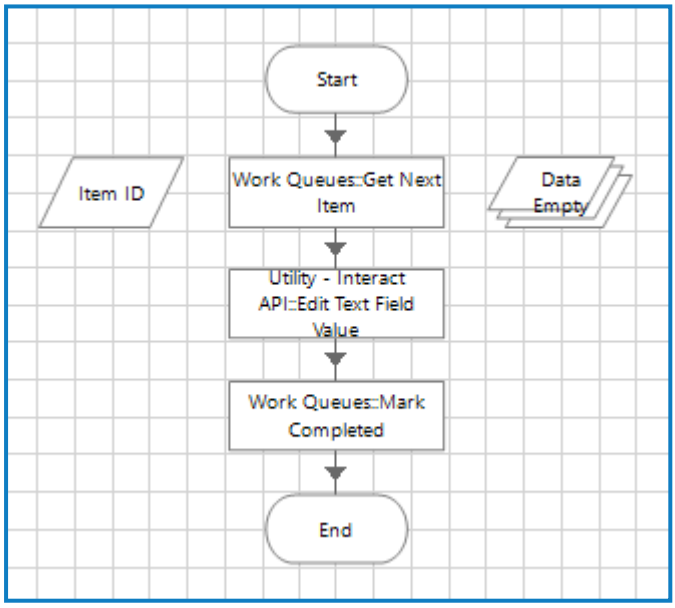
a. Configure el **Objeto de negocio** como **Colas de trabajo**.

b. Configure la **Acción** como **Marcar completado**.

c. En la pestaña Entrada, en el valor **Id. de elemento**, ingrese *[Id. de elemento]*. Este es el tipo de datos de texto generado por la primera acción.

3. Conecte las fases de acción entre sí y con las fases de Inicio y Fin.

   Su proceso debe ser similar a este:



4. Ejecute el proceso.
5. Cuando se complete:

   a. Abra las colas en Blue Prism. El formulario enviado anteriormente debe marcarse como completo.

   b. Abra Interact, seleccione **Historial**, haga clic en los puntos suspensivos (**...**) junto al formulario enviado y haga clic en **Ver**. El formulario debe mostrar el texto enviado desde Blue Prism.

Verificación finalizada

Esto completa la verificación de la instalación y demuestra que Blue Prism puede comunicarse con Interact e Interact con Blue Prism.

Ahora puede eliminar cualquier elemento de prueba que haya creado, como:

- Elimine la cola de trabajo si ya no es necesaria; consulte Flujo de trabajo: colas de trabajo.
- Eliminar el formulario del complemento de Interact: consulte la guía del usuario del complemento de Interact.
- Eliminar el proceso empresarial: consulte la guía del usuario de Automation Lifecycle Management.
- Eliminar el rol de prueba: consulte la guía del administrador de Hub.

Solucionar problemas en una instalación de Interact

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 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 7.
- 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.

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.

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.

Usar RabbitMQ con AMQPS

Si utiliza RabbitMQ con AMQPS (Advanced Message Queuing Protocol - Secure), los grupos de aplicaciones creados como parte de la instalación de Interact deben recibir permisos para el certificado RabbitMQ. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el Administrador de certificados. Para hacerlo, escriba *Certificados* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrar certificados del equipo**.
2. Navegue hasta en el certificado que se identificó y haga clic con el botón derecho en él para usarlo con RabbitMQ AMQPS durante la instalación de Hub; a continuación, seleccione **Todas las tareas** y haga clic en **Administrar claves privadas...**.

   Aparece el diálogo Permisos para el certificado.
3. Haga clic en **Agregar** y luego ingrese los siguientes grupos de aplicaciones en el campo **Ingresar los nombres de objetos para seleccionar**:

   ```
   iis apppool\Blue Prism - IADA;
   iis apppool\Blue Prism - Interact;
   iis apppool\Blue Prism - Remote API de Interact;
   ```

   > Estos son los nombres predeterminados del grupo de aplicaciones. Si ingresó otros nombres durante la instalación, asegúrese de que la lista refleje los nombres que utilizó.
4. Si está utilizando la autenticación de Windows, agregue también el nombre de la cuenta de servicio que se utiliza para los siguientes servicios de Windows:
   - Blue Prism: oyente del servicio de auditoría
   - Blue Prism: servicio de registro
   - Blue Prism: Submit Form Manager
5. Haga clic en **Comprobar nombres**.

   Los nombres deben validarse. Si no se validan, verifique que el nombre coincida con el grupo de aplicaciones o la cuenta de servicio que está intentando usar y corríjalos según sea necesario.
6. Haga clic en **Aceptar**.
7. Seleccione cada grupo de aplicaciones a su vez en la lista **Nombres de grupo o usuario** y asegúrese de que la opción **Control completo** esté seleccionada en la lista **Permisos para {account name}**.
8. Haga clic en **Aceptar**.

   Los grupos de aplicaciones ahora tienen acceso al certificado.

Autenticación de Windows

La cuenta que se utiliza para ejecutar la instalación debe tener los permisos del Servidor SQL pertinentes para llevar a cabo la instalación; es decir, membresía en los roles de servidor fijos de sysadmin o dbcreator. Consulte Preparación para obtener más detalles.

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

- La capacidad de realizar los procesos de la base de datos SQL, consulte Permisos mínimos de SQL en la página 14.
- Propiedad sobre grupo de aplicaciones de IIS.
- Permisos para los certificados requeridos.

Asignación de la cuenta de servicio de Windows como propietaria en certificados

Se deben otorgar permisos a la cuenta de servicio de Windows para los certificados de BluePrismCloud. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el Administrador de certificados. Para hacerlo, escriba *Certificados* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrar certificados del equipo**.
2. En el panel de navegación, amplíe **Personal** y haga clic en **Certificados**.
3. Siga los pasos a continuación para los certificados BluePrismCloud_Data_Protection y BluePrismCloud_IMS_JWT:
    a. Haga clic con el botón derecho en el certificado y seleccione **Todas las tareas** y haga clic en **Administrar claves privadas...**.

    Aparece el diálogo Permisos para el certificado.

    b. Haga clic en **Agregar** y luego ingrese la cuenta de servicio y haga clic en **Aceptar**.
    c. Con la cuenta de servicio seleccionada en la lista **Nombres de grupo o usuario**, asegúrese de que la opción **Control completo** esté seleccionada en la lista **Permisos para {account name}**.
    d. Haga clic en **Aceptar**.

    La cuenta de servicio ahora tiene acceso al certificado.

Asignación de una cuenta de servicio de Windows al grupo de aplicaciones

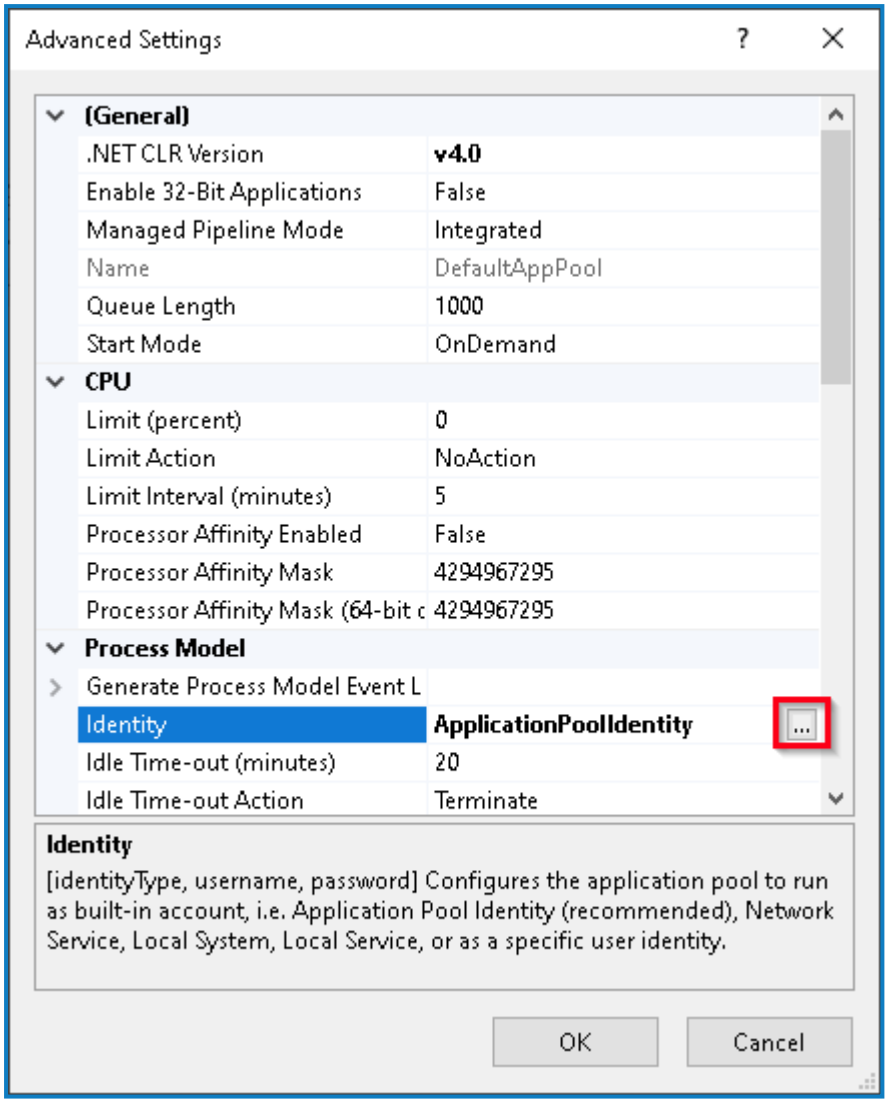
De manera predeterminada, los grupos de aplicaciones se crean con la identidad "ApplicationPoolIdentity". Después de que el instalador haya finalizado, se deberá asignar la cuenta de servicio de Windows para administrar los grupos de aplicaciones. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el administrador de Internet Information Services (IIS).
2. En el panel Conexiones, expanda el host y seleccione **Grupos de aplicaciones**.
3. Revise los valores de la columna **Identidad**.

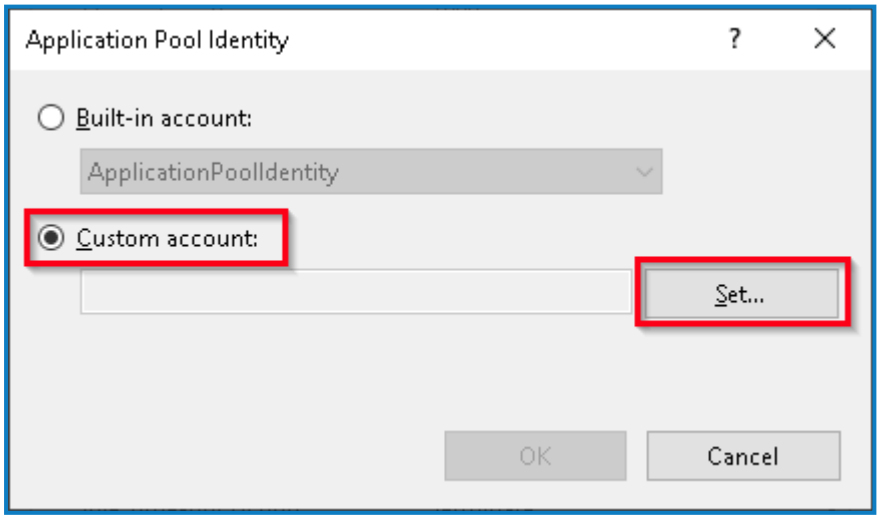
    La identidad de un grupo de aplicaciones debe coincidir con la cuenta de servicio de Windows específica.
4. Para cualquier grupo de aplicaciones que tenga *ApplicationPoolIdentity* en la columna **Identidad**, haga clic con el botón derecho en la fila y seleccione **Configuración avanzada...**.

    Aparece el diálogo Configuración avanzada.

5. Seleccione la configuración **Identidad** y luego haga clic en el botón **...** (elipsis):



6. En el diálogo Identidad del grupo de aplicaciones, seleccione la opción **Cuenta personalizada** y haga clic en **Establecer...**.



Aparece el diálogo Establecer credenciales.

7. Ingrese las credenciales para la cuenta de servicio de Windows requerida y haga clic en **Aceptar**.

8. Repita el procedimiento para cualquier grupo de aplicaciones que necesite cambiar.
9. Reinicie el servicio de RabbitMQ.
10. Reinicie todos los grupos de aplicaciones.
11. Reinicie Internet Information Services.

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.

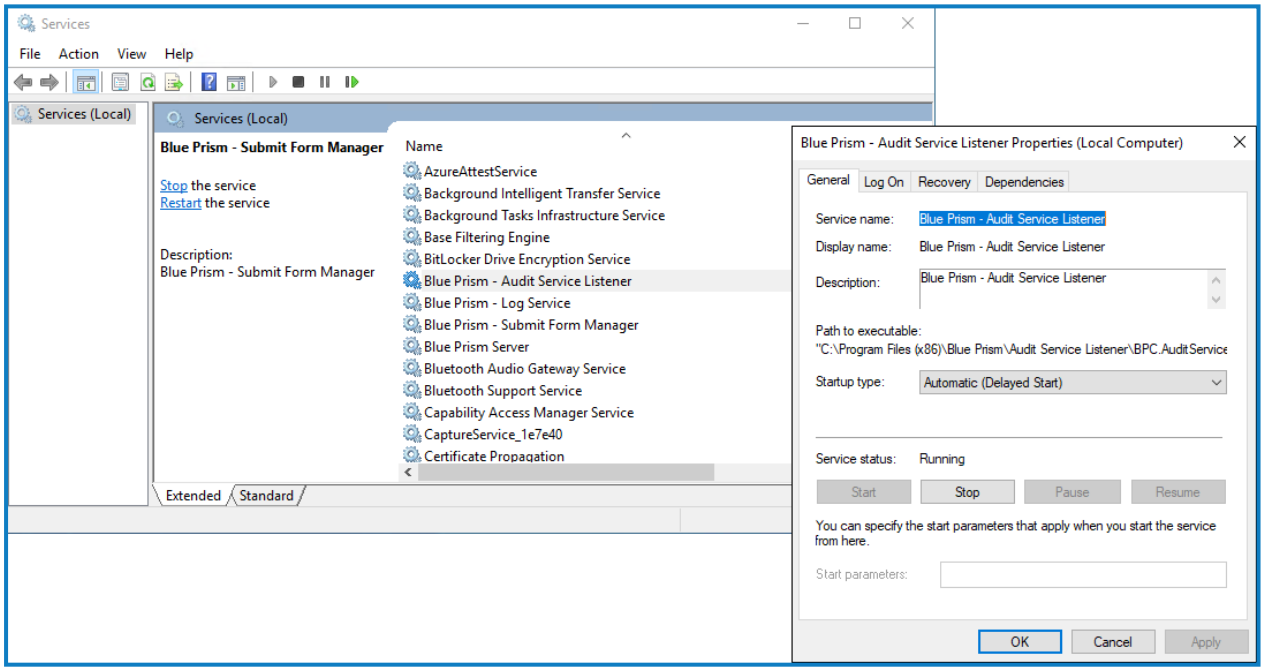
Asignación de una cuenta de servicio de Windows a un servicio

La cuenta de servicio de Windows debe asignarse para administrar los siguientes servicios:

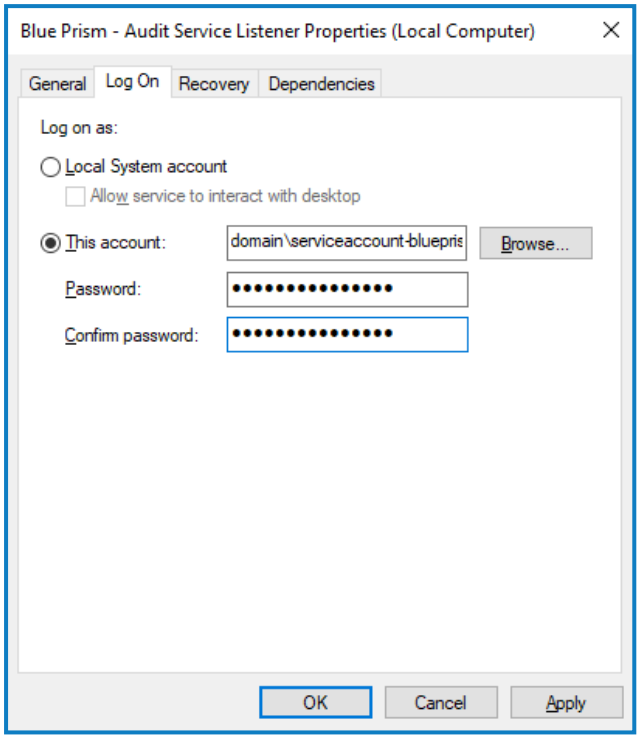
- Blue Prism: oyente del servicio de auditoría
- Blue Prism: servicio de registro
- Blue Prism: Submit Form Manager

Para hacerlo, siga estos pasos:

1. En el servidor web, abra Servicios.
2. Haga clic derecho en el servicio y, a continuación, haga clic en **Propiedades**.



3. En la pestaña Iniciar sesión, seleccione **Esta cuenta** y luego ingrese el nombre de la cuenta o haga clic en **Examinar** para encontrar la cuenta que desea usar.



4. Ingrese la contraseña de la cuenta y haga clic en **Aceptar**.
5. En la ventana Servicios, haga clic derecho en el servicio y, a continuación, haga clic en **Reiniciar**.
6. Repita este procedimiento para los otros servicios de Blue Prism.

Mensajes atascados en RabbitMQ

Si no se agrega un envío a la cola de trabajo esperada de Blue Prism Enterprise, esto puede deberse a que el envío no se ha pasado correctamente a través del servidor de agente de mensajería (ejecutando RabbitMQ).

Si hay una interrupción del sistema de Hub o Interact, los formularios de Interact pueden enviarse a una cola de error de RabbitMQ en lugar de la cola de mensajes adecuada en RabbitMQ (que luego dirige los envíos a las colas de trabajo en Blue Prism Enterprise). El administrador del sistema (con acceso a RabbitMQ) deberá sacar el envío de la cola de errores.

Para obtener información sobre cómo trasladar los envíos de formularios de Interact desde la cola de errores de RabbitMQ, consulte este artículo de la base de conocimientos: Cómo trasladar envíos de formularios de Interact desde una cola de errores de RabbitMQ.

Otra causa por la que los mensajes se atascan en RabbitMQ es cuando IADA no ha podido procesar los mensajes y actualizar las colas. IADA tiene una dependencia en la función de inicialización de la aplicación IIS, que debería haberse instalado de forma predeterminada durante el proceso de instalación. Sin embargo, si no se instaló, puede hacerlo de la siguiente manera:

1. En el servidor web donde se instalan Interact e IADA, abra el administrador de servidores. Para ello, escriba *Servidor* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrador de servidores**.
2. Haga clic en **Agregar roles y funciones**.

   Aparece el Asistente para agregar roles y funciones.

3. Haga clic en **Siguiente** hasta llegar a la página Roles del servidor.
4. Amplíe **Servidor web (IIS)**, **Servidor web** y **Desarrollo de aplicaciones**, y luego seleccione **Inicialización de aplicaciones**.
5. Haga clic en **Siguiente** hasta llegar a la página Confirmar selecciones de instalación.
6. Haga clic en **Instalar**.
7. Una vez finalizada la instalación, reinicie el servidor web.

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.

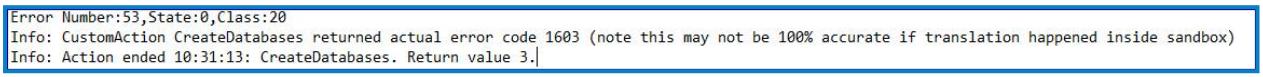
Si no se pueden cumplir estos requisitos, la instalación se detendrá.

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 .
- 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.



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, se debe realizar una copia de seguridad de las bases de datos originales y se deben eliminar 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 7.

Usar RabbitMQ con AMQPS

Si utiliza RabbitMQ con AMQPS (Advanced Message Queuing Protocol - Secure), los grupos de aplicaciones creados como parte de la instalación de Hub deben recibir permisos para el certificado RabbitMQ. Para hacerlo, siga estos pasos:

1. En el servidor web, abra el Administrador de certificados. Para hacerlo, escriba *Certificados* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrar certificados del equipo**.
2. Navegue hasta en el certificado que se identificó y haga clic con el botón derecho en él para usarlo con RabbitMQ AMQPS durante la instalación de Hub; a continuación, seleccione **Todas las tareas** y haga clic en **Administrar claves privadas...**.

   Aparece el diálogo Permisos para el certificado.
3. Haga clic en **Agregar** y luego ingrese los siguientes grupos de aplicaciones en el campo **Ingresar los nombres de objetos para seleccionar**:

   > Estos son los nombres predeterminados del grupo de aplicaciones. Si ingresó otros nombres durante la instalación, asegúrese de que la lista refleje los nombres que utilizó.
4. Si está utilizando la autenticación de Windows, agregue también el nombre de la cuenta de servicio que se utiliza para los siguientes servicios de Windows:
   - Blue Prism: oyente del servicio de auditoría
   - Blue Prism: servicio de registro
5. Haga clic en **Comprobar nombres**.

   Los nombres deben validarse. Si no se validan, verifique que el nombre coincida con el grupo de aplicaciones o la cuenta de servicio que está intentando usar y corríjalos según sea necesario.

6. Haga clic en **Aceptar**.
7. Seleccione cada grupo de aplicaciones a su vez en la lista **Nombres de grupo o usuario** y asegúrese de que la opción **Control completo** esté seleccionada en la lista **Permisos para {account name}**.
8. Haga clic en **Aceptar**.

   Los grupos de aplicaciones ahora tienen acceso al certificado.

File Service

Si el File Service no encuentra las imágenes para Authentication Server 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.

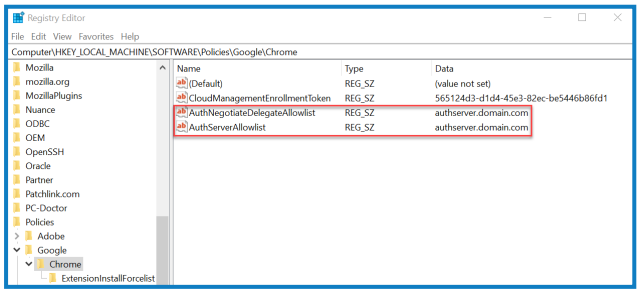
Configurar navegadores para la autenticación de Windows integrada

En el caso de que los usuarios de Directorio Activo no puedan iniciar sesión en Blue Prism Hub después de la instalación, verifique que haya configurado los navegadores web compatibles para la autenticación de Windows integrada, a fin de que puedan recuperarse los usuarios conectados actualmente de la máquina cliente. Los pasos de configuración son diferentes para cada navegador web compatible con Hub.

Configurar Google Chrome

1. Cierre todas las instancias abiertas de Chrome.
2. Abra el Editor de registro e ingrese lo siguiente en la barra superior:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
3. Haga clic derecho en la carpeta Chrome y seleccione **Nuevo** > **Valor de cadena**.
4. Agregue los siguientes valores de cadena: `AuthNegotiateDelegateAllowlist` y `AuthServerAllowlist`.
5. Haga clic derecho en cada valor de cadena a su vez y seleccione **Modificar**.
6. En el campo **Datos de valor** para ambos valores de cadena, ingrese el nombre de host del sitio web del Authentication Server, por ejemplo, authserver.domain.com, y haga clic en **Aceptar**.

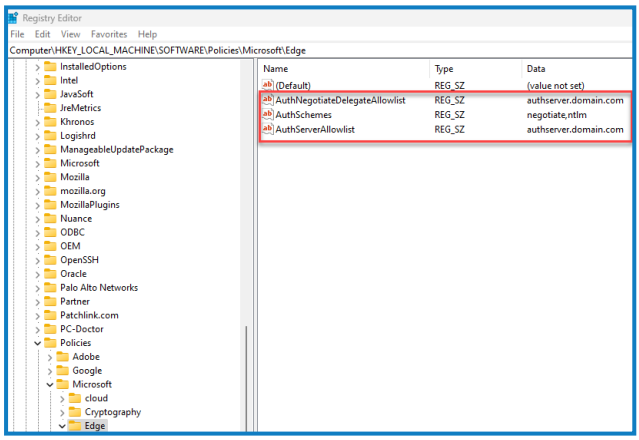


Configurar Microsoft Edge

1. Cierre todas las instancias abiertas de Edge.
2. Abra el Editor de registro e ingrese lo siguiente en la barra superior:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Haga clic derecho en la carpeta Edge y seleccione **Nuevo** > **Valor de cadena**.
4. Agregue los siguientes valores de cadena: `AuthNegotiateDelegateAllowlist`, `AuthServerAllowlist` y `AuthSchemes`.
5. Haga clic derecho en cada valor de cadena a su vez y seleccione **Modificar**.
6. En el campo **Datos de valor** para `AuthNegotiateDelegateAllowlist` y `AuthServerAllowlist`, ingrese el nombre de host del sitio web de Authentication Server, por ejemplo, authserver.domain.com, y haga clic en **Aceptar**.
7. En el campo **Datos de valor** para `AuthSchemes`, ingrese `negotiate, ntlm` y haga clic en **Aceptar**. Para obtener más información, consulte la documentación de Microsoft sobre las políticas de Microsoft Edge.

   > Este valor de cadena no es necesario si su organización solo está configurada para la autenticación de Kerberos; consulte a continuación para obtener más información.

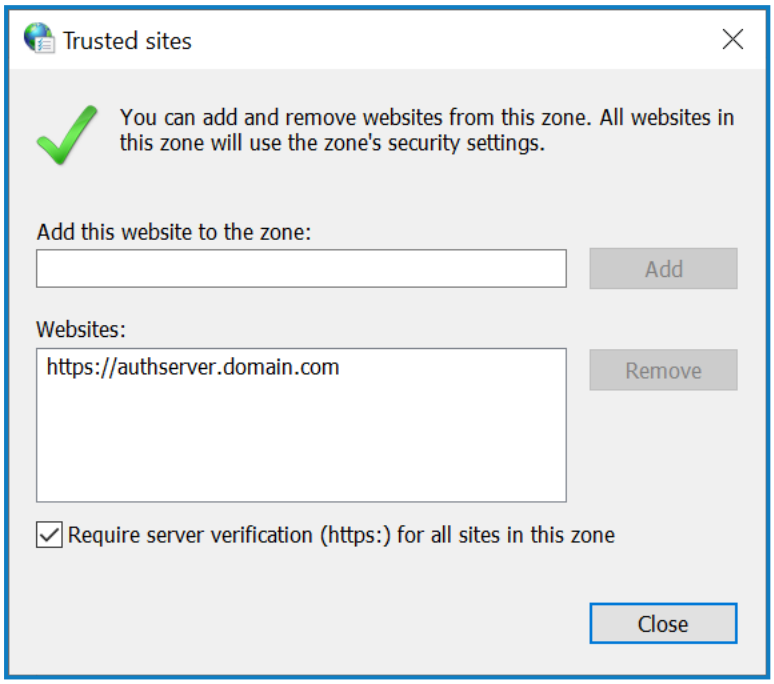


Como alternativa, puede seguir estos pasos para Microsoft Edge:

1. Cierre todas las instancias abiertas de Edge.
2. Navegue hasta **Panel de control** > **Red e Internet** > **Opciones de Internet**.
3. En la pestaña Opciones avanzadas, en Seguridad, seleccione **Habilitar autenticación de Windows integrada**.
4. En la pestaña Seguridad, haga clic en **Sitios de confianza** > **Sitios**.

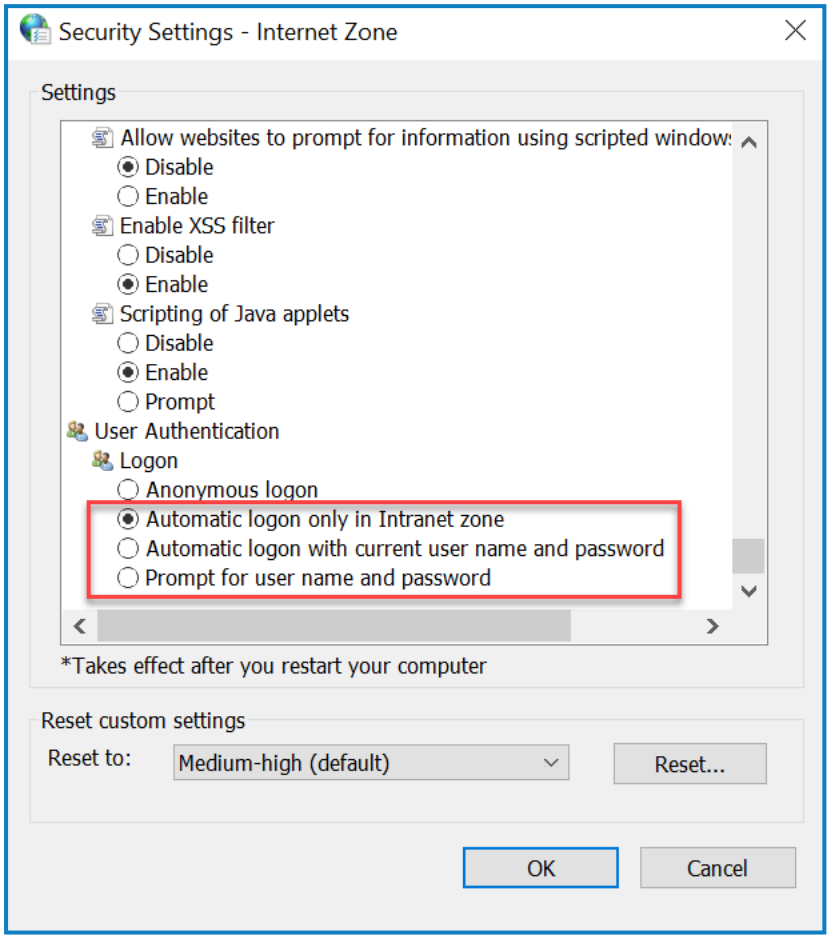
5. En el diálogo Sitios de confianza, ingrese la URL para Authentication Server (por ejemplo, https://authserver.domain.com) en el campo **Agregar este sitio web a la zona** y haga clic en **Agregar**.

   La URL se muestra en el campo **Sitios web**.



6. Haga clic en **Cerrar**.
7. En la pestaña Seguridad del diálogo Opciones de Internet, haga clic en **Sitios de confianza** > **Nivel personalizado**.

8. En **Autenticación de usuario** > **Inicio de sesión**, confirme que la opción **Inicio de sesión anónimo** no esté seleccionada. En su lugar, utilice cualquiera de las configuraciones que permiten al navegador recoger credenciales de usuario, como se muestra a continuación.



9. Haga clic en **Aceptar**.

Configurar la autenticación de Kerberos

Los pasos anteriores no serán suficientes si la autenticación de Windows New Technology LAN Manager (NTLM) se ha desactivado para su entorno. En este caso, también debe configurar la autenticación de Kerberos y un nombre principal de servicio (SPN). Según la configuración de su organización, es posible que también deba agregar una clave de registro Microsoft Edge WebView2. Para obtener más información, consulte la documentación de Microsoft sobre NTLM y la autenticación de Kerberos.

1. En el servidor web, abra el administrador de Internet Information Services (IIS).
2. En la lista de conexiones, seleccione **Blue Prism: Authentication Server**.

   Este es el nombre de sitio predeterminado; si ha utilizado un nombre de sitio personalizado, seleccione la conexión adecuada.
3. En Internet Information Services, haga doble clic en **Autenticación**.

   Aparecerá la página Autenticación.
4. Seleccione **Autenticación de Windows** (asegúrese de que esté configurada en *Habilitada*) y luego haga clic en **Proveedores...**.

   Aparecerá el cuadro de diálogo Proveedores.

5. Agregue uno o más proveedores de la lista de proveedores disponibles, según la configuración de su organización, y haga clic en **Aceptar**.

Configuración del nombre principal del servicio (SPN)

También será necesario configurar y registrar un nombre principal de servicio (SPN) para la URL de Authentication Server a fin de asegurarse de que la autenticación de Kerberos funcione correctamente. Consulte la documentación de Microsoft sobre este tema para obtener más detalles, incluidos los permisos requeridos. Este es un paso esencial para revisar con el equipo de TI de su organización a fin de asegurarse de que el comando `Setspn` no falle al ejecutarse debido a la falta de permisos de cuenta.

1. Abra el símbolo del sistema como administrador en el servidor web y ejecute el comando aplicable a continuación.

   Si el grupo de aplicaciones de Blue Prism - Authentication Server se ejecuta como una cuenta del sistema local, utilice:

   ```
   Setspn -S HTTP/WEBSITE_URL COMPUTER_HOSTNAME
   ```

   Si el grupo de aplicaciones de Blue Prism - Authentication Server se está ejecutando como una cuenta de servicio, utilice:

   ```
   Setspn -S HTTP/WEBSITE_URL DOMAIN/Username
   ```

   > HTTP cubre tanto HTTP como HTTPS. No cambie el comando para incluir HTTPS específicamente, ya que la configuración fracasará.

2. Ejecute la `purga de Klist` para actualizar los tickets de Kerberos.
3. Inicie sesión en Authentication Server para verificar que la autenticación de Kerberos funcione correctamente.

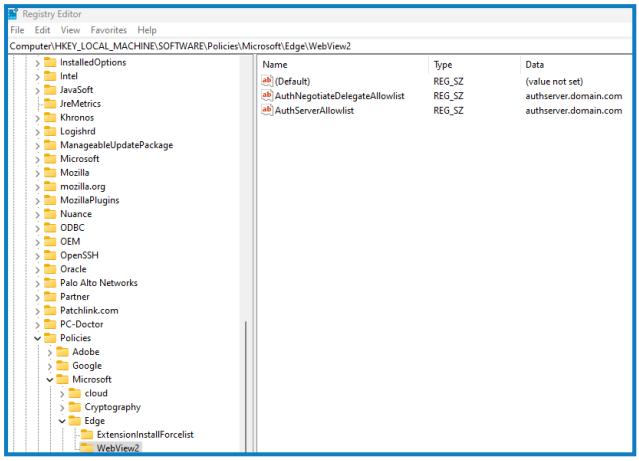
Agregar una clave de registro Microsoft Edge WebView2

Si su organización solo está configurada para la autenticación de Kerberos, y también se utiliza Authentication Server para iniciar sesión en Blue Prism Enterprise, se debe agregar una clave de registro para el navegador Microsoft Edge WebView2:

1. Cierre todas las instancias abiertas de Edge.
2. Abra el Editor de registro e ingrese lo siguiente en la barra superior:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Haga clic con el botón derecho en la carpeta Edge y seleccione **Nuevo** > **Clave**.
4. Nombre la nueva clave **WebView2**.
5. Haga clic con el botón derecho en la carpeta WebView2 y agregue los siguientes valores de cadena: `AuthNegotiateDelegateAllowlist` y `AuthServerAllowlist`.
6. Haga clic derecho en cada valor de cadena a su vez y seleccione **Modificar**.

7. En el campo **Datos de valor** para `AuthNegotiateDelegateAllowlist` y `AuthServerAllowlist`, ingrese el nombre de host del sitio web de Authentication Server, por ejemplo, authserver.domain.com, y haga clic en **Aceptar**.



Hub muestra un error en el inicio

Si un usuario inicia sesión en Authentication Server, selecciona Hub y aparece el siguiente mensaje:

Se produjo un error al iniciar la aplicación

Esto significa que es necesario reiniciar los sitios de IIS. Este error afecta a los sistemas que están instalados en un solo servidor y ocurre si RabbitMQ se inicia después de los sitios de IIS. Por lo tanto, se recomienda que los sitios de IIS tengan configurado un retraso de inicio para permitir que RabbitMQ se inicie primero.

Si se produce este error, se puede resolver de la siguiente manera:

1. En el servidor, abra el Administrador de Internet Information Services (IIS) y detenga todos los sitios de Blue Prism. Para obtener una lista, consulte Sitios web de Hub.
2. Reinicie el servicio de RabbitMQ.
3. Reinicie todos los grupos de aplicaciones de Blue Prism.
4. Inicie los sitios de Blue Prism que se detuvieron en el paso 1.

Para retrasar el inicio del servicio de los sitios de IIS, haga lo siguiente:

1. En el servidor, abra Servicios.
2. Haga clic con el botón derecho en **Servicio de publicación World Wide Web** y seleccione **Propiedades**.
3. En la pestaña General, configure **Tipo de inicio** como **Automático (Inicio retrasado)**.
4. Haga clic en **Aceptar** y cierre la ventana Servicios.

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.

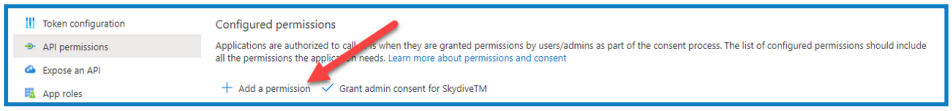
El servidor web debe iniciarse después de que se hayan iniciado todos los servicios de RabbitMQ. Si los servicios del servidor web se inician antes de que el servicio RabbitMQ esté listo, ir a la configuración SMTP en Hub resultará en un mensaje de “algo salió mal”.

Al guardar la configuración SMTP, devuelve un error al usar OAuth 2.0

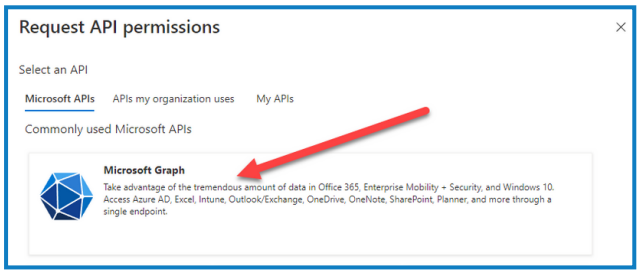
Si recibe un error al guardar una configuración de correo electrónico con OAuth 2.0, verifique que el permiso Mail.Send esté configurado para la aplicación en Directorio Activo de Azure.

Para agregar el permiso Mail.Send:

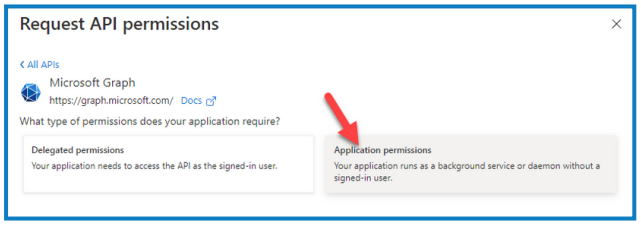
1. En Directorio Activo de Azure, abra las propiedades de la aplicación a la que está vinculando Hub.
2. Haga clic en **Permisos de API**.
3. Haga clic en **Agregar un permiso**.



4. En Seleccionar una API, en API de Microsoft, seleccione **Microsoft Graph**.

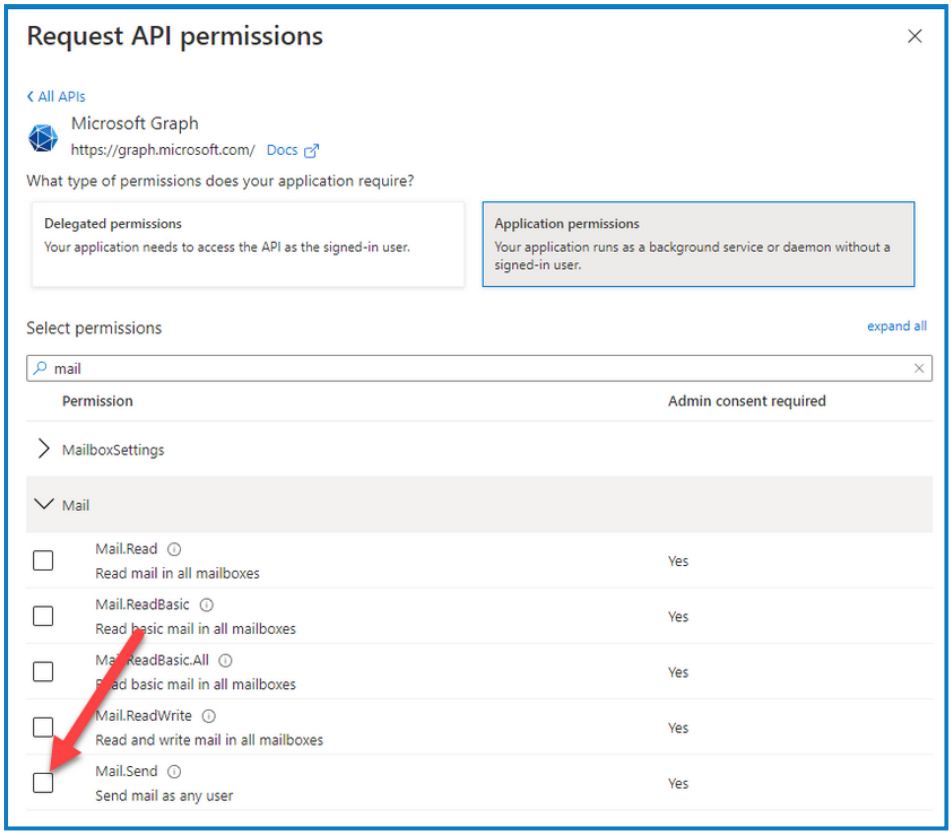


5. En Microsoft Graph, haga clic en **Permisos de aplicación**.

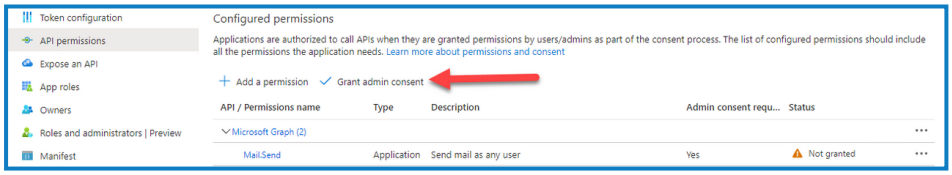


6. Escriba *Mail* en el campo de búsqueda y presione Intro.

7. En la lista Mail que se muestra, seleccione **Mail.Send** y haga clic en **Agregar permisos**.



8. En la página de permisos de aplicación, haga clic en **Otorgar consentimiento de administrador**.



Actualización de la identificación del cliente después de la instalación

Si necesita ingresar o actualizar su Id. de cliente después de la instalación, deberá actualizar el archivo de configuración appsettings.json de License Manager. Una vez que se haya actualizado el archivo de configuración, deberá reiniciar el License Manager en el administrador de Internet Information Services (IIS).

Para actualizar su Id. de cliente en el archivo appsetting.json:

1. Abra el Explorador de Windows y navegue hasta `C:\Archivos de programa (x86)\Blue Prism\LicenseManager\appsettings.json`.

   Esta es la ubicación de instalación predeterminada; ajústela si utilizó una ubicación personalizada.

2. Abra el archivo appsettings.json en un editor de texto.

3. Busque la sección `License:CustomerId` del archivo e ingrese su nueva id. de cliente, por ejemplo:

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

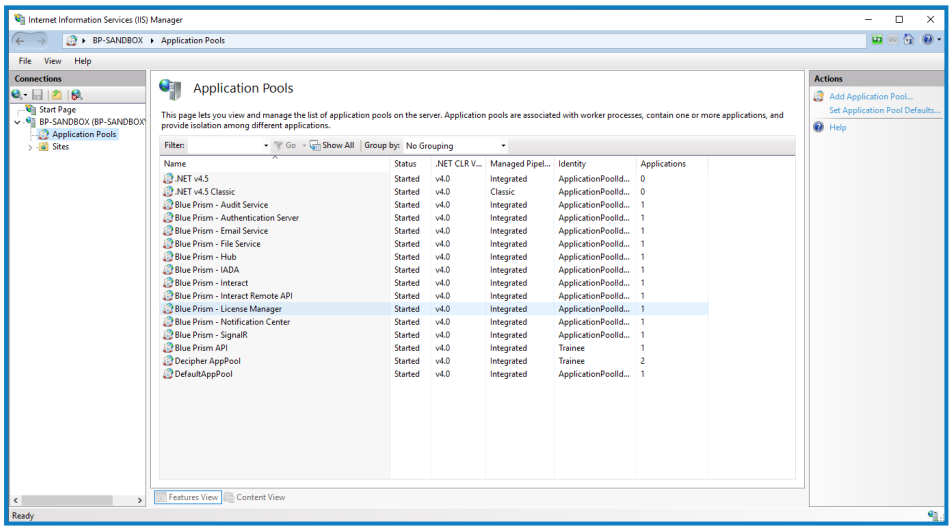
4. Guarde el archivo.

Para reiniciar el License Manager:

1. Abra el administrador de Internet Information Services (IIS).
2. En la lista de conexiones, seleccione **Blue Prism -License Manager**.

> Este es el nombre de sitio predeterminado; si ha utilizado un nombre de sitio personalizado, seleccione la conexión adecuada.

3. Haga clic en **Reiniciar** desde los controles Administrar sitio web.



Se reinicia el License Manager.

Desinstalar Interact

Debe ser administrador del sistema para desinstalar Blue Prism Interact.

Para desinstalar por completo Interact 4.7, debe hacer lo siguiente:

1. Detener los grupos de aplicaciones usando IIS.
2. Eliminar Interact mediante la aplicación Programas y características.
3. Eliminar las bases de datos.
4. Eliminar los datos de RabbitMQ.
5. Eliminar los certificados.
6. Eliminar los archivos restantes.

Detener los grupos de aplicaciones usando IIS

1. Abra el administrador de Internet Information Services (IIS). Para ello, escriba *IIS* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **administrador de Internet Information Services (IIS)**.
2. En el panel **Conexiones**, haga clic en **Grupos de aplicaciones**.
3. Detenga todos los grupos de aplicaciones asociados con los sitios de Blue Prism: selecciónelos de a uno por vez y haga clic en **Detener**. Para acceder a una lista, consulte Sitios web de Interact en la página 14.

Eliminar Interact mediante Programas y características

1. Abra el Panel de control. Para ello, escriba *panel de control* en el cuadro de búsqueda de la barra de tareas de Windows y, luego, haga clic en **Panel de control**.
2. Haga clic en **Programas** y, luego, en **Programas y características**.
3. Seleccione Blue Prism Interact.
4. Haga clic en **Desinstalar**.
5. Confirme que desea continuar con la desinstalación.

Eliminar las bases de datos

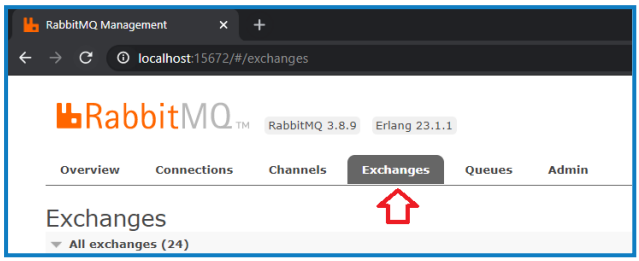
Solo debe eliminar bases de datos para sistemas de prueba. Si está considerando eliminar una base de datos para un sistema que ha estado en producción, debe considerar si los datos deben ser archivados por su organización o utilizados para fines de auditoría.

Después de la desinstalación de Interact, si se vuelve a instalar en una fecha posterior utilizando las mismas bases de datos, se deben borrar los datos de las bases de datos antes de la reinstalación.

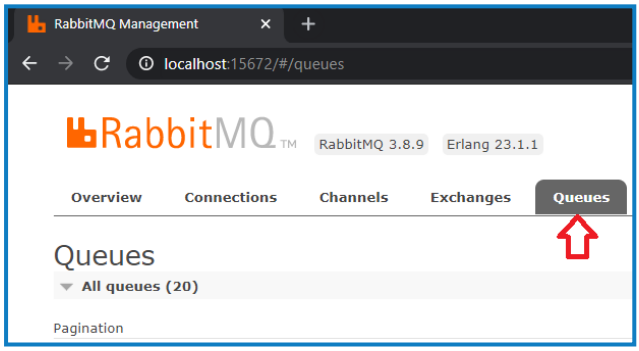
1. Elimine o archive la base de datos de la aplicación Interact.

Eliminar los datos de RabbitMQ

1. Abra la página de administración de RabbitMQ. De manera predeterminada, la URL es http://localhost:15672/ en el equipo local.
2. Haga clic en **Intercambios**.



3. Busque y elimine los siguientes elementos:
   - bpc.interact.*
4. Haga clic en **Colas**.



5. Busque y elimine los siguientes elementos:
   - bpc.interact.*

Eliminar los certificados

Hub también utiliza estos certificados. Si Interact y Hub están instalados en el mismo servidor, omita esta sección y elimínelos cuando desinstale Hub. Para obtener más información, consulte la Guía de instalación de Hub.

1. Abra el Administrador de certificados. Para hacerlo, escriba *Certificados* en el cuadro de búsqueda de la barra de tareas de Windows y luego haga clic en **Administrar certificados del equipo**.
2. En el panel de navegación, amplíe **Certificado de confianza** y haga clic en **Certificados**.
3. Seleccione y elimine cualquier certificado que se haya creado para los sitios de Blue Prism, así como:
   - BluePrismCloud_Data_Protection
   - BluePrismCloud_IMS_JWT

Eliminar los archivos restantes

1. En el Explorador de Windows, abra la carpeta principal para la instalación de Interact. De manera predeterminada, esta es `C:\\Archivos de programa (x86)\\Blue Prism`, pero es posible que se haya cambiado durante la instalación de Interact.

2. Elimine las siguientes carpetas y archivos:
    - IADA
    - Interact
    - Remote API de Interact
    - Submit Form Manager