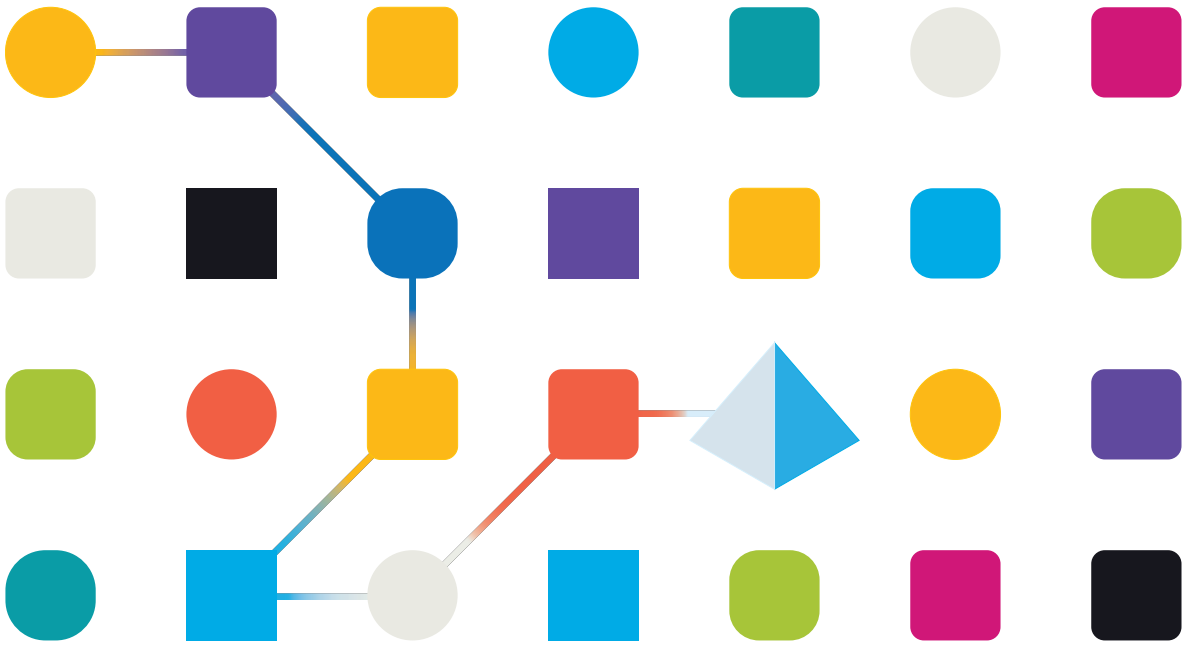
blueprism®

Interact 4.7

Installationshandbuch

Dokumentrevision: 4.0



Marken- und Urheberrechtshinweise

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registriert in England: Reg.- Nr. 4260035. Tel.: +44 370 879 3000. Web: www.blueprism.com

Inhalt

Einleitung

Dieses Handbuch erklärt die Installation von Blue Prism® Interact und zeigt Ihnen, wie Sie den Erfolg der Installation überprüfen können.

Blue Prism Interact wird nur im Rahmen einer Mehrgerätebereitstellung unterstützt, bei der Blue Prism Komponenten auf mehreren Geräten bereitgestellt werden. Die Gründe hierfür sind:

- Das ergibt eine umfassende Bereitstellung von Blue Prism für vielfältige Szenarien.
- Erweiterte Methoden zur Bereitstellung zusätzlicher Dienste oder zum Schutz und zur Absicherung der Umgebung erfordern typischerweise diesen Bereitstellungstyp.

In diesem Handbuch finden Sie auch eine Reihe von erweiterten Themen, die Informationen zur Fehlerbehebung bei Installationen und zur Konfiguration von erweiterten Einstellungen und Optionen enthalten.

Wenn Sie weitere Hilfe zu diesem Dokument benötigen, wenden Sie sich an Ihren Blue Prism Konto-Manager oder den technischen Support. Weitere Informationen finden Sie unter Kontakt.

Diese Informationen beziehen sich nur auf die Version 4.7 von Blue Prism Interact.

Die Installation von Blue Prism Hub ist Voraussetzung für die Installation von Interact.

Interact aktualisieren

Wenn Sie ein Upgrade von einer früheren Version auf Interact 4 durchführen möchten, können Sie den Upgrader von Blue Prism verwenden. Weitere Informationen finden Sie unter Hub und Interact aktualisieren.

Zielgruppe

Dieser Leitfaden richtet sich an IT-Experten mit Erfahrung in der Konfiguration und Verwaltung von Netzwerken, Servern und Datenbanken. Der Installationsprozess erfordert die Vertrautheit mit der Installation und Konfiguration von Webservern und Datenbanken.

Videos

Zusätzlich zu dieser Installationsanleitung können Sie sich unsere Videos ansehen, die den Installationsprozess demonstrieren. Klicken Sie hier, um die Interact Installationsvideos anzuzeigen.

Zugehörige Dokumente

Die folgenden Dokumente enthalten weitere Informationen zu spezifischen Aspekten der Implementierung von Hub und Interact.

Dokumenttitel	Beschreibung
Hub Benutzerhandbuch	Ein Dokument, das sich an Hub Benutzer richtet und erklärt, wie sie das Beste aus Hub herausholen können.
Hub Administratorhandbuch	Ein umfassendes Dokument für Hub Administratoren zur optimalen Nutzung von Hub mit Informationen zum Benutzerzugriff, zur Lizenzierung von Plug-ins und zur Personalisierung von Hub.

Dokumenttitel	Beschreibung
Benutzerhandbuch zum Interact Plug-in	Ein umfassendes Dokument zur optimalen Nutzung von Interact mit Informationen zur Erstellung von Formularen und deren Zuweisung zu Rollen.
Interact Benutzerhandbuch	Ein detailliertes Dokument, das erklärt, wie Interact zum Einreichen und Genehmigen von Formularen verwendet wird.
Interact Web-API-Dienst Benutzerhandbuch	Ein Dokument mit genauen Informationen zur Nutzung des Interact Web-API-Diensts und des damit verbunden Blue Prism Objekts.

Vorbereitung

Vor der Installation von Blue Prism Interact ist es wichtig, sicherzustellen, dass die Architektur so konfiguriert ist, dass sie die Installation unterstützt. Mehrere Systeme sind erforderlich, um Interact zu installieren.

Planung

Bevor die Installation durchgeführt wird, müssen die folgenden Bedingungen erfüllt sein:

- Es muss ein SQL Server verfügbar sein, um die Blue Prism Komponentendatenbanken zu hosten, zum Beispiel Authentication Server , Hub, Audit, Interact, InteractCache usw. Während des gesamten Installationsprozesses ist der Zugriff auf Administratorebene erforderlich. Weitere Details erhalten Sie unter Minimale SQL-Berechtigungen.
- Es muss ein Message-Broker-Server, der RabbitMQ Message Broker hostet, verfügbar sein.
- Es muss ein Webserver für das ebenfalls vorhandene Hub (siehe Voraussetzungen auf der nächsten Seite) und die Interact Installationen verfügbar sein.
- Es muss Administratorzugriff für die Geräte verfügbar sein, auf denen Blue Prism Interact installiert werden soll. Alle Geräte müssen die Mindestanforderungen erfüllen und sie müssen über das Netzwerk miteinander kommunizieren können. Dies umfasst die Kommunikation mit Ihrer Blue Prism Datenbank.
- Das Konto, das die Installation durchführt, muss Zugriff auf die Hostdatei haben. Dies wird normalerweise in C:\Windows\System32\drivers\etc\hosts oder %SYSTEMROOT%\System32\drivers\etc\hosts gespeichert.

Bei der Planung Ihrer Bereitstellung sollten die folgenden Punkte berücksichtigt werden:

- Wird die Datenbank zu einem vorhandenen Datenbankserver hinzugefügt oder wird eine neue Datenbank in Auftrag gegeben?

  Blue Prism empfiehlt, Datenbanken auf separaten Datenbankservern zu speichern.
- Gibt es ausreichend Platz und Ressourcen, um die hinzugefügten Datenbanken zu hosten?

  Sie sollten überprüfen und sicherstellen, dass ausreichend Speicherplatz und Rechenressourcen für die zusätzliche Last vorhanden sind.
- Welcher Authentifizierungsmodus ist für die SQL-Datenbank erforderlich (SQL-native oder Windows-Authentifizierung)?

  Das ist die Entscheidung Ihrer IT-Organisationen.
- Wurde der Message-Broker-Server eingerichtet und konfiguriert, um die Installation von Hub zu unterstützen?

  Ein Message-Broker-Server ist erforderlich, um die Installation von Hub abzuschließen.
- Erfüllen alle Geräte, auf denen Blue Prism Hub installiert werden soll, die Mindestanforderungen?

  Weitere Informationen finden Sie unter Software-Anforderungen und Berechtigungen.

Voraussetzungen

Unter Software-Anforderungen und Berechtigungen erfahren Sie mehr über die Software-Anforderungen und die minimalen SQL-Berechtigungen.

Die Installation von Interact erfordert die folgenden Voraussetzungen:

- SQL Server muss für die Verwendung der SSL-Verschlüsselung konfiguriert werden. Wenn Ihre Organisation noch keine SSL-Verschlüsselung verwendet (Sie haben Ihre Umgebung ohne Zertifikate für Ihren SQL Server ausgeführt oder Sie haben ein selbstsigniertes Zertifikat verwendet), sollte Ihre Organisation ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle abrufen und es in SQL Server importieren, um sie zu aktivieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

  Importieren des Zertifikats in SQL Server:

  1. Öffnen Sie den **SQL Server-Konfigurations-Manager** in der Windows-Taskleiste.
  2. Erweitern Sie im SQL Server-Konfigurations-Manager die Option **SQL Server-Netzwerkkonfiguration**, klicken Sie mit der rechten Maustaste auf **Protokolle für <SqlServerInstanceName>** und klicken Sie dann auf **Eigenschaften**.
  3. Wählen Sie im Dialogfeld für die Eigenschaften der Protokolle für <SqlServerInstanceName> die Registerkarte **Zertifikat** aus, um dann das gewünschte Zertifikat auszuwählen oder zu importieren.
  4. Klicken Sie auf **Anwenden**.

  ⚠ Zertifikate von vertrauenswürdigen Zertifizierungsstellen sollten für Produktionsumgebungen verwendet werden. Ein selbstsigniertes Zertifikat kann hingegen für Proof-of-Concept- oder Entwicklungsumgebungen verwendet werden. Es ist wichtig, dass der von SQL Server verwendete Fully Qualified Domain Name (FQDN) mit dem im Zertifikat definierten FQDN übereinstimmt. **Wenn diese nicht übereinstimmen, wird keine Verbindung zur Datenbank hergestellt und Ihre Installation wird nicht richtig funktionieren.** Informationen zum Verwenden und Konfigurieren von selbstsignierten Zertifikaten finden Sie unter Selbstsignierte Zertifikate im Blue Prism Hub Installationshandbuch.

  Zusätzlich zu den vom Hub Installationsprogramm installierten Datenbanken muss Ihre Blue Prism Datenbank auch SSL-Verschlüsselung verwenden. Dabei muss ein Zertifikat verwendet werden, dem der Hub Server vertraut, z. B. von einer vertrauenswürdigen Zertifizierungsstelle.

- Für Blue Prism Hub muss ein Message-Broker-Server installiert und konfiguriert werden.
- Der Message-Broker-Server-Build ist ein generisches Setup und die Basisinstallation eines RabbitMQ-Message-Broker-Dienstes. Es wird empfohlen, die Standardpasswörter zu ändern und alle Sicherheitsanforderungen wie die Anwendung von SSL-Zertifikaten von Ihrer IT-Abteilung zu erfüllen.

  Zur Fertigstellung des Message-Broker-Builds muss Folgendes heruntergeladen werden:

  - Erlang/OTP, siehe hier: https://www.rabbitmq.com/which-erlang.html
  - RabbitMQ Server (Versionen 3.8.0 bis 3.8.8 werden unterstützt), verfügbar unter: https://github.com/rabbitmq/rabbitmq-server/releases/

  Den Installationsleitfaden finden Sie hier: https://www.rabbitmq.com/install-windows-manual.html

- Blue Prism Hub ist auf dem Webserver installiert und erfordert daher Internet Information Services Manager (IIS), und die installierten .Net Core-Komponenten. Diese müssen für eine erfolgreiche Installation von Blue Prism Hub vorinstalliert sein. Weitere Informationen finden Sie unter Webserver installieren und konfigurieren auf Seite 26.
- Das Interact System ist ein Webserver und erfordert daher IIS Web Server und Installation der .NET Core-Komponenten. Wenn Sie die Installationsmedien für Blue Prism Hub und Blue Prism Interact verwenden, werden diese als Teil der Installation von Blue Prism Interact ebenfalls installiert.
- Sie erstellen die folgenden Websites mit dem Interact Installationsprogramm – Sie sollten die URLs basierend auf der Domain Ihrer Organisation definieren:

Website in IIS	Standard-URL
Websites mit einer Benutzeroberfläche zur Verwendung durch Endbenutzer	
Blue Prism – Interact	https://interact.local
Websites nur zur Nutzung durch die Anwendung (Dienste)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

⚠ Die oben gezeigten Standard-URLs eignen sich für eine eigenständige Umgebung, wie z. B. eine Testumgebung. Die DNS- und Domänenstrukturen Ihrer Organisation müssen bei der Auswahl von Hostnamen für Ihre Installation berücksichtigt werden.

Diese gelten zusätzlich zu den vom Hub Installationsprogramm erstellten Websites, eine Liste finden Sie unter SSL-Zertifikate konfigurieren auf Seite 27.

- Zertifikate – Während des Installationsvorgangs werden Sie nach den SSL-Zertifikaten für die Websites gefragt, die eingerichtet werden. Je nach den Sicherheitsanforderungen Ihrer Infrastruktur und IT-Organisation kann es sich dabei um ein intern erstelltes SSL-Zertifikat oder ein erworbenes Zertifikat zum Schutz der Websites handeln. Das Installationsprogramm kann ausgeführt werden, ohne dass die Zertifikate vorhanden sind. Damit die Websites funktionieren können, müssen die Bindungen auf der IIS-Website jedoch mit gültigen SSL-Zertifikaten konfiguriert werden. Weitere Informationen finden Sie unter SSL-Zertifikate konfigurieren.
- Standardmäßig werden IIS-Anwendungspools verwendet. Anwendungspools müssen Zugriff auf die Anwendungsdateien und Zertifikate haben, die während der Installation aus Datenschutz- und Autorisierungsgründen erstellt werden. Die Zertifikate BluePrismCloud_Data_Protection und BluePrismCloud_IMS_JWT befinden sich im Standardordner von Windows für Zertifikate. Wenn Sie Windows-Autorisierung für den Zugriff auf SQL-Server verwenden, muss diese manuell konfiguriert werden. Mehr erfahren Sie unter Standardanwendungsinformationen auf Seite 16.
- Standardmäßig wird das „Lokale Systemkonto“ für Dienste verwendet. Dieses Konto muss den Zugriff auf Anwendungsdateien ermöglichen. Wenn Sie Windows-Autorisierung für den Zugriff auf SQL-Server verwenden, muss diese manuell konfiguriert werden.

Liste der Software-Downloads

Blue Prism Hub

Hier sind alle Downloads aufgeführt, die zur Installation von Hub erforderlich sind. Diese sind alle später im Installationshandbuch aufgeführt:

Link zu Software und Referenz	Weitere Anleitungen
RabbitMQ 3.9.22 bis 3.10.7, oder 3.11.9 bis 3.11.10 Mehr erfahren Sie unter siehe RabbitMQ herunterladen und installieren.	Message-Broker-Server installieren auf Seite 21
Erlang/OTP 24.x oder 25.x Welche Version von Erlang Sie benötigen, hängt von der RabbitMQ-Version ab, die Sie verwenden möchten. Mehr erfahren Sie unter siehe Anforderungen für RabbitMQ Erlang-Version.	
IIS 10.0 Enthalten in Windows Server 2016, 2019 und 2022.	Webserver installieren und konfigurieren auf Seite 26
ASP.NET Core Runtime 6.0.9 oder 6.0.10 (Windows Hosting Bundle) https://dotnet.microsoft.com/download/dotnet/6.0 – Wählen Sie die benötigte Version aus. Wählen Sie unter **ASP.NET Core Runtime** die Option **Hosting-Paket** aus.	
.NET Desktop Runtime 6.0.9 oder 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 – Wählen Sie die benötigte Version aus. Wählen Sie unter **.NET Desktop Runtime** den benötigten Download aus.	
.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 Unter Windows Server 2022 wird dies standardmäßig installiert. Sie müssen .NET Framework nur installieren, wenn Sie Windows Server 2016 Datacenter oder Windows Server 2019 verwenden.	
Blue Prism Hub 4.7 Laden Sie Hub von einer der folgenden Produkt-Downloadseiten im Blue Prism Portal herunter: • Automation Lifecycle Management • Decision • Interact	
Authentication Server SAML 2.0 Erweiterung Download von der Digital Exchange – Dies ist ein optionales Installationsprogramm. Dies ist nur erforderlich, wenn Sie beabsichtigen, die SAML 2.0-Authentifizierung zu verwenden.	Siehe die Installationsanleitung auf der Digital Exchange.

Blue Prism Interact

Blue Prism Interact ist ein lizenzbasiertes Plug-in in Hub und eine zusätzliche Website für Endbenutzer. Wenn Ihre Organisation Interact verwenden möchte, müssen Sie zusätzlich zu den in Blue Prism Hub auf der vorherigen Seite aufgeführten Downloads Folgendes herunterladen.

Link zu Software und Referenz	Weitere Anleitungen
Blue Prism Interact 4.7 Im Blue Prism Portal zum Download verfügbar.	Blue Prism Interact installieren
Blue Prism Interact Remote API.bprelease-Datei Im Blue Prism Portal zum Download verfügbar.	Interact Web-API-Dienst installieren und konfigurieren

Mindesthardwareanforderungen

Die folgenden Informationen beschreiben die empfohlenen Mindesthardwareanforderungen zur effektiven Installation und Verwendung von Hub und Interact 4.7. Weitere Informationen zu Softwareanforderungen finden Sie unter Software-Anforderungen und Berechtigungen auf der nächsten Seite.

Laufzeitressource

Bitte beachten Sie die Mindestanforderungen im Installationshandbuch für die von Ihnen installierte Blue Prism Version. In der Hilfe von Blue Prism erfahren Sie mehr.

Datenbankserver

- Intel Xeon Vierkernprozessor
- 8 GB RAM
- SQL Server:
  - 2016, 2017 oder 2019 (64-Bit) – Express-, Standard- oder Enterprise-Editionen

    SQL Express-Editionen eignen sich nur für Nicht-Produktionsumgebungen, z. B. für Demonstrationszwecke.
  - Azure SQL-Datenbank – Während der Installation sind mindestens 100 eDTUs erforderlich. Dieser Wert kann nach der Installation auf 50 eDTUs gesenkt werden.
  - SQL Server auf Azure Virtual Machines
  - Azure SQL Managed Instance
- Entsprechenden Betriebssystemsupport finden Sie hier:
  - SQL Server 2016 oder 2017: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-ver15
  - SQL Server 2019: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

Message-Broker-Server

- Intel Xeon Doppelkernprozessor
- 8 GB RAM
- Windows Server 2016 Datacenter oder 2019 oder 2022

Webserver

- Intel Xeon Doppelkernprozessor
- 8 GB RAM
- Windows Server 2016 Datacenter oder 2019 oder 2022
- Voraussetzungen wie unter Vorbereitung auf Seite 7

Software-Anforderungen und Berechtigungen

Software-Anforderungen

Folgende Technologien werden zur Verwendung mit der Software unterstützt:

Betriebssystem

Version	Webserver	Message-Broker
Windows Server 2016 Datacenter	✓	✓
Windows Server 2019	✓	✓
Windows Server 2022	✓	✓

Wenn die Komponenten von Blue Prism auf einem 64-Bit-Betriebssystem installiert werden, wird es als 32-Bit-Anwendung ausgeführt.

Microsoft SQL Server

Folgende Versionen von Microsoft SQL Server werden zum Verorten der Blue Prism Komponentendatenbanken unterstützt:

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

Hinweis:

- SQL Express eignet sich nur für Nicht-Produktionsumgebungen, z. B. für Demonstrationszwecke.
- SQL Server muss für die Verwendung der SSL-Verschlüsselung konfiguriert werden. Wenn Ihre Organisation noch keine SSL-Verschlüsselung verwendet (Sie haben Ihre Umgebung ohne Zertifikate für Ihren SQL Server ausgeführt oder Sie haben ein selbstsigniertes Zertifikat verwendet), sollte Ihre Organisation ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle abrufen und es in SQL Server importieren, um sie zu aktivieren. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

  Schritte zum Importieren von Zertifikaten in SQL Server finden Sie unter Voraussetzungen auf Seite 8.

  Zertifikate von vertrauenswürdigen Zertifizierungsstellen sollten für Produktionsumgebungen verwendet werden. Ein selbstsigniertes Zertifikat kann hingegen für Proof-of-Concept- oder Entwicklungsumgebungen verwendet werden. Es ist wichtig, dass der von SQL Server verwendete Fully Qualified Domain Name (FQDN) mit dem im Zertifikat definierten FQDN übereinstimmt. **Wenn diese nicht übereinstimmen, wird keine Verbindung zur Datenbank hergestellt und Ihre Installation wird nicht richtig funktionieren.** Informationen zum Verwenden und Konfigurieren von selbstsignierten Zertifikaten finden Sie unter Selbstsignierte Zertifikate.

Folgendes wird ebenfalls unterstützt:

- Azure SQL-Datenbank – Während der Installation sind mindestens 100 eDTUs erforderlich. Dieser Wert kann nach der Installation auf 50 eDTUs gesenkt werden.
- SQL Server auf Azure Virtual Machines.
- Azure SQL Managed Instance, allerdings müssen die Datenbanken vor der Installation erstellt werden.

Message-Broker-Server

Die folgende Software ist auf dem Message-Broker-Server erforderlich:

- RabbitMQ 3.9.22 bis 3.10.7, oder 3.11.9 bis 3.11.10
- Erlang/OTP 24.x oder 25.x – Welche Version von Erlang Sie benötigen, hängt von der RabbitMQ-Version ab, die Sie verwenden möchten.

  Informationen zur Unterstützung von Erlang/OTP finden Sie unter siehe Anforderungen für RabbitMQ Erlang-Version.

  Informationen zur Unterstützung von Betriebssystemen finden Sie unter https://www.rabbitmq.com/platforms.html.

Weitere Informationen finden Sie unter Message-Broker-Server installieren auf Seite 21.

Blue Prism versucht, neue RabbitMQ-Versionen innerhalb von zwei Monaten nach der allgemeinen Verfügbarkeit der Software mit der neuesten Hub Version zu testen. Wenn eine nachfolgende Hub Entwicklung erforderlich ist, um eine neue RabbitMQ-Version zu unterstützen, werden alle Aktualisierungen gemäß unserem Release-Zyklus in eine zukünftige Version von Hub integriert.

Webserver

Die folgende Software ist auf dem Webserver erforderlich:

- .NET Framework 4.8 – Standardmäßig auf Windows Server 2022 installiert.
- IIS 10.0
- ASP.NET Core Runtime 6.0.9 oder 6.0.10 (Windows Hosting Bundle)
- .NET Desktop Runtime 6.0.9 oder 6.0.10

⚠ Interact 4.7 unterstützt nur die oben gezeigten Versionen von ASP.NET Core Runtime und .NET Desktop Runtime. Wenn Sie eine spätere Version, wie 7.x.x, verwenden, können Probleme auftreten.

Weitere Informationen finden Sie unter Webserver installieren und konfigurieren auf Seite 26.

Webbrowser auf Client-Computern

Die neuesten Versionen der folgenden Webbrowser werden von Interact unterstützt:

- Google Chrome
- Microsoft Edge (Chromium-basiert)

Damit sich Active Directory-Benutzer mit einem Chrome- oder Edge-Browser bei Interact anmelden können, müssen die Browser für die integrierte Windows-Authentifizierung konfiguriert werden.

Microsoft Internet Explorer und Mozilla Firefox werden nicht unterstützt.

Blue Prism

Um Interact zu verwenden, ist Blue Prism 6.4.0 oder höher erforderlich.

Minimale SQL-Berechtigungen

Die minimalen SQL-Berechtigungen für den Benutzer, der sich während des Installationsprozesses mit der Datenbank verbindet, müssen die Berechtigungen zum Erstellen oder Konfigurieren einer Datenbank innerhalb des Produkts umfassen. Deshalb muss ein entsprechendes Administratorkonto verwendet werden, wenn die Installation durchgeführt wird:

- Datenbank erstellen: dbcreator (Serverrolle) oder sysadmin (Serverrolle)
- Datenbank konfigurieren: sysadmin (Serverrolle) oder db_owner (Datenbankrolle)

Der Datenbankbenutzer, der sich während des normalen Betriebs mit den Datenbanken verbindet, muss über die minimalen SQL-Berechtigungen verfügen, um auf die Interact und Interact Cache Datenbanken zugreifen zu können. Die erforderlichen Berechtigungen sind:

- db_datareader
- db_datawriter

Während des Installationsvorgangs und bei der ersten Ausführung der Anwendung sollte der Benutzer über einen db_owner-Zugriff verfügen. Danach kann der Datenbankzugriff des Benutzers zu db_datareader und db_datawriter geändert werden.

Weitere Informationen finden Sie unter Standardanwendungsinformationen auf der nächsten Seite.

Standardanwendungsinformationen

Die folgenden Informationen zeigen die Anwendungen, die von der Interact Installation erstellt werden, unter Verwendung der Standardwerte. Alle Anwendungen sollten vollen Zugriff auf das Zertifikat BluePrismCloud_Data_Protection haben, das sich im Zertifikatspeicher auf dem lokalen Computer befindet. IIS APPPOOL\ Blue Prism – IADA erfordert auch Zugriff auf das Zertifikat BPC_SQL_ CERTIFICATE.

Informationen zu Hub Anwendungen finden Sie unter Hub Software-Anforderungen und Berechtigungen.

Interact Websites

Anwendungsname	Beispielservice Kontoname für SQL Windows Authentifizierung	SQL Server Berechtigungen erforderlich während Installation	Datenbank Berechtigungen erforderlich während Anwendung läuft	Standarddatenbankname
Blue Prism - Interact	IIS APPPOOL\ Blue Prism – Interact	dbcreator / sysadmin	db_datawriter / db_datareader	InteractDB, InteractCacheDB
Blue Prism - Interact Remote API	IIS APPPOOL\ Blue Prism – Interact Remote API	dbcreator / sysadmin	db_datawriter / db_datareader	AuthenticationServerDB, InteractDB
Blue Prism - IADA	IIS APPPOOL\ Blue Prism – IADA	dbcreator / sysadmin	db_datawriter / db_datareader	IadaDB

Interact Dienste

Anwendungsname	Beispielservice Kontoname für SQL Windows Authentifizierung	SQL Server Berechtigungen erforderlich während Installation	Datenbank Berechtigungen erforderlich während Anwendung läuft	Standarddatenbankname
Blue Prism - Manager für die Formularübermittlung	NT AUTHORITY\ SYSTEM	–	db_datawriter / db_datareader	InteractDB

Überlegungen zu Mehrgerätebereitstellungen

Wenn Sie eine Mehrgerätebereitstellung durchführen, müssen Sie sich vor der Installation mit den folgenden Aspekten vertraut machen.

Bereich	Umgebungsüberlegungen (Entwicklung/Test/Vorproduktion/Produktion)
Allgemeine Konnektivität	Die Konnektivität zwischen den verschiedenen Geräten muss korrekt konfiguriert sein. Dies erfordert typischerweise, dass das DNS so konfiguriert wird, dass sich die Geräte gegenseitig basierend auf ihrem FQDN auflösen dürfen. Zudem müssen geeignete Firewallregeln gelten, damit die Geräte auf den erforderlichen Ports kommunizieren können.
Message-Broker-Server	Dies ist ein einzelnes Gerät, das für die Bereitstellung von Message-Broking-Diensten zwischen Blue Prism Komponenten verwendet wird. Es wird ein Gerät pro Umgebung empfohlen.
Webserver	Ein einzelnes Gerät, das mehrere Blue Prism Komponenten hosten kann. Es wird nicht empfohlen, dass Umgebungen auf diesem Gerät gemeinsam genutzt werden. Stattdessen sollte ein separates Gerät pro Umgebung verwendet werden.
Datenbankserverinstanz	Überlegen Sie, ob sich die Zuweisungsart von Ressourcen zu SQL Server Instanzen dafür eignet, eine einzelne gemeinsame Instanz für Bereitstellungen von Blue Prism zu verwenden, je nachdem wie wichtig oder kritisch sie sind. (Zum Beispiel sind Produktionsumgebungen meistens am kritischsten für das Unternehmen). Es wird empfohlen, dass verschiedene Arten von Umgebungen, wie Entwicklungs-, UAT- und Produktionsumgebungen, ihre eigene dedizierte SQL Server-Instanz haben. Sie können jedoch mehrere Entwicklungsumgebungen auf derselben SQL Server-Instanz ausführen.
Zertifikate für Digital Workers	Entscheiden Sie, ob zertifikatbasierte Sicherheit als zusätzliche Anforderung auf die Anweisungen von den interaktiven Clients und Anwendungsservern für jeden Digital Worker angewendet werden soll (und auf Kommunikationen, die bei den Digital Workers eingehen, wenn sie Webdienste hosten). Wenn ein Zertifikat erforderlich ist, muss es manuell erzeugt und auf jedem betreffenden Digital Worker installiert werden. Der allgemeine Name auf dem Zertifikat muss mit der Adresse übereinstimmen, die die Blue Prism Komponenten per Konfiguration bei der Kommunikation mit den Geräten verwenden werden (z. B. FQDN oder der Kurzname des Computers). Zudem müssen alle Geräte, die sich mit den Digital Workers verbinden, der Zertifizierungsstelle vertrauen, die das/die manuell erzeugte(n) Zertifikat(e) ausgestellt hat.

Netzwerkports

Um die Netzwerkkonnektivität zwischen Geräten innerhalb der Architektur sicherzustellen, muss die Windows-Firewall auf den entsprechenden Servern die folgenden Datenverkehrsflüsse zulassen:

Datenbankserver	Port 1433, um SQL Server-Konnektivität vom Webserver zuzulassen. Wenn es sich bei der SQL Server-Instanz um eine benannte Instanz handelt, ist außerdem Folgendes erforderlich: • Der TCP-Port für die benannte Instanz (der standardmäßig dynamisch aus dem flüchtigen Bereich ausgewählt wird) oder der festgelegte Port (bei einem statischen Port), um SQL Server-Konnektivität vom Webserver zu ermöglichen. • UDP Port 1434 für den SQL Server-Browserdienst, um SQL Server-Konnektivität vom Webserver zu ermöglichen.
Message-Broker-Server	Port 5672, um Konnektivität mit RabbitMQ Messaging zu ermöglichen. Port 15672, um Konnektivität mit der RabbitMQ Managementkonsole zu ermöglichen.
Webserver	Port 443 für HTTPS-Konnektivität.
Digital Workers	Port 443 für HTTPS-Konnektivität.

Es empfiehlt sich, beim Konfigurieren der Ports mit dem Experten für Netzwerkinfrastruktur Ihrer Organisation Rücksprache zu halten. Möglicherweise müssen andere Ports konfiguriert werden, um die Konnektivität in Ihrer Organisation sicherzustellen.

Typische Bereitstellung

In einer typischen Bereitstellung, die für den Einsatz innerhalb sowie außerhalb der Produktion geeignet ist, werden alle Blue Prism Interact Komponenten auf separaten Computern bereitgestellt.

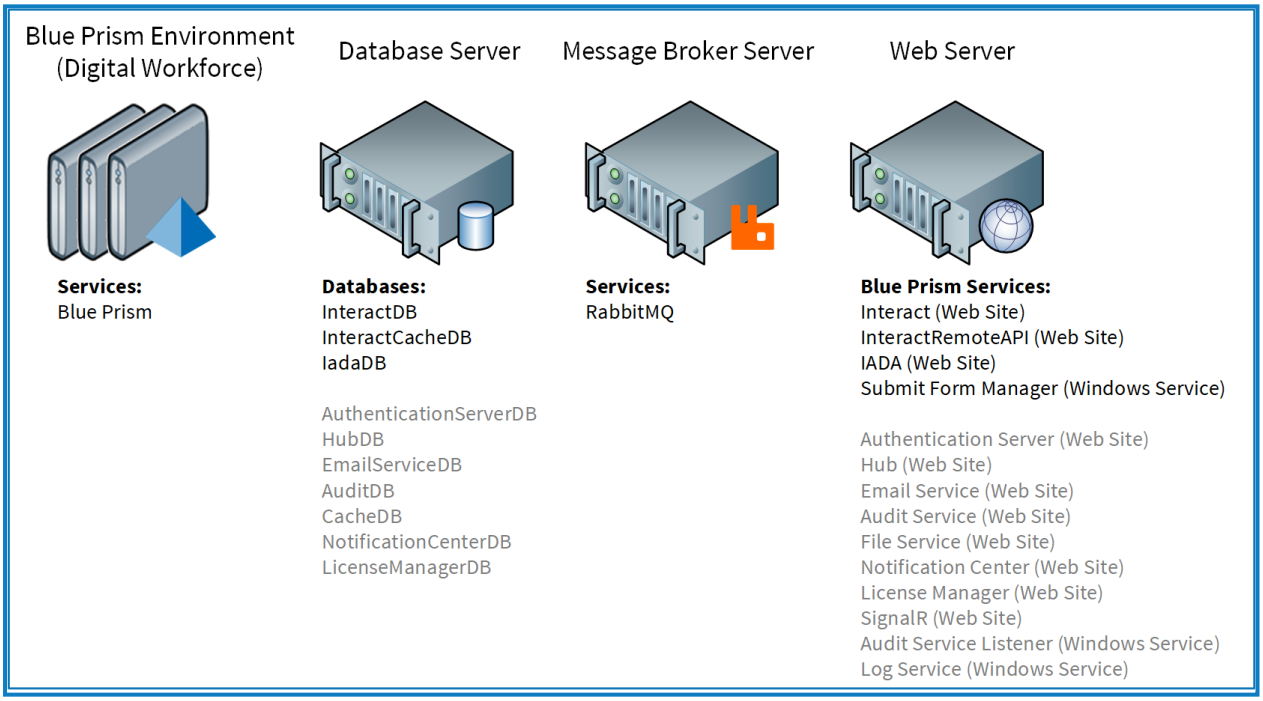
Bevor Sie diese Anleitung befolgen, lesen Sie die Informationen unter Vorbereitung durch.

In Produktionsumgebungen sind mindestens vier Ressourcen erforderlich:

- Webserver
- Message-Broker-Server
- Digital Workers
- SQL Server

Vor der Installation von Blue Prism Interact müssen die Message-Broker-Server- und SQL Server-Instanzen konfiguriert werden.

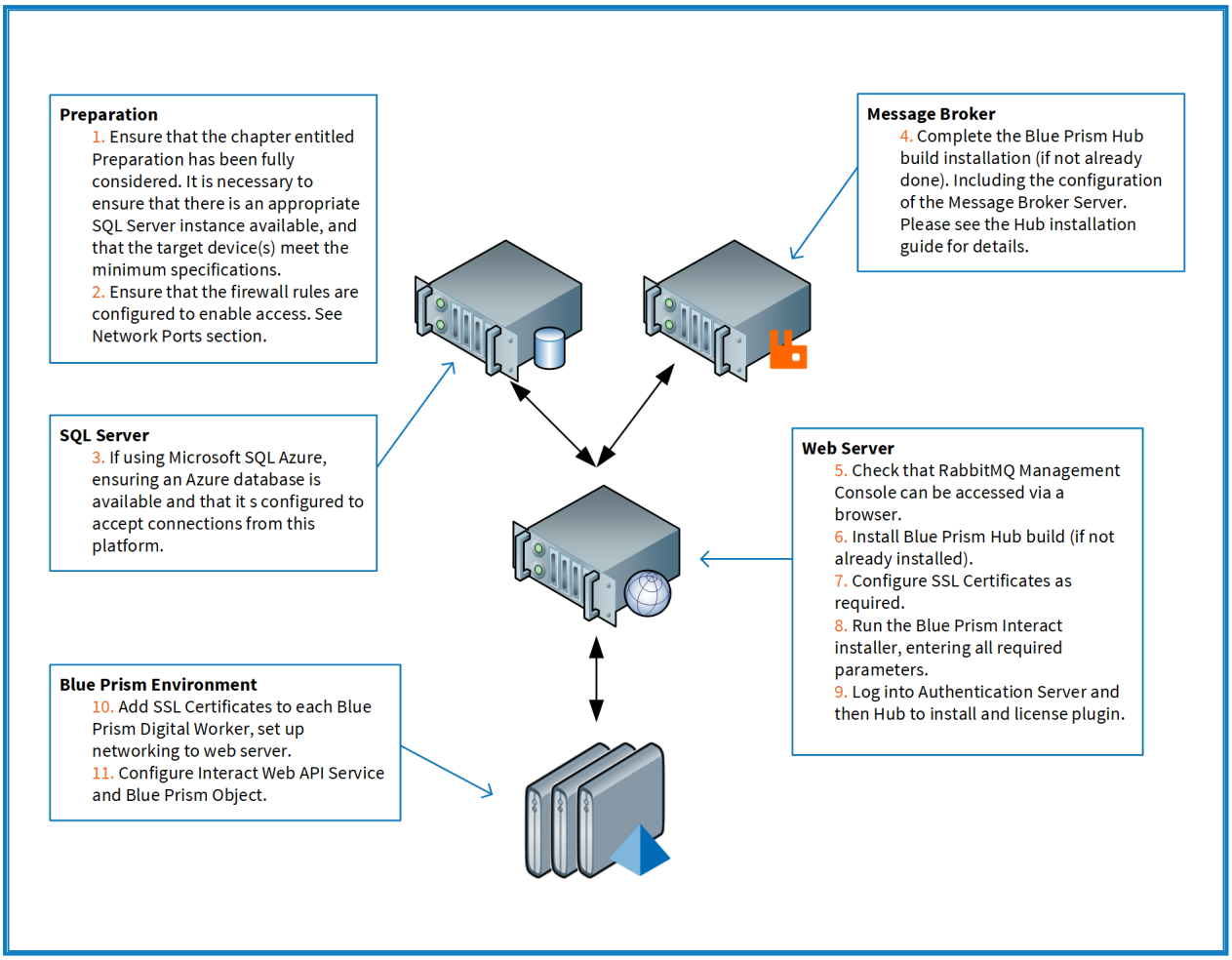
Das folgende Diagramm veranschaulicht die typische Architektur für eine Umgebung.



Elemente in Grau werden als Teil der Blue Prism Hub Installation bereitgestellt.

Übersicht der typischen Installationsschritte

Eine Übersicht der für eine typische Bereitstellung nötigen Schritte finden Sie im Folgenden.



Bei Problemen während der Installation siehe Fehlerbehebung einer Installation.

Message-Broker-Server installieren

Installieren und konfigurieren Sie den Message-Broker-Server, einschließlich der Konfiguration der Windows-Firewall zur Aktivierung der Netzwerkverbindung und der RabbitMQ Managementkonsole.

Anleitungsvideos zur Installation der Software für den Message-Broker-Server finden Sie unter: https://bpdocs.blueprism.com/video/installation.htm.

Informationen zu den Softwareversionen finden Sie unter Software-Anforderungen auf Seite 13.

Wenn der Message-Broker nicht bereits installiert und konfiguriert ist, führen Sie die folgenden Schritte aus:

1. Laden Sie Erlang herunter, installieren Sie es und bestätigen Sie dabei die Standardeinstellungen im Installationsassistenten.

   Welche Version von Erlang Sie benötigen, hängt von der RabbitMQ-Version ab, die Sie verwenden möchten. Informationen:
   - zu Erlang/OTP-Version und -Support siehe Anforderungen für RabbitMQ Erlang-Version.
   - zur Installation finden Sie im Erlang-/OTP-Installationshandbuch.
   - Downloads finden Sie unter Download von Erlang/OTP.

   Dieser Installationsschritt wird in unserem Erlang-Installationsvideo gezeigt.

2. Laden Sie RabbitMQ herunter, installieren Sie es und akzeptieren Sie die Standardeinstellungen.

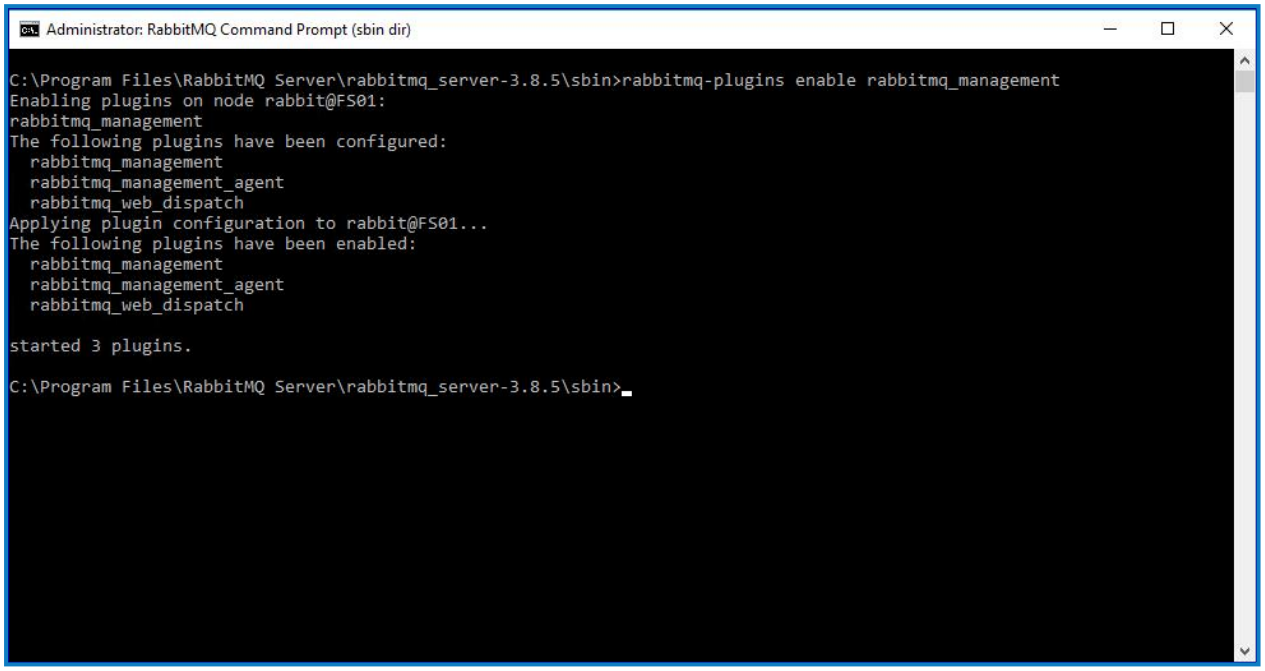
   Mehr erfahren Sie unter siehe RabbitMQ herunterladen und installieren.

   Dieser Installationsschritt wird in unserem RabbitMQ-Installationsvideo gezeigt.

3. Konfigurieren Sie Windows Firewall, um eingehenden Datenverkehr an die Ports 5672 und 15672 zu aktivieren.
4. Wählen Sie im Menü „Start“ unter dem Ordner „RabbitMQ Server“ die Datei „RabbitMQ Command Prompt“ (sbin dir).

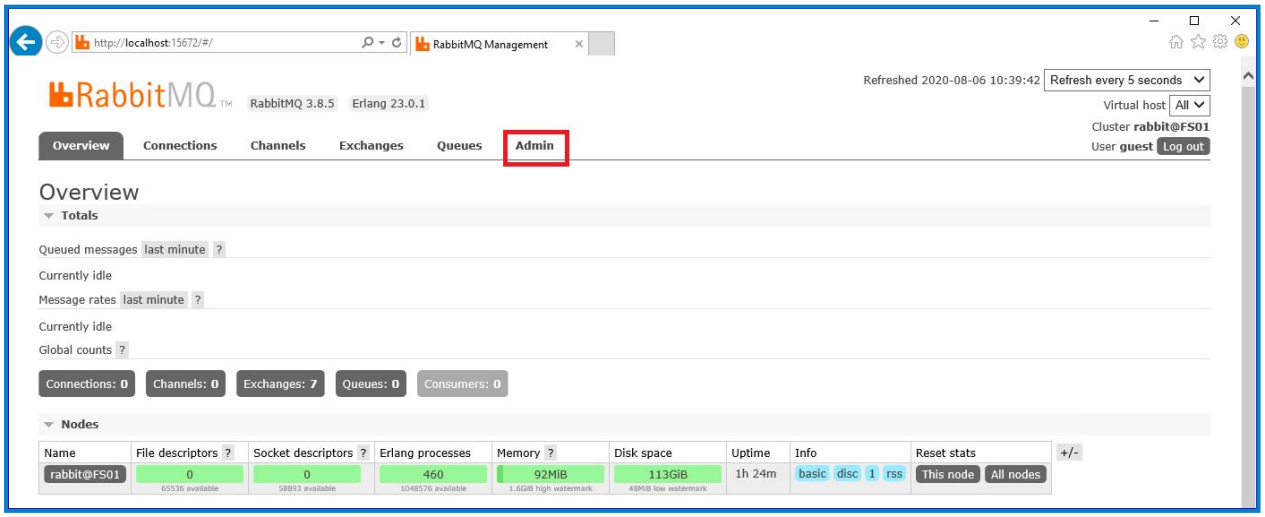
5. Geben Sie im Fenster „RabbitMQ Command Prompt“ den folgenden Befehl ein:

```
rabbitmq-plugins enable rabbitmq_management
```

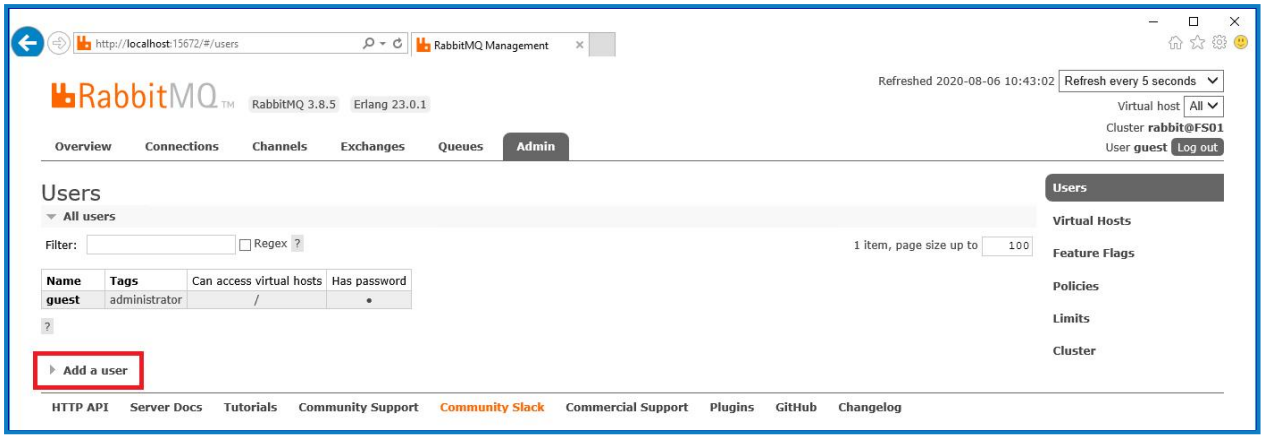


6. Starten Sie einen Browser und navigieren Sie zur folgenden URL: http://localhost:15672
7. Melden Sie sich in der RabbitMQ-Konsole mit den Standard-Anmeldedaten „guest/guest“ an.

8. Klicken Sie in der Konsole auf **Admin**.



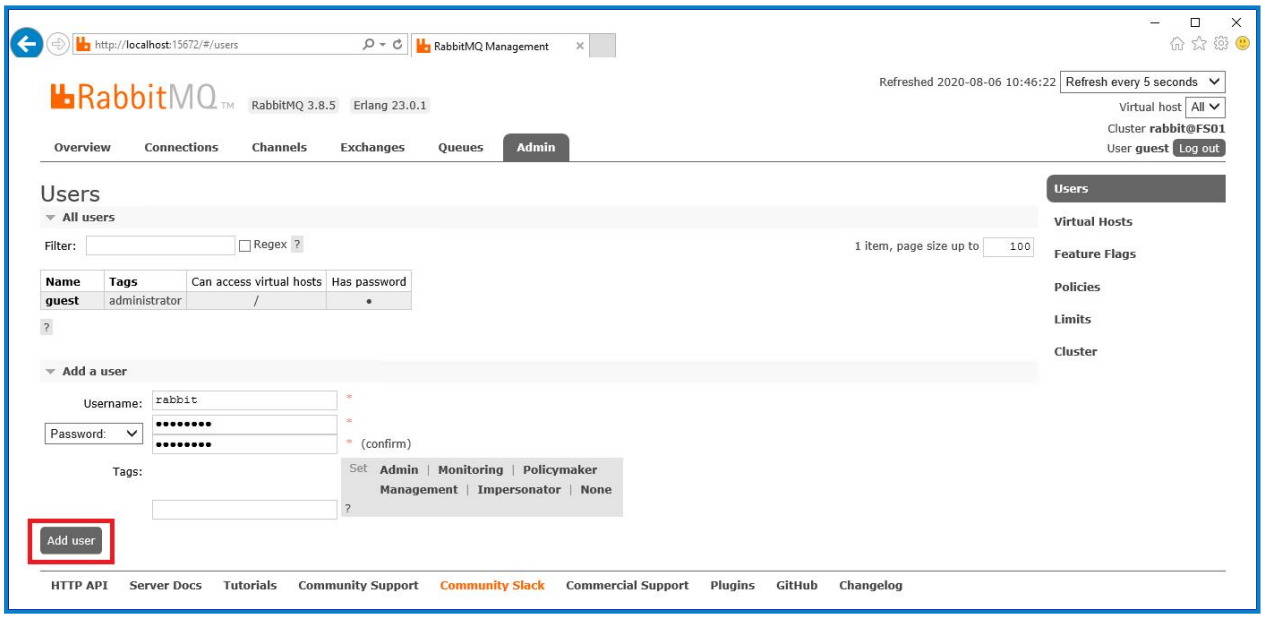
9. Klicken Sie auf **Add a user** (Einen Benutzer hinzufügen).



10. Geben Sie die Details für einen neuen Benutzer ein, indem Sie den Benutzernamen und das Passwort angeben. Der Benutzer benötigt keine speziellen Berechtigungen, die Voreinstellung „None“ (Keine) kann beibehalten werden.

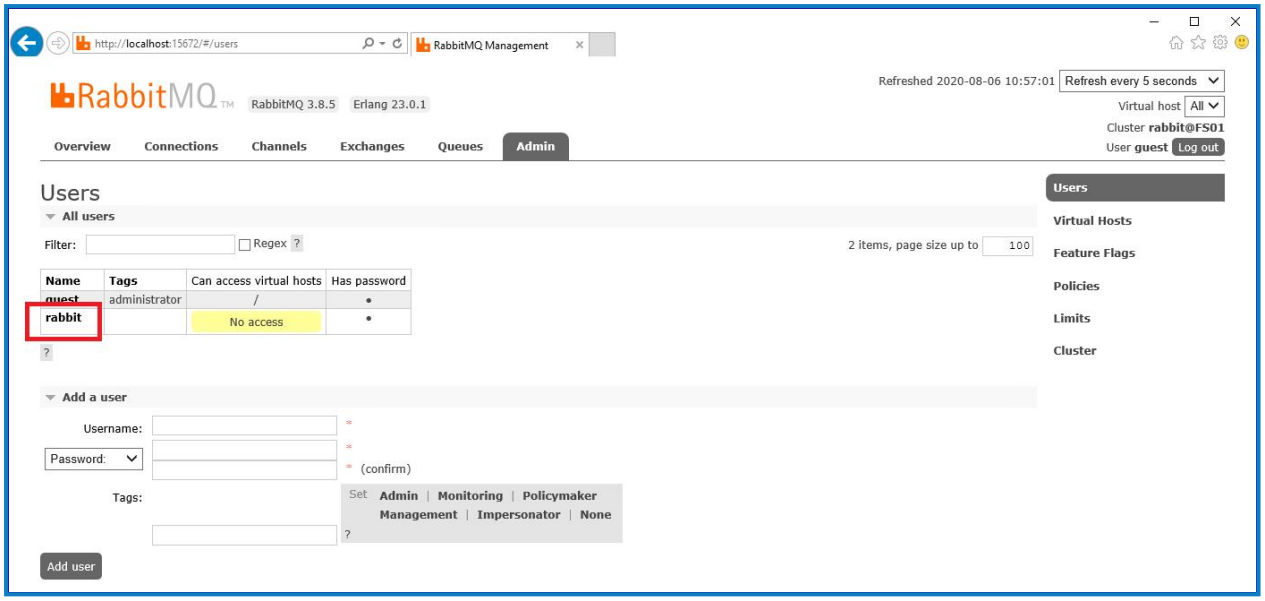
> Die folgenden Zeichen dürfen bei der Erstellung des RabbitMQ-Benutzers nicht für das Passwort verwendet werden: **# / : ? @ \ ` " $ '**.

11. Klicken Sie auf **Add User** (Benutzer hinzufügen).

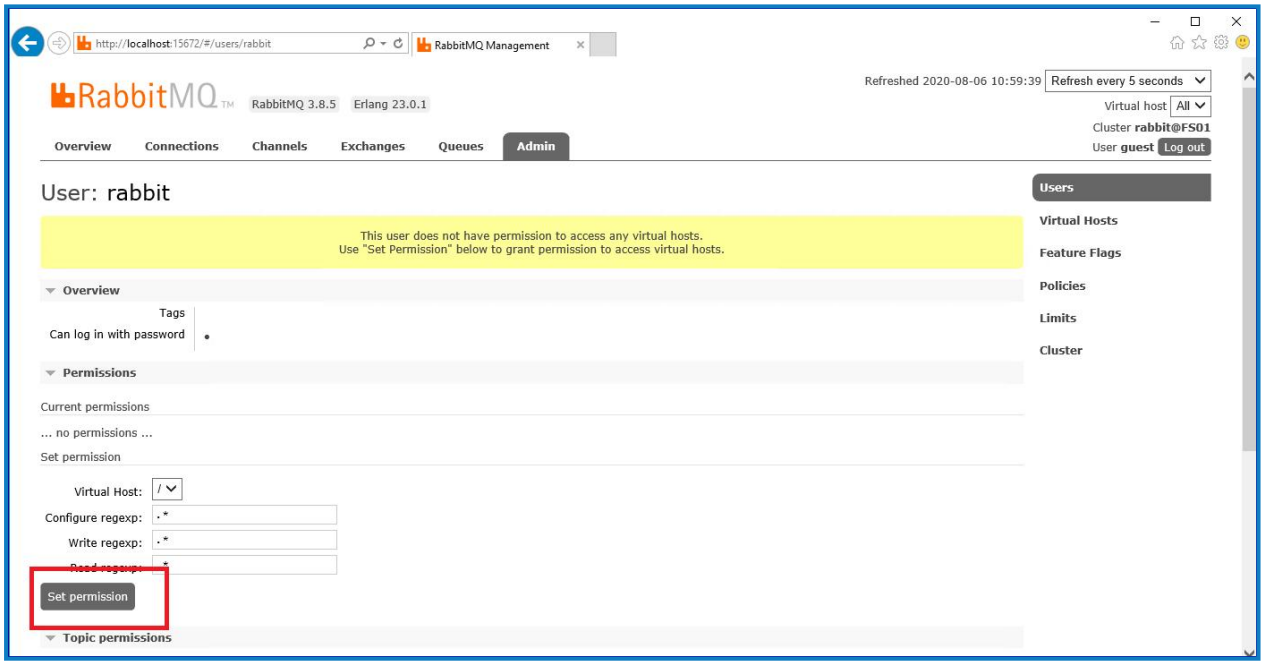


Als Nächstes werden die Berechtigungen des Benutzers festgelegt.

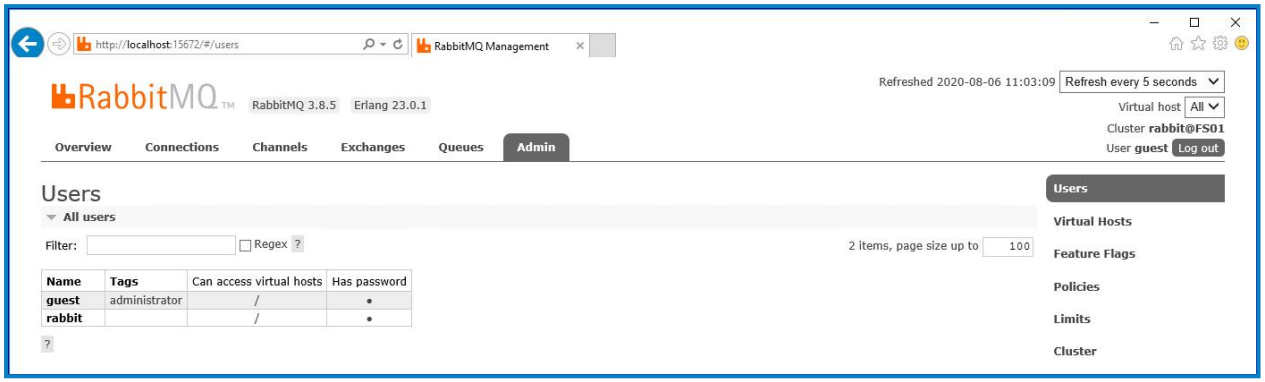
12. Klicken Sie auf den Benutzernamen des Benutzers, den Sie gerade erstellt haben.



13. Klicken Sie auf **Set Permission** (Berechtigung festlegen), um die Standardberechtigungen zuzuweisen.



14. Wählen Sie oben auf der Registerkarte **Admin** aus und überprüfen Sie, ob die Berechtigungen ordnungsgemäß festgelegt wurden, wie unten gezeigt.



Dieses Konto hat keinen Zugriff auf die Managementkonsole. Wenn Sie also die soeben erstellten Anmeldedaten verwenden, wird kein Zugriff gewährt.

Hierbei handelt es sich um ein generisches Setup und die Basisinstallation eines RabbitMQ-Message-Broker-Dienstes. Es wird empfohlen, die Standardpasswörter zu ändern und alle Sicherheitsanforderungen wie die Anwendung von SSL-Zertifikaten von Ihrer IT-Abteilung zu erfüllen.

Es wird empfohlen, ein neues Administratorkonto zu erstellen und das Standard-Gästekonto zu entfernen. Wenn Sie das Standard-Gästekonto verfügbar lassen, kann dies ein Sicherheitsrisiko darstellen.

Konnektivität des RabbitMQ-Message-Broker überprüfen

Starten Sie einen Browser und geben Sie die folgende URL ein: http://<Message Broker Hostname>:15672

Die Anmeldungsseite für die RabbitMQ Managementkonsole sollte angezeigt werden.

Sie können sich nicht bei der Managementkonsole anmelden, da das Gästekonto standardmäßig auf den lokalen Zugriff beschränkt ist und das von Ihnen erstellte Konto nicht für den Zugriff auf die Managementkonsole autorisiert ist.

Wenn die Konsole nicht angezeigt wird, starten Sie den RabbitMQ Dienst neu. Wenn die Konsole immer noch nicht angezeigt wird, siehe Fehlerbehebung einer Hub Installation auf Seite 99.

Webserver installieren und konfigurieren

Lesen Sie vor dem Installieren des Hub Webservers die Informationen unter Vorbereitung auf Seite 7.

Installieren und konfigurieren Sie den Webserver, um sicherzustellen, dass das System mit dem RabbitMQ Message Broker kommunizieren kann .

Der Prozess besteht aus den folgenden Schritten:

1. IIS installieren
2. SSL-Zertifikate konfigurieren
3. .NET Core-Komponenten installieren
4. Blue Prism Hub installieren
5. Authentication Server SAML 2.0-Erweiterung – Dies ist nur erforderlich, wenn Sie die SAML 2.0-Authentifizierung verwenden möchten.

Die Standard-Hostnamen, die in den folgenden Verfahren angegeben sind, eignen sich nur für eine eigenständige Umgebung, wie z. B. eine Testumgebung. Die DNS- und Domänenstrukturen Ihrer Organisation müssen bei der Auswahl von Hostnamen in Ihrer Installation berücksichtigt werden.

Anleitungsvideos zur Installation von der erforderlichen Software und Blue Prism Hub finden Sie unter: https://bpdocs.blueprism.com/de-de/video/installation.htm.

IIS installieren

Für das System müssen IIS Web Server und die .NET Core-Komponenten installiert werden.

Es ist wichtig, dass IIS vor der Installation der .NET Core-Komponenten und des Blue Prism Hub installiert wird. Die IIS-Funktionen und -Rollen werden automatisch mit Blue Prism Hub installiert.

Skriptinstallation

Führen Sie den folgenden Befehl mithilfe der PowerShell-Eingabeaufforderung aus:

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

Dieser Installationsschritt wird in unserem IIS-Installationsvideo gezeigt.

Standardmäßig wird IIS mit aktivierter **anonymer Authentifizierung** installiert. Diese Einstellung ist für Hub und die zugehörigen Websites erforderlich. Wenn Sie **Anonyme Authentifizierung** deaktiviert haben, müssen Sie diese aktivieren, bevor Sie das Hub Installationsprogramm ausführen. Weitere Informationen zur anonymen Authentifizierung finden Sie auf der Seite Anonyme Authentifizierung von Microsoft.

SSL-Zertifikate konfigurieren

Während des Installationsvorgangs werden Sie nach den SSL-Zertifikaten für die Websites gefragt, die eingerichtet werden. Je nach den Sicherheitsanforderungen Ihrer Infrastruktur und IT-Organisation kann dies ein intern erstelltes SSL-Zertifikat oder ein erworbenes Zertifikat zum Schutz der Website sein.

> Geben Sie beim Generieren eines Zertifikats den Hostnamen in Kleinbuchstaben ein. Wenn Sie nicht ausschließlich Kleinbuchstaben verwenden, kann es beim Verwenden des Hub Installationsprogramms passieren, dass der Name im Zertifikat nicht mit dem Hostnamen übereinstimmt. Das kann dazu führen, dass das Zertifikat nicht angewandt wird und das Installationsprogramm Sie daran hindert, mit der Installation fortzufahren.

Das Installationsprogramm kann ausgeführt werden, ohne dass die Zertifikate vorhanden sind. Damit die Websites funktionieren können, müssen die Bindungen auf der IIS-Website jedoch mit gültigen SSL-Zertifikaten konfiguriert werden.

In den folgenden Tabellen sind die erforderlichen SSL-Zertifikate aufgeführt.

Hub Websites:

Website in IIS	Standard-URL (nur Beispiel)
Websites mit einer Benutzeroberfläche zur Nutzung durch Endbenutzer	
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – Hub	https://hub.local
Websites nur zur Nutzung durch die Anwendung (Dienste)	
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

Interact Websites:

Website in IIS	Standard-URL
Websites mit einer Benutzeroberfläche zur Verwendung durch Endbenutzer	
Blue Prism – Interact	https://interact.local
Websites nur zur Nutzung durch die Anwendung (Dienste)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

> Die oben gezeigten Standard-URLs eignen sich für eine eigenständige Umgebung, wie z. B. eine Testumgebung. Die DNS- und Domänenstrukturen Ihrer Organisation müssen bei der Auswahl von Hostnamen für Ihre Installation berücksichtigt werden.

Selbstsignierte Zertifikate

Selbstsignierte Zertifikate können verwendet werden, werden jedoch nur für Demonstrations- (Proof Of Concept, POC), POV- (Proof Of Value) und Entwicklungsumgebungen empfohlen. Verwenden Sie für Produktionsumgebungen Zertifikate von der von Ihrer Organisation genehmigten Zertifizierungsstelle. Es wird empfohlen, dass Sie sich an Ihr IT-Sicherheitsteam wenden und die bestehenden Anforderungen in Erfahrung bringen.

So generieren und verwenden Sie ein selbstsigniertes Zertifikat für SQL Server:

Microsoft stellt ein Skript bereit, mit dem ein selbstsigniertes Zertifikat für SQL Server generiert werden kann. Weitere Informationen finden Sie in der Microsoft-Dokumentation. Es ist wichtig, dass der vom SQL Server verwendete Fully Qualified Domain Name (FQDN) mit dem im Zertifikat definierten FQDN übereinstimmt. **Wenn diese nicht übereinstimmen, wird keine Verbindung zur Datenbank hergestellt und Ihre Installation wird nicht richtig funktionieren.**

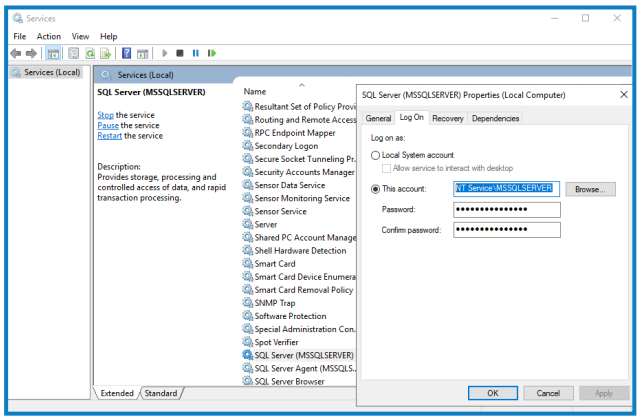
1. Starten Sie die PowerShell als Administrator und führen Sie das Microsoft-Skript mit den Informationen für Ihren SQL Server aus.

   Dadurch wird das Zertifikat generiert und auf dem SQL Server installiert.

2. Auf Ihrem SQL Server:

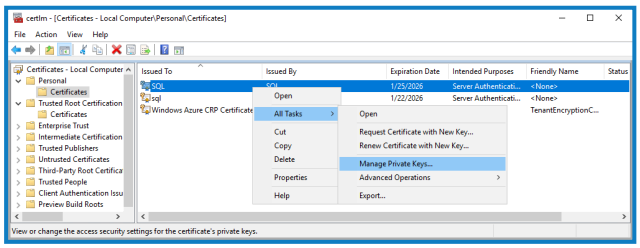
   a. Aktivieren Sie den Zugriff auf den privaten Schlüssel des Zertifikats für das SQL Server-Dienstkonto. Gehen Sie dazu wie folgt vor:

      i. Wenn Sie ihn noch nicht kennen, suchen Sie den Dienstkontonamen für Ihren SQL Server. Er wird auf der Registerkarte „Anmelden“ der SQL Server-Eigenschaften angezeigt, die auf Ihrem SQL Server unter „Dienste“ verfügbar sind.

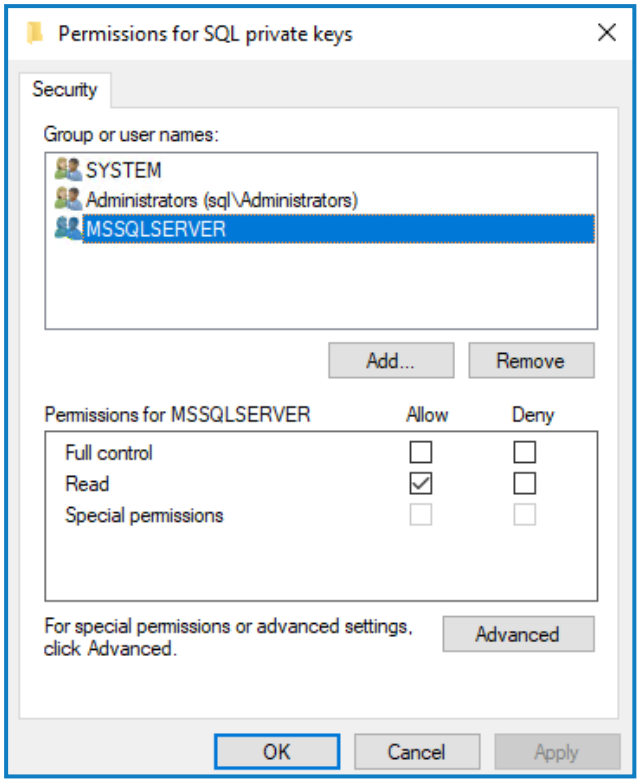


      ii. Öffnen Sie den Zertifikat-Manager auf dem SQL Server.

      iii. Erweitern Sie **Eigene Zertifikate**, dann **Zertifikate**, klicken Sie mit der rechten Maustaste auf **SQL**, wählen Sie **Alle Aufgaben** aus und klicken Sie dann auf **Private Schlüssel verwalten...**



iv. Fügen Sie im Dialogfeld mit den Berechtigungen für private SQL-Schlüssel Ihr SQL Server-Dienstkonto mit Leseberechtigungen hinzu. Zum Beispiel:



v. Klicken Sie auf **OK**, um die Änderungen anzuwenden und das Dialogfeld zu schließen.

b. Aktivieren Sie SSL auf Ihrem SQL Server und geben Sie das Zertifikat an. Gehen Sie dazu wie folgt vor:

i. Öffnen Sie den **SQL Server-Konfigurations-Manager** in der Windows-Taskleiste.

ii. Erweitern Sie im SQL Server-Konfigurations-Manager die Option **SQL Server-Netzwerkkonfiguration**, klicken Sie mit der rechten Maustaste auf **Protokolle für <SqlServerInstanceName>** und klicken Sie dann auf **Eigenschaften**.

iii. Wählen Sie im Dialogfeld für die Eigenschaften der Protokolle für <SqlServerInstanceName> die Registerkarte **Zertifikat** aus, um dann das gewünschte Zertifikat auszuwählen oder zu importieren.

iv. Klicken Sie auf **Anwenden**.

v. Klicken Sie auf **OK**, um das Eigenschaften-Dialogfeld zu schließen.

c. Starten Sie den SQL Server-Dienst neu.

d. Kopieren Sie das Zertifikat „C:\sqlservercert.cer“. Sie müssen es zu den Website-Hostservern für Hub und Interact hinzufügen.

3. Auf den Website-Hostservern:

a. Fügen Sie „sqlservercert.cer“ in die Website-Hostserver für Hub und Interact ein.

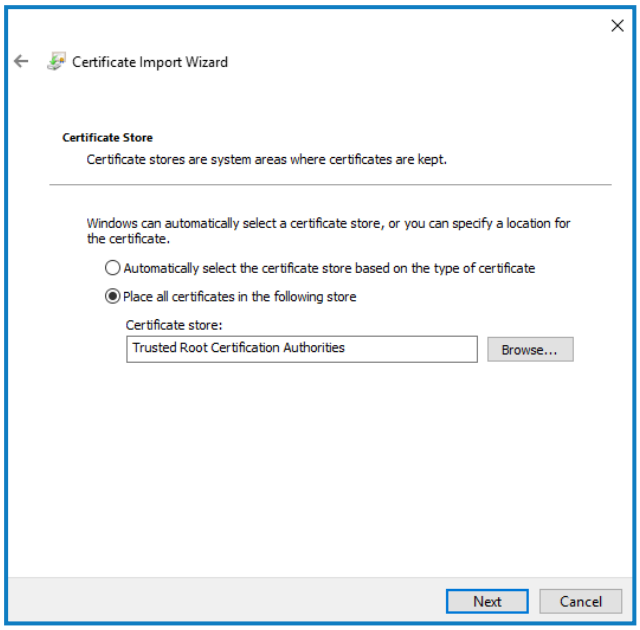
b. Fügen Sie das Zertifikat zum Zertifikatspeicher für die vertrauenswürdigen Stammzertifizierungsstellen des Servers hinzu. Gehen Sie dazu wie folgt vor:

i. Doppelklicken Sie auf das Zertifikat und klicken Sie auf **Zertifikat installieren...**.

Der Zertifikatimport-Assistent wird angezeigt.

ii. Wählen Sie auf der Willkommensseite die Option **Lokaler Computer** unter **Speicherort** aus und klicken Sie auf **Weiter**.

iii. Wählen Sie auf der Seite „Zertifikatspeicher“ die Option **Alle Zertifikate in folgendem Speicher speichern** aus und geben Sie **Vertrauenswürdige Stammzertifizierungsstelle** ein.



iv. Klicken Sie auf **Weiter** und folgen Sie dem Assistenten bis zum Abschluss.

c. Testen Sie die Verbindung vom Website-Hostserver zum SQL Server.

So generieren Sie ein selbstsigniertes Zertifikat für eine Website:

1. Führen Sie die PowerShell als Administrator aus und verwenden Sie den folgenden Befehl, wobei Sie `[Website]` und `[ExpiryYears]` durch entsprechende Werte ersetzen:

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

Zum Beispiel:

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

Dieses Beispiel erstellt ein selbstsigniertes Zertifikat namens *MySiteCertAuthentication* im persönlichen Zertifikatspeicher mit dem Betreff *authentication.local* und ist ab dem Zeitpunkt der Erstellung 10 Jahre lang gültig.

Geben Sie beim Generieren eines Zertifikats den Hostnamen (`[Website]`) in Kleinbuchstaben ein. Wenn Sie nicht ausschließlich Kleinbuchstaben verwenden, kann es beim Verwenden des Hub Installationsprogramms passieren, dass der Name im Zertifikat nicht mit dem Hostnamen übereinstimmt. Das kann dazu führen, dass das Zertifikat nicht angewandt wird und das Installationsprogramm Sie daran hindert, mit der Installation fortzufahren.

2. Öffnen Sie die Anwendung **Computerzertifikate verwalten** auf Ihrem Webserver (geben Sie den Namen der Anwendung in die Suchleiste ein).
3. Öffnen Sie „Eigene Zertifikate“ > „Zertifikate zur vertrauenswürdigen Stammzertifizierung“ > „Zertifikate“, um das Zertifikat zu kopieren und einzufügen.
4. Wiederholen Sie diesen Prozess für jede Website.

Geskriptete Erstellung der Website selbstsignierter Zertifikate

Dieser Prozess wird für Produktionsumgebungen nicht empfohlen. Dieser Prozess erstellt ein einziges Zertifikat, das auf jede Website angewendet werden kann.

Führen Sie die folgenden PowerShell-Befehle aus:

```
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 muss durch den Host-Servernamen ersetzt werden.

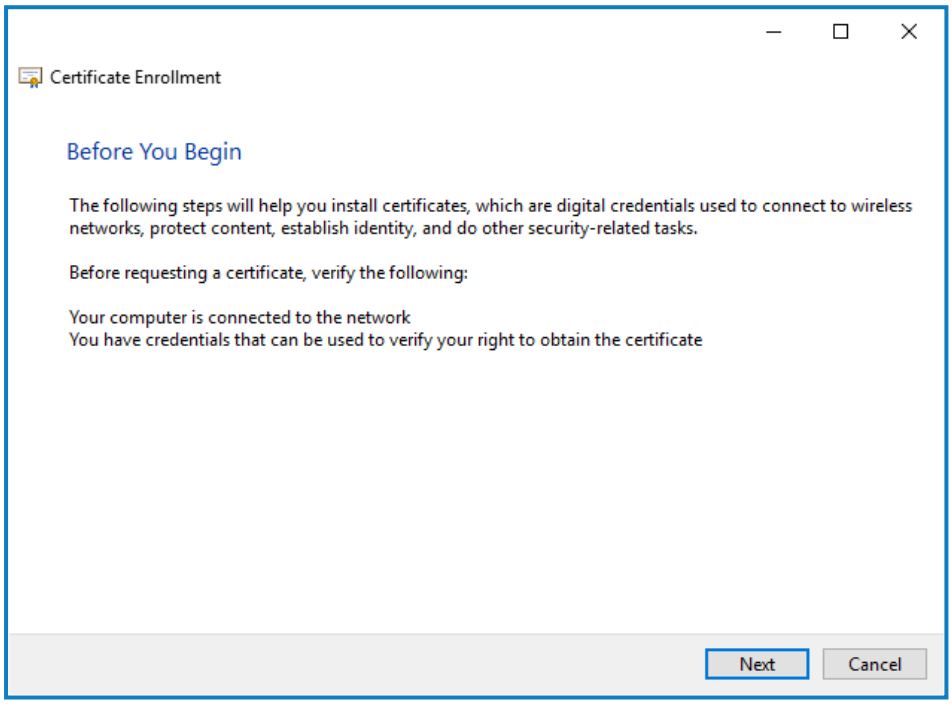
Öffnen Sie nach der Erstellung den Zertifikat-Manager des lokalen Computers (certlm) und kopieren Sie die Zertifikate in den Zertifikatspeicher für vertrauenswürdige Root-Zertifikate.

Offline-Zertifikatanforderung erstellen

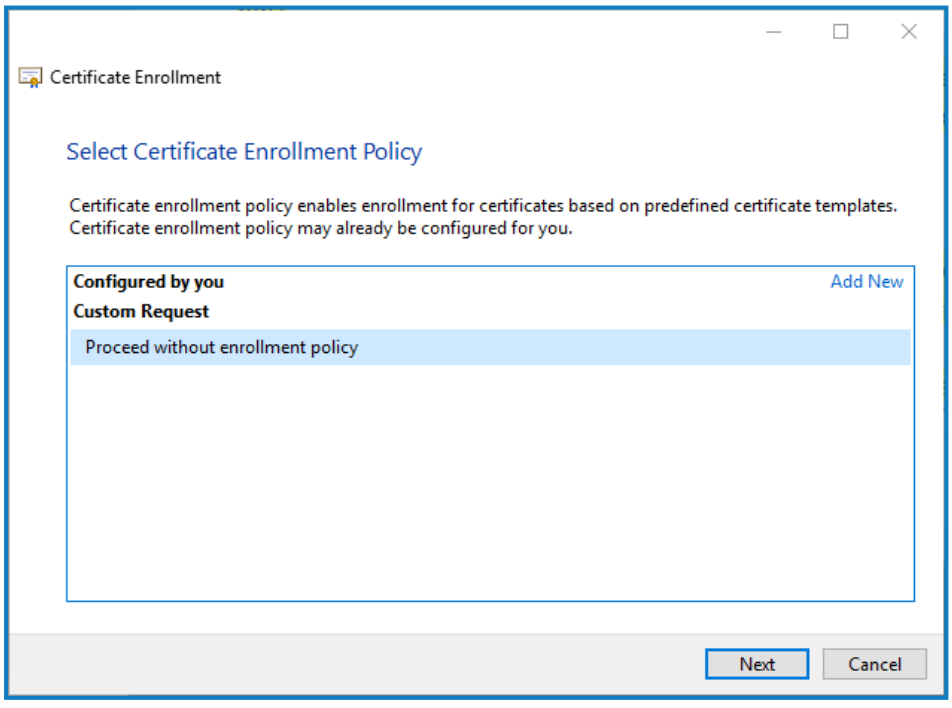
Um eine Offline-Zertifikatanforderung zu erstellen, führen Sie für jedes Zertifikat dieses Verfahren aus:

1. Öffnen Sie die Anwendung „Computerzertifikate verwalten“ auf Ihrem Webserver (geben Sie **Verwalteter Computer** in die Suchleiste ein).
2. Klicken Sie mit der rechten Maustaste auf **Persönlich** > **Zertifikate** und wählen Sie im Kontextmenü **Alle Aufgaben** > **Erweiterte Vorgänge** > **Benutzerdefinierte Anforderung erstellen** aus.

   Der Assistent zur Zertifikatsregistrierung wird angezeigt.

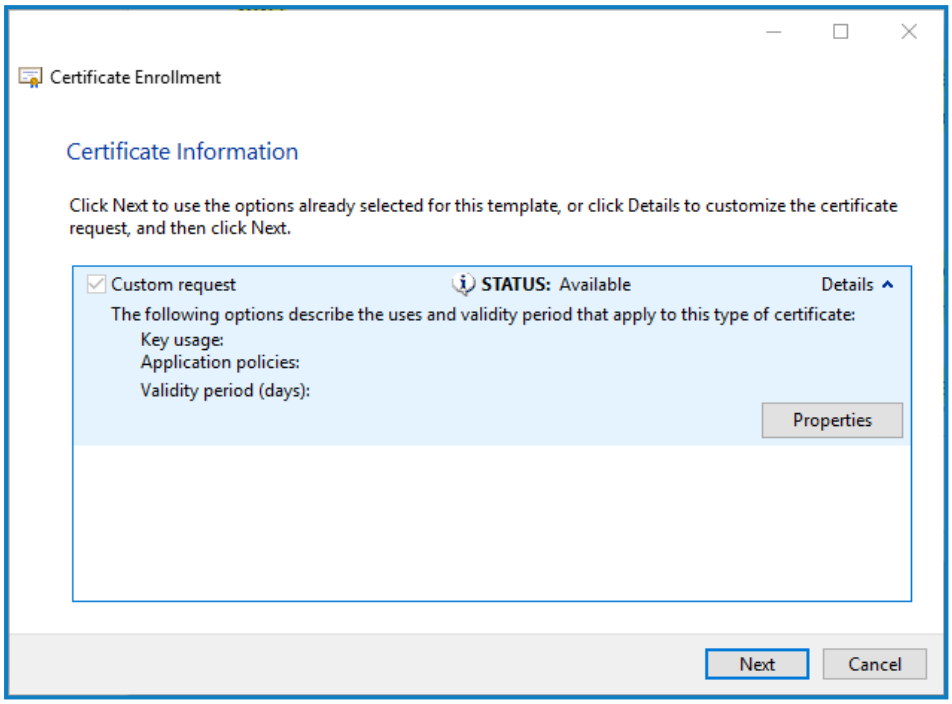


3. Klicken Sie auf **Weiter**.



4. Wählen Sie **Den Vorgang ohne Registrierungsrichtlinie fortsetzen** und klicken Sie auf **Weiter**.

5. Klicken Sie auf dem Bildschirm „Benutzerdefinierte Anforderung“ auf **Weiter**.
6. Klicken Sie auf dem Bildschirm „Zertifikatsinformationen“ auf die Dropdown-Liste **Details** und dann auf **Eigenschaften**.



7. Geben Sie auf der Registerkarte „Allgemein“ im Dialogfeld „Zertifikateigenschaften“ einen Anzeigenamen und eine Beschreibung ein, die auf der Website basieren, auf die dieses Zertifikat angewendet wird.
8. Ändern Sie auf der Registerkarte „Antragsteller“ den Namenstyp des Antragstellers zu **Allgemeiner Name**, geben Sie die URL der Website in das Feld **Wert** ein und klicken Sie auf **Hinzufügen**.

   Der allgemeine Name (CN) wird im rechten Panel angezeigt.
9. Klicken Sie auf der Registerkarte „Erweiterungen“ auf **Erweiterte Schlüsselverwendung**, wählen Sie **Serverauthentifizierung** und klicken Sie auf **Hinzufügen**.
10. Klicken Sie auf der Registerkarte „Privater Schlüssel“ auf **Schlüsseloptionen**, wählen Sie eine Schlüssellänge Ihrer Wahl aus und wählen Sie **Privaten Schlüssel exportierbar machen**.
11. Klicken Sie auf der Registerkarte „Privater Schlüssel“ auf **Hashalgorithmus** und wählen Sie einen geeigneten Hash aus (optional).
12. Klicken Sie auf **OK**.

    Sie gelangen zurück zum Bildschirm „Zertifikatsregistrierung“.
13. Klicken Sie auf **Weiter**.
14. Fügen Sie einen Dateinamen und Pfad hinzu und klicken Sie auf **Fertigstellen**.

Nachdem Sie Ihre Zertifikatanforderung erstellt haben, müssen Sie sie an eine Zertifizierungsstelle übermitteln, damit diese Ihre Anforderung bearbeiten und ein Zertifikat ausstellen kann. Die Zertifikatanforderung ist eine Textdatei. Normalerweise müssen Sie den Text aus der Datei kopieren und in ein Online-Einreichungsformular auf der Website der Zertifizierungsstelle eingeben. Sie müssen sich direkt an Ihre Zertifizierungsstelle wenden, um Anweisungen zum Prozess zur Einreichung Ihrer Zertifikatanforderung zu erhalten.

.NET Core-Komponenten installieren

Die .NET Core-Komponenten müssen heruntergeladen und installiert werden.

Schritt	Details
1	Laden Sie die folgenden Komponenten herunter und speichern Sie sie in einem temporären Verzeichnis, zum Beispiel C:\temp: • ASP.NET Core Runtime 6.0.9 oder 6.0.10 (Windows Hosting Bundle) https://dotnet.microsoft.com/download/dotnet/6.0 – Wählen Sie die benötigte Version aus. Wählen Sie unter **ASP.NET Core Runtime** die Option **Hosting-Paket** aus. • .NET Desktop Runtime 6.0.9 oder 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 – Wählen Sie die benötigte Version aus. Wählen Sie unter **.NET Desktop Runtime** den benötigten Download aus. • .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 Unter Windows Server 2022 wird dies standardmäßig installiert. Sie müssen .NET Framework nur installieren, wenn Sie Windows Server 2016 Datacenter oder Windows Server 2019 verwenden.

2	Um die .NET-Abhängigkeiten zu installieren, führen Sie jeden der folgenden Befehle mit der PowerShell-Eingabeaufforderung aus und warten Sie, bis jeder abgeschlossen ist, bevor Sie den nächsten Befehl ausführen:
	Für Windows Server 2016 und 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`
	Für 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`
	Stellen Sie sicher, dass der Dateiname und der Dateipfad mit den Dateien übereinstimmen, die in Schritt 1 gespeichert wurden.

3	Starten Sie Ihren Server neu, bevor Sie Blue Prism Hub installieren, um sicherzustellen, dass die Komponenten vollständig installiert und registriert sind.

Dieser Installationsschritt wird in unserem .NET-Installationsvideo gezeigt.

Blue Prism Hub installieren

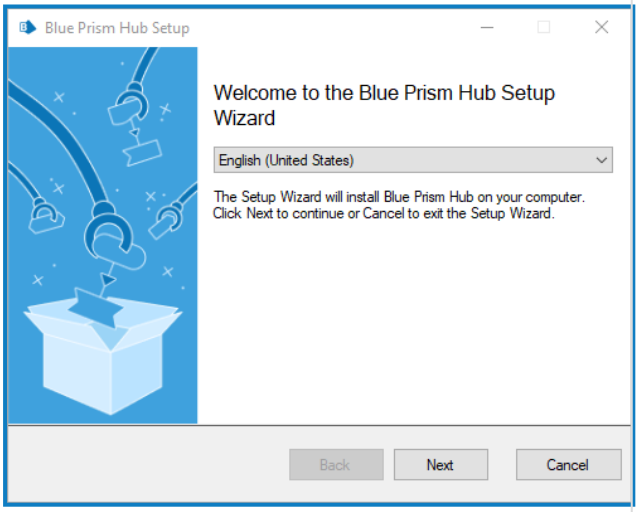
Bevor Sie Blue Prism Hub installieren:

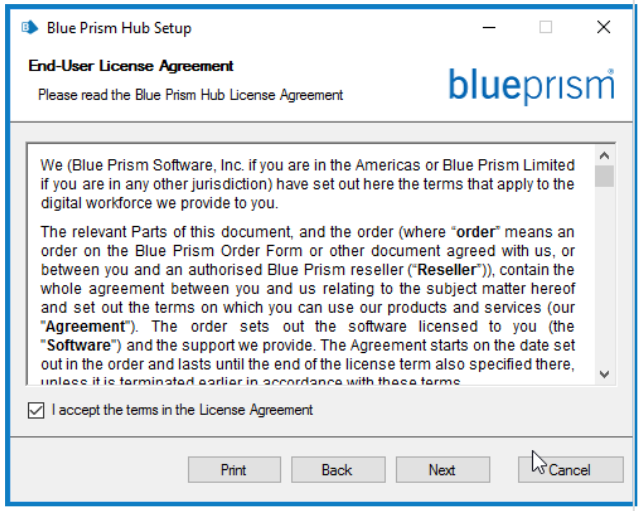
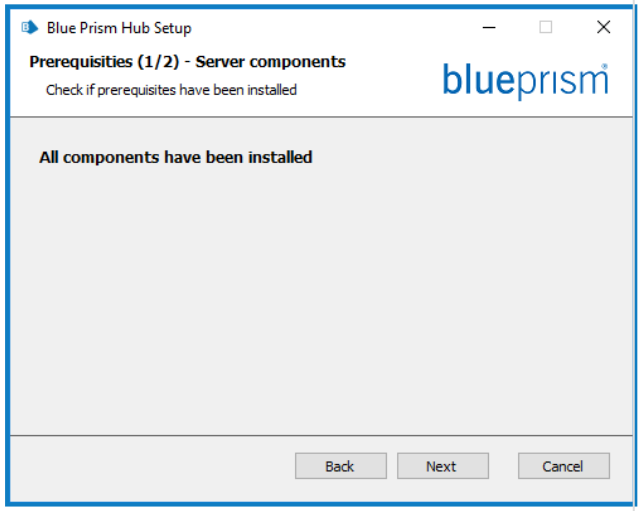
- Wenn Sie ALM, Decision oder Interact gekauft haben, benötigen Sie während der Installation von Hub Ihre Kunden-ID. Diese finden Sie in der E-Mail, die Ihnen beim Kauf von ALM, Decision oder Interact zugesandt wurde.
- Wenn Sie das Blue Prism Decision Plug-in in Hub verwenden möchten, müssen Sie den Blue Prism Decision Model Service Container auf einem Docker-Host installieren, bevor Sie den Hub Installationsassistenten ausführen. Weitere Informationen finden Sie unter Blue Prism Decision installieren.
- Wenn Sie Blue Prism Hub nach vorherigem Verwenden und Entfernen neu installieren und dieselben Datenbanknamen verwendet werden sollen, wird empfohlen, alte Daten vor der Neuinstallation aus den Datenbanken zu löschen.

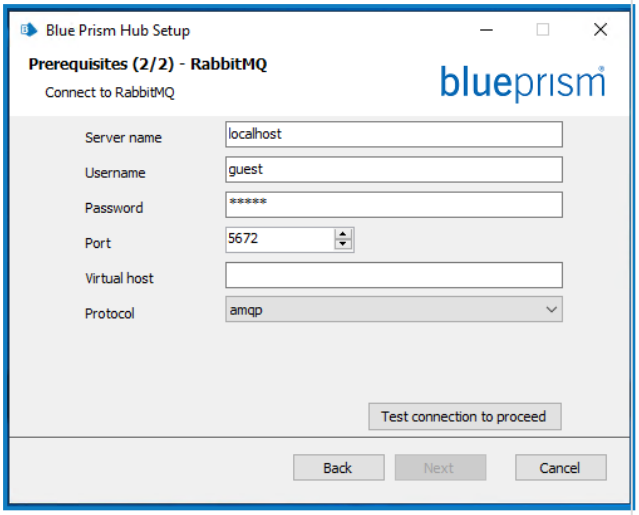
Sehen Sie sich das Blue Prism Hub Installationsvideo für die Installation und Konfiguration von Hub an.

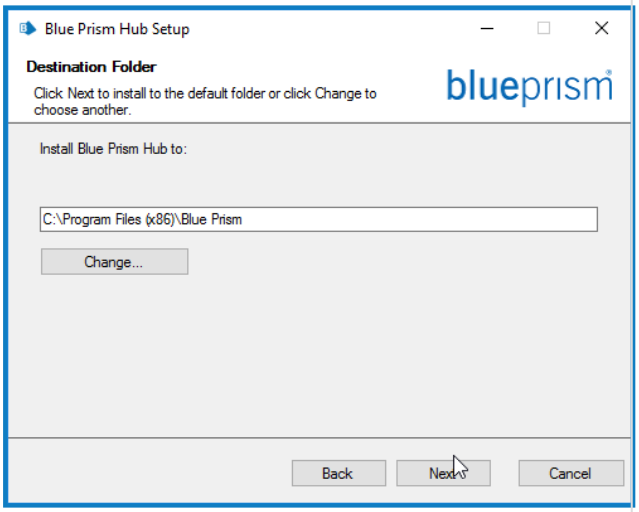
Die folgenden Schritte beschreiben den Prozess zur Installation der Blue Prism Hub Software. Dazu gehören Authentication Server, Hub und andere zugehörige Dienste. Der Installationsprozess wird alle neuen Datenbanken erstellen, die erforderlich sind.

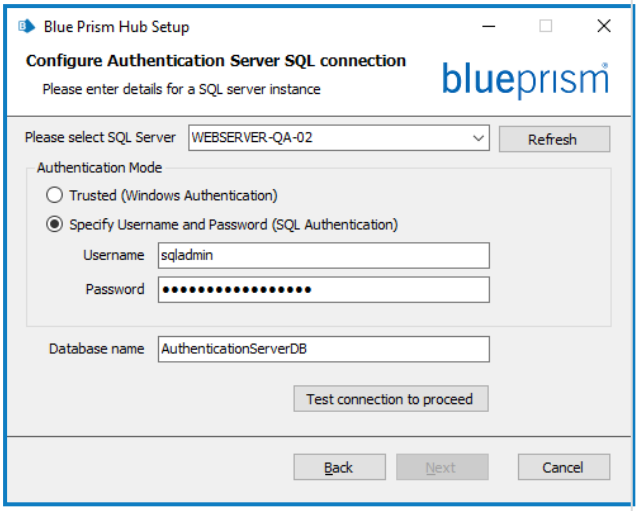
Laden Sie das Blue Prism Hub Installationsprogramm aus dem Blue Prism Portal herunter, führen Sie es aus und gehen Sie wie folgt vor. Das Installationsprogramm muss mit Administratorrechten ausgeführt werden.

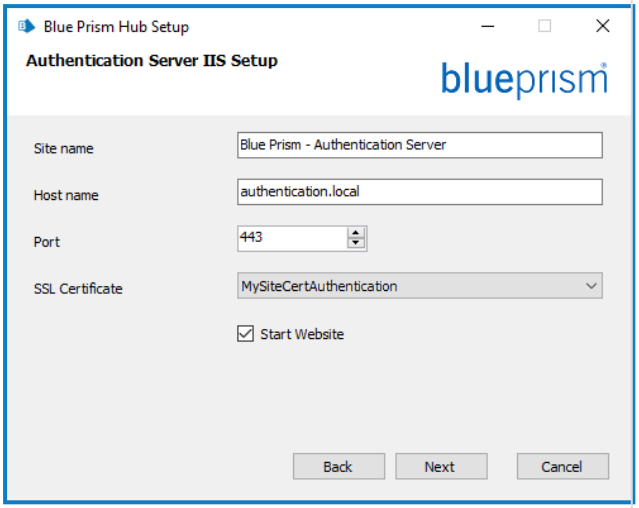
Schritt	Seite des Installationsprogramms	Details
1		**Willkommen** Falls erforderlich, wählen Sie für das Installationsprogramm eine andere Sprache in der Dropdown-Liste aus. Die Standardsprache ist Englisch (USA). Klicken Sie auf **Weiter**.

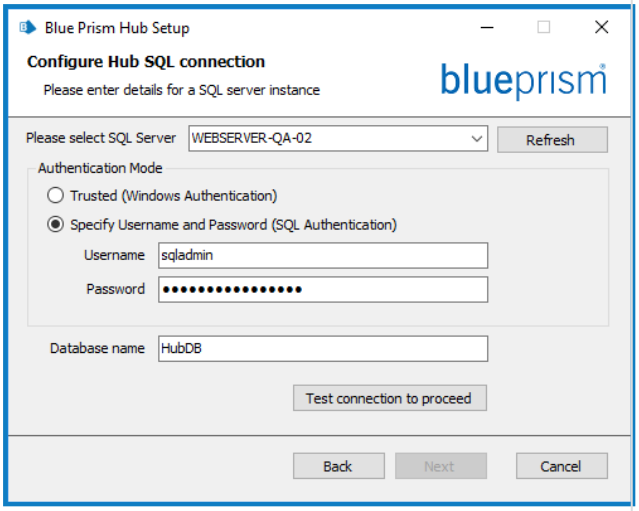
Schritt	Seite des Installationsprogramms	Details
2		**Lizenzvereinbarung** Lesen Sie die Endbenutzer-Lizenzvereinbarung. Wenn Sie den Bedingungen zustimmen, aktivieren Sie das Kontrollkästchen.
3		**Voraussetzungen 1 – Serverkomponenten** Das Installationsprogramm überprüft, ob die Voraussetzungen installiert wurden. Diejenigen, die nicht installiert sind, werden identifiziert. Sie können nicht fortfahren, bis alle Voraussetzungen installiert sind. Wurden fehlende Voraussetzungen erkannt, brechen Sie das Installationsprogramm ab und installieren Sie die fehlenden Komponenten, bevor Sie das Installationsprogramm neu starten. Andernfalls fahren Sie mit der Installation fort.

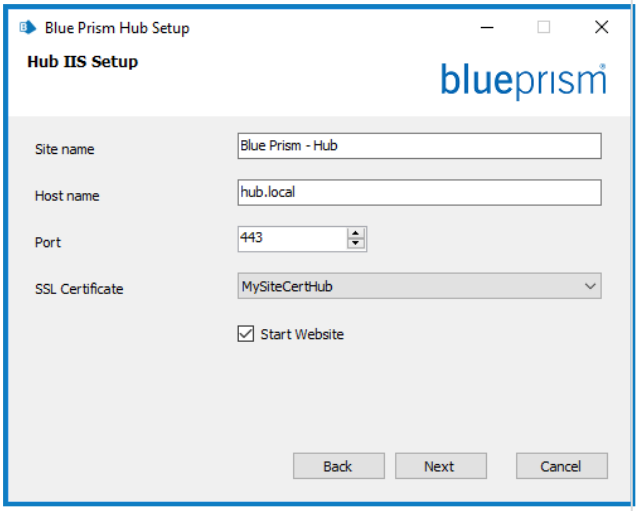
Schritt	Seite des Installationsprogramms	Details
4		**Voraussetzungen 2 – RabbitMQ** Geben Sie den Servernamen oder die IP-Adresse des Message-Broker-Servers und die Anmeldeinformationen des von Ihnen erstellten Benutzers ein. Der Standard-Port für Nachrichtenwarteschlangen ist 5672. Dies sollte nur geändert werden, wenn die Standard-Ports von Ihrer IT-Support-Organisation geändert wurden. Standardmäßig ist das Feld **Virtueller Host** leer. Sie können es leer lassen und die Verbindung wird mit dem RabbitMQ-Root hergestellt. Alternativ können Sie eine Verbindung zu einem bestimmten Host herstellen, wenn Sie virtuelle Hosts in RabbitMQ eingerichtet haben. Geben Sie bei **Virtueller Host** den Namen des virtuellen Hosts auf RabbitMQ ein, mit dem Sie eine Verbindung herstellen möchten. Der virtuelle Host muss bereits auf RabbitMQ vorhanden sein. Sie können keinen neuen Namen eingeben, da dieses Installationsprogramm keinen neuen virtuellen Host erstellt. Weitere Informationen über virtuelle Hosts finden Sie auf der RabbitMQ-Website – Virtuelle Hosts. Wählen Sie in der Dropdown-Liste **Protokoll** das Protokoll aus, das Sie verwenden möchten. Sie können entweder AMQP oder AMQPS auswählen. Wenn Sie AMQPS auswählen, wird ein zusätzliches Feld angezeigt, in dem Sie das Zertifikat eingeben können, das für die Verbindung verwendet werden soll. Weitere Informationen über die TLS-Konfiguration und -Zertifikate finden Sie auf der RabbitMQ-Website – TLS-Unterstützung.

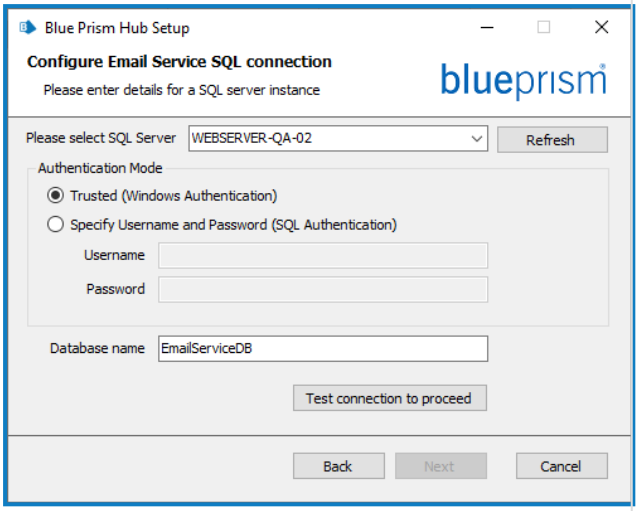
Schritt	Seite des Installationsprogramms	Details
		Wenn Sie AMQPS verwenden, müssen Sie den Blue Prism IIS-Anwendungspools die volle Kontrolle über das RabbitMQ-Zertifikat geben. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 99. Klicken Sie auf **Verbindung testen**, um die Konnektivität zu überprüfen. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, finden Sie weitere Informationen unter Fehlerbehebung einer Hub Installation auf Seite 99.
5		**Zielordner** Geben Sie den erforderlichen Installationsordner an. Der Standardspeicherort ist C:\Programme (x86)\Blue Prism, aber Sie können Ihren eigenen über die Schaltfläche **Ändern** auswählen.

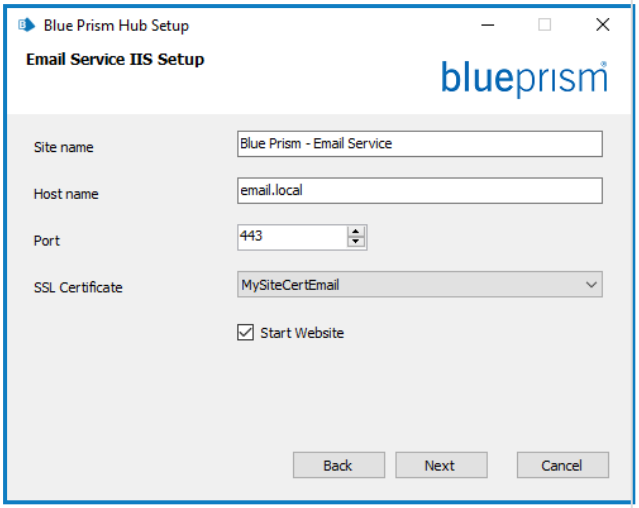
Schritt	Seite des Installationsprogramms	Details
6		**Authentication Server SQL-Verbindung** Einstellungen für die Authentication Server Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

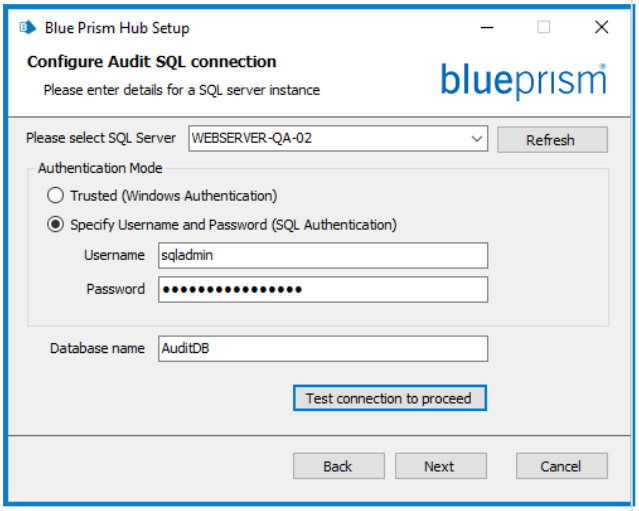
Schritt	Seite des Installationsprogramms	Details
7		**Authentication Server IIS-Einrichtung** Konfigurieren Sie IIS für die Authentication Server Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet. Sobald die Installation abgeschlossen ist, wird die IIS-Funktion **Windows-Authentifizierung** auf der Authentication Server Website aktiviert.

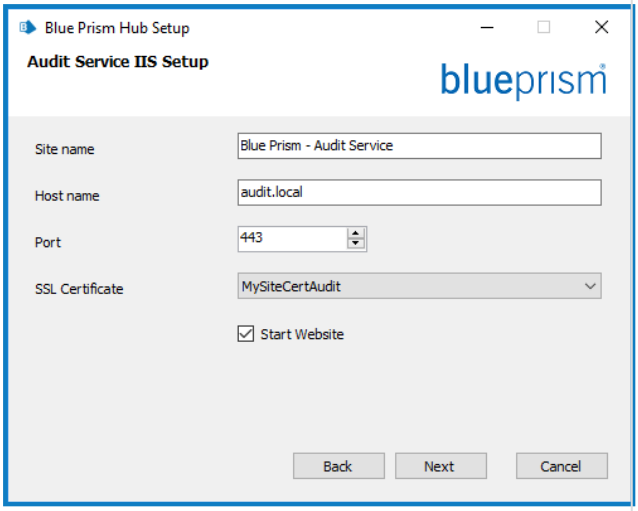
Schritt	Seite des Installationsprogramms	Details
8		**Hub SQL-Verbindung** Einstellungen für die Hub Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

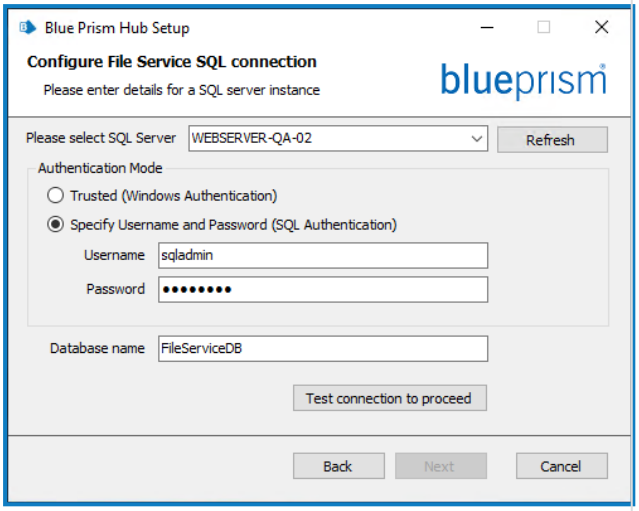
Schritt	Seite des Installationsprogramms	Details
9		**Hub IIS-Setup** Konfigurieren Sie die Hub Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

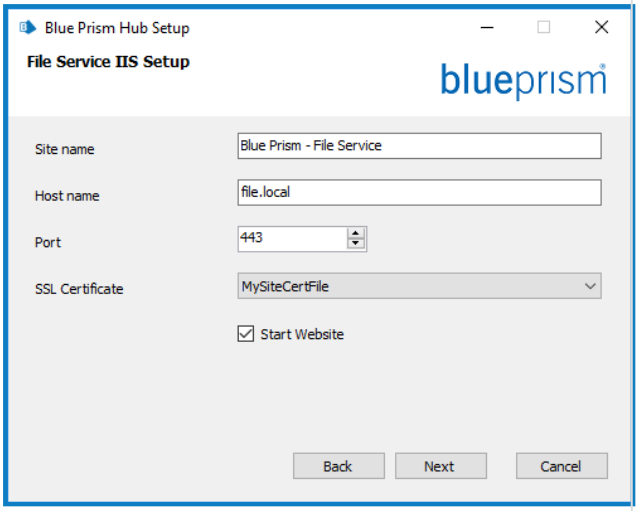
Schritt	Seite des Installationsprogramms	Details
10		**Email Service SQL-Verbindung** Einstellungen für die Email Service Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

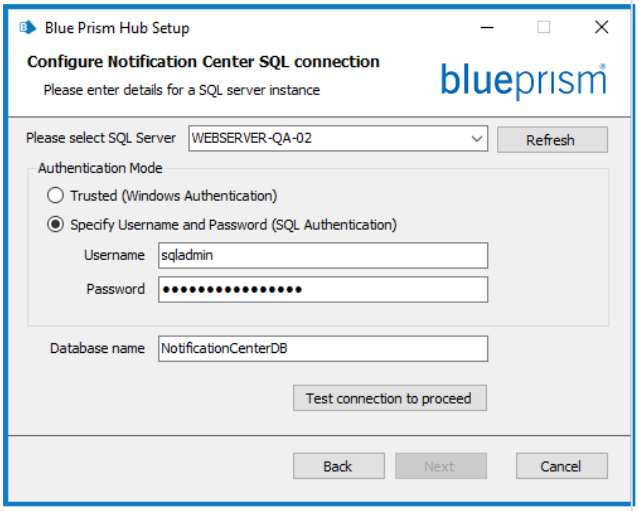
Schritt	Seite des Installationsprogramms	Details
11		**Email Service IIS-Einrichtung** Konfigurieren Sie die Email Service-Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

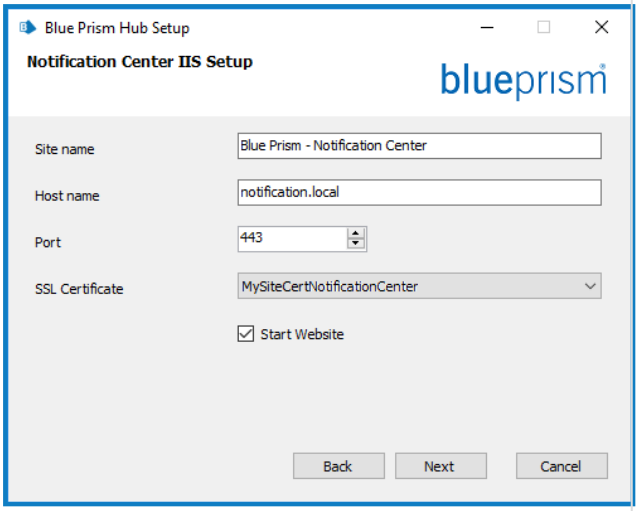
Schritt	Seite des Installationsprogramms	Details
12		**Audit SQL-Verbindung konfigurieren** Einstellungen für die Audit Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

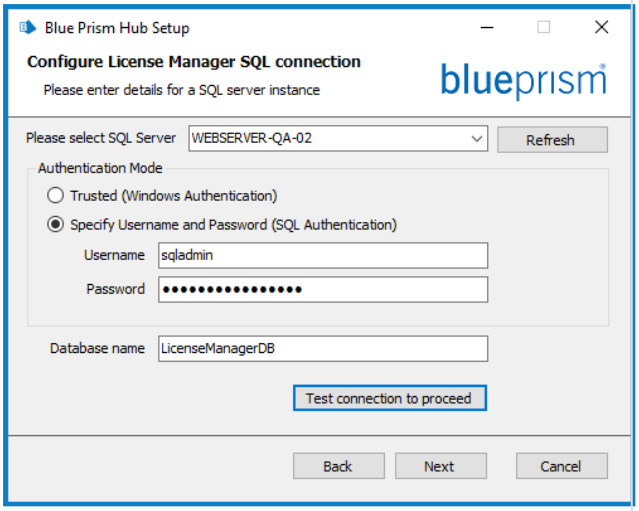
Schritt	Seite des Installationsprogramms	Details
13		**Audit Service IIS-Einrichtung** Konfigurieren Sie die Audit Service Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

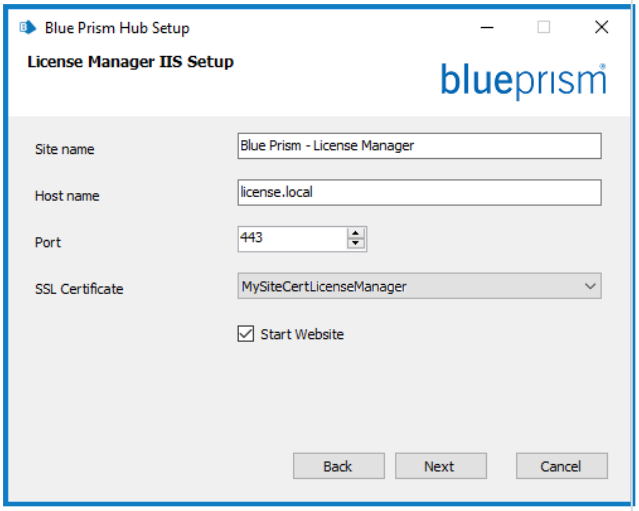
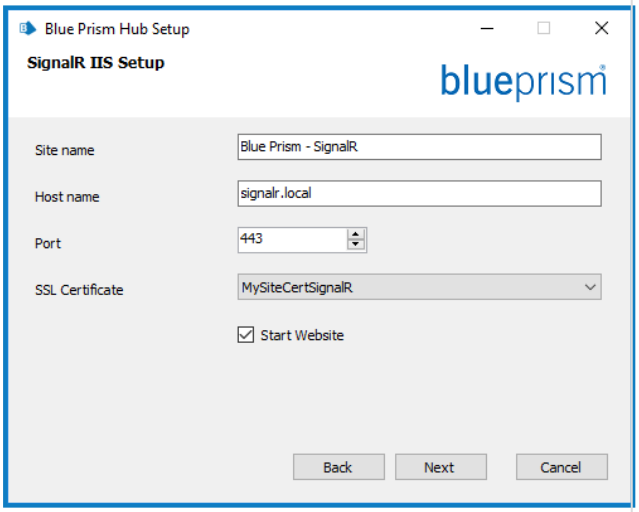
Schritt	Seite des Installationsprogramms	Details
14		**File Service SQL-Verbindung konfigurieren** Einstellungen für die File Service Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

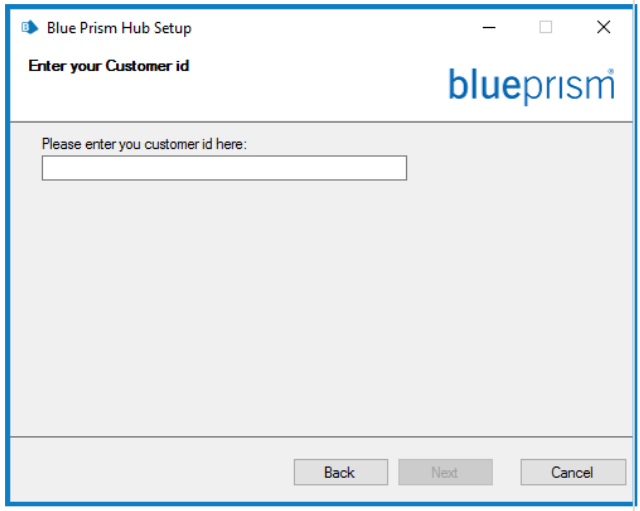
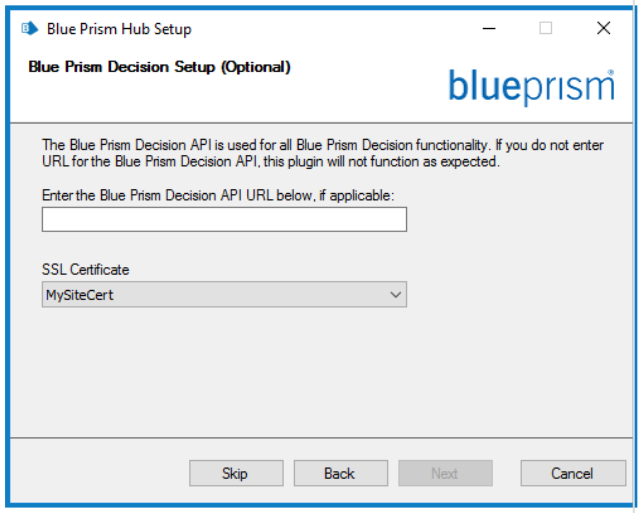
Schritt	Seite des Installationsprogramms	Details
15		**File Service IIS-Setup** Konfigurieren Sie die File Service Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

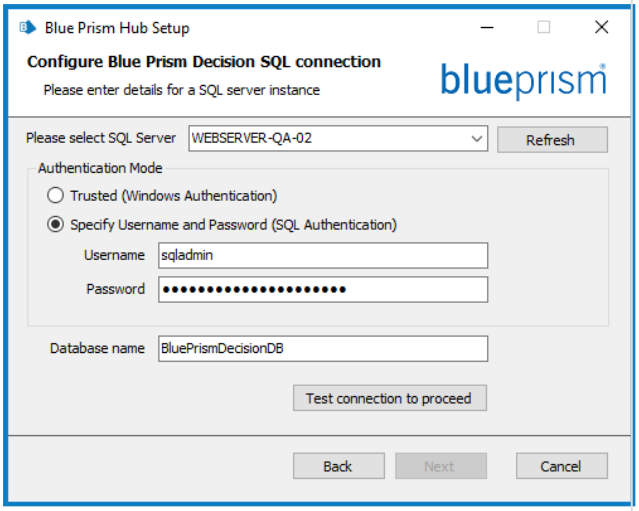
Schritt	Seite des Installationsprogramms	Details
16		**Notification Center SQL-Verbindung** Einstellungen für die Notification Center Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

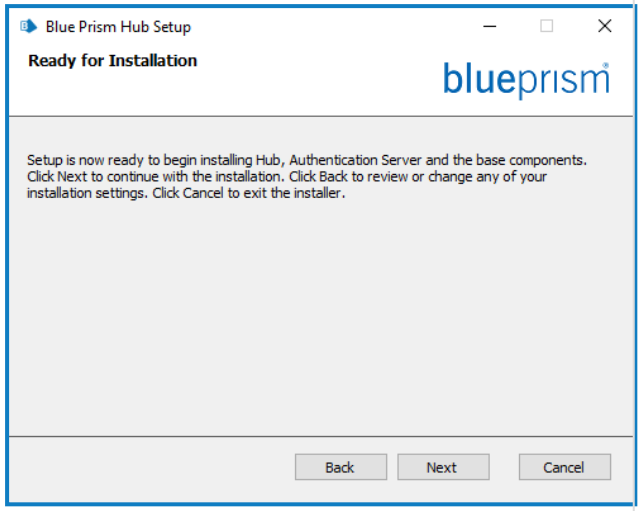
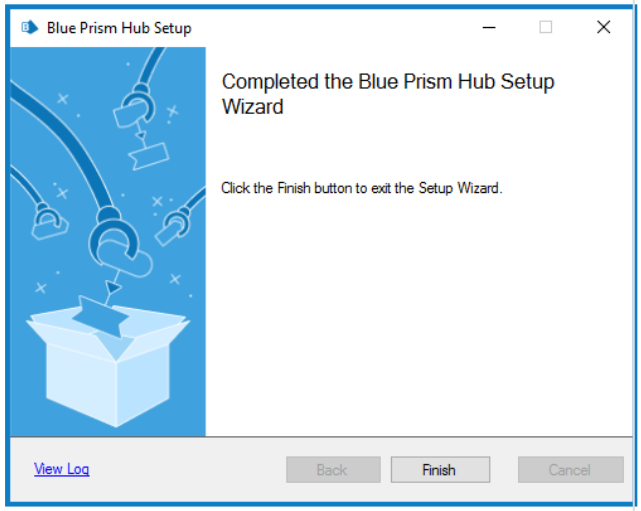
Schritt	Seite des Installationsprogramms	Details
17		**Notification Center IIS-Setup** Konfigurieren Sie die Notification Center Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

Schritt	Seite des Installationsprogramms	Details
18		**License Manager SQL-Verbindung** Einstellungen für die License Manager Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

Schritt	Seite des Installationsprogramms	Details
19		**License Manager IIS-Setup** Konfigurieren Sie die License Manager Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.
20		**SignalR IIS-Setup** Konfigurieren Sie die SignalR-Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

Schritt	Seite des Installationsprogramms	Details
21		**Geben Sie Ihre Kunden-ID ein** Geben Sie Ihre Kundenkennung ein. Diese Kennung wird Ihnen von Blue Prism zur Verfügung gestellt, wenn Sie Ihre Produktlizenz für ALM oder Interact erhalten. Wenn Sie kein lizenziertes Plug-in gekauft haben, können Sie Ihren eigenen Wert eingeben. Wenn Sie später ein lizenziertes Plug-in kaufen, muss Ihre Kunden-ID innerhalb der Konfigurationsdatei geändert werden. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 99.
22		**Setup von Blue Prism Decision (optional)** Wenn Sie Blue Prism Decision verwenden möchten, müssen Sie: • Geben Sie die URL für den Blue Prism Decision Model Service Container ein, gefolgt von der Portnummer. Die URL sollte das Format https://<FQDN>:<Portnummer> haben, beispielsweise https://decision.blueprism.com:50051. Die URL muss mit dem FQDN übereinstimmen, der im Zertifikat angegeben wurde. Die Portnummer muss mit dem Port übereinstimmen, der definiert wurde, als der Container zur Ausführung eingerichtet wurde. Weitere Informationen finden Sie unter Blue Prism Decision installieren. • Wählen Sie das entsprechende SSL-Zertifikat aus. Wenn Sie Blue Prism Decision nicht verwenden möchten, klicken Sie auf **Überspringen**. Der Bildschirm Bereit zur Installation wird angezeigt.

Schritt	Seite des Installationsprogramms	Details
23		**Blue Prism Decision SQL-Verbindung** Einstellungen für die Blue Prism Decision Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Details.

Schritt	Seite des Installationsprogramms	Details
24		**Bereit zur Installation** Klicken Sie auf **Weiter**, um Hub zu installieren.
25		**Installation abgeschlossen** Wenn die Installation fehlschlägt, finden Sie unter der Option **Log anzeigen** Details zum aufgetretenen Fehler. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 99.

Authentication Server SAML 2.0-Erweiterung installieren

Wenn Ihr Unternehmen beabsichtigt, die SAML 2.0-Authentifizierung für Ihre Benutzer zu verwenden, müssen Sie die Authentication Server SAML 2.0-Erweiterung auf Ihrem Webserver installieren, auf dem Hub und Authentication Server installiert sind. Weitere Informationen finden Sie im Installationshandbuch zur Authentication Server SAML 2.0-Erweiterung 4.7 auf der Digital Exchange.

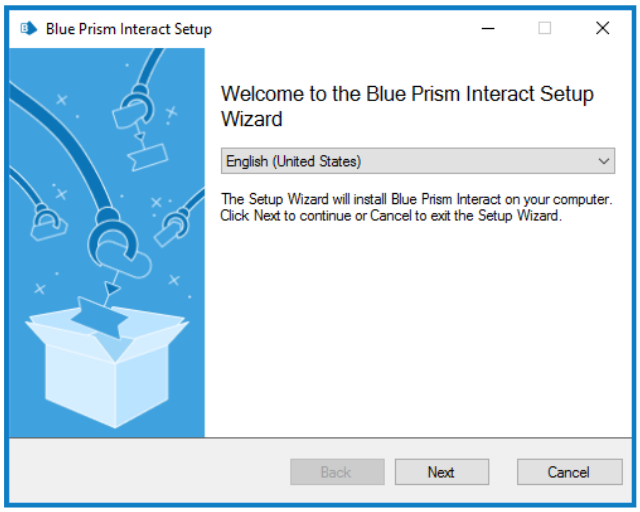
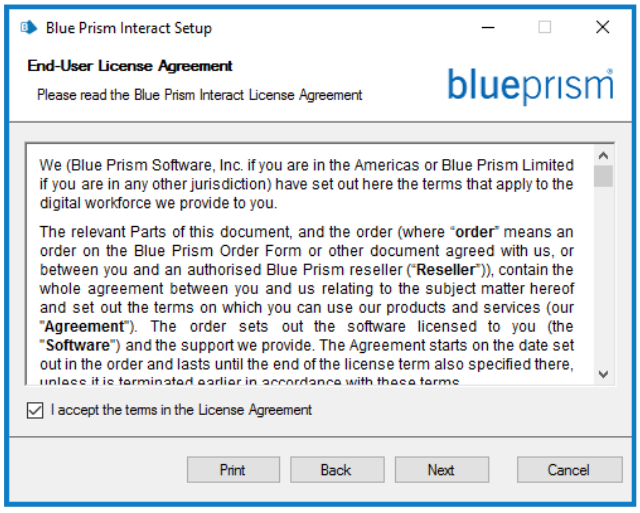
Wenn Ihr Unternehmen nicht beabsichtigt, die SAML 2.0-Authentifizierung für Ihre Benutzer zu verwenden, müssen Sie nichts weiter installieren.

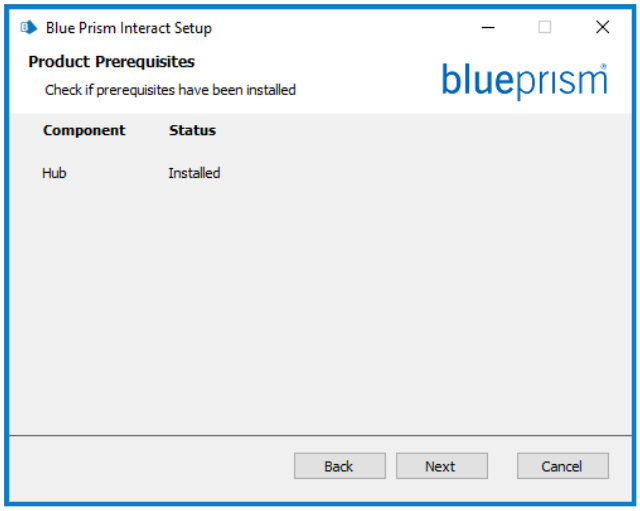
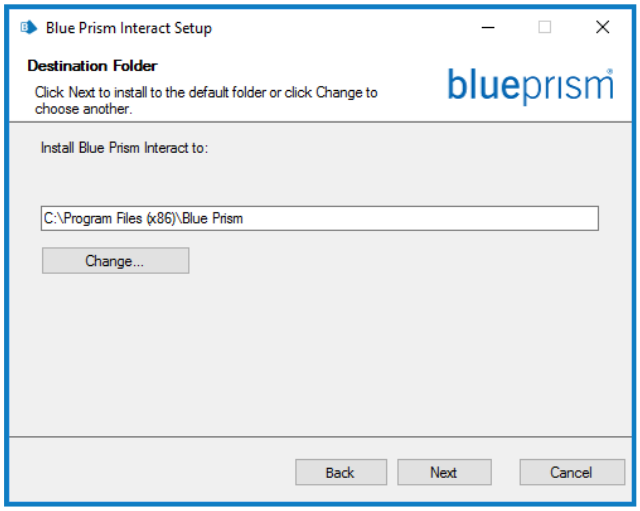
Blue Prism Interact installieren

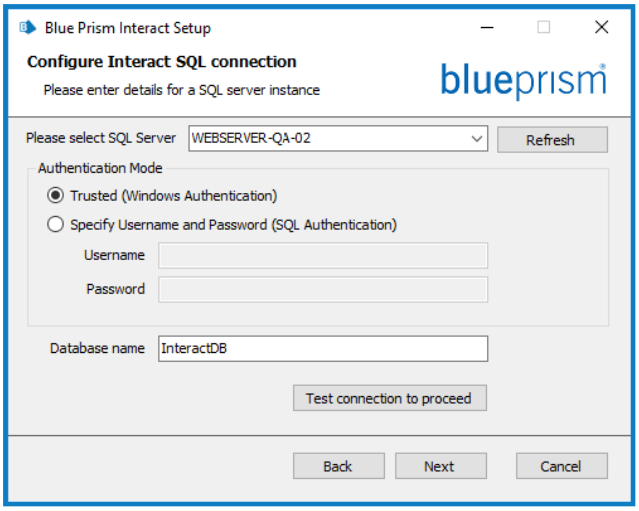
Die folgenden Schritte beschreiben den Prozess zur Installation der Blue Prism Interact Software. Diese Installation setzt die Installation von Blue Prism Hub voraus. Dazu gehören Authentication Server, Hub und andere zugehörige Dienste.

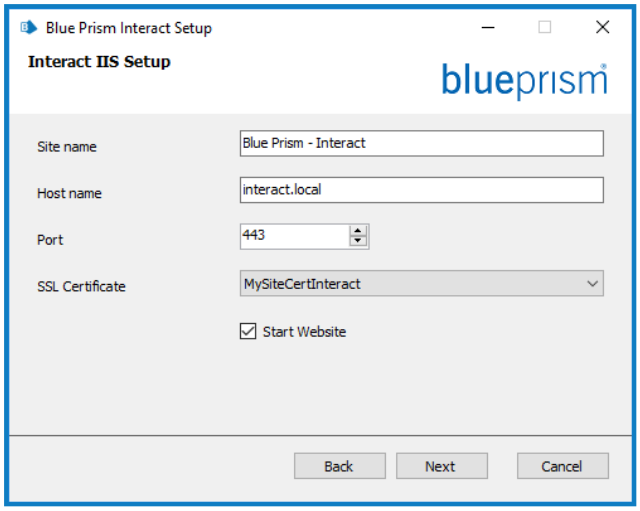
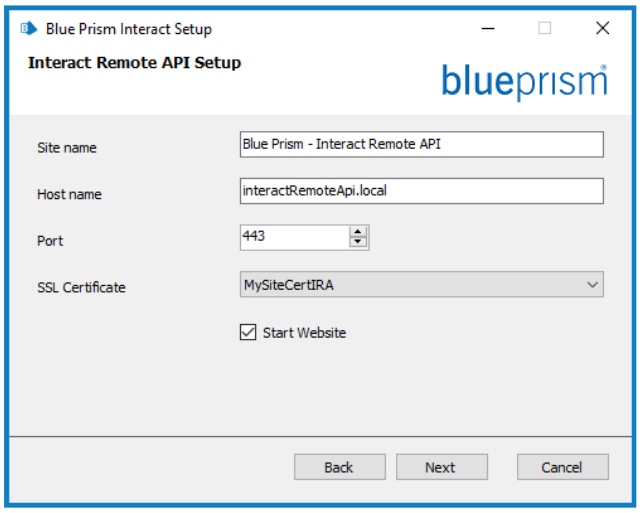
Laden Sie das Blue Prism Interact Installationsprogramm aus dem Blue Prism Portal herunter, führen Sie es aus und gehen Sie wie folgt vor. Das Installationsprogramm muss mit Administratorrechten ausgeführt werden.

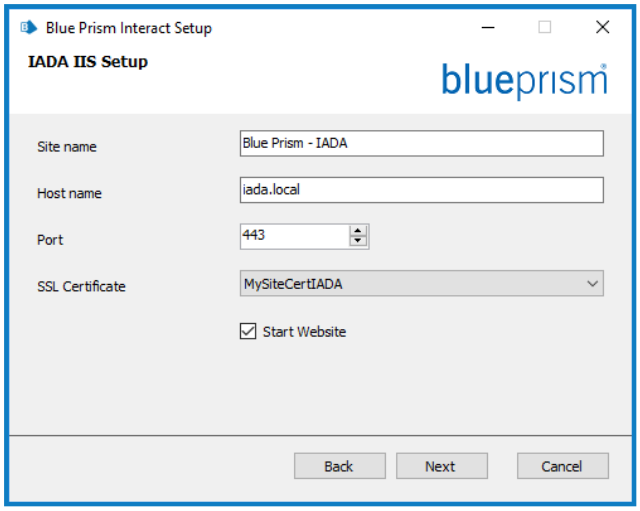
Sehen Sie sich das Blue Prism Interact Installationsvideo für die Installation und Konfiguration von Interact an.

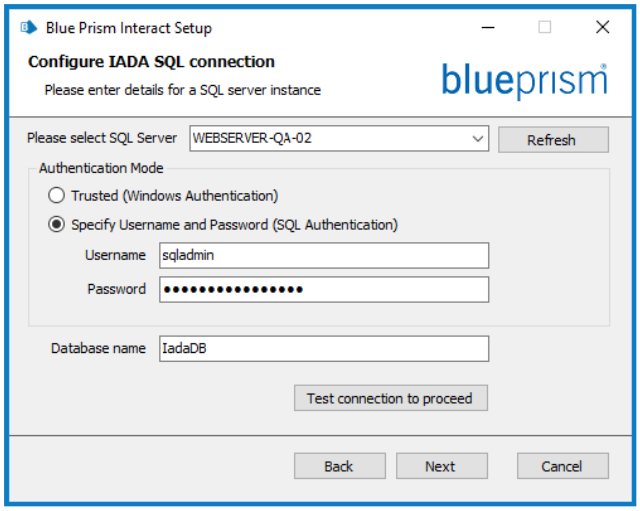
Schritt	Seite des Installationsprogramms	Details
1		**Willkommen** Falls erforderlich, wählen Sie für das Installationsprogramm eine andere Sprache in der Dropdown-Liste aus. Die Standardsprache ist Englisch (USA). Klicken Sie auf **Weiter**.
2		**Lizenzvereinbarung** Lesen Sie die Endbenutzer-Lizenzvereinbarung. Wenn Sie den Bedingungen zustimmen, aktivieren Sie das Kontrollkästchen.

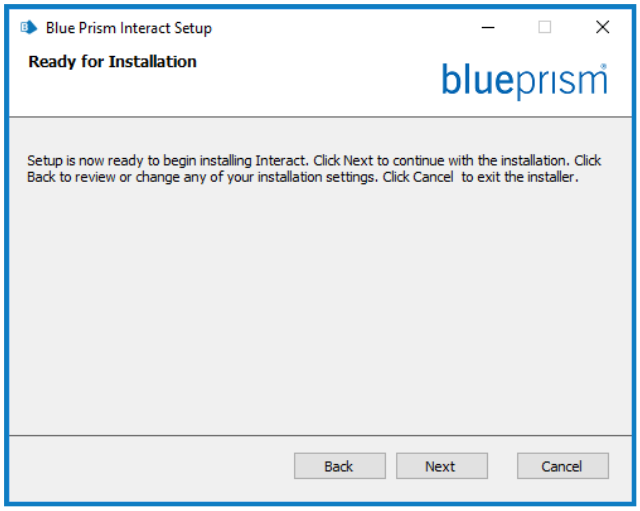
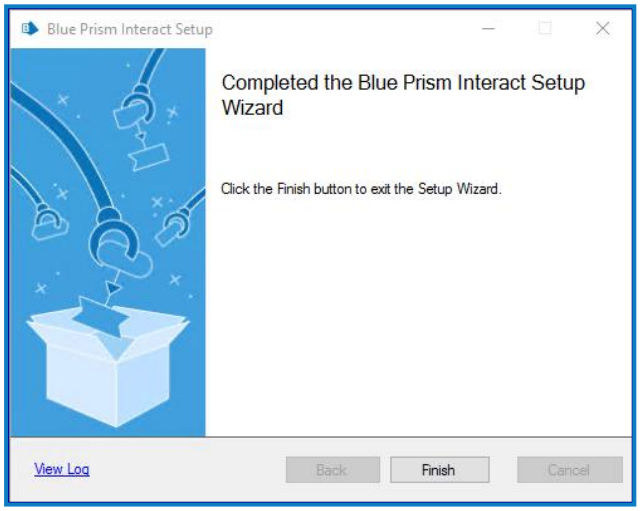
Schritt	Seite des Installationsprogramms	Details
3		**Produktvoraussetzungen** Das Installationsprogramm überprüft, ob die Voraussetzungen installiert wurden. Sollten Voraussetzungen fehlen, erhalten Sie eine Benachrichtigung. Andernfalls können Sie mit der Installation fortfahren. Sie können nicht fortfahren, bis alle Voraussetzungen installiert sind.
4		**Zielordner** Geben Sie den erforderlichen Installationsordner an. Der Standardspeicherort ist C:\Programme (x86)\Blue Prism, aber Sie können Ihren eigenen über die Schaltfläche **Ändern** auswählen.

Schritt	Seite des Installationsprogramms	Details
5		**Interact SQL-Konfiguration konfigurieren** Einstellungen für die Interact Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehler in einer Interact Installation beheben auf Seite 92 weitere Details.

Schritt	Seite des Installationsprogramms	Details
6		**Interact IIS-Setup** Interact Website konfigurieren. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.
7		**Interact Remote API-Setup** Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

Schritt	Seite des Installationsprogramms	Details
8		**IADA IIS-Setup** Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens Ihre DNS- und Domänenstruktur berücksichtigen. • Geben Sie die Portnummer ein. • Wählen Sie das entsprechende SSL-Zertifikat aus. • Lassen Sie **Website starten** ausgewählt, es sei denn, Sie möchten nicht, dass die Website am Ende der Installation automatisch startet.

Schritt	Seite des Installationsprogramms	Details
9		**IADA SQL-Konfiguration konfigurieren** Einstellungen für IADA konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 63. • Wenn **SQL-Authentifizierung** ausgewählt ist, geben Sie den Benutzernamen und das Passwort ein. ⚠ Sie müssen sicherstellen, dass Ihr Datenbankpasswort kein Gleichheitszeichen (=) und keinen Strichpunkt (;) enthält. Diese Zeichen werden nicht unterstützt und führen zu Problemen, wenn versucht wird, eine Verbindung zur Datenbank herzustellen. Der Datenbankname kann als Standardwert beibehalten oder nach Bedarf geändert werden. Klicken Sie auf **Verbindung testen, um fortzufahren**, testen Sie die SQL-Anmeldedaten und prüfen Sie die Konnektivität. Eine Benachrichtigung zeigt das Ergebnis des Tests an. Sie können nur dann mit dem nächsten Schritt fortfahren, wenn der Test erfolgreich ist. Wenn der Test fehlgeschlagen ist, erfahren Sie unter Fehler in einer Interact Installation beheben auf Seite 92 weitere Details.

Schritt	Seite des Installationsprogramms	Details
10		**Bereit zur Installation** Klicken Sie auf **Weiter**, um Interact zu installieren.
11		**Installation abgeschlossen** Wenn die Installation fehlschlägt, finden Sie unter der Option **Log anzeigen** Details zum aufgetretenen Fehler. Weitere Informationen finden Sie unter Fehlerbehebung einer Installation. Klicken Sie auf **Fertigstellen**.

mit Windows-Authentifizierung installieren

Das Konto, auf dem die Installation ausgeführt wird, muss über die entsprechenden SQL Server-Berechtigungen verfügen, um die Installation durchzuführen, also die Mitgliedschaft in der festen Serverrolle „sysadmin“ oder „dbcreator“.

Wenn die Windows-Authentifizierung während des Installationsprozesses ausgewählt wurde, muss ein Windows-Dienstkonto für die Anwendungspools und -dienste mit den erforderlichen Berechtigungen verwendet werden, um die Aufgaben und Prozesse während des normalen Betriebs auszuführen. Das Windows-Dienstkonto benötigt:

- Die Fähigkeit, die SQL-Datenbankprozesse auszuführen, siehe Minimale SQL-Berechtigungen auf Seite 15.
- Berechtigungen für die erforderlichen Zertifikate.
- Die Eigentümerschaft des IIS-Anwendungspools.
- Die Eigentümerschaft der von Hub und Interact installierten Windows-Dienste.

⚠ Sie müssen die Anwendungspools und -dienste zur Verwendung von Windows-Konten zuweisen, bevor Sie eine Umgebung in Hub erstellen. Wenn Sie die Konten nach dem Erstellen einer Umgebung zuweisen, können Leistungsprobleme auftreten, z. B. werden Formulare, die mit dem Interact Plug-in erstellt wurden, möglicherweise nicht für Benutzer in Interact angezeigt.

Zuweisen des Windows-Dienstkontos als Eigentümer auf Zertifikaten

Dem Windows-Dienstkonto müssen Berechtigungen für die BluePrismCloud-Zertifikate gewährt werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie den Zertifikat-Manager auf dem Webserver. Dazu geben Sie *Zertifikate* in das Suchfeld in der Windows-Taskleiste ein und klicken dann auf **Computerzertifikate verwalten**.
2. Erweitern Sie im Navigationsbereich **Persönlich** und klicken Sie auf **Zertifikate**.
3. Befolgen Sie die folgenden Schritte für die BluePrismCloud_Data_Protection- und BluePrismCloud_IMS_JWT-Zertifikate:
    a. Klicken Sie mit der rechten Maustaste auf das Zertifikat, wählen Sie **Alle Aufgaben** aus und klicken Sie auf **Private Schlüssel verwalten ...**.

    Das Dialogfeld „Berechtigungen“ für das Zertifikat wird angezeigt.

    b. Klicken Sie auf **Hinzufügen**, geben Sie dann das Dienstkonto ein und klicken Sie auf **OK**.
    c. Wählen Sie das Dienstkonto in der Liste **Gruppen- oder Benutzername** aus und stellen Sie sicher, dass **Vollzugriff** in der Liste **Berechtigungen für {Kontoname}** ausgewählt ist.
    d. Klicken Sie auf **OK**.

    Das Dienstkonto hat nun Zugriff auf das Zertifikat.

Zuweisen eines Windows-Dienstkontos zum Anwendungspool

Standardmäßig werden die Anwendungspools mit der Identität „ApplicationPoolIdentity“ erstellt. Nachdem das Installationsprogramm abgeschlossen ist, muss das Windows-Dienstkonto zur Verwaltung der Anwendungspools zugewiesen werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie auf dem Webserver „Internet Information Services (IIS) Manager“.
2. Erweitern Sie im Panel „Verbindungen“ den Host und wählen Sie **Anwendungspools** aus.

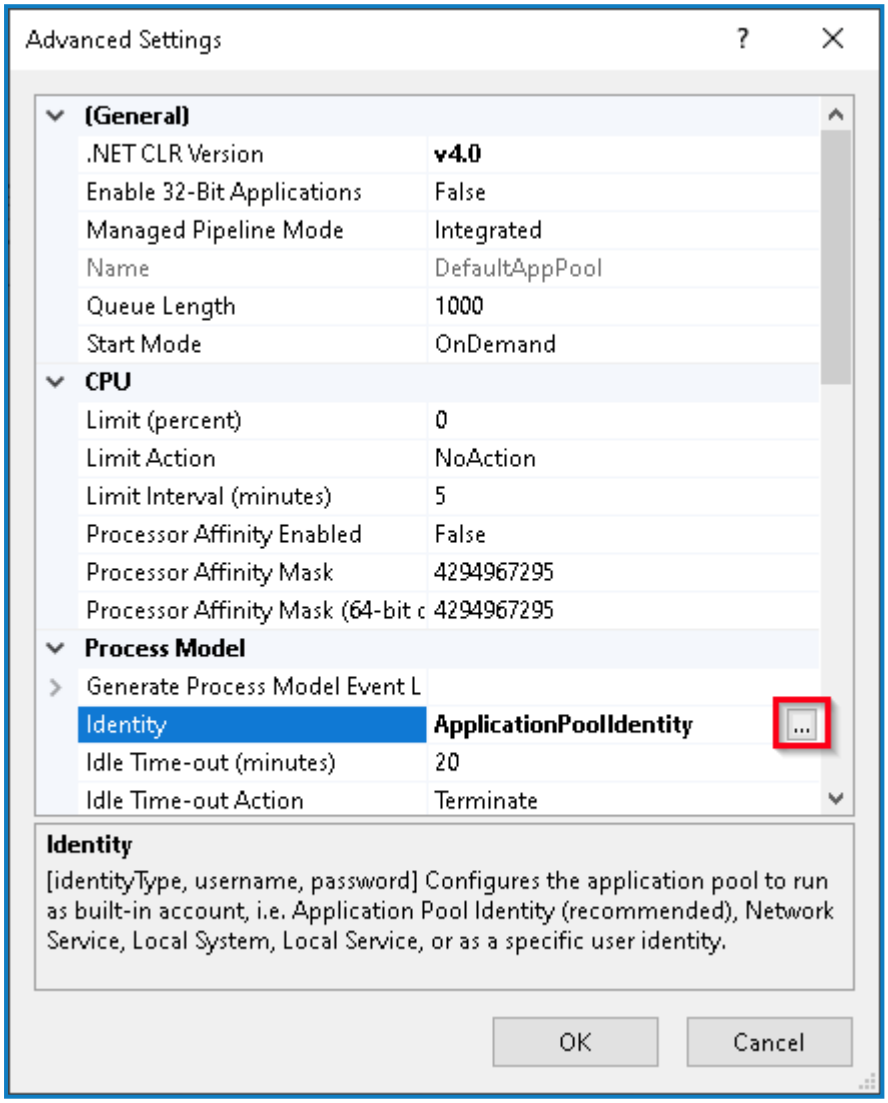
3. Überprüfen Sie die Werte in der Spalte **Identität**.

   Die Identität für einen Anwendungspool sollte mit dem betreffenden Windows-Dienstkonto übereinstimmen.

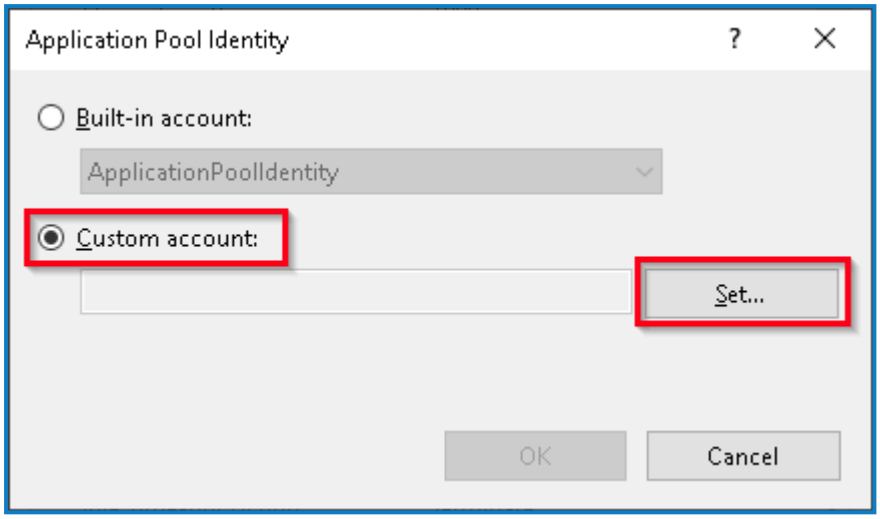
4. Bei Anwendungspools, bei denen *ApplicationPoolIdentity* in der Spalte **Identität** steht, klicken Sie mit der rechten Maustaste auf die Zeile und wählen **Erweiterte Einstellungen...** aus.

   Das Dialogfeld „Erweiterte Einstellungen“ wird angezeigt.

5. Wählen Sie die Einstellung **Identität** aus und klicken Sie dann auf die Schaltfläche **...** (Ellipse):



6. Wählen Sie im Dialogfeld „Anwendungspoolidentität“ die Option **Benutzerdefiniertes Konto** aus und klicken Sie auf **Einstellen...**.



   Das Dialogfeld „Anmeldedaten festlegen“ wird angezeigt.
7. Geben Sie die Anmeldedaten für das erforderliche Windows-Dienstkonto ein und klicken Sie auf **OK**.
8. Wiederholen Sie dies für alle Anwendungspools, die geändert werden müssen.
9. Starten Sie den RabbitMQ-Dienst neu.
10. Starten Sie alle Anwendungspools neu.
11. Starten Sie IIS neu.

Stellen Sie bei Problemen mit dem Audit Service sicher, dass das Windows-Dienstkonto Zugriff auf den Audit Service Listener sowie auf die Audit Datenbank hat.

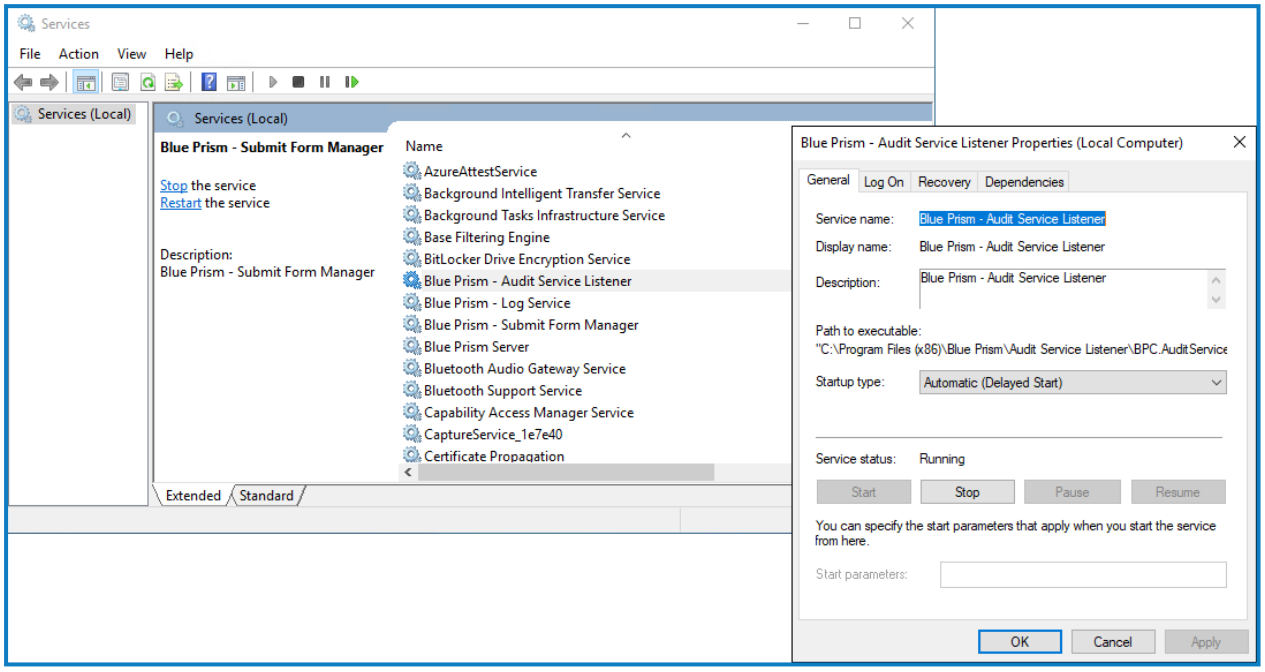
Zuweisen eines Windows-Dienstkontos zu einem Dienst

Das Windows-Dienstkonto muss zugewiesen werden, um die folgenden Dienste zu verwalten:

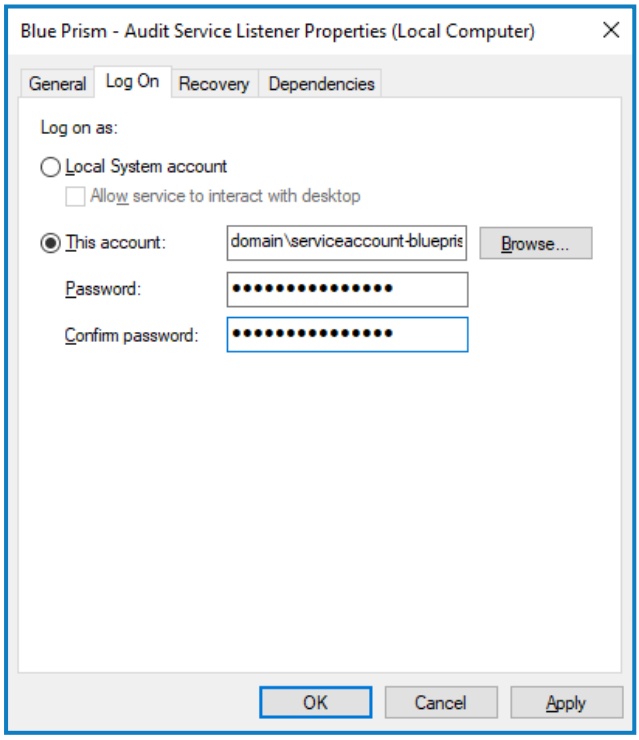
- Blue Prism – Audit-Dienst-Listener
- Blue Prism – Log Service
- Blue Prism – Manager für die Formularübermittlung

Gehen Sie dazu wie folgt vor:

1. Öffnen Sie „Dienste“ auf dem Webserver.
2. Klicken Sie mit der rechten Maustaste auf den Dienst und klicken Sie dann auf **Eigenschaften**.



3. Wählen Sie auf der Registerkarte „Anmelden“ die Option **Dieses Konto** aus und geben Sie dann den Kontonamen ein oder klicken Sie auf **Durchsuchen**, um das Konto auszuwählen, das Sie verwenden möchten.



4. Geben Sie das Passwort für das Konto ein und klicken Sie auf **OK**.
5. Klicken Sie im Fenster „Dienste“ mit der rechten Maustaste auf den Dienst und klicken Sie dann auf **Neu starten**.
6. Wiederholen Sie dies für die anderen Blue Prism Dienste.

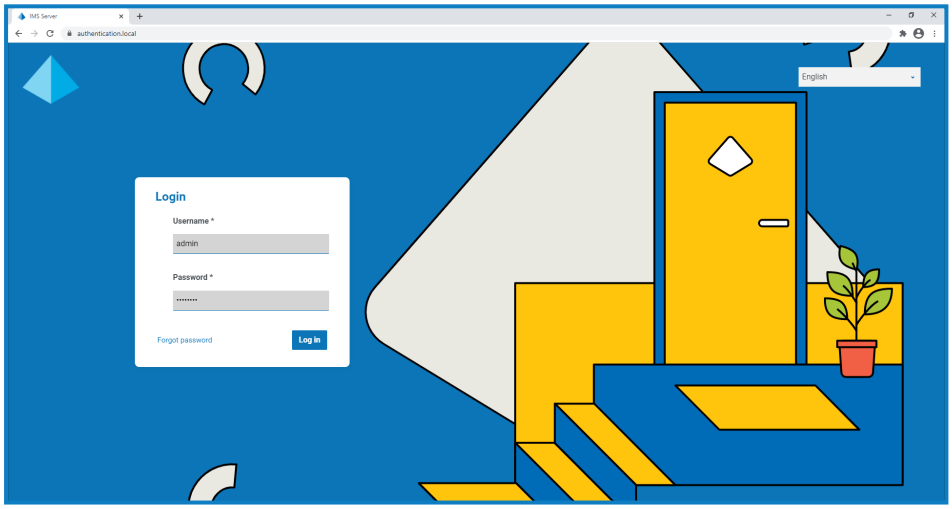
Erstmalige Hub Konfiguration

Sie können sich jetzt zum ersten Mal anmelden und einige systemweite Konfigurationen vornehmen.

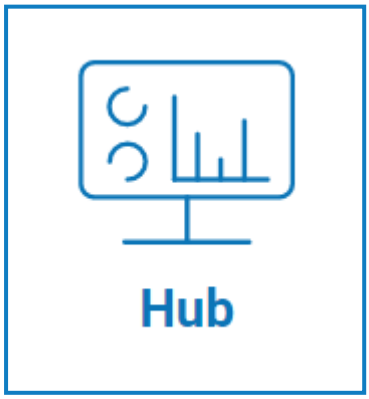
Wenn Sie die Anmeldeseite für Authentication Server öffnen, wendet ihr Webbrowser automatisch Lokalisierungseinstellungen an. Die Anmeldeseite und Hub werden in der Sprache angezeigt, die am besten zu den im Browser festgelegten Spracheinstellungen passt. Wenn die in den Einstellungen Ihres Browsers ausgewählte Sprache nicht unterstützt wird, wird standardmäßig Englisch verwendet. Falls erforderlich, können Sie die Sprache manuell über die Dropdown-Liste auf der Anmeldeseite ändern.

Sehen Sie sich das Blue Prism Hub Installationsvideo für die Installation und Konfiguration von Hub an.

1. Starten Sie Ihren Browser und gehen Sie zur Website Authentication Server, in unserem Beispiel: https://authentication.local



2. Melden Sie sich mit den Standard-Anmeldedaten an.
   - **Benutzername:** admin
   - **Passwort**: Qq1234!!
3. Klicken Sie auf **Hub**, um die Hub Website zu starten.



4. Ändern Sie das Standardpasswort zu einem neuen sicheren Passwort.
    a. Klicken Sie in Hub auf das Profilsymbol, um die Seite „Einstellungen“ zu öffnen, und klicken Sie dann auf **Profil**.
    b. Klicken Sie auf **Passwort aktualisieren**.

       Das Dialogfeld „Passwort aktualisieren“ wird angezeigt.
    c. Geben Sie das aktuelle Administratorpasswort ein. Geben Sie dann das neue Passwort zweimal ein.
    d. Klicken Sie auf **Aktualisieren**.

       Das Administratorpasswort wird geändert.

Datenbankeinstellungen

⚠ Wenn Sie Ihre Umgebung so installiert haben, dass Windows-Authentifizierung verwendet wird, müssen Sie die Anwendungspools und -dienste zur Verwendung von Windows-Konten zuweisen, bevor Sie eine Umgebung in Hub erstellen. Wenn dies nicht der Fall ist, können Leistungsprobleme auftreten, z. B. werden Formulare, die mit dem Interact Plug-in erstellt wurden, möglicherweise nicht für Benutzer in Interact angezeigt. Weitere Informationen finden Sie unter mit Windows-Authentifizierung installieren auf Seite 63.

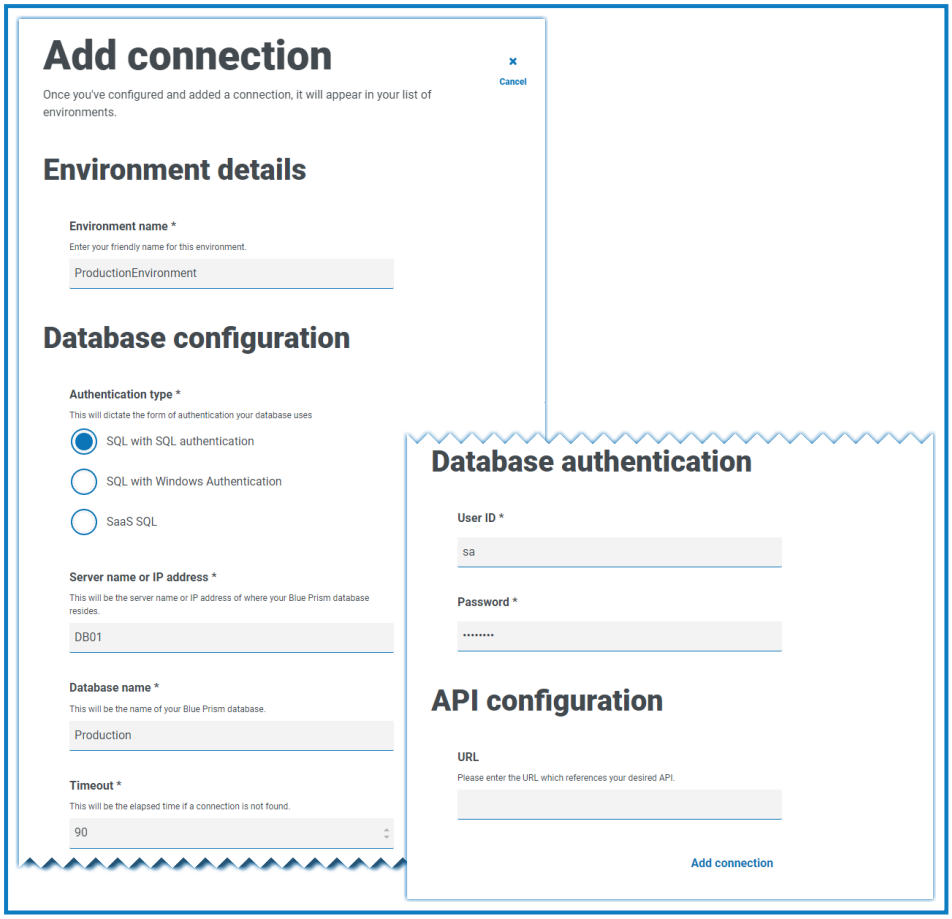
SSL-Verschlüsselung wird von allen Datenbanken verwendet, die durch das Hub Installationsprogramm installiert wurden. Damit Hub erfolgreich eine Verbindung zur Blue Prism Datenbank herstellen kann, muss die Blue Prism Datenbank auch für die Verwendung der SSL-Verschlüsselung konfiguriert werden. Weitere Informationen finden Sie unter Voraussetzungen auf Seite 8.

Konfigurieren Sie den Zugriff auf die Blue Prism Datenbank:

1. Klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **Umgebungsmanager**.

   Die Seite „Umgebungsmanager“ wird angezeigt.

2. Klicken Sie auf **Verbindung hinzufügen** und geben Sie die Details der Blue Prism Datenbank ein. Ein Beispiel wird im Folgenden gezeigt:



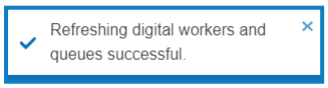
Der Timeout-Wert ist in Sekunden angegeben.

3. Klicken Sie auf **Verbindung hinzufügen**, um die Details zu speichern.

   Die Verbindung wird erstellt und im Umgebungsmanager angezeigt.

4. Klicken Sie im Umgebungsmanager für Ihre neue Verbindung auf das Symbol „Aktualisieren“. Dadurch werden die Informationen in Hub mit der Digital Workforce und den Warteschlangen in der Datenbank aktualisiert.

   Ist die Verbindung erfolgreich, wird in der oberen rechten Ecke der Hub Benutzeroberfläche folgende Meldung angezeigt, die die Installation bestätigt.



   Wenn die Nachricht nicht angezeigt wird, finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 99 weitere Informationen.

Einen Administrator erstellen

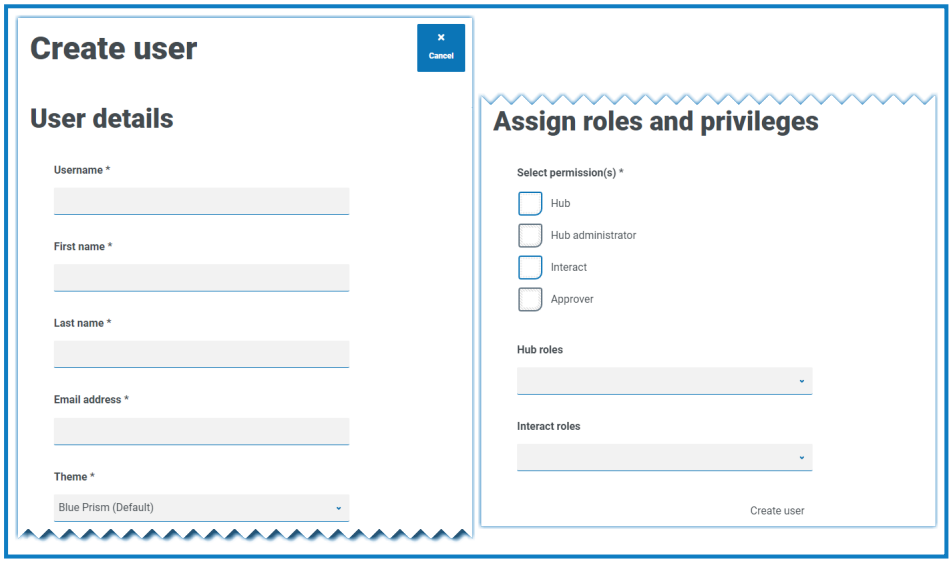
Sie müssen ein Administratorkonto mit gültigen Informationen erstellen, um die Hub Konfiguration abzuschließen. Sie sollten das generische Administratorkonto nicht verwenden, um die Konfiguration abzuschließen. Der Grund:

- Eine echte E-Mail-Adresse wird benötigt, um die E-Mail-Konfiguration zu testen.
- Für einen vollständigen Audit-Trail sollte ein benannter Benutzer verwendet werden, um Konfigurationsänderungen vorzunehmen, anstatt des generischen Kontos.

So erstellen Sie einen neuen Administrator:

1. Klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **Benutzer**.
2. Klicken Sie auf der Seite „Benutzer“ auf **Benutzer hinzufügen**.

   Der Bereich „Benutzer erstellen“ wird angezeigt.



3. Geben Sie die folgenden Details ein:
   - Benutzername
   - Vorname
   - Nachname
   - E-Mail-Adresse
4. Wählen Sie die Berechtigungen **Hub** und **Hub Administrator** aus.
5. Klicken Sie auf **Benutzer erstellen**.

   Das Dialogfeld „Passwort erstellen“ wird angezeigt.
6. Wählen Sie **Benutzerpasswort manuell aktualisieren** aus.

   Passwörter müssen den Einschränkungen von Hub entsprechen.
7. Klicken Sie auf **Weiter** und führen Sie die Anweisungen auf dem Bildschirm aus.
8. Klicken Sie dann auf **Erstellen**, um den Benutzer zu erstellen.

   Der neue Benutzer wird in der Liste der Benutzer angezeigt.
9. Melden Sie sich bei Hub ab und melden Sie sich mit Ihrem neuen Konto wieder an.

E-Mail-Einstellungen

Wir empfehlen, die SMTP-Einrichtung abzuschließen. Dadurch können System-E-Mails gesendet werden, z. B. E-Mails wegen vergessener Passwörter.

Die E-Mail-Adresse, die zum Senden von E-Mails verwendet wird, wird bei der Einrichtung Ihres Profils konfiguriert.

> Um die E-Mail-Einstellungen zu konfigurieren, müssen Sie sich mit dem Benutzer anmelden, den Sie in Einen Administrator erstellen auf Seite 69 erstellt haben. Dies liegt daran, dass der Konfigurationsprozess eine Test-E-Mail sendet und daher einen Benutzer mit einer aktiven E-Mail-Adresse erfordert.

Sie können Ihre E-Mail-Einstellungen so konfigurieren, dass eine der folgenden Authentifizierungsmethoden verwendet wird:

- **Benutzername und Passwort** – Diese Authentifizierungsmethode erfordert die folgenden Informationen:
  - **SMTP-Host** – Die Adresse Ihres SMTP-Hosts.
  - **Portnummer** – Die Portnummer, die vom Server für ausgehende E-Mails verwendet wird.
  - **E-Mail-Adresse des Absenders** – Die E-Mail-Adresse, die beim Senden von E-Mails verwendet wird. Die E-Mail-Empfänger werden diese Adresse im Feld „Von“ sehen.
  - **Verschlüsselung** – Die Verschlüsselungsmethode, die vom E-Mail-Server zum Senden der E-Mails verwendet wird.
  - **Benutzername** – Der Benutzername für die SMTP-Authentifizierung.
  - **Passwort** – Das Passwort für das Konto.
  - **Empfänger der Test-E-Mail** – Die Test-E-Mail wird an diese E-Mail-Adresse gesendet. Das ist standardmäßig die E-Mail-Adresse des Benutzers, der die Änderungen vornimmt. Sie kann nicht geändert werden.
- **Microsoft OAuth 2.0** – Diese Authentifizierungsmethode erfordert die folgenden Informationen:
  - **E-Mail-Adresse des Absenders** – Die E-Mail-Adresse, die beim Senden von E-Mails verwendet wird. Die E-Mail-Empfänger werden diese Adresse im Feld „Von“ sehen.
  - **Anwendungs-ID** – Dies ist die Anwendungs-ID (Client-ID), die in Azure AD definiert ist und Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird.
  - **Verzeichnis-ID** – Dies ist die Verzeichnis-ID (Mandanten-ID), die in Azure AD definiert ist und Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird.
  - **Client-Geheimnis** – Hierbei handelt es sich um das von Azure AD generierte Client-Geheimnis, das Ihnen von Ihrem IT-Support-Team zur Verfügung gestellt wird und den Authentifizierungsprozess steuert.

    > Informationen zum Auffinden dieser Details in Azure AD finden Sie in der Microsoft-Dokumentation.
  - **Empfänger der Test-E-Mail** – Die Test-E-Mail wird an diese E-Mail-Adresse gesendet. Das ist standardmäßig die E-Mail-Adresse des Benutzers, der die Änderungen vornimmt. Sie kann nicht geändert werden.

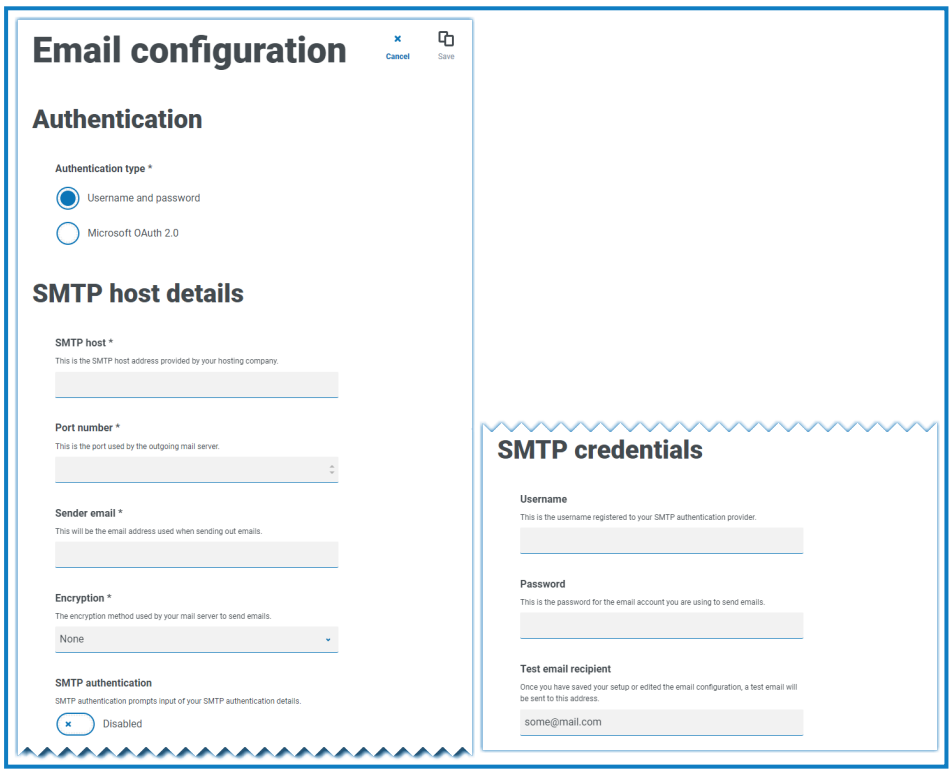
> Wenn Sie Microsoft OAuth 2.0 verwenden, muss die Berechtigung „Mail.Send“ in Azure Active Directory aktiviert sein. Dies finden Sie auf der Registerkarte „API-Berechtigung“ unter den Anwendungseigenschaften in Azure Active Directory. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 99.

So konfigurieren Sie E-Mail-Einstellungen:

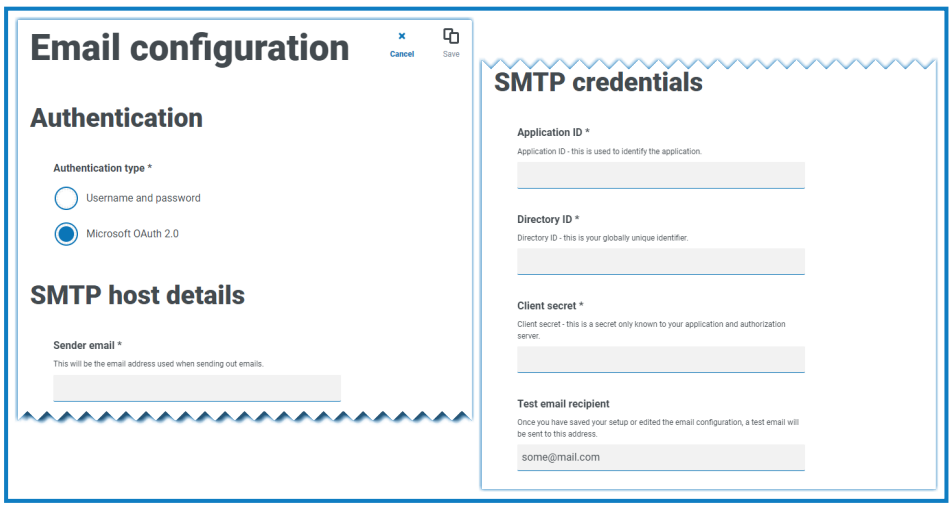
1. Klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **E-Mail-Konfiguration**.
2. Klicken Sie auf **Bearbeiten**.
3. Wählen Sie den Authentifizierungstyp aus, den Sie verwenden möchten.

   Die Felder auf der Seite hängen von Ihrer Auswahl ab, wie oben beschrieben. Bei der Auswahl:

   - **Benutzername und Passwort**, die Seite „E-Mail-Konfiguration“ wird wie folgt angezeigt:



   - **Microsoft OAuth 2.0**, die Seite „E-Mail-Konfiguration“ wird wie folgt angezeigt:



4. Geben Sie die erforderlichen Informationen ein.
5. Klicken Sie auf **Speichern**.

Wenn die E-Mail-Einstellungen nicht erfolgreich konfiguriert werden können, liegt es wahrscheinlich daran, dass der Message-Broker-Server nicht erreicht werden kann. Siehe Fehlerbehebung einer Hub Installation auf Seite 99 für weitere Informationen.

Weitere Informationen zum Konfigurieren von E-Mail-Einstellungen finden Sie im Hub Administrator Handbuch.

Authentication Server konfigurieren

Authentication Server ermöglicht es Benutzern, sich mit denselben Anmeldedaten bei Blue Prism, Hub und Interact anzumelden. Authentication Server ist mit Blue Prism 7.0 und höher kompatibel.

Mit Blue Prism 6

Wenn Ihr Unternehmen Blue Prism 6 verwendet:

- Authentication Server kann nicht zur Authentifizierung von Benutzern zwischen Blue Prism und Hub genutzt werden. Benutzer können sich über unabhängige Konten bei Blue Prism und Authentication Server anmelden.
- Sie sollten die Authentifizierungseinstellungen in Hub konfigurieren. Siehe Authentifizierungseinstellungen auf der nächsten Seite.

Mit Blue Prism 7

Wenn Ihr Unternehmen Blue Prism 7 verwendet, sollten Sie überlegen, ob Benutzer dasselbe Konto für die Blue Prism Anwendungen verwenden sollen.

- Wenn Ihr Unternehmen dieselben Benutzerkonten verwenden möchte:
    1. Konfigurieren Sie Authentication Server, siehe hierzu das Authentication Server Konfigurationshandbuch.
    2. Konfigurieren Sie die Authentifizierungseinstellungen in Hub. Siehe Authentifizierungseinstellungen auf der nächsten Seite.
- Wenn Ihr Unternehmen nicht dieselben Benutzerkonten verwenden möchte, konfigurieren Sie nur die Authentifizierungseinstellungen in Hub. Siehe Authentifizierungseinstellungen auf der nächsten Seite.

Weitere Informationen zu den Konfigurationsschritten finden Sie in unserem Video zur Konfiguration von Authentication Server.

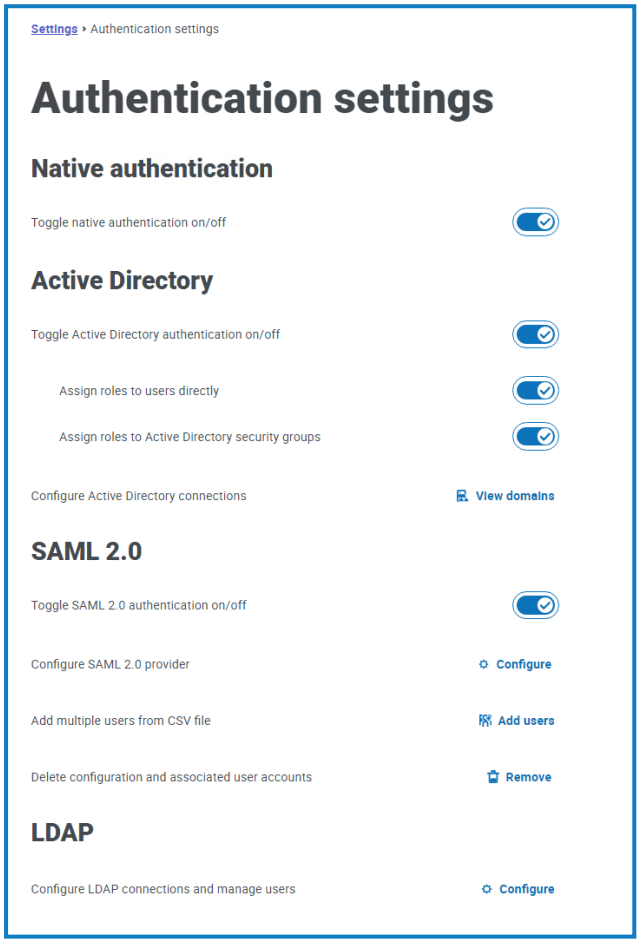
Authentifizierungseinstellungen

Authentifizierungseinstellungen für eine Hub Umgebung können auf der Seite „Authentifizierungseinstellungen“ konfiguriert werden.

Konfigurieren der Authentifizierungseinstellungen:

1. Klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen, und klicken Sie dann auf **Authentifizierungseinstellungen**.

   Die Seite „Authentifizierungseinstellungen“ wird angezeigt.



2. Wählen Sie den/die Authentifizierungstyp(en) aus, den/die Sie verwenden möchten, und die zugehörigen Optionen, falls erforderlich.
   - **Native Authentifizierung** – Dies wird standardmäßig in neuen Umgebungen oder beim Upgrade des Hubs aktiviert.
   - **Active Directory** – Dies kann nur aktiviert werden, wenn der Server, der Authentication Server hostet, Mitglied einer Active Directory-Domain ist. Wenn diese Option aktiviert ist, können auch Active Directory-Domänen und Benutzerrollenverwaltung konfiguriert werden.
   - **SAML 2.0** – Diese Option ist nur auf der Seite „Authentifizierungseinstellungen“ sichtbar, wenn die Authentication Server SAML 2.0-Erweiterung auf dem Host-Webserver installiert wurde, auf dem Authentication Server installiert ist.
   - **LDAP** – Um die LDAP-Authentifizierung zu aktivieren, muss mindestens eine LDAP-Verbindung erstellt werden.

Basierend auf den Anforderungen Ihrer Organisation haben Sie die folgenden Optionen:

- Aktivieren Sie alle Authentifizierungstypen.
- Deaktivieren Sie einen oder mehrere Authentifizierungstypen. Dies ist nur möglich, wenn mindestens ein Administratorbenutzer im System vorhanden ist, der so konfiguriert ist, dass er sich mit einem anderen Authentifizierungstyp als dem/den zu deaktivierenden Typ(en) anmeldet.

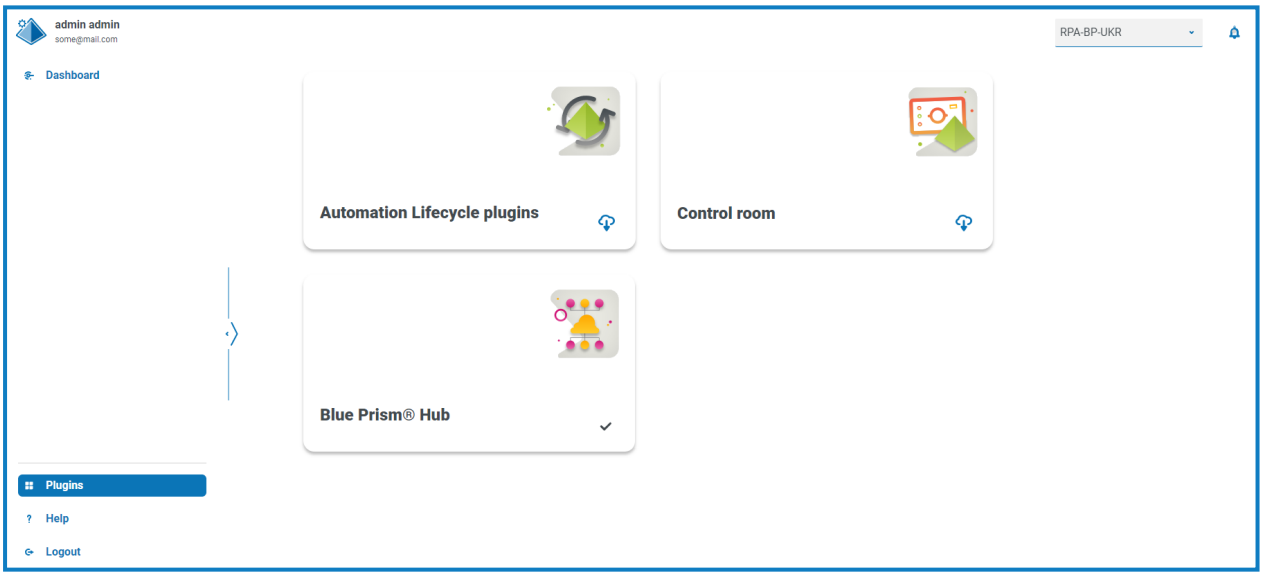
Weitere Informationen zur Konfiguration von Authentifizierungseinstellungen finden Sie im Hub Administratorhandbuch.

Plug-ins installieren

Im Rahmen der Installation von Hub werden die Hub Plug-ins automatisch installiert. Wenn Sie jedoch ALM oder Interact verwenden möchten, müssen Sie zuerst das frei verfügbare Geschäftsprozess-Plug-in installieren.

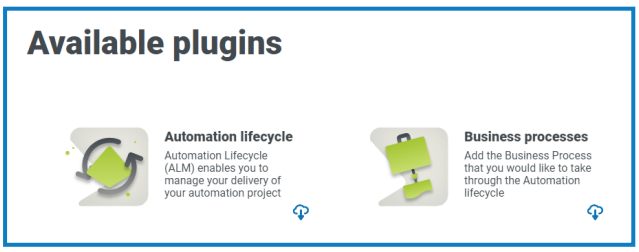
Diesen Installationsschritt können Sie auch im Geschäftsprozess-Plug-in-Installationsvideo sehen.

1. Melden Sie sich bei Hub an.
2. Klicken Sie auf **Plug-ins**, um das Plug-in-Repository zu öffnen.



3. Klicken Sie auf **Automatisierungslebenszyklus**.

   Die verfügbaren Plug-in-Komponenten werden angezeigt.



4. Klicken Sie auf das Download-Symbol in der unteren Ecke der Kachel **Geschäftsprozesse**, um die Installation zu starten.

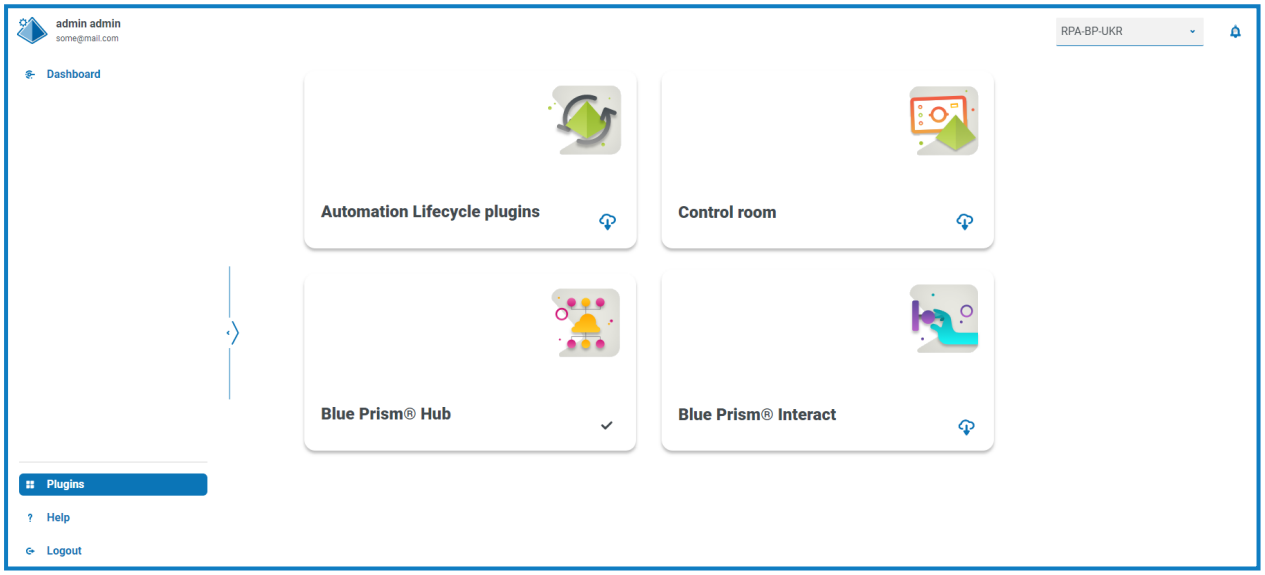
   Die Site wird neu gestartet.

Interact Plug-in installieren

Das Interact Plug-in ist vom Geschäftsprozess-Plug-in abhängig, da Sie ohne Geschäftsprozess kein Formular erstellen können. Das Geschäftsprozess-Plug-in steht im Plug-in-Repository kostenlos zur Verfügung. Sie finden es unter Automation Lifecycle Management (ALM). Stellen Sie sicher, dass Sie das Geschäftsprozess-Plug-in installiert haben, bevor Sie Interact installieren. Mehr erfahren Sie unter Plug-ins installieren auf der vorherigen Seite.

Das Interact Plug-in muss mit der zugehörigen Lizenz installiert werden.

1. Melden Sie sich bei Hub an.
2. Klicken Sie auf **Plug-ins**, um das Plug-in-Repository zu öffnen.



3. Klicken Sie auf der **Interact** Kachel auf das Download-Symbol in der unteren Ecke, um die Installation zu starten und die erforderliche Lizenz zu aktivieren.

   Die Site wird neu gestartet.

Digital Workers konfigurieren

Dieser Abschnitt beschreibt die Schritte, die Sie für jeden Digital Worker durchführen müssen, damit sich dieser mit Interact verbinden kann.

Folgende Schritte sind erforderlich:

- SSL-Zertifikate installieren
- Netzwerk konfigurieren
- Interact Web-API-Dienst installieren und konfigurieren

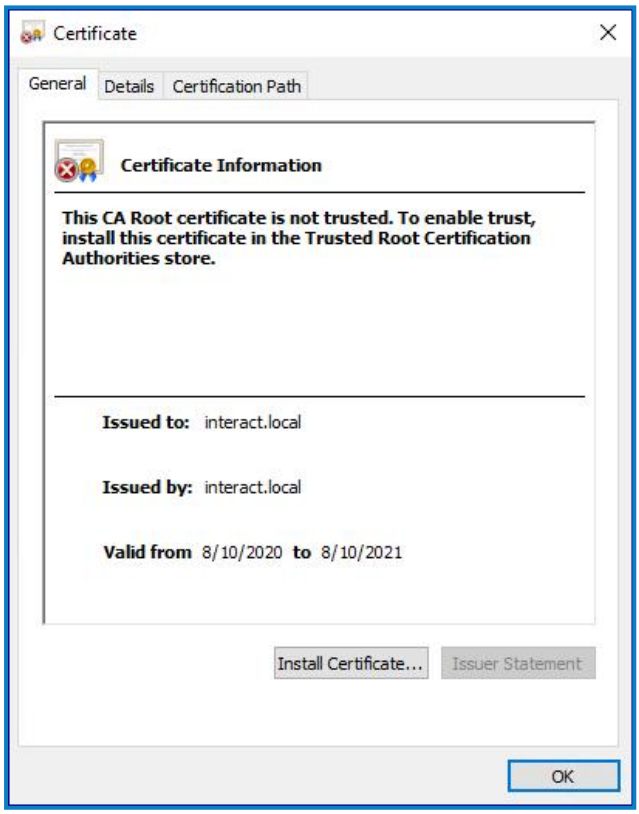
Bei diesen Anweisungen wird davon ausgegangen, dass der Benutzer bereits mit Blue Prism vertraut ist.

SSL-Zertifikate installieren

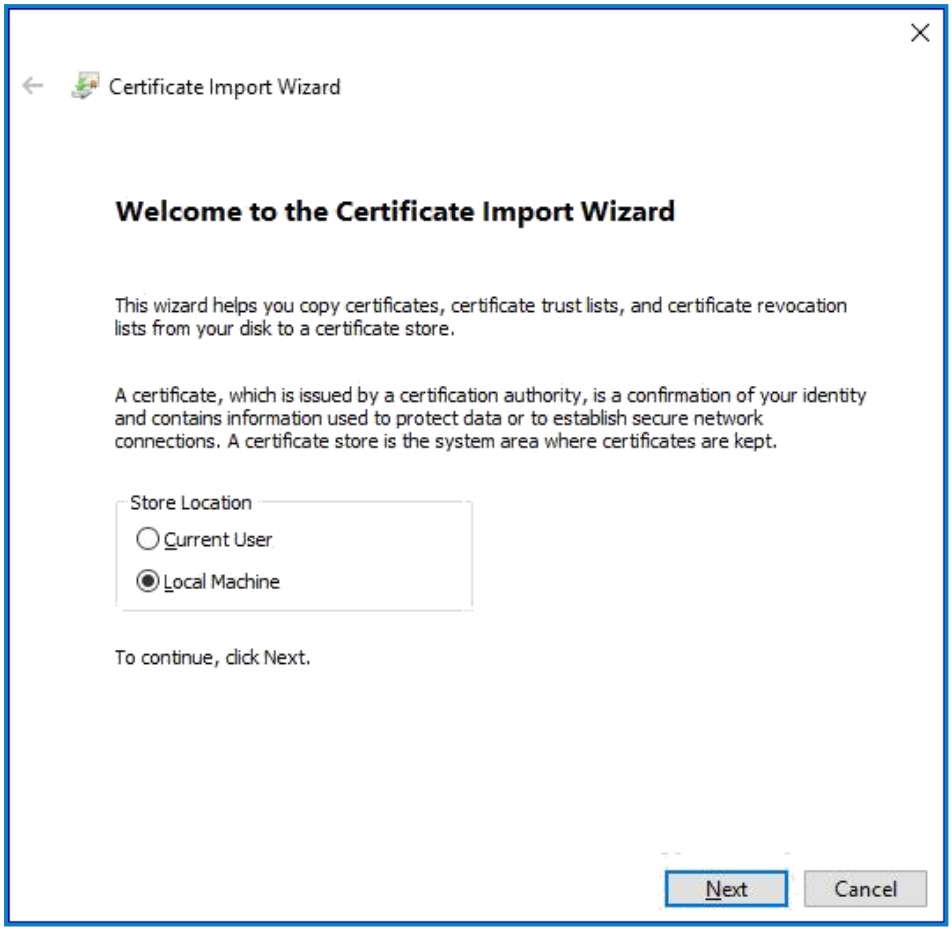
Melden Sie sich bei jedem Digital Worker an und kopieren Sie die SSL-Zertifikate für Interact, IADA, Interact Remote API, Authentication Server und SignalR.

Da dies für jeden Digital Worker durchgeführt werden muss, können Sie auch unterstützende Drittanbietertools oder GPOs verwenden.

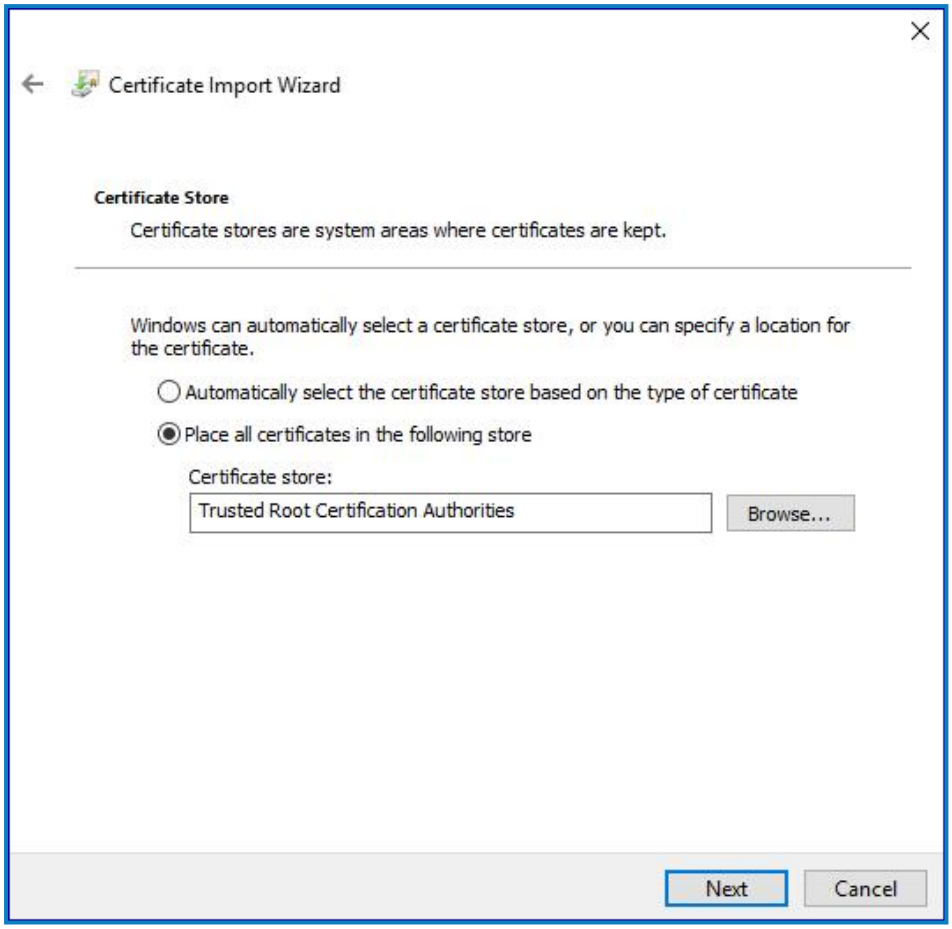
1. Doppelklicken Sie auf jedes SSL-Zertifikat und wählen Sie **Zertifikat installieren** aus.



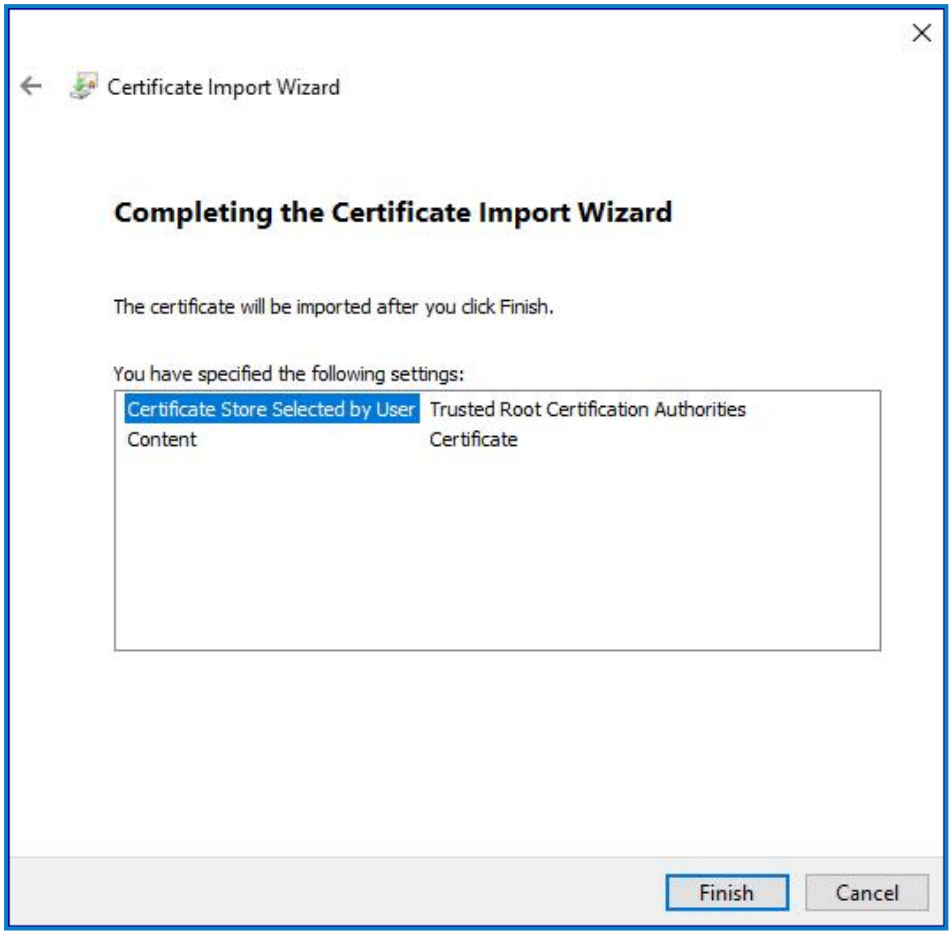
2. Ändern Sie den Speicherort zu **Lokaler Computer**.



3. Wählen Sie **Alle Zertifikate in folgendem Speicher speichern** aus, klicken Sie auf **Durchsuchen** und wählen Sie dann **Speicher vertrauenswürdiger Stammzertifizierungsstellen** aus.



4. Überprüfen Sie, ob das SSL-Zertifikat im richtigen Speicher zugewiesen ist, und klicken Sie dann auf **Fertigstellen**.



5. Bestätigen Sie die Erfolgsmeldung.
6. Wiederholen Sie die Schritte für alle SSL-Zertifikate.

Netzwerk konfigurieren

Es ist wichtig, dass die Interact Website und insbesondere die Interact Remote API Website erreicht werden können.

Dies hängt von der bereitgestellten Architekturstruktur ab. Wenn die Systeme mit einer Domain verbunden sind und die IT-Organisation die Server konfiguriert hat, könnte dies bereits der Fall sein. Alternativ muss möglicherweise die lokale Host-Datei angepasst werden, um sicherzustellen, dass die Websites erreicht werden können.

Folgende Websites müssen für alle Digital Workers erreichbar sein:

Website in IIS	Standard-URL
Blue Prism – Interact	https://interact.local
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local
Blue Prism – SignalR	https://signalr.local

Authentication Server und SignalR werden im Rahmen der Hub Installation installiert.

Interact Web-API-Dienst installieren und konfigurieren

Blue Prism und Interact kommunizieren über die Blue Prism Interact Remote API. Um diese API zu verwenden, sollte die Interact API Service Release-Datei in Blue Prism importiert werden. Dazu gehören ein Web API Service und ein VBO. Nach dem Import muss er mit der entsprechenden Basis-URL und den Autorisierungscodes aktualisiert werden, um eine sichere Kommunikation zu ermöglichen.

Im Webdienst gibt es eine Reihe von definierten Aktionen, weitere Informationen finden Sie im Benutzerhandbuch des Interact Web-API-Diensts.

Um Blue Prism für die Verwendung von Interact zu konfigurieren, müssen Sie Folgendes tun:

1. Dienstkonto einrichten in Hub und geheimen Schlüssel generieren.
2. Das Interact API Service VBO in Blue Prism importieren.
3. Anmeldedaten einrichten für das Interact Web-API-Dienstkonto in Blue Prism.
4. Den Interact API Service konfigurieren, damit Blue Prism mit Interact kommunizieren kann.

Dienstkonto einrichten

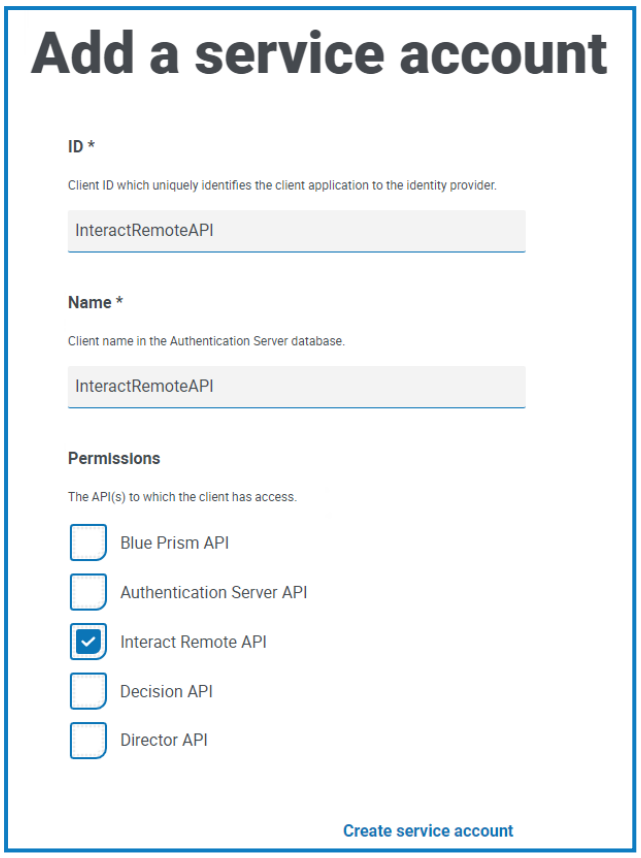
Um die Interact Remote API-Anmeldedaten in Blue Prism einzurichten, ist ein geheimer Schlüssel erforderlich. Dieser wird vom zugehörigen Dienstkonto in Hub zur Verwendung mit der Interact Remote API generiert. Wenn Sie den Schlüssel verlieren, können Sie im Dienstkonto einen weiteren generieren. Weitere Informationen finden Sie unter Dienstkonten.

So erstellen Sie ein Dienstkonto:

1. Klicken Sie in Blue Prism Hub auf der Dienstkonten-Seite auf **Konto hinzufügen**.
2. Geben Sie eine eindeutige ID und einen Anzeigenamen ein, zum Beispiel *InteractRemoteAPI*.

   Verwenden Sie nicht *InteractRemoteClient*. Dieser Name wird intern im System vergeben.

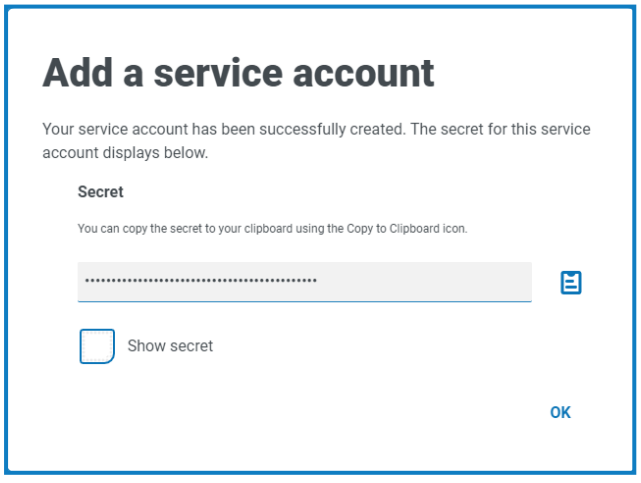
3. Wählen Sie unter **Berechtigungen** die Option **Interact Remote API** aus.



4. Klicken Sie auf **Dienstkonto erstellen**.

   Das Dialogfeld „Dienstkonto hinzufügen“ wird mit einem generierten geheimen Schlüssel angezeigt. Sie müssen diesen Schlüssel im interaktiven Blue Prism Client eingeben, wenn Sie die entsprechenden Anmeldedaten konfigurieren.

5. Kopieren Sie den generierten geheimen Schlüssel in Ihre Zwischenablage, um ihn im interaktiven Blue Prism Client einfügen zu können.



6. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

   Die Dienstkonten-Seite wird mit dem neu erstellten Konto angezeigt.

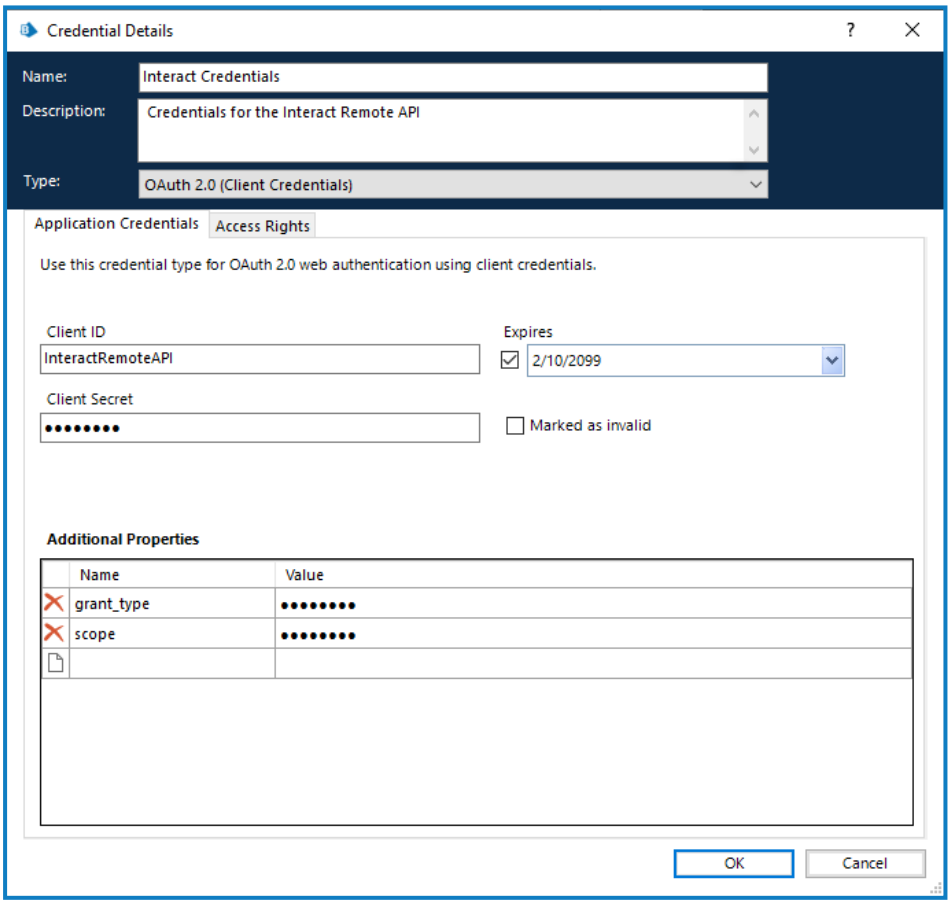
Importieren des VBO

1. Laden Sie die Releasedatei des Interact API Service im Blue Prism Portal herunter.
2. Wählen Sie in Blue Prism **Datei** aus, klicken Sie auf **Importieren** >**Release/Fertigkeit** und folgen Sie den Anweisungen, um die Releasedatei in Blue Prism zu importieren. Weitere Informationen finden Sie unter Datei importieren.

Anmeldedaten in Blue Prism einrichten

1. Melden Sie sich beim interaktiven Blue Prism Client an, wählen Sie **System** aus und klicken Sie dann auf **Sicherheit** > **Anmeldedaten**. Siehe Sicherheit > Anmeldedaten für zusätzliche Informationen.
2. Klicken Sie auf **Neu**.

   Das Dialogfeld „Anmeldedatendetails“ wird angezeigt.
3. Auf der Registerkarte „Anwendungsanmeldedaten“ im Dialogfeld „Anmeldedaten-Details“:
   a. Geben Sie einen Namen ein.
   b. Ändern Sie den **Typ** zu **OAuth 2.0 (Client-Anmeldedaten)**.
   c. Geben Sie in **Client-ID** die ID ein, die Sie zum Erstellen des Dienstkontos oben in Digital Workers konfigurieren auf Seite 77 verwendet haben, zum Beispiel *InteractRemoteAPI*.
   d. Geben Sie in **Client-Geheimnis** den für das Dienstkonto generierten geheimen Schlüssel ein.

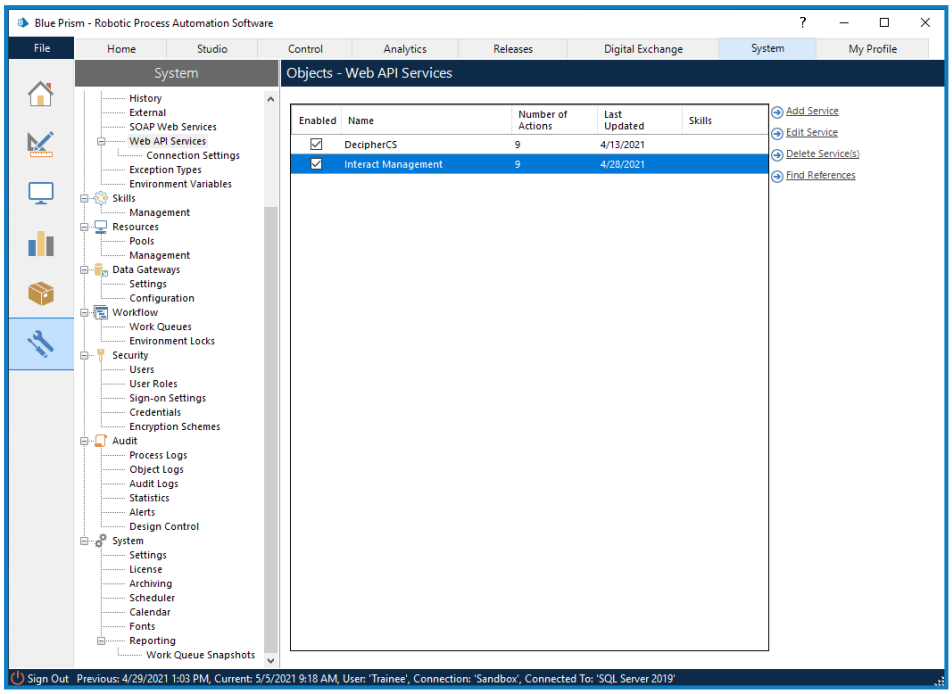


4. Richten Sie auf der Registerkarte „Zugriffsrechte“ im Dialogfeld „Anmeldedaten-Details“ die erforderlichen Zugriffsberechtigungen ein.
5. Klicken Sie auf **OK**.

Webdienst konfigurieren

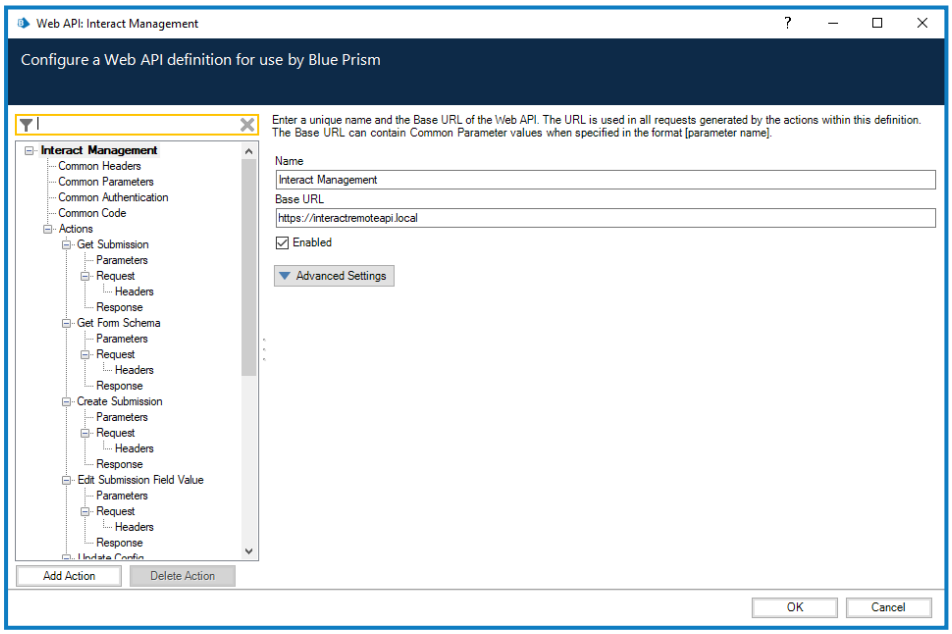
1. Wählen Sie in Blue Prism **System** aus und klicken Sie dann auf **Objekte** > **Web-API-Dienste**.

   Der Bildschirm „Objekte – Web-API-Dienste“ wird angezeigt. Zum Beispiel:



2. Wählen Sie **Interact Management** aus und klicken Sie auf **Dienst bearbeiten**.

   Der Bildschirm „Web-API: Interact Management“ wird angezeigt.



3. Geben Sie auf dem Bildschirm „Web-API: Interact Management“ unter **Basis-URL** die URL für den Interact API-Dienst Ihres Unternehmens ein. Diese wurde bei der Installation von Interact definiert.
4. Wählen Sie **Allgemeine Authentifizierung** in der Navigationsstruktur aus und führen Sie dann Folgendes aus:
   a. Stellen Sie sicher, dass der **Authentifizierungstyp** auf **OAuth 2.0 (Client-Anmeldedaten)** festgelegt ist.

b. Geben Sie unter **Autorisierungs-URI** die Authentication Server URL im folgenden Format ein:

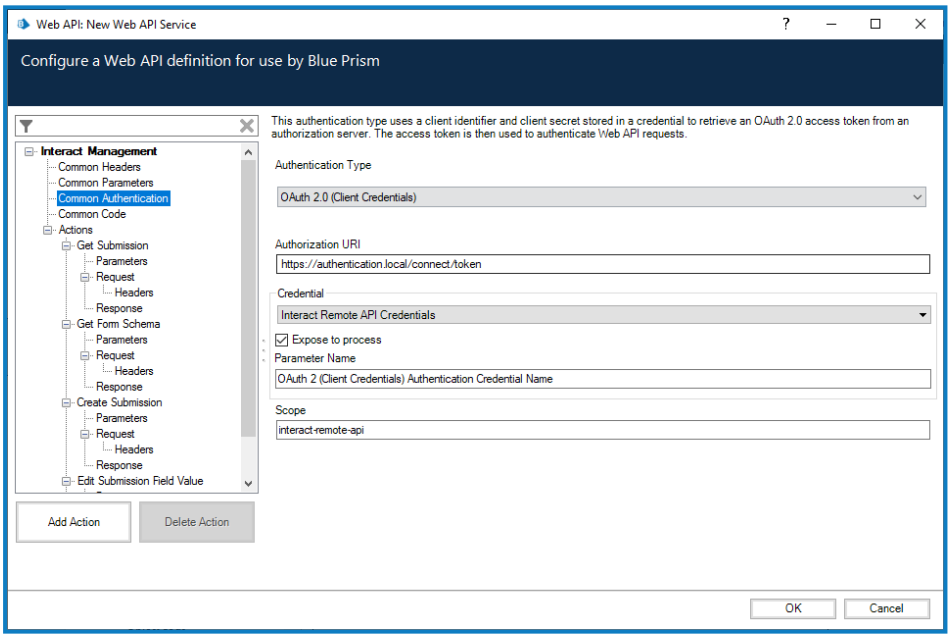
`<Authentication Server URL>:<Port, falls bei Installation festgelegt>/connect/token`

Zum Beispiel: `https://authentication.blueprism.com:5000/connect/token`

Oder, wenn der Standard-Port verwendet wurde:
`https://authentication.blueprism.com/connect/token`.

> Wenn Sie ein Upgrade von einer älteren Version als 4.3 durchgeführt haben, wird Ihr System noch IMS verwenden. In diesem Fall sollten Sie die Informationen im folgenden Format eingeben:
>
> `<IMS-URL>:<Port, falls festgelegt>/connect/token`
>
> Zum Beispiel: `https://ims.blueprism.com:5000/connect/token`.

c. Wählen Sie unter **Anmeldedaten** die Anmeldedaten aus, die Sie in Anmeldedaten in Blue Prism einrichten auf Seite 83 erstellt haben.



5. Klicken Sie auf **OK**, um die Einrichtung des Web-API-Dienstes zu speichern und abzuschließen.

Überprüfen einer Installation

Dieser Abschnitt bietet ein einfaches Szenario, um zu testen, ob die Grundkomponenten der Interact Installation wie erwartet funktionieren. Dieser Verifizierungsprozess hat folgende Voraussetzungen:

- Eine Verbindung zu einer Blue Prism Datenbank wurde in Hub konfiguriert. Weitere Informationen finden Sie unter Datenbankeinstellungen auf Seite 68.
- In der Blue Prism Umgebung ist eine gültige Arbeitswarteschlange vorhanden, die für diesen Test verwendet werden kann.
- Der Interact API Service wird in Blue Prism installiert und konfiguriert. Weitere Informationen finden Sie unter Digital Workers konfigurieren auf Seite 77.

Schritte zur Verifizierung:

- Überprüfen, ob Interact Informationen an eine Arbeitswarteschlange in Blue Prism übermitteln kann:
  - Erstellen eines Geschäftsprozesses in Hub – Jedes Formular ist mit einem Geschäftsprozess verknüpft.
  - Erstellen eines Interact Formulars – Erstellen Sie ein neues Formular mit einer Seite und einem Feld, das für den Verifizierungstest verwendet werden soll.
  - Hinzufügen des Formulars zu einer Rolle – Geben Sie einem Benutzer Zugriff auf das Formular in Interact.
  - Senden des Formulars und Sicherstellen, dass es in einer Warteschlange in Blue Prism angezeigt wird.
- Überprüfen, ob Blue Prism Informationen an Interact übermitteln kann:
  - Erstellen eines einfachen Blue Prism Prozesses.

Bei diesen Anweisungen wird davon ausgegangen, dass der Benutzer bereits mit Blue Prism vertraut ist.

Kommt es zu Problemen beim Verifizieren der Installation, siehe Fehlerbehebung einer Installation.

⚠ Wenn Sie Ihre Umgebung so installiert haben, dass Windows-Authentifizierung verwendet wird, müssen Sie die Anwendungspools und -dienste zur Verwendung von Windows-Konten zuweisen und dann eine Umgebung in Hub erstellen, bevor Sie diese Überprüfung durchführen. Wenn Sie dies nicht tun, werden die im Interact Plug-in erstellten Formulare den Benutzern in Interact nicht angezeigt. Weitere Informationen finden Sie unter mit Windows-Authentifizierung installieren auf Seite 63 und Erstmalige Hub Konfiguration auf Seite 67.

Einen Geschäftsprozess innerhalb von Hub erstellen

1. Melden Sie sich bei Authentication Server mit einem Administrator-Benutzerkonto an und wählen Sie **Hub**.
2. Wählen Sie in der linken Navigationsleiste **Automatisierungslebenszyklus** aus und klicken Sie auf **Geschäftsprozesse**.
3. Klicken Sie auf **Neu hinzufügen**.
4. Geben Sie eine eindeutige Kennung und einen Namen für den Geschäftsprozess ein. Geben Sie optional eine Beschreibung ein.
5. Geben Sie bei Bedarf weitere Notizen ein und klicken Sie auf **Geschäftsprozess erstellen**.

Weitere Informationen zum Erstellen von Geschäftsprozessen finden Sie im Benutzerhandbuch zu Automation Lifecycle Management.

Interact Formular erstellen

Sie müssen ein Formular erstellen, das mindestens eine Seite mit einem Feld enthält.

1. Wählen Sie in Hub in der linken Navigationsleiste **Interact** aus und klicken Sie auf **Formulare**.
2. Wählen Sie **Formular erstellen** aus, um ein neues Interact Formular zu erstellen.
3. Wählen Sie den von Ihnen erstellten Geschäftsprozess aus der Dropdown-Liste aus, wenn er nicht bereits ausgewählt ist.
4. Geben Sie einen Namen für das Interact Formular und eine Beschreibung ein, z. B. *Testformular*.
5. Wählen Sie unter **Bereitstellungsmethode Warteschlange** aus.
6. Wählen Sie die Umgebung aus der Dropdown-Liste aus und wählen Sie dann den gewünschten Warteschlangennamen aus.

   Wenn die erforderliche Warteschlange nicht in der Liste angezeigt wird, klicken Sie auf das Symbol „Aktualisieren“, um die Warteschlangen zu aktualisieren.
7. Geben Sie bei **Priorität**, **SLA**, **E-Mail** und **Interact Rolle** nichts ein.
8. Lassen Sie den **Standardgenehmigungstyp** auf **Ohne** gesetzt.
9. Geben Sie unter **Kategorie** einen Namen für die Kategorie ein. Beispiel: *TestKategorie*.
10. Wählen Sie ein Symbol aus den voreingestellten Symbolen aus, um das Formular in Interact darzustellen.
11. Klicken Sie auf **Formular erstellen**.

    Die Seite „Formular bearbeiten“ wird angezeigt.
12. Klicken Sie auf **Seite erstellen**.

    Der Abschnitt „Seite erstellen“ wird angezeigt.
13. Geben Sie einen Namen und eine Beschreibung für die neue Seite ein und klicken Sie auf **Speichern**.

    Auf der Seite „Formular bearbeiten“ wird die von Ihnen erstellte Seite angezeigt.
14. Klicken Sie auf die drei Punkte (**...**) auf der Seite, die Sie gerade erstellt haben, und klicken Sie auf **Feld erstellen**.

    Das Dialogfeld „Erfassungstyp auswählen“ wird angezeigt.
15. Klicken Sie auf **Text**.
16. Geben Sie auf der Seite „Text erstellen“ *TestTextFeld* in das Feld **Beschriftung** ein und lassen Sie überall sonst die Standardeinstellungen.
17. Klicken Sie auf **Feld erstellen**.
18. Klicken Sie auf der Seite „Formular bearbeiten“ auf **Speichern**.
19. Geben Sie im Fenster Nebenversion erhöhen einen Aktualisierungshinweis ein und klicken Sie auf **Speichern**.

Weitere Informationen zur Erstellung von Geschäftsprozessen finden Sie im Benutzerhandbuch für das Interact Plug-in.

Das Formular zu einer Rolle hinzufügen

1. Klicken Sie in Hub auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **Rollen und Berechtigungen**.

   Die Seite „Rollen und Berechtigungen“ wird angezeigt.
2. Klicken Sie auf **Rolle erstellen**.

   Der Abschnitt „Rolle erstellen“ wird angezeigt.
3. Geben Sie einen Rollennamen ein, z. B. *Interact Testrolle*. Geben Sie optional eine Beschreibung ein.
4. Ändern Sie den **Rollentyp** in **Interact**.
5. Wählen Sie in **Formular hinzufügen** das Formularaus der Dropdown-Liste aus, das Sie gerade erstellt haben. Wenn Sie den Beispielnamen aus Interact Formular erstellen auf der vorherigen Seite verwendet haben, heißt es **Testformular**.
6. Wählen Sie unter **Benutzer hinzufügen** den/die Benutzer aus, der/die Zugriff auf Ihr erstelltes Formular haben soll/-en. Fügen Sie mindestens den Administratorbenutzer hinzu, den Sie verwenden.
7. Klicken Sie auf **Speichern**.
8. Melden Sie sich von Hub ab.

Weitere Informationen zum Bereitstellen von Geschäftsprozessen finden Sie im Benutzerhandbuch für das Interact Plug-in.

Das Formular an eine Arbeitswarteschlange in Blue Prism senden

1. Melden Sie sich bei Authentication Server mit den Anmeldedaten eines Mitglieds der Rolle an, die Sie dem Formular zugewiesen haben, und wählen Sie **Interact** aus.

   Für die Zwecke des Tests können Sie entweder den der Rolle zugewiesenen Administrator oder einen Benutzer verwenden. Nur Mitglieder der Rolle können das Formular in Interact sehen, unabhängig von ihren Administratorrechten.
2. Klicken Sie auf das Formular, das Sie gerade erstellt haben (**Testformular**).

   Das Formular wird mit dem einzelnen Textfeld angezeigt.
3. Geben Sie Text in das Feld ein und klicken Sie dann auf **Senden**.
4. Melden Sie sich bei Blue Prism an und prüfen Sie, ob sich ein Element in der Arbeitswarteschlange befindet, das beim Erstellen des Formulars angegeben wurde.

Weitere Informationen zur Verwendung von Interact als Endbenutzer finden Sie im Interact Benutzerhandbuch.

Damit ist die Überprüfung der Installation abgeschlossen, die beweist, dass Interact mit Blue Prism kommunizieren kann. Als nächstes muss überprüft werden, ob Blue Prism Informationen zurück an Interact senden kann.

Einen einfachen Blue Prism Prozess erstellen

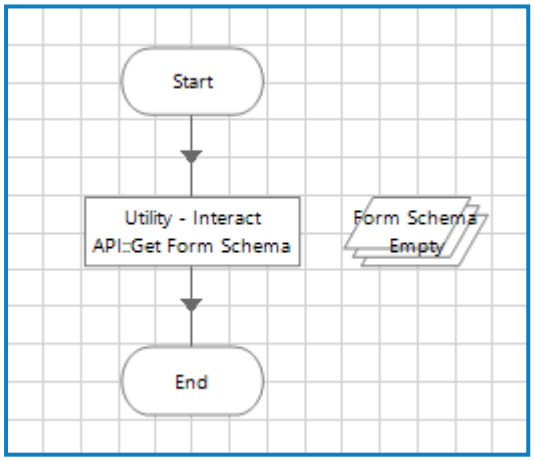
Sie können einen der beiden folgenden Prozesse verwenden. Beide zeigen, dass eine Kommunikation zwischen Blue Prism und Interact besteht. Diese Prozesse zeigen:

- Option 1 – Blue Prism kann den Formularnamen abfragen und eine Antwort von Interact erhalten, in diesem Fall den Formularnamen.
- Option 2 – Blue Prism kann einen Wert in einem Formular ändern, wobei die Änderung in Interact angezeigt wird.

Option 1: Den Formularnamen abrufen

1. Einen Prozess in Blue Prism erstellen
2. Fügen Sie Ihrem Prozess eine Aktion hinzu und legen Sie die folgenden Eigenschaften fest:
   a. Setzen Sie das **Geschäftsobjekt** auf **Dienstprogramm – Interact API**.
   b. Setzen Sie die **Aktion** auf **Formularschema abrufen**.
   c. Geben Sie auf der Registerkarte „Input“ unter **Formularnamenswert** den Namen des von Ihnen erstellten Formulars ein. Setzen Sie ihn in doppelte Anführungszeichen, z. B. “*Testformular*”.
   d. Erstellen Sie auf der Registerkarte „Output“ die standardmäßige Sammlung „Formularschema“.
3. Verbinden Sie die Aktionsphase mit den Start- und Endphasen.

   Ihr Prozess sollte nun ungefähr so aussehen:



4. Starten Sie den Prozess.
5. Öffnen Sie nach Abschluss die Sammlung „Formularschema“ und wählen Sie die Registerkarte **Aktuelle Werte** aus. Darin sollten Sie den Inhalt des Formulars sehen – in diesem Fall nur das Textfeld „TestTextFeld“.

Option 2: Einen Feldwert ändern

Dieser Prozess erfordert, dass sich ein Element in der Arbeitswarteschlange befindet – eines wurde im Rahmen von Das Formular an eine Arbeitswarteschlange in Blue Prism senden auf der vorherigen Seite gesendet.

1. Einen Prozess in Blue Prism erstellen
2. Fügen Sie Ihrem Prozess drei Aktionen hinzu und legen Sie die folgenden Eigenschaften fest:

Aktion 1:

a. Setzen Sie das **Geschäftsobjekt** auf **Arbeitswarteschlangen**.

b. Setzen Sie die **Aktion** auf **Nächstes Element abrufen**.

c. Geben Sie auf der Registerkarte „Input“ unter **Warteschlangenwert** den Namen der Warteschlange ein, in die das Formular gesendet werden soll. Diesen haben Sie unter Interact Formular erstellen auf Seite 87 in Schritt 6 eingegeben. Der Warteschlangenname muss in doppelten Anführungszeichen eingegeben werden, zum Beispiel *"InteractWarteschlange"*.

d. Erstellen Sie auf der Registerkarte „Output“ die Standarddatenerfassung und das Feld „Element-ID“.

Aktion 2:

a. Setzen Sie das **Geschäftsobjekt** auf **Dienstprogramm – Interact API**.

b. Setzen Sie die **Aktion** auf **Textfeldwert bearbeiten**.

c. Geben Sie auf der Registerkarte „Input“ die folgenden Werte ein:

- Geben Sie für **Einsende-ID** *[Data._requestId]* ein.
- Geben Sie für **Feldname** den Namen für das Feld zwischen doppelten Anführungszeichen ein, z. B. *"TestTextFeld"*.
- Geben Sie für **Feldwert** die Phase zwischen doppelten Anführungszeichen ein, die Sie an Interact zurücksenden möchten, z. B. *Beispieltext im Feld"*.

Aktion 3:

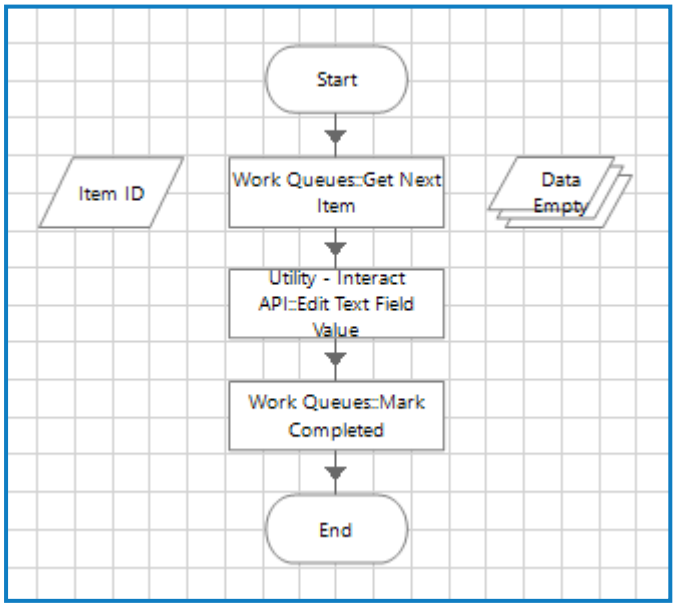
a. Setzen Sie das **Geschäftsobjekt** auf **Arbeitswarteschlangen**.

b. Setzen Sie die **Aktion** auf **Abgeschlossen markieren**.

c. Geben Sie auf der Registerkarte „Input“ im Wert **Element-ID** *[Element-ID]* ein. Dies ist der Datentyp „Text“, der durch die erste Aktion generiert wird.

3. Verbinden Sie die Aktionsphase untereinander und mit den Start- und Endphasen.

   Ihr Prozess sollte nun ungefähr so aussehen:



4. Starten Sie den Prozess.

5. Bei Abschluss:
    a. Öffnen Sie die Warteschlangen in Blue Prism. Das vorher eingesendete Formular muss als abgeschlossen gekennzeichnet sein.
    b. Öffnen Sie Interact, wählen Sie **Verlauf** aus, klicken Sie auf die drei Punkte (**...**) neben dem eingesendeten Formular und klicken Sie auf **Anzeigen**. Das Formular sollte den von Blue Prism gesendeten Text anzeigen.

Überprüfung abgeschlossen

Damit ist die Überprüfung der Installation abgeschlossen, die beweist, dass Blue Prism mit Interact und Interact mit Blue Prism kommunizieren kann.

Sie können jetzt alle von Ihnen erstellten Testelemente entfernen, wie z. B.:

- Löschen der Arbeitswarteschlange, wenn sie nicht mehr benötigt wird – siehe Workflow – Arbeitswarteschlangen.
- Löschen des Formulars aus dem Interact Plug-in – siehe im Benutzerhandbuch zum Interact Plug-in.
- Löschen des Geschäftsprozesses – siehe im Benutzerhandbuch für Automation Lifecycle Management.
- Löschen der Testrolle – siehe im Hub Administratorhandbuch.

Fehler in einer Interact Installation beheben

In den folgenden Abschnitten erhalten Sie Informationen zu spezifischen Problemen bei der Installation oder bei der Überprüfung, ob die Installation erfolgreich war.

Datenbankverbindung

Die Schaltfläche **Verbindung testen, um fortzufahren** im Installationsprogramm überprüft Folgendes:

- Wenn die Datenbank vorhanden ist:
  - Dass eine Verbindung dazu hergestellt werden kann.
  - Dass der SQL Server, auf dem die Datenbank gehostet wird, über ein gültiges Zertifikat verfügt.
  - Dass das Konto über die Rechte zum Lesen, Schreiben und Bearbeiten der Datenbank verfügt.
- Wenn die Datenbank nicht vorhanden ist:
  - Dass das Konto das Recht hat, die Datenbank zu erstellen.
  - Dass der SQL Server über ein gültiges Zertifikat verfügt.

Wenn diese Anforderungen nicht erfüllt werden können, wird die Installation angehalten.

Wenn über das LAN keine Verbindung zu einem SQL Server hergestellt werden kann, können Sie Folgendes überprüfen:

- Korrekte Netzwerkverbindung – Vergewissern Sie sich, dass alle relevanten Geräte mit demselben Netzwerk verbunden sind und kommunizieren können.
- SSL-Verschlüsselung – Stellen Sie sicher, dass der SQL Server über ein gültiges Zertifikat verfügt. Weitere Informationen finden Sie unter Voraussetzungen auf Seite 8.
- SQL-Anmeldedaten – Prüfen Sie die SQL-Anmeldedaten und ob der Benutzer auf dem SQL Server über die erforderlichen Berechtigungen verfügt.
- Firewall – Überprüfen Sie, ob die Firewalls auf dem Server selbst oder innerhalb des Netzwerks die Kommunikation verhindern.
- SQL-Browserdienst – Stellen Sie sicher, dass der SQL-Browserdienst auf dem SQL Server aktiviert ist und so eine SQL-Instanz finden kann. Bei SQL Server Express ist dieser Dienst meist standardmäßig deaktiviert.
- TCP-/IP-Verbindung aktivieren – Wenn für SQL eine Remoteverbindung erforderlich ist, prüfen Sie, ob die TCP-/IP-Verbindung für die SQL Instanz aktiviert ist. Microsoft bietet für jede Version von SQL spezifische Hilfsartikel zum Aktivieren des TCP-/IP-Netzwerkprotokolls für SQL Server.

Eine weitere mögliche Fehlerquelle ist, dass das Konto, das zum Erstellen der Datenbanken im Installationsprogramm verwendet wird, nicht über ausreichende Berechtigungen zum Erstellen der Datenbanken verfügt.

Webserver

Während des Installationsprozesses prüft das Installationsprogramm, ob alle Voraussetzungen installiert sind. Wenn die vorausgesetzten Komponenten nicht installiert sind, beenden Sie das Installationsprogramm, installieren Sie die vorausgesetzten Komponenten und starten Sie die Installation neu.

RabbitMQ mit AMQPS verwenden

Wenn Sie RabbitMQ mit AMQPS (Advanced Message Queuing Protocol – Secure) verwenden, müssen die im Rahmen der Interact Installation erstellten Anwendungspools Berechtigungen für das RabbitMQ-Zertifikat erhalten. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie den Zertifikat-Manager auf dem Webserver. Dazu geben Sie *Zertifikate* in das Suchfeld in der Windows-Taskleiste ein und klicken dann auf **Computerzertifikate verwalten**.
2. Navigieren Sie zu dem Zertifikat, das für die Verwendung mit RabbitMQ AMQPS während der Hub Installation identifiziert wurde, klicken Sie mit der rechten Maustaste auf das Zertifikat, wählen Sie **Alle Aufgaben** aus und klicken Sie auf **Private Schlüssel verwalten ...**.

   Das Dialogfeld „Berechtigungen“ für das Zertifikat wird angezeigt.
3. Klicken Sie auf **Hinzufügen** und geben Sie dann die folgenden Anwendungspools in das Feld **Auszuwählende Objektnamen eingeben** ein:

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

   > Dies sind die standardmäßigen Anwendungspoolnamen. Wenn Sie während der Installation unterschiedliche Namen eingegeben haben, stellen Sie sicher, dass die Liste die Namen enthält, die Sie verwendet haben.
4. Wenn Sie die Windows-Authentifizierung verwenden, fügen Sie auch den Namen des Dienstkontos hinzu, das für die folgenden Windows-Dienste verwendet wird:
   - Blue Prism – Audit-Dienst-Listener
   - Blue Prism – Log Service
   - Blue Prism – Manager für die Formularübermittlung
5. Klicken Sie auf **Namen überprüfen**.

   Die Namen sollten validiert werden. Wenn dies nicht der Fall ist, überprüfen Sie, ob der Name mit dem Anwendungspool oder dem Dienstkonto übereinstimmt, das Sie verwenden möchten, und korrigieren Sie ihn nach Bedarf.
6. Klicken Sie auf **OK**.
7. Wählen Sie nacheinander jeden Anwendungspool in der Liste **Gruppen- oder Benutzername** aus und stellen Sie sicher, dass **Vollzugriff** in der Liste **Berechtigungen für {Kontoname}** ausgewählt ist.
8. Klicken Sie auf **OK**.

   Die Anwendungspools haben nun Zugriff auf das Zertifikat.

Windows-Authentifizierung

Das Konto, auf dem die Installation ausgeführt wird, muss über die entsprechenden SQL Server-Berechtigungen verfügen, um die Installation durchzuführen, also die Mitgliedschaft in der festen Serverrolle „sysadmin“ oder „dbcreator“. Siehe Vorbereitung für Details.

Wenn die Windows-Authentifizierung während des Installationsprozesses ausgewählt wurde, empfehlen wir die Verwendung eines Windows-Dienstkontos mit den erforderlichen Berechtigungen, um die Aufgaben und Prozesse während des normalen Betriebs auszuführen. Das Windows-Dienstkonto benötigt:

- Die Fähigkeit, die SQL-Datenbankprozesse auszuführen, siehe Minimale SQL-Berechtigungen auf Seite 15.
- Die Eigentümerschaft des IIS-Anwendungspools.
- Berechtigungen für die erforderlichen Zertifikate.

Zuweisen des Windows-Dienstkontos als Eigentümer auf Zertifikaten

Dem Windows-Dienstkonto müssen Berechtigungen für die BluePrismCloud-Zertifikate gewährt werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie den Zertifikat-Manager auf dem Webserver. Dazu geben Sie *Zertifikate* in das Suchfeld in der Windows-Taskleiste ein und klicken dann auf **Computerzertifikate verwalten**.
2. Erweitern Sie im Navigationsbereich **Persönlich** und klicken Sie auf **Zertifikate**.
3. Befolgen Sie die folgenden Schritte für die BluePrismCloud_Data_Protection- und BluePrismCloud_IMS_JWT-Zertifikate:
    a. Klicken Sie mit der rechten Maustaste auf das Zertifikat, wählen Sie **Alle Aufgaben** aus und klicken Sie auf **Private Schlüssel verwalten ...**.

    Das Dialogfeld „Berechtigungen“ für das Zertifikat wird angezeigt.
    b. Klicken Sie auf **Hinzufügen**, geben Sie dann das Dienstkonto ein und klicken Sie auf **OK**.
    c. Wählen Sie das Dienstkonto in der Liste **Gruppen- oder Benutzername** aus und stellen Sie sicher, dass **Vollzugriff** in der Liste **Berechtigungen für {Kontoname}** ausgewählt ist.
    d. Klicken Sie auf **OK**.

    Das Dienstkonto hat nun Zugriff auf das Zertifikat.

Zuweisen eines Windows-Dienstkontos zum Anwendungspool

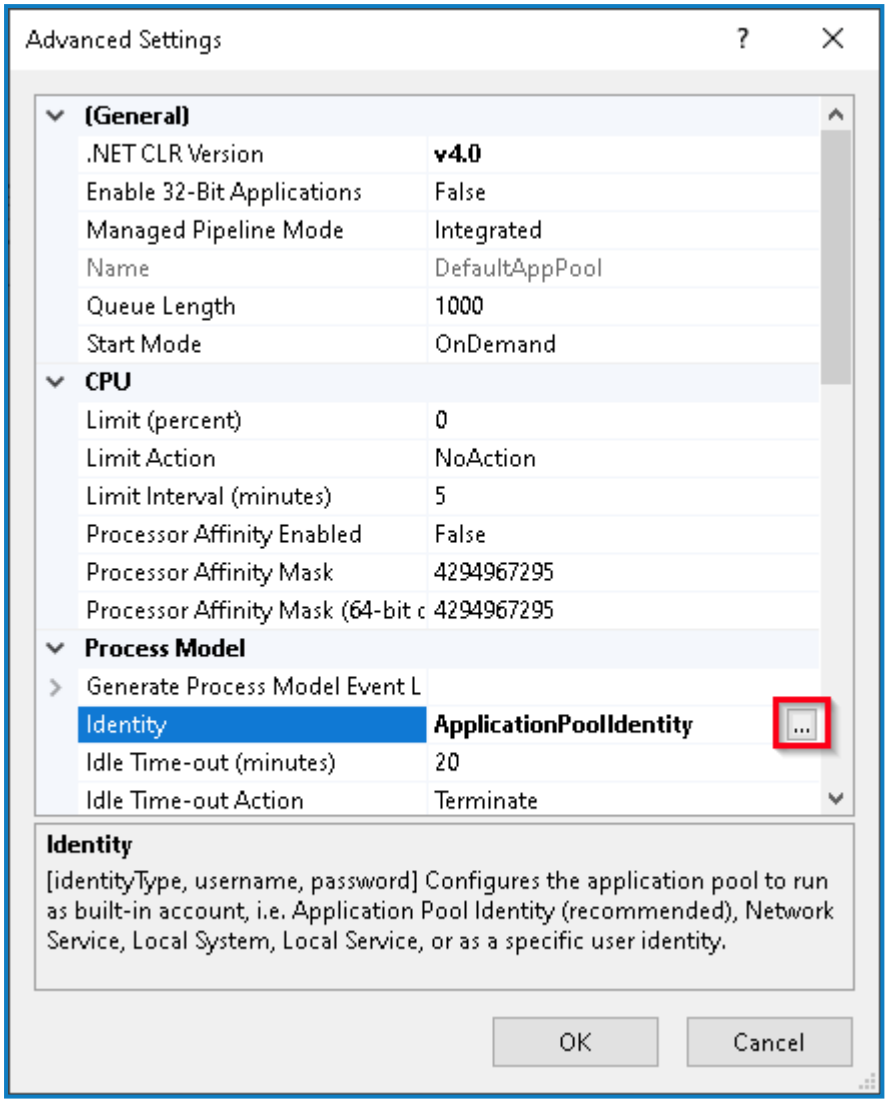
Standardmäßig werden die Anwendungspools mit der Identität „ApplicationPoolIdentity“ erstellt. Nachdem das Installationsprogramm abgeschlossen ist, muss das Windows-Dienstkonto zur Verwaltung der Anwendungspools zugewiesen werden. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie auf dem Webserver „Internet Information Services (IIS) Manager“.
2. Erweitern Sie im Panel „Verbindungen“ den Host und wählen Sie **Anwendungspools** aus.
3. Überprüfen Sie die Werte in der Spalte **Identität**.

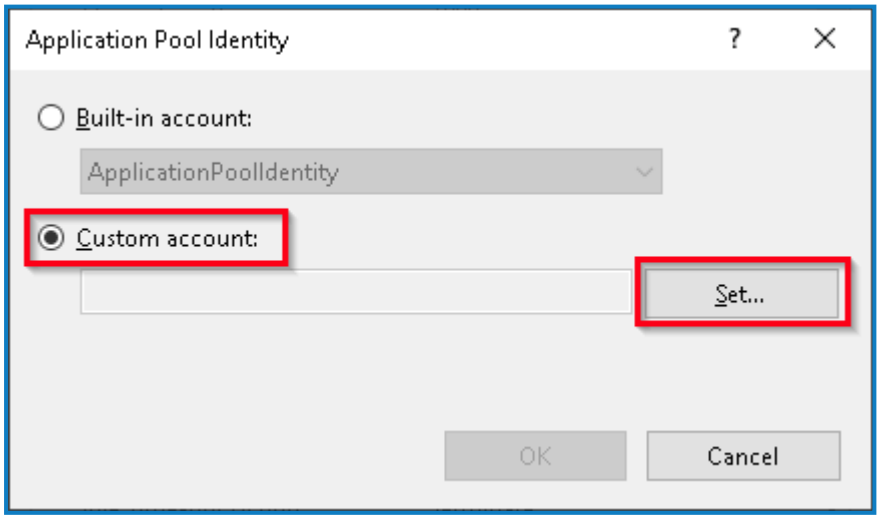
    Die Identität für einen Anwendungspool sollte mit dem betreffenden Windows-Dienstkonto übereinstimmen.
4. Bei Anwendungspools, bei denen *ApplicationPoolIdentity* in der Spalte **Identität** steht, klicken Sie mit der rechten Maustaste auf die Zeile und wählen **Erweiterte Einstellungen...** aus.

    Das Dialogfeld „Erweiterte Einstellungen“ wird angezeigt.

5. Wählen Sie die Einstellung **Identität** aus und klicken Sie dann auf die Schaltfläche **...** (Ellipse):



6. Wählen Sie im Dialogfeld „Anwendungspoolidentität“ die Option **Benutzerdefiniertes Konto** aus und klicken Sie auf **Einstellen...**.



Das Dialogfeld „Anmeldedaten festlegen“ wird angezeigt.

7. Geben Sie die Anmeldedaten für das erforderliche Windows-Dienstkonto ein und klicken Sie auf **OK**.
8. Wiederholen Sie dies für alle Anwendungspools, die geändert werden müssen.
9. Starten Sie den RabbitMQ-Dienst neu.
10. Starten Sie alle Anwendungspools neu.
11. Starten Sie IIS neu.

Stellen Sie bei Problemen mit dem Audit Service sicher, dass das Windows-Dienstkonto Zugriff auf den Audit Service Listener sowie auf die Audit Datenbank hat.

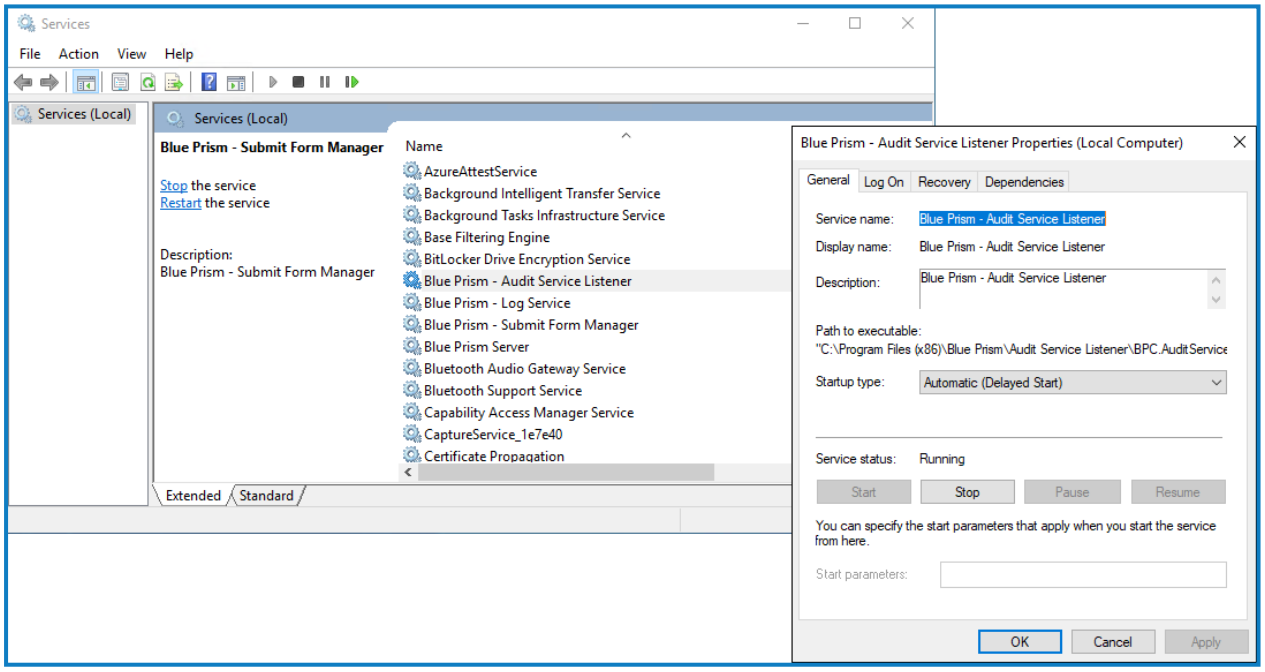
Zuweisen eines Windows-Dienstkontos zu einem Dienst

Das Windows-Dienstkonto muss zugewiesen werden, um die folgenden Dienste zu verwalten:

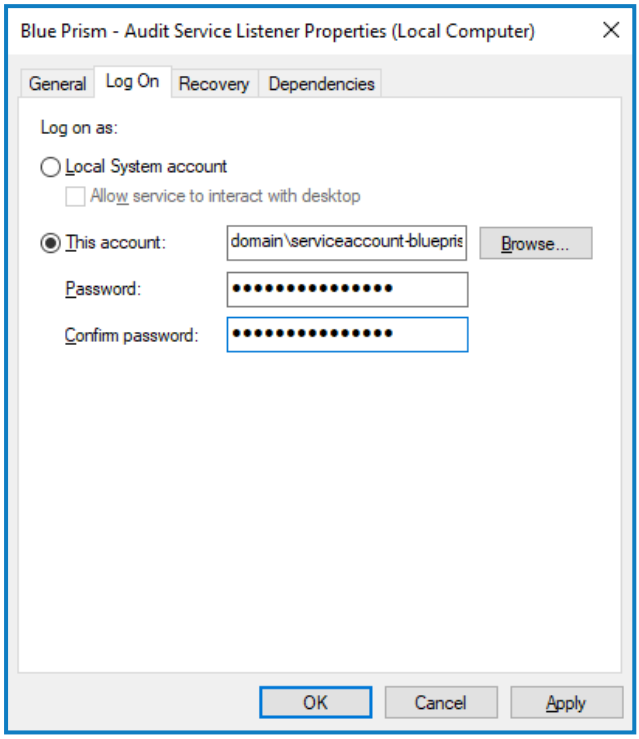
- Blue Prism – Audit-Dienst-Listener
- Blue Prism – Log Service
- Blue Prism – Manager für die Formularübermittlung

Gehen Sie dazu wie folgt vor:

1. Öffnen Sie „Dienste“ auf dem Webserver.
2. Klicken Sie mit der rechten Maustaste auf den Dienst und klicken Sie dann auf **Eigenschaften**.



3. Wählen Sie auf der Registerkarte „Anmelden“ die Option **Dieses Konto** aus und geben Sie dann den Kontonamen ein oder klicken Sie auf **Durchsuchen**, um das Konto auszuwählen, das Sie verwenden möchten.



4. Geben Sie das Passwort für das Konto ein und klicken Sie auf **OK**.
5. Klicken Sie im Fenster „Dienste“ mit der rechten Maustaste auf den Dienst und klicken Sie dann auf **Neu starten**.
6. Wiederholen Sie dies für die anderen Blue Prism Dienste.

In RabbitMQ steckengebliebene Nachrichten

Wenn eine Einsendung nicht zur erwarteten Blue Prism Enterprise Arbeitswarteschlange hinzugefügt wird, kann dies daran liegen, dass die Einsendung nicht korrekt durch den Message-Broker-Server (mit RabbitMQ) übergeben wurde.

Wenn ein Systemausfall von Hub oder Interact auftritt, können Interact Formular Einsendungen an eine RabbitMQ-Fehlerwarteschlange anstatt an die korrekte Nachrichtenwarteschlange in RabbitMQ (die dann die Einsendungen an die Arbeitswarteschlangen in Blue Prism Enterprise weiterleitet) gesendet werden. Ihr Systemadministrator (mit Zugriff auf RabbitMQ) muss die Einsendung aus der Fehlerwarteschlange entfernen.

Informationen zum Entfernen von Interact Formular Einsendungen aus der RabbitMQ-Fehlerwarteschlange finden Sie in diesem Knowledge-Base-Artikel: Interact Formular Einsendungen aus einer RabbitMQ-Fehlerwarteschlange entfernen.

Nachrichten können auch dann in RabbitMQ stecken bleiben, wenn IADA sie nicht verarbeiten und die Warteschlangen nicht aktualisieren konnte. IADA hängt von der Funktion „IIS-Anwendungsinitialisierung“ ab, die standardmäßig während des Installationsprozesses installiert werden sollte. Wenn es jedoch nicht installiert wurde, können Sie wie folgt vorgehen:

1. Öffnen Sie auf dem Webserver, auf dem Interact und IADA installiert sind, den Server Manager. Geben Sie hierzu Server im Suchfeld der Windows-Taskleiste ein und klicken Sie dann auf **Server Manager**.
2. Klicken Sie auf **Rollen und Funktionen hinzufügen**.

   Der Assistent zum Hinzufügen von Rollen und Funktionen wird angezeigt.
3. Klicken Sie auf **Weiter**, bis Sie die Seite „Serverrollen“ erreichen.
4. Erweitern Sie **Web Server (IIS),** erweitern Sie **Web Server**, erweitern Sie **Anwendungsentwicklung**, und wählen Sie dann **Anwendungsinitialisierung**.
5. Klicken Sie auf **Weiter**, bis Sie die Seite „Installationsauswahl bestätigen“ erreichen.
6. Klicken Sie auf **Installieren**.
7. Starten Sie den Webserver nach Abschluss der Installation neu.

Fehlerbehebung einer Hub Installation

In den folgenden Abschnitten erhalten Sie Informationen zu spezifischen Problemen bei der Installation oder bei der Überprüfung, ob die Installation erfolgreich war.

Message-Broker-Konnektivität

Um die Konnektivität zwischen dem Webserver und dem Message-Broker zu überprüfen, vergewissern Sie sich, ob die RabbitMQ Managementkonsole über einen Webbrowser zugänglich ist.

Es könnte mehrere Gründe dafür geben, dass die Verbindung fehlschlägt:

- Korrekte Netzwerkverbindung – Vergewissern Sie sich, dass alle relevanten Geräte mit demselben Netzwerk verbunden sind und kommunizieren können.
- Firewall – Überprüfen Sie, ob die Firewalls auf dem Server selbst oder innerhalb des Netzwerks die Kommunikation verhindern.

> Die RabbitMQ Managementkonsole kommuniziert standardmäßig auf Port 15672. Die Message-Broker-Warteschlangen verwenden standardmäßig einen anderen Port, 5672. Die Firewall sollte auf TCP-Zugriff auf allen Ports überprüft werden. Dies gilt insbesondere für die IT-Organisation, die nicht-standardmäßige Ports angegeben hat.

Datenbankverbindung

Die Schaltfläche **Verbindung testen, um fortzufahren** im Installationsprogramm überprüft Folgendes:

- Wenn die Datenbank vorhanden ist:
  - Dass eine Verbindung dazu hergestellt werden kann.
  - Dass der SQL Server, auf dem die Datenbank gehostet wird, über ein gültiges Zertifikat verfügt.
  - Dass das Konto über die Rechte zum Lesen, Schreiben und Bearbeiten der Datenbank verfügt.
- Wenn die Datenbank nicht vorhanden ist:
  - Dass das Konto das Recht hat, die Datenbank zu erstellen.
  - Dass der SQL Server über ein gültiges Zertifikat verfügt.

Wenn diese Anforderungen nicht erfüllt werden können, wird die Installation angehalten.

Wenn über das LAN keine Verbindung zu einem SQL Server hergestellt werden kann, können Sie Folgendes überprüfen:

- Korrekte Netzwerkverbindung – Vergewissern Sie sich, dass alle relevanten Geräte mit demselben Netzwerk verbunden sind und kommunizieren können.
- SSL-Verschlüsselung – Stellen Sie sicher, dass der SQL Server über ein gültiges Zertifikat verfügt. Weitere Informationen finden Sie unter .
- SQL-Anmeldedaten – Prüfen Sie die SQL-Anmeldedaten und ob der Benutzer auf dem SQL Server über die erforderlichen Berechtigungen verfügt.
- Firewall – Überprüfen Sie, ob die Firewalls auf dem Server selbst oder innerhalb des Netzwerks die Kommunikation verhindern.
- SQL-Browserdienst – Stellen Sie sicher, dass der SQL-Browserdienst auf dem SQL Server aktiviert ist und so eine SQL-Instanz finden kann. Bei SQL Server Express ist dieser Dienst meist standardmäßig deaktiviert.

- TCP-/IP-Verbindung aktivieren – Wenn für SQL eine Remoteverbindung erforderlich ist, prüfen Sie, ob die TCP-/IP-Verbindung für die SQL Instanz aktiviert ist. Microsoft bietet für jede Version von SQL spezifische Hilfsartikel zum Aktivieren des TCP-/IP-Netzwerkprotokolls für SQL Server.

Wenn beim Ausführen des Installationsprogramms der Installationsprozess mit Datenbankfehlern fehlschlägt (siehe unten), dann testen Sie, ob der Webserver über eine SQL–Verbindung zur Datenbank verfügt. Dies könnte auf einen der oben aufgeführten Gründe zurückzuführen sein.

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

Eine weitere mögliche Fehlerquelle ist, dass das Konto, das zum Erstellen der Datenbanken im Installationsprogramm verwendet wird, nicht über ausreichende Berechtigungen zum Erstellen der Datenbanken verfügt.

Fehler können auch auftreten, wenn es sich um eine Neuinstallation nach dem Löschen der Software handelt. Wenn dabei die gleichen Datenbanknamen verwendet wurden, sollten die ursprünglichen Datenbanken vor der Neuinstallation gesichert und gelöscht werden.

Webserver

Während des Installationsprozesses prüft das Installationsprogramm, ob alle Voraussetzungen installiert sind. Wenn die vorausgesetzten Komponenten nicht installiert sind, beenden Sie das Installationsprogramm, installieren Sie die vorausgesetzten Komponenten und starten Sie die Installation neu.

Weitere Informationen finden Sie unter Voraussetzungen auf Seite 8.

RabbitMQ mit AMQPS verwenden

Wenn Sie RabbitMQ mit AMQPS (Advanced Message Queuing Protocol – Secure) verwenden, müssen die im Rahmen der Hub Installation erstellten Anwendungspools Berechtigungen für das RabbitMQ-Zertifikat erhalten. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie den Zertifikat-Manager auf dem Webserver. Dazu geben Sie *Zertifikate* in das Suchfeld in der Windows-Taskleiste ein und klicken dann auf **Computerzertifikate verwalten**.
2. Navigieren Sie zu dem Zertifikat, das für die Verwendung mit RabbitMQ AMQPS während der Hub Installation identifiziert wurde, klicken Sie mit der rechten Maustaste auf das Zertifikat, wählen Sie **Alle Aufgaben** aus und klicken Sie auf **Private Schlüssel verwalten ...**.
   Das Dialogfeld „Berechtigungen“ für das Zertifikat wird angezeigt.
3. Klicken Sie auf **Hinzufügen** und geben Sie dann die folgenden Anwendungspools in das Feld **Auszuwählende Objektnamen eingeben** ein:

   > Dies sind die standardmäßigen Anwendungspoolnamen. Wenn Sie während der Installation unterschiedliche Namen eingegeben haben, stellen Sie sicher, dass die Liste die Namen enthält, die Sie verwendet haben.

4. Wenn Sie die Windows-Authentifizierung verwenden, fügen Sie auch den Namen des Dienstkontos hinzu, das für die folgenden Windows-Dienste verwendet wird:
   - Blue Prism – Audit-Dienst-Listener
   - Blue Prism – Log Service

5. Klicken Sie auf **Namen überprüfen**.

   Die Namen sollten validiert werden. Wenn dies nicht der Fall ist, überprüfen Sie, ob der Name mit dem Anwendungspool oder dem Dienstkonto übereinstimmt, das Sie verwenden möchten, und korrigieren Sie ihn nach Bedarf.
6. Klicken Sie auf **OK**.
7. Wählen Sie nacheinander jeden Anwendungspool in der Liste **Gruppen- oder Benutzername** aus und stellen Sie sicher, dass **Vollzugriff** in der Liste **Berechtigungen für {Kontoname}** ausgewählt ist.
8. Klicken Sie auf **OK**.

   Die Anwendungspools haben nun Zugriff auf das Zertifikat.

File Service

Wenn File Service das Bildmaterial für Authentication Server und Hub nicht findet, wird dies durch eine Deinstallation und Neuinstallation der Blue Prism Produkte verursacht. Dieses Problem tritt bei erstmaligen Installationen nicht auf.

Während des Löschens werden die Datenbanken nicht entfernt, und wenn die Neuinstallation die gleichen Datenbanknamen verwendet, werden die ursprünglichen Pfade zu den File Services und URLs weiterhin verwendet.

Um dies zu vermeiden, löschen oder bereinigen Sie die Datenbanken nach dem Löschen, sodass bisherige Pfade gelöscht werden, oder verwenden Sie alternative Datenbanknamen bei der Neuinstallation.

Browser für integrierte Windows-Authentifizierung konfigurieren

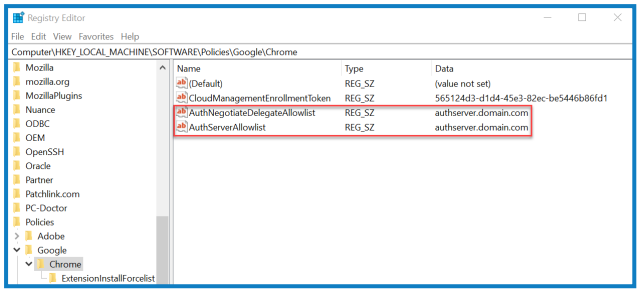
Falls sich Active Directory-Benutzer nach der Installation nicht bei Blue Prism Hub anmelden können, überprüfen Sie, ob Sie die unterstützten Webbrowser für die integrierte Windows-Authentifizierung konfiguriert haben, damit die derzeit angemeldeten Benutzer vom Client-Computer abgerufen werden können. Die Konfigurationsschritte sind für jeden von Hub unterstützten Webbrowser unterschiedlich.

Google Chrome konfigurieren

1. Schließen Sie alle offenen Instanzen von Chrome.
2. Öffnen Sie den Registrierung-Editor und geben Sie Folgendes in die obere Leiste ein:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
3. Klicken Sie mit der rechten Maustaste auf den Chrome-Ordner und wählen Sie **Neu** > **Zeichenfolgenwert**.
4. Fügen Sie die folgenden Zeichenfolgenwerte hinzu: `AuthNegotiateDelegateAllowlist` und `AuthServerAllowlist`.
5. Klicken Sie nacheinander mit der rechten Maustaste auf jeden Zeichenfolgenwert und wählen Sie **Ändern** aus.

6. Geben Sie im Feld **Wertdaten** für beide Zeichenfolgenwerte den Hostnamen der Authentication Server Website ein, z. B. authserver.domain.com, und klicken Sie auf **OK**.

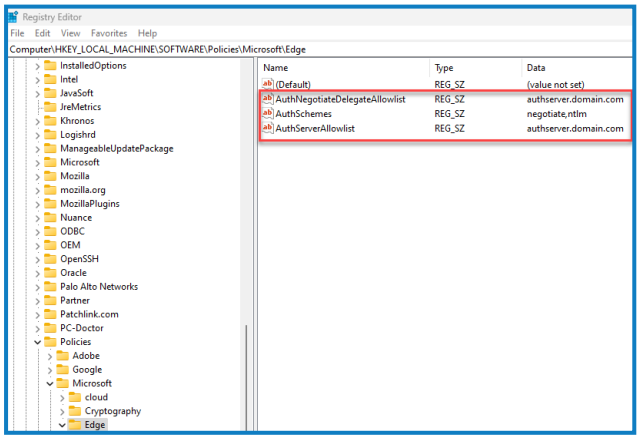


Microsoft Edge konfigurieren

1. Schließen Sie alle offenen Instanzen von Edge.
2. Öffnen Sie den Registrierung-Editor und geben Sie Folgendes in die obere Leiste ein:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Klicken Sie mit der rechten Maustaste auf den Edge-Ordner und wählen Sie **Neu** > **Zeichenfolgenwert** aus.
4. Fügen Sie die folgenden Zeichenfolgenwerte hinzu: `AuthNegotiateDelegateAllowlist`, `AuthServerAllowlist` und `AuthSchemes`.
5. Klicken Sie nacheinander mit der rechten Maustaste auf jeden Zeichenfolgenwert und wählen Sie **Ändern** aus.
6. Geben Sie im Feld **Wertdaten** für `AuthNegotiateDelegateAllowlist` und `AuthServerAllowlist` den Hostnamen der Authentication Server Website ein, z. B. authserver.domain.com, und klicken Sie auf **OK**.
7. Geben Sie `negotiate, ntlm` im Feld **Wertdaten** für `AuthSchemes` ein und klicken Sie auf **OK**. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu Microsoft Edge-Richtlinien.

> Dieser Zeichenfolgenwert ist nicht erforderlich, wenn in Ihrer Organisation nur die Kerberos-Authentifizierung eingerichtet ist. Unten finden Sie weitere Informationen.

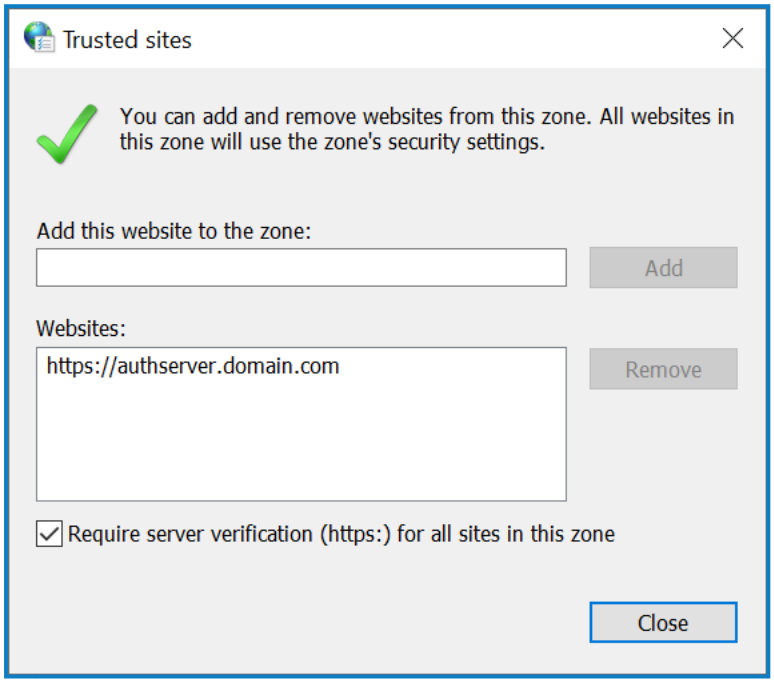


Alternativ können Sie die folgenden Schritte für Microsoft Edge ausführen:

1. Schließen Sie alle offenen Instanzen von Edge.
2. Navigieren Sie zu **Systemsteuerung** > **Netzwerk und Internet** > **Internetoptionen**.

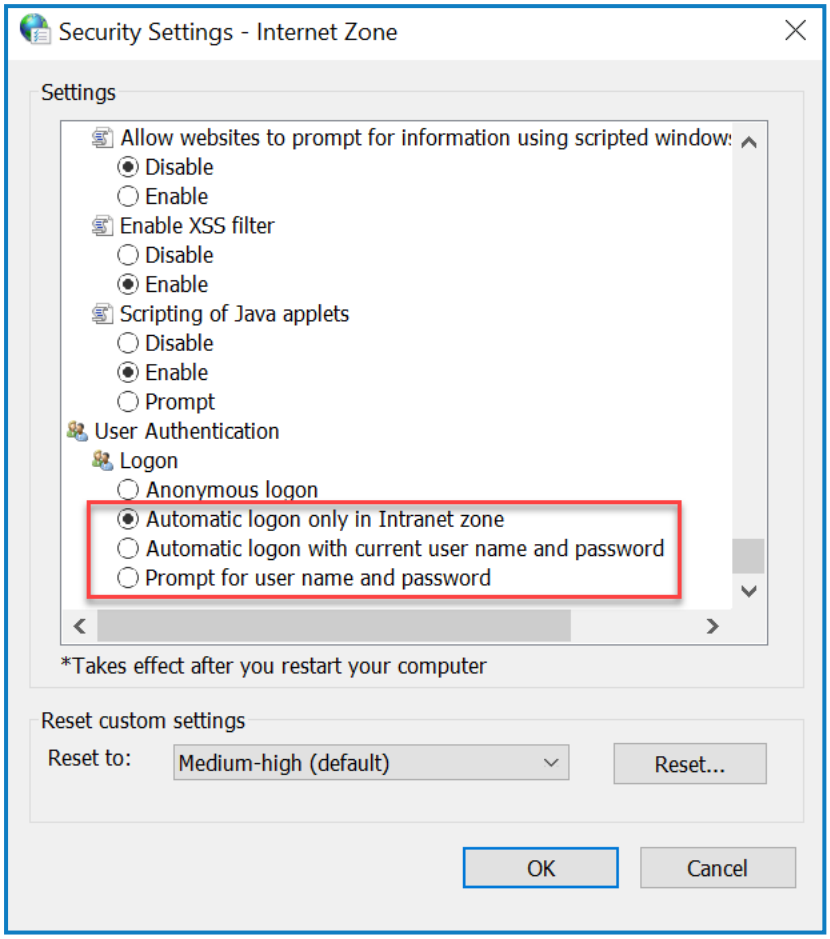
3. Wählen Sie auf der Registerkarte „Erweitert“ unter „Sicherheit“ die Option **Integrierte Windows-Authentifizierung aktivieren**.
4. Klicken Sie auf der Registerkarte „Sicherheit“ auf **Vertrauenswürdige Websites** > **Websites**.
5. Geben Sie im Dialogfeld „Vertrauenswürdige Websites“ die URL für Authentication Server (z. B. https://authserver.domain.com) in das Feld **Add this website to the zone (Diese Website zur Zone hinzufügen)** ein und klicken Sie auf **Hinzufügen**.

   Die URL wird im Feld **Websites** angezeigt.



6. Klicken Sie auf **Schließen**.
7. Klicken Sie auf der Registerkarte „Sicherheit“ im Dialogfeld „Internetoptionen“ auf **Vertrauenswürdige Websites** > **Benutzerdefinierte Ebene**.

8. Unter **Benutzerauthentifizierung** > **Anmeldung** bestätigen Sie, dass **Anonyme Anmeldung** nicht ausgewählt ist. Verwenden Sie stattdessen eine der Einstellungen, die es dem Browser ermöglicht, Benutzeranmeldeinformationen abzurufen, wie unten dargestellt.



9. Klicken Sie auf **OK**.

Kerberos-Authentifizierung konfigurieren

Die obigen Schritte reichen nicht aus, wenn die Windows-NTLM-Authentifizierung (New Technology LAN Manager) für Ihre Umgebung deaktiviert wurde. In diesem Fall müssen Sie auch die Kerberos-Authentifizierung und einen Service Principal Name (SPN) konfigurieren. Je nach Einrichtung Ihrer Organisation müssen Sie eventuell auch einen Microsoft Edge WebView2-Registrierungsschlüssel hinzufügen. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu NTLM und zur Kerberos-Authentifizierung.

1. Öffnen Sie auf dem Webserver „Internet Information Services (IIS) Manager“.
2. Wählen Sie in der Liste der Verbindungen **Blue Prism – Authentication Server** aus.

   Dies ist der Standard-Site-Name – wenn Sie einen benutzerdefinierten Site-Namen verwendet haben, wählen Sie die entsprechende Verbindung aus.
3. Doppelklicken Sie unter „IIS“ auf **Authentifizierung**.

   Die Seite „Authentifizierung“ wird angezeigt.
4. Wählen Sie **Windows-Authentifizierung** aus (stellen Sie sicher, dass sie auf *Aktiviert* eingestellt ist) und klicken Sie dann auf **Anbieter...**.

   Das Dialogfeld „Anbieter“ wird angezeigt.

5. Fügen Sie einen oder mehrere Anbieter aus der Liste der verfügbaren Anbieter basierend auf der Einrichtung Ihrer Organisation hinzu und klicken Sie auf **OK**.

Service Principal Name (SPN) konfigurieren

Ein Service Principal Name (SPN) muss auch für die Authentication Server URL konfiguriert und registriert werden, um sicherzustellen, dass die Kerberos-Authentifizierung korrekt funktioniert. Weitere Details, einschließlich der erforderlichen Berechtigungen, finden Sie in der Microsoft-Dokumentation in diesem Thema. Dies ist ein wesentlicher Schritt, den Sie mit dem IT-Team Ihrer Organisation besprechen müssen, um sicherzustellen, dass der Befehl `Setspn` nicht aufgrund von fehlenden Kontoberechtigungen fehlschlägt.

1. Öffnen Sie die Eingabeaufforderung als Administrator auf dem Webserver und führen Sie den zutreffenden folgenden Befehl aus.

   Wenn der Blue Prism – Authentication Server Anwendungspool als lokales Systemkonto ausgeführt wird, verwenden Sie:

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

   Wenn der Blue Prism – Authentication Server Anwendungspool als Dienstkonto ausgeführt wird, verwenden Sie:

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

   HTTP deckt HTTP sowie HTTPS ab. Ändern Sie den Befehl nicht, um HTTPS einzuschließen, da die Konfiguration fehlschlägt.

2. Führen Sie `Klist purge` aus, um die Kerberos-Tickets zu aktualisieren.
3. Melden Sie sich bei Authentication Server an, um zu überprüfen, ob die Kerberos-Authentifizierung korrekt funktioniert.

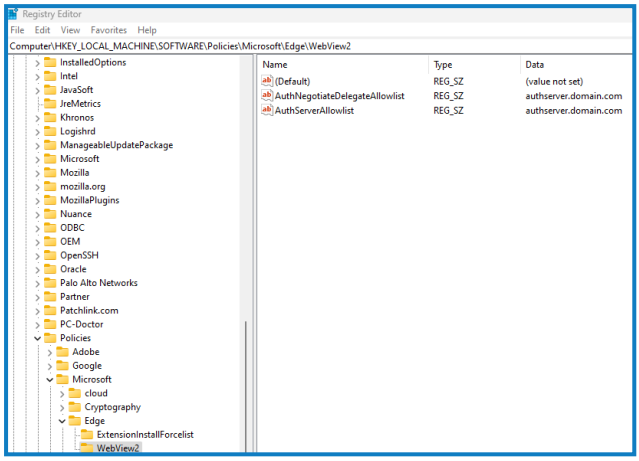
Microsoft Edge WebView2-Registrierungsschlüssel hinzufügen

Wenn in Ihrer Organisation nur die Kerberos-Authentifizierung eingerichtet ist und Authentication Server auch zur Anmeldung bei Blue Prism Enterprise verwendet wird, muss ein Registrierungsschlüssel für den Microsoft Edge WebView2-Browser hinzugefügt werden:

1. Schließen Sie alle offenen Instanzen von Edge.
2. Öffnen Sie den Registrierung-Editor und geben Sie Folgendes in die obere Leiste ein:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Klicken Sie mit der rechten Maustaste auf den Edge-Ordner und wählen Sie **Neu** > **Schlüssel** aus.
4. Nennen Sie den neuen Schlüssel **WebView2**.
5. Klicken Sie mit der rechten Maustaste auf den WebView2-Ordner und fügen Sie die folgenden Zeichenfolgenwerte hinzu: `AuthNegotiateDelegateAllowlist` und `AuthServerAllowlist`.
6. Klicken Sie nacheinander mit der rechten Maustaste auf jeden Zeichenfolgenwert und wählen Sie **Ändern** aus.

7. Geben Sie im Feld **Wertdaten** für `AuthNegotiateDelegateAllowlist` und `AuthServerAllowlist` den Hostnamen der Authentication Server Website ein, z. B. authserver.domain.com, und klicken Sie auf **OK**.



Hub meldet einen Fehler beim Starten

Wenn sich ein Benutzer beim Authentication Server anmeldet und Hub auswählt, wird die folgende Nachricht angezeigt:

Beim Starten der Anwendung ist ein Fehler aufgetreten

Das bedeutet, dass die IIS-Sites neu gestartet werden müssen. Dieser Fehler betrifft Systeme, die auf einem einzigen Server installiert sind, und tritt auf, wenn RabbitMQ nach den IIS-Sites gestartet wird. Daher wird empfohlen, dass eine Startverzögerung für die IIS-Sites festgelegt wird, damit RabbitMQ zuerst gestartet wird.

Wenn dieser Fehler auftritt, kann er auf folgende Weise behoben werden:

1. Öffnen Sie auf dem Server den Internet Information Services (IIS) Manager und stoppen Sie alle Blue Prism Sites. Eine Liste finden Sie unter Hub Websites.
2. Starten Sie den RabbitMQ-Dienst neu.
3. Starten Sie alle Blue Prism Anwendungspools neu.
4. Starten Sie die Blue Prism Sites, die in Schritt 1 gestoppt wurden.

So verzögern Sie den Start des IIS-Sites-Diensts:

1. Öffnen Sie „Dienste“ auf dem Server.
2. Klicken Sie mit der rechten Maustaste auf **WWW-Publishingdienst** und wählen Sie **Eigenschaften** aus.
3. Auf der Registerkarte „Allgemein“ legen Sie den **Starttyp** auf **Automatisch (Verzögerter Start)** fest.
4. Klicken Sie auf **OK** und schließen Sie das Dienste-Fenster.

SMTP-Einstellungen in Hub können nicht konfiguriert werden

Wenn Sie die SMTP-Einstellungen in Hub nicht konfigurieren können, hängt dies normalerweise mit der Startreihenfolge der Dienste zusammen.

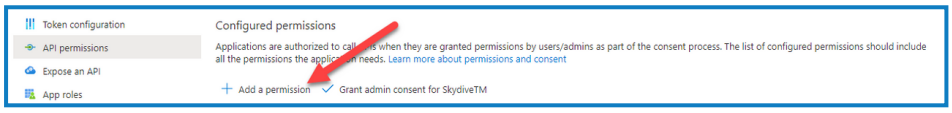
Der Webserver muss nach dem Start der RabbitMQ-Dienste gestartet werden. Wenn die Webserver-Dienste starten, bevor der RabbitMQ-Dienst bereit ist, dann führt das beim Öffnen der SMTP-Einstellungen in Hub zu einer Fehlermeldung.

Das Speichern der SMTP-Einstellung gibt einen Fehler zurück, wenn OAuth 2.0 verwendet wird

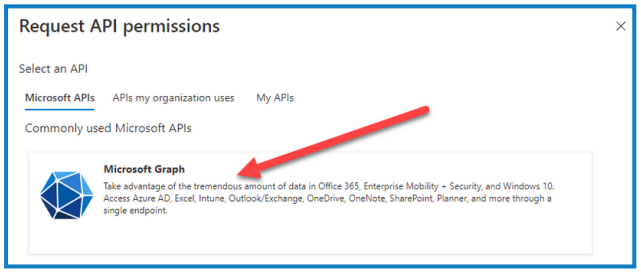
Wenn Sie beim Speichern einer E-Mail-Konfiguration mit OAuth 2.0 einen Fehler erhalten, überprüfen Sie, ob die Berechtigung Mail.Send für die Anwendung in Azure Active Directory konfiguriert ist.

So fügen Sie die Berechtigung Mail.Send hinzu:

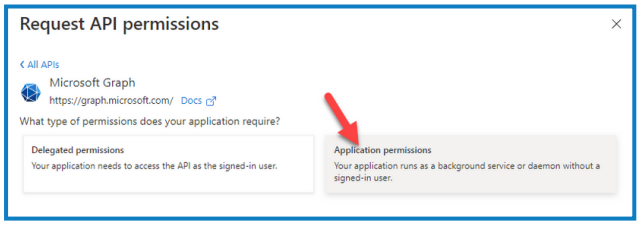
1. Öffnen Sie in Azure Active Directory die Anwendungseigenschaften der Anwendung, mit der Sie Hub verknüpfen.
2. Klicken Sie auf **API-Berechtigungen**.
3. Klicken Sie auf **Berechtigung hinzufügen**.



4. Wählen Sie unter „Microsoft-APIs“ eine API und dann die Option **Microsoft Graph** aus.

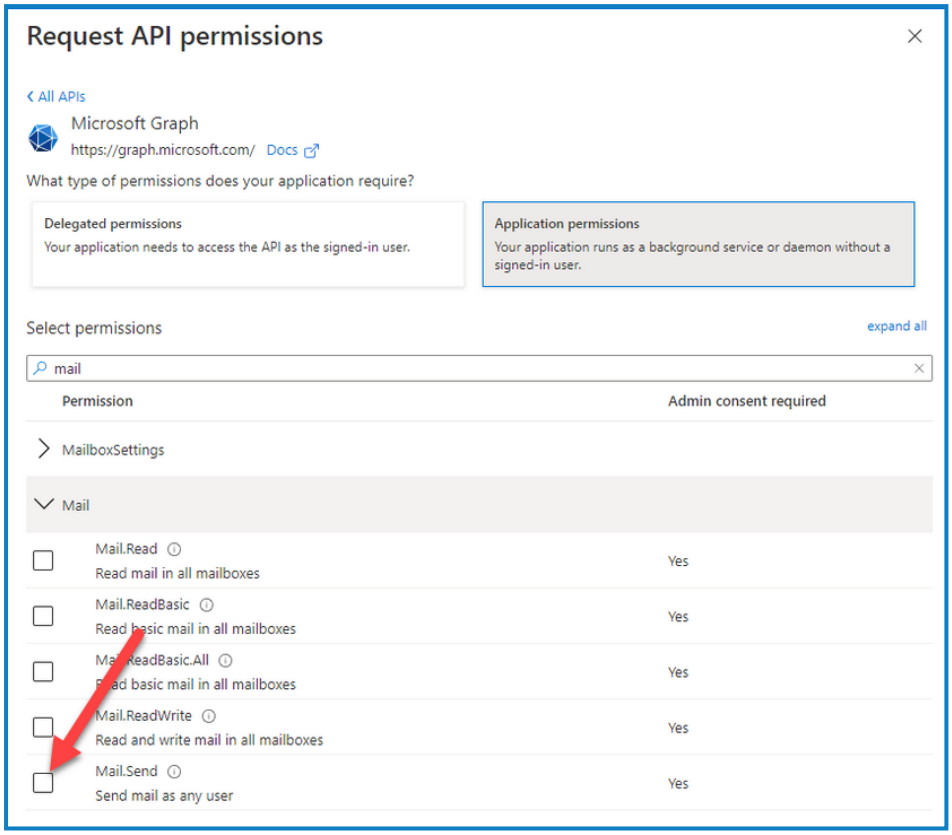


5. Klicken Sie unter Microsoft Graph auf **Anwendungsberechtigungen**.

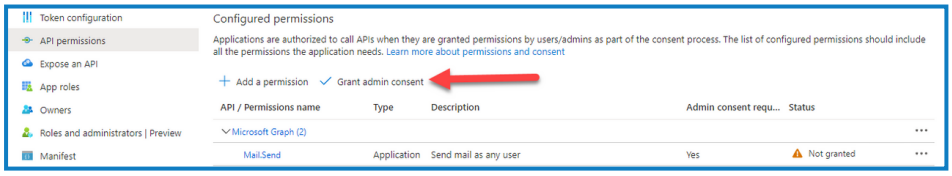


6. Geben Sie *Mail* in das Suchfeld ein und drücken Sie die Eingabetaste.

7. Wählen Sie in der angezeigten Mail-Liste **Mail.Send** aus und klicken Sie auf **Berechtigungen hinzufügen**.



8. Klicken Sie auf der Seite mit den Anwendungsberechtigungen auf **Administratoreinwilligung gewähren**.



Kunden-ID nach der Installation aktualisieren

Wenn Sie Ihre Kunden-ID nach der Installation eingeben oder aktualisieren müssen, müssen Sie die Konfigurationsdatei von License Manager appsettings.json aktualisieren. Nachdem die Konfigurationsdatei aktualisiert wurde, muss License Manager in Internet Information Services (IIS) Manager neu gestartet werden.

So aktualisieren Sie Ihre Kunden-ID in der Datei „appsetting.json“:

1. Öffnen Sie den Windows Explorer und navigieren Sie zu `C:\Programme (x86)\Blue Prism\LicenseManager\appsettings.json`.

   Das ist das standardmäßige Installationsverzeichnis. Passen Sie es an, wenn Sie ein eigenes Verzeichnis verwendet haben.

2. Öffnen Sie die Datei „appsettings.json“ in einem Texteditor.

3. Suchen Sie den Abschnitt `License:CustomerId` der Datei und geben Sie Ihre neue Kunden-ID ein, zum Beispiel:

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

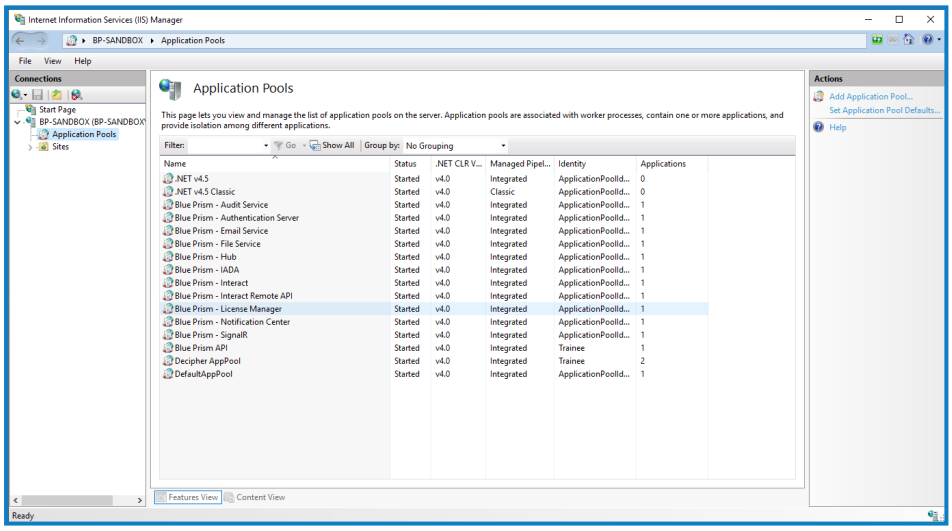
4. Speichern Sie die Datei.

So starten Sie License Manager neu:

1. Öffnen Sie Internet Information Services (IIS) Manager.
2. Wählen Sie in der Liste der Verbindungen **Blue Prism - License Manager** aus.

> Dies ist der Standard-Site-Name – wenn Sie einen benutzerdefinierten Site-Namen verwendet haben, wählen Sie die entsprechende Verbindung aus.

3. Klicken Sie unter „Website verwalten“ auf **Neu starten**.



License Manager wird neu gestartet.

Interact deinstallieren

Sie müssen ein Systemadministrator sein, um Blue Prism Interact deinstallieren zu können.

Um Interact 4.7 vollständig zu deinstallieren, müssen Sie:

1. Stoppen Sie die Anwendungspools mit IIS.
2. Interact über „Programme und Features“ entfernen.
3. Entfernen Sie die Datenbanken.
4. Entfernen Sie die RabbitMQ-Daten.
5. Entfernen Sie die Zertifikate.
6. Entfernen Sie alle verbleibenden Dateien.

Die Anwendungspools mit IIS stoppen

1. Öffnen Sie den Internet Information Services (IIS) Manager. Geben Sie hierzu *IIS* im Suchfeld der Windows-Taskleiste ein und klicken Sie dann auf **Internet Information Services (IIS) Manager**.
2. Klicken Sie im Bereich **Verbindungen** auf **Anwendungspools**.
3. Stoppen Sie alle Anwendungspools, die mit den Blue Prism Websites verknüpft sind – wählen Sie jeden nacheinander aus und klicken Sie auf **Stopp**. Eine Liste finden Sie unter Interact Websites auf Seite 16.

Interact über „Programme und Features“ entfernen

1. Die Systemsteuerung öffnen. Geben Sie hierzu *Systemsteuerung* im Suchfeld der Windows-Taskleiste ein und klicken Sie dann auf **Systemsteuerung**.
2. Klicken Sie auf **Programme** und dann auf **Programme und Features**.
3. Wählen Sie Blue Prism Interact aus.
4. Klicken Sie auf **Deinstallieren**.
5. Bestätigen Sie, dass Sie mit der Deinstallation fortfahren möchten.

Datenbanken entfernen

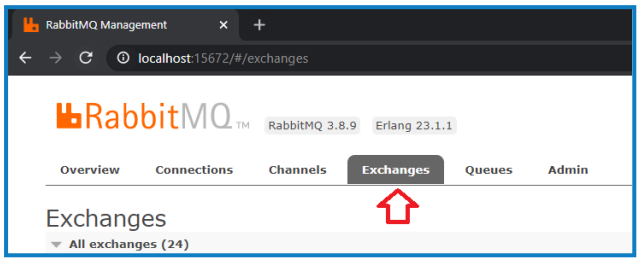
Sie sollten nur Datenbanken für Testsysteme entfernen. Wenn Sie eine Datenbank für ein System, das sich in der Produktion befand, entfernen möchten, sollten Sie überlegen, ob die Daten von Ihrem Unternehmen archiviert oder für Audit-Zwecke genutzt werden sollen.

> Wenn Sie Interact deinstallieren und es später mit denselben Datenbanken erneut installieren, sollten Sie vor der Neuinstallation alle Daten aus den Datenbanken entfernen.

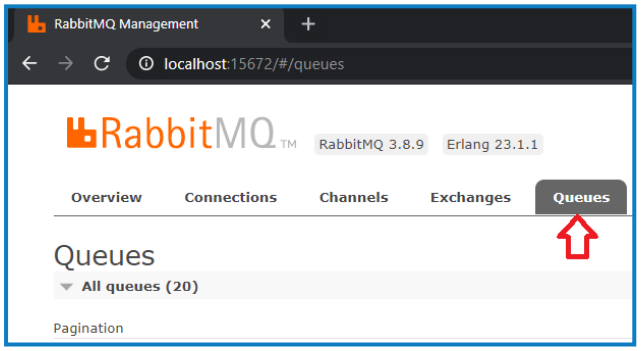
1. Löschen oder archivieren Sie die Datenbank für die Interact Anwendung.

RabbitMQ-Daten entfernen

1. Öffnen Sie die Administratorseite von RabbitMQ. Standardmäßig ist die URL http://localhost:15672/ auf dem lokalen Computer.
2. Klicken Sie auf **Exchanges** (Austausche).



3. Suchen und entfernen Sie die folgenden Elemente:
   - bpc.interact.*
4. Klicken Sie auf **Queues** (Warteschlangen).



5. Suchen und entfernen Sie die folgenden Elemente:
   - bpc.interact.*

Zertifikate entfernen

Diese Zertifikate werden auch von Hub verwendet. Wenn Interact und Hub auf demselben Server installiert sind, überspringen Sie diesen Abschnitt und entfernen Sie sie, wenn Sie Hub deinstallieren. Mehr erfahren Sie im Hub Installationshandbuch.

1. Öffnen Sie den Zertifikat-Manager. Dazu geben Sie *Zertifikate* in das Suchfeld in der Windows-Taskleiste ein und klicken dann auf **Computerzertifikate verwalten**.
2. Erweitern Sie im Navigationsbereich **Vertrauenswürdiges Root-Zertifikat** und klicken Sie auf **Zertifikate**.
3. Wählen und löschen Sie alle Zertifikate, die für die Blue Prism Sites erstellt wurden, sowie:
   - BluePrismCloud_Data_Protection
   - BluePrismCloud_IMS_JWT

Alle verbleibenden Dateien entfernen

1. Öffnen Sie im Windows-Explorer den übergeordneten Ordner für die Interact Installation. Normalerweise finden Sie den Ordner unter `C:\Programme (x86)\Blue Prism`, wenn bei der Interact Installation kein anderer Speicherort ausgewählt wurde.

2. Löschen Sie die folgenden Ordner und Dateien:
    - IADA
    - Interact
    - Interact Remote API
    - Submit Form Manager