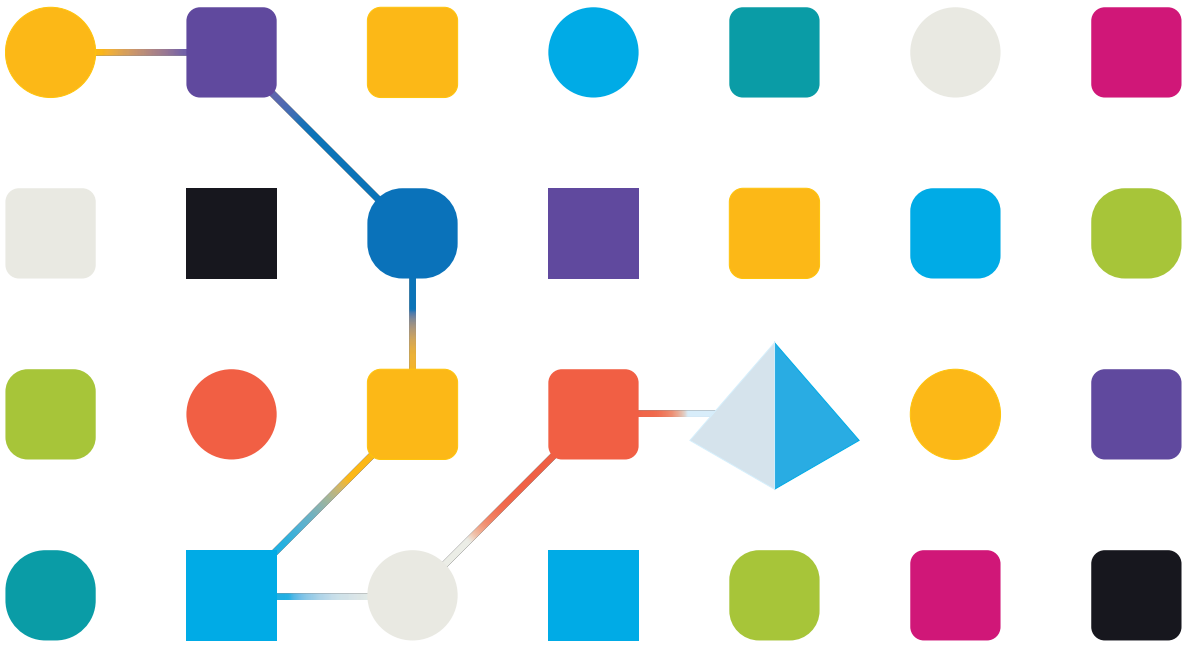
blueprism®

Hub 4.6

Installationshandbuch

Dokumentrevision: 3.0



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

Hub installieren

Dieses Handbuch erklärt die Installation von Blue Prism® Hub

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. Es wird davon ausgegangen, dass die Person, die die Installation von Hub durchführt, über Vorkenntnisse oder Erfahrungen mit Blue Prism, der Konfiguration von SSL-Zertifikaten und RabbitMQ verfügt.

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 auf die Version 4.6 von Blue Prism Hub.

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

Hub upgraden

Wenn Sie ein Upgrade von einer früheren Version auf Hub 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 Hub Installationsvideos anzuzeigen.

Weitere Anleitungen

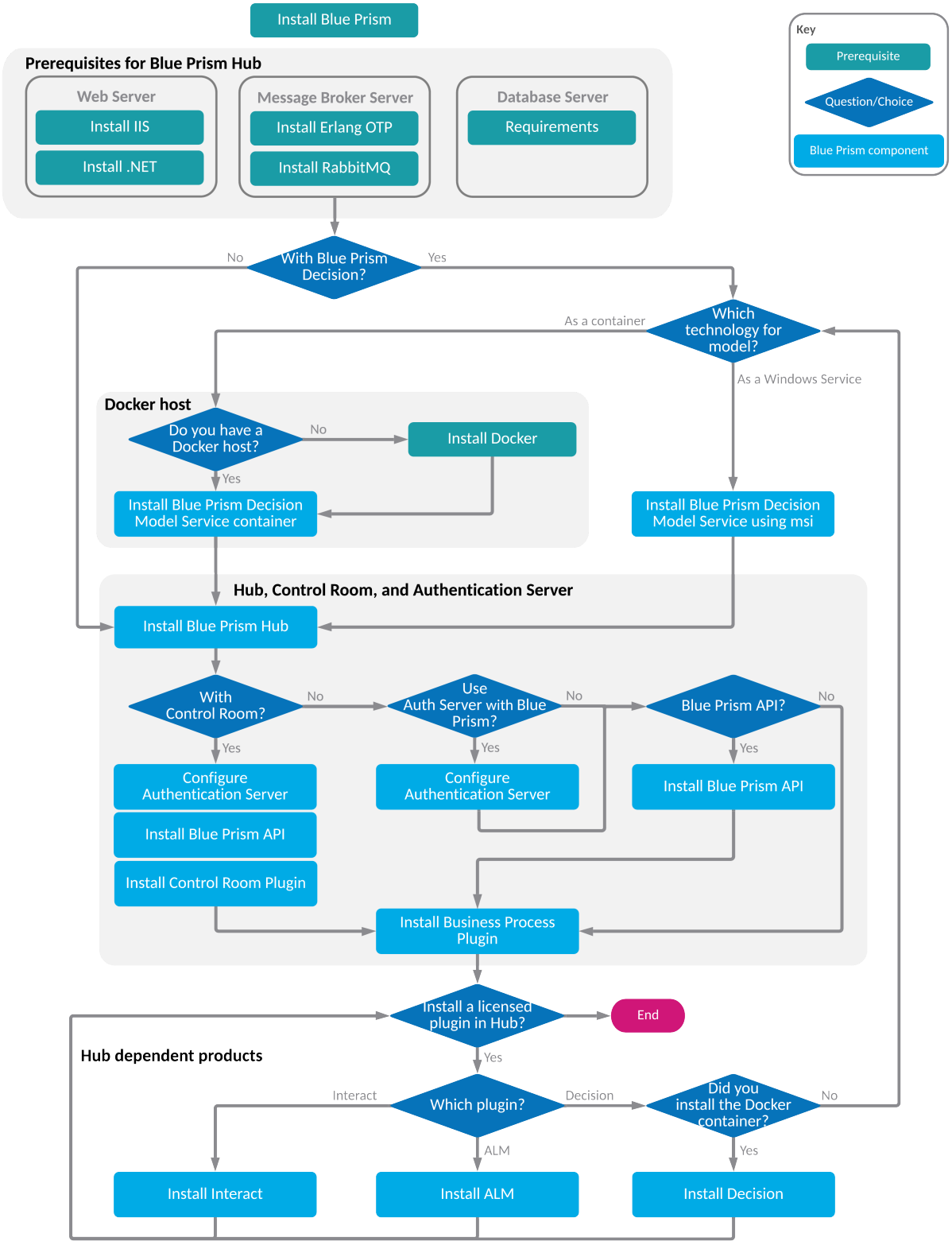
Die folgenden Dokumente enthalten weitere Informationen zu spezifischen Aspekten der Implementierung von Hub und seinen Plug-ins.

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.
Authentication Server – Konfigurationshandbuch	Ein Dokument, das erklärt, wie Authentication Server für Blue Prism Hub und Blue Prism Benutzerauthentifizierung konfiguriert wird.
ALM Benutzerhandbuch	Ein Dokument zur Verwendung des ALM Plug-ins (Automation Lifecycle Management). Dies ist ein lizenziertes Produkt.
Control Room Benutzerhandbuch	Ein Dokument zur Verwendung des Control Room Plug-ins. Das Plug-in ist frei verfügbar und kompatibel mit Blue Prism 7.0 oder höher.

Dokumenttitel	Beschreibung
Decision Installationshandbuch	Ein Dokument, das die Schritte zur Installation von Blue Prism Decision erklärt. Dies ist ein lizenziertes Produkt.
Decision Benutzerhandbuch	Ein Dokument zur Verwendung des Decision Plug-ins. Dies ist ein lizenziertes Produkt.
Interact Installationshandbuch	Ein Dokument, das die Schritte zur Installation von Interact erläutert. Dies ist ein lizenziertes Produkt.
Benutzerhandbuch zum Interact Plug-in	Ein Dokument, das erklärt, wie Sie das Interact Plug-in verwenden, um Formulare für die Interact Webanwendung zu erstellen. Dies ist ein lizenziertes Produkt.
Benutzerhandbuch zur Interact Webanwendung	Ein Dokument, das erklärt, wie die Interact Webanwendung als Endbenutzer verwendet wird. Dies ist ein lizenziertes Produkt.
Wireframer Benutzerhandbuch	Ein Dokument zur Nutzung der Wireframer Option, die Teil des ALM Plug-ins ist. Dies ist ein lizenziertes Produkt.

Installationsvorgang im Überblick

Im Diagramm unten ist der Installationsvorgang visuell dargestellt:



Vorbereiten

Vor der Installation von Blue Prism Hub ist es wichtig, sicherzustellen, dass die Architektur so konfiguriert ist, dass sie die Installation unterstützt. Mehrere Systeme sind erforderlich, um Hub 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 usw. Während des gesamten Installationsprozesses ist der Zugriff auf Administratorebene erforderlich. Weitere Details erhalten Sie unter Minimale SQL-Berechtigungen auf Seite 15.
- Es muss ein Message-Broker-Server, der RabbitMQ Message Broker hostet, verfügbar sein. Weitere Informationen finden Sie unter Message-Broker-Server installieren auf Seite 22.
- Ein Webserver für die Installation von Hub. Mehr erfahren Sie unter Voraussetzungen auf der nächsten Seite.
- Es muss Administratorzugriff für die Geräte verfügbar sein, auf denen Blue Prism Hub 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. DNS sollte für alle Komponenten verfügbar sein.
- 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?

  Details finden Sie unter Software-Anforderungen und Berechtigungen auf Seite 14.

Voraussetzungen

Unter Software-Anforderungen und Berechtigungen auf Seite 14 erfahren Sie mehr über die Software-Anforderungen und die minimalen SQL-Berechtigungen.

Die Installation von Hub erfordert die folgenden Voraussetzungen:

- 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 27.
- Sie erstellen die folgenden Websites – Sie sollten die URLs basierend auf der Domain Ihres Unternehmens definieren:

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

  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.

- 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 auf Seite 28.

- Ihre Kunden-ID – Während des Installationsprozesses werden Sie aufgefordert, Ihre Kunden-ID einzugeben. Diese finden Sie in der E-Mail, die Ihnen beim Kauf von ALM, Decision oder Interact zur Verwendung mit Hub zugesandt wurde.

  > Wenn Sie nur Control Room installieren, benötigen Sie keine Kunden-ID. Kunden-IDs werden nur mit ALM, Decision oder Interact zur Verfügung gestellt und werden von ihnen verlangt.

- Bei der Verwendung von Windows-Authentifizierung sind definierte Windows-Dienstkonten für die Verwendung mit der Blue Prism Umgebung erforderlich. Dadurch können Windows-Dienste und Anwendungspools für die während der Hub Installation erstellten Websites korrekt konfiguriert werden. Weitere Informationen finden Sie unter mit Windows-Authentifizierung installieren auf Seite 54.
- 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. Der Anwendungspool für Hub benötigt auch Zugriff auf das BPC_SQL_CERTIFICATE-Zertifikat. 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 3.8.16 bis 3.9.8, oder 3.11.9 bis 3.11.10 Mehr erfahren Sie unter siehe RabbitMQ herunterladen und installieren.	Message-Broker-Server installieren auf Seite 22
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.	

Link zu Software und Referenz	Weitere Anleitungen
IIS 10.0 Enthalten in Windows Server 2016 und Windows Server 2019.	Webserver installieren und konfigurieren auf Seite 27
.NET Core Windows Server Hosting 3.1.11 oder höhere Versionen von 3.1 https://dotnet.microsoft.com/download/dotnet/3.1 – Wählen Sie die benötigte Version aus. Wählen Sie unter **ASP.NET Core Runtime** die Option **Hosting-Paket** aus.	
.NET Core Windows Desktop Runtime 3.1.11 oder höhere Versionen von 3.1 https://dotnet.microsoft.com/download/dotnet/3.1 – Wählen Sie die benötigte Version aus. Wählen Sie unter **.NET Desktop Runtime** den benötigten Download aus.	
Visual C++ Redistributable 2012 (x64) https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe	
.NET Framework 4.7.2 https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer Unter Windows Server 2019 wird dies standardmäßig installiert. Sie müssen .NET Framework nur installieren, wenn Sie Windows Server 2016 verwenden.	
Blue Prism Hub 4.6 Laden Sie Hub von einer der folgenden Produkt-Downloadseiten im Blue Prism Portal herunter: • Automation Lifecycle Management • Decision • Interact	

Blue Prism Decision

Blue Prism Decision ist ein lizenzbasiertes Plug-in in Hub. Wenn Ihre Organisation Decision verwenden möchte, müssen Sie zusätzlich zu den in Blue Prism Hub auf der vorherigen Seite aufgeführten Downloads Folgendes herunterladen.

Der Decision Model Service ist mit zwei verschiedenen Technologien verfügbar:

- Als Windows-Dienst
- Als Linux-Container

Es muss nur eine davon installiert werden. Sie sollten die Version herunterladen, die am besten zur technischen Infrastruktur Ihres Unternehmens passt.

Software und Link	Weitere Anleitungen
OpenSSL https://www.openssl.org/source/ Dies ist ein optionaler Download, über den Sie selbstsignierte SSL-Zertifikate erstellen können. Dies sollte nur für POC/POV/Dev-Umgebungen verwendet werden.	Siehe OpenSSL-Website.
So führen Sie den Decision Model Service über den Container aus:	
Docker Engine ist die Mindestanforderung zur Ausführung des Decision Containers. https://www.docker.com/products/container-runtime Blue Prism empfiehlt, dass Ihre Produktionsumgebung einen Linux-Server als Host verwendet. Für POC- oder Dev-Umgebungen kann ein Windows-Server verwendet werden, auf dem Docker Desktop ausgeführt wird. https://www.docker.com/products/docker-desktop	Weitere Informationen zur Installation von Docker: • Auf einem Linux-Server finden Sie in der Docker-Hilfe unter Docker Engine installieren. • Auf einem Windows-Server finden Sie in der Docker-Hilfe unter Docker Desktop unter Windows installieren.
Blue Prism Decision Model Service Container Im Docker Hub zum Download verfügbar.	Blue Prism Decision installieren
So führen Sie den Decision Model Service als Windows-Dienst aus:	
Blue Prism Decision Model Service MSI. Im Blue Prism Portal zum Download verfügbar.	Blue Prism Decision installieren
Verwenden von Decision mit Blue Prism:	
Blue Prism Decision API.bprelease-Datei Im Blue Prism Portal zum Download verfügbar.	Blue Prism Decision installieren

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 Seite 10 aufgeführten Downloads Folgendes herunterladen.

Link zu Software und Referenz	Weitere Anleitungen
Blue Prism Interact 4.6 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 4.6. Die 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

Webserver

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

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	✓	✓

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)	✓	✓	✓

SQL Express eignet sich nur für Nicht-Produktionsumgebungen, z. B. für Demonstrationszwecke.

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 3.8.16 bis 3.9.8, 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 22.

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 4.7.2 – Standardmäßig auf Windows Server 2019 installiert.
- IIS 10.0
- .NET Core Windows Server Hosting 3.1.11 oder höhere Versionen von 3.1
- .NET Core Windows Desktop Runtime 3.1.11 oder höhere Versionen von 3.1
- Visual C++ Redistributable 2012 (x64)

Weitere Informationen finden Sie unter Webserver installieren und konfigurieren auf Seite 27.

Webbrowser auf Client-Computern

Die neuesten Versionen der folgenden Webbrowser werden von Hub unterstützt:

- Google Chrome
- Microsoft Edge (Chromium-basiert)

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

Microsoft Internet Explorer und Mozilla Firefox werden nicht unterstützt.

Blue Prism

Hub selbst erfordert nicht, dass Blue Prism verfügbar ist. Einige der Komponenten oder Plug-ins mit Hub erfordern jedoch Blue Prism. Diese sind:

- Authentication Server – Erfordert Blue Prism 7.1.0 oder höher.
- Blue Prism® Automation Lifecycle Management (ALM) – erfordert Blue Prism 6.4.0 oder höher.
- Control Room – erfordert Blue Prism 7.1.0 oder höher
- Blue Prism® Decision – erfordert Blue Prism 6.4.0 oder höher.
- Blue Prism® Interact – erfordert Blue Prism 6.4.0 oder höher.

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 der Datenbanken 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 Hub und Authentication Server Datenbanken zugreifen zu können. Die erforderlichen Berechtigungen sind:

- db_datareader
- db_datawriter

Weitere Informationen finden Sie unter Standardanwendungsinformationen unten.

Standardanwendungsinformationen

Die folgenden Informationen zeigen die Anwendungen, die von der 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. Zudem:

- IIS APPPOOL\ Blue Prism – Authentication Server und IIS APPPOOL\ Blue Prism – SignalR erfordert auch Zugriff auf das BluePrismCloud_IMS_JWT-Zertifikat.
- IIS APPPOOL\ Blue Prism – Hub erfordert auch Zugriff auf das Zertifikat BPC_SQL_CERTIFICATE.

Wenn Sie die Windows-Authentifizierung zur Authentifizierung mit SQL Server verwenden, empfehlen wir, dass ein dedizierter Active Directory-Benutzer der Identität des IIS-Anwendungspools zugewiesen wird (die Standardnamen sind in den Tabellen unten aufgeführt). Sie müssen sicherstellen, dass dieser Anwendungspool-Benutzer so eingestellt ist, dass er die Regionseinstellung **Englisch (USA)** verwendet. Um dies zu tun, öffnen Sie Systemsteuerung > Uhrzeit und Region > Region und stellen Sie das **Format** auf **Englisch (USA)** für den Anwendungspool-Benutzer ein.

Hub Websites

Anwendungsname	Beispielservice Kontoname für SQL Windows Authentifizierung	SQL Server Berechtigungen erforderlich während Installation	Datenbank Berechtigungen erforderlich während Anwendung läuft	Standarddatenbankname
Blue Prism - Authentication Server	IIS APPPOOL\ Blue Prism – Authentication Server	dbcreator / sysadmin	db_datawriter / db_datareader	AuthenticationServerDB
Blue Prism - Hub	IIS APPPOOL\ Blue Prism – Hub	dbcreator / sysadmin	Für die erste Anmeldung und anfängliche Konfiguration: dbcreator / sysadmin Nachfolgende Anmeldungen: db_datawriter / db_datareader	HubDB
Blue Prism - Email Service	IIS APPPOOL\ Blue Prism – Email Service	dbcreator / sysadmin	db_datawriter / db_datareader	EmailServiceDB
Blue Prism - Audit Service	IIS APPPOOL\ Blue Prism – Audit Service	dbcreator / sysadmin	db_datawriter / db_datareader	AuditDB
Blue Prism - File Service	IIS APPPOOL\ Blue Prism – File Service	dbcreator / sysadmin	db_datawriter / db_datareader	FileServiceDB
Blue Prism – Notification Center	IIS APPPOOL\ Blue Prism – Notification Center	dbcreator / sysadmin	db_datawriter / db_datareader	NotificationCenterDB

Anwendungsname	Beispielservice Kontoname für SQL Windows Authentifizierung	SQL Server Berechtigungen erforderlich während Installation	Datenbank Berechtigungen erforderlich während Anwendung läuft	Standarddatenbankname
Blue Prism – License Manager	IIS APPPOOL\ Blue Prism – License Manager	dbcreator / sysadmin	db_owner Oder db_datawriter / db_datareader mit Ausführungsberechtigungen (siehe unten)	LicenseManagerDB
Blue Prism – SignalR	IIS APPPOOL\ Blue Prism – SignalR	–	–	–

Wenn die Anwendung ausgeführt wird, benötigt License Manager die entsprechenden Berechtigungen, um gespeicherte Verfahren auszuführen. Wenn Sie db_owner nicht als Berechtigungsstufe verwenden möchten, können Sie db_datawriter/db_datareader verwenden und das folgende SQL-Skript ausführen, um diesem Benutzer die erforderliche Stufe zu gewähren:

```
USE [LicenseManagerDB]GRANT EXECUTE to "IIS APPPOOL\Blue Prism - License Manager"
```

Dabei gilt:

- [LicenseManagerDB] ist der Datenbankname für License Manager.
- „IIS APPPOOL\Blue Prism – License Manager" ist der Benutzername.

Hub Dienste

Anwendungsname	Beispielservice Kontoname für SQL Windows Authentifizierung	SQL Server Berechtigungen erforderlich während Installation	Datenbank Berechtigungen erforderlich während Anwendung läuft	Standarddatenbankname
Blue Prism - Audit Service Listener	NT AUTHORITY\ SYSTEM	dbcreator / sysadmin	db_datawriter / db_datareader	AuditDB
Blue Prism - Log Service	NT AUTHORITY\ SYSTEM	–	–	–

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 von

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

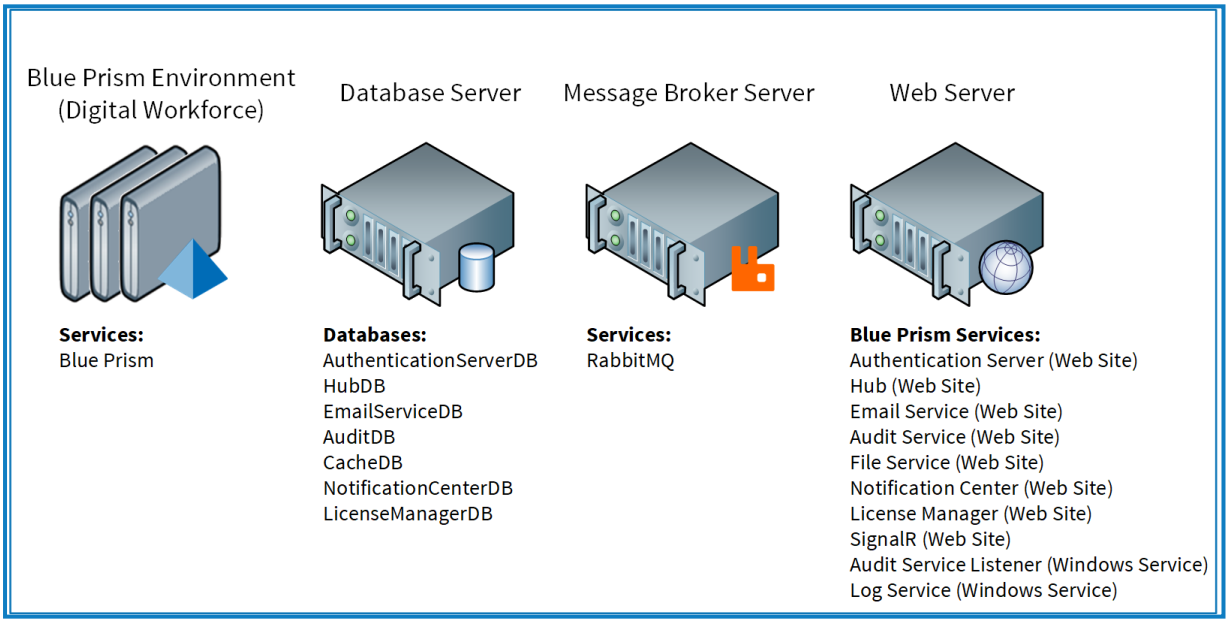
Bevor Sie diese Anleitung befolgen, lesen Sie die Informationen unter Vorbereiten auf Seite 8 durch.

In Produktionsumgebungen sind mindestens vier Ressourcen erforderlich:

- Blue Prism Umgebung (Digital Workforce)
- Datenbankserver (SQL Server)
- Message-Broker-Server
- Webserver

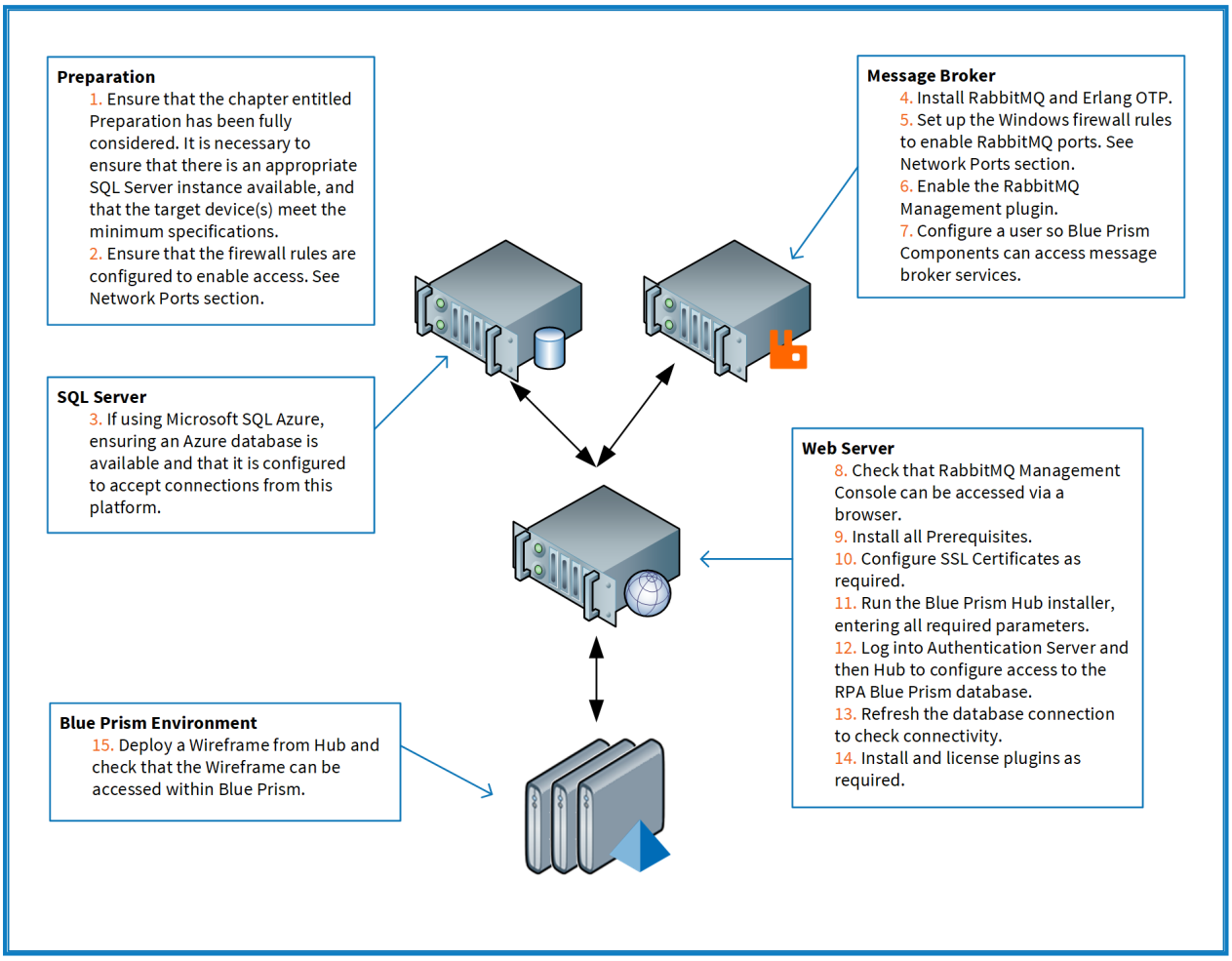
Vor der Installation von Blue Prism Hub müssen die Message-Broker-Server- und SQL Server-Instanzen konfiguriert werden.

Das folgende Diagramm veranschaulicht die typische Architektur für eine Umgebung.



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 Hub Installation auf Seite 67.

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 14.

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.

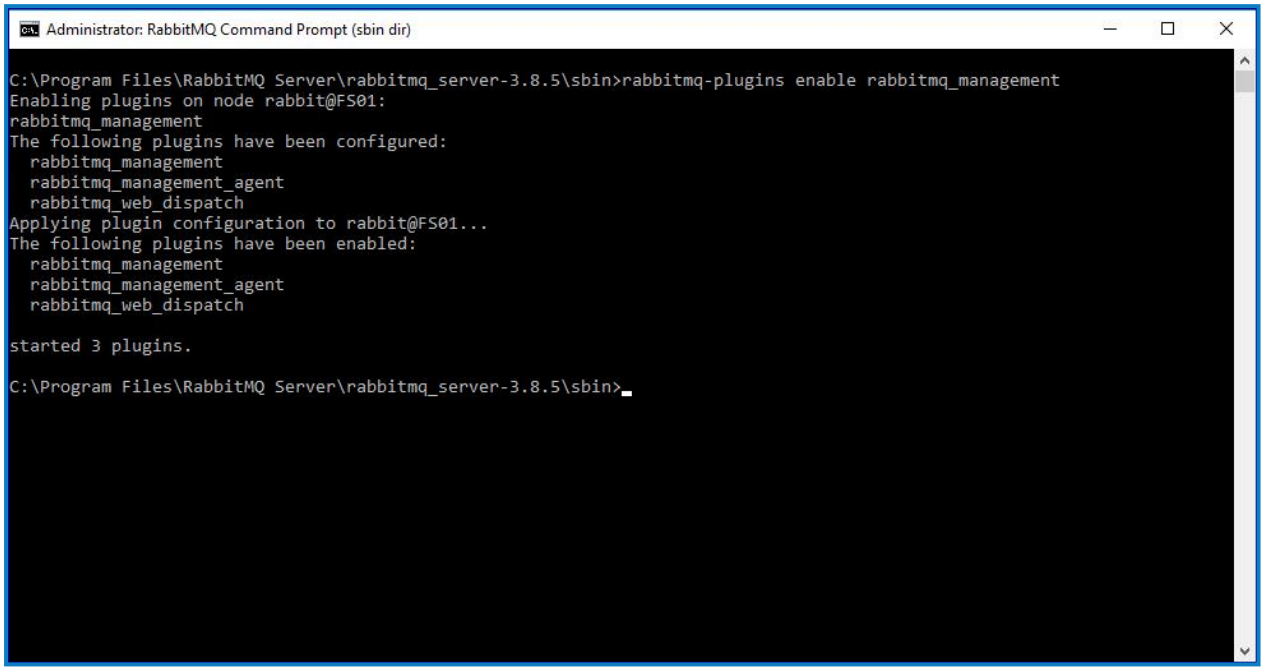
   Mehr erfahren Sie unter siehe RabbitMQ herunterladen und installieren.

   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).

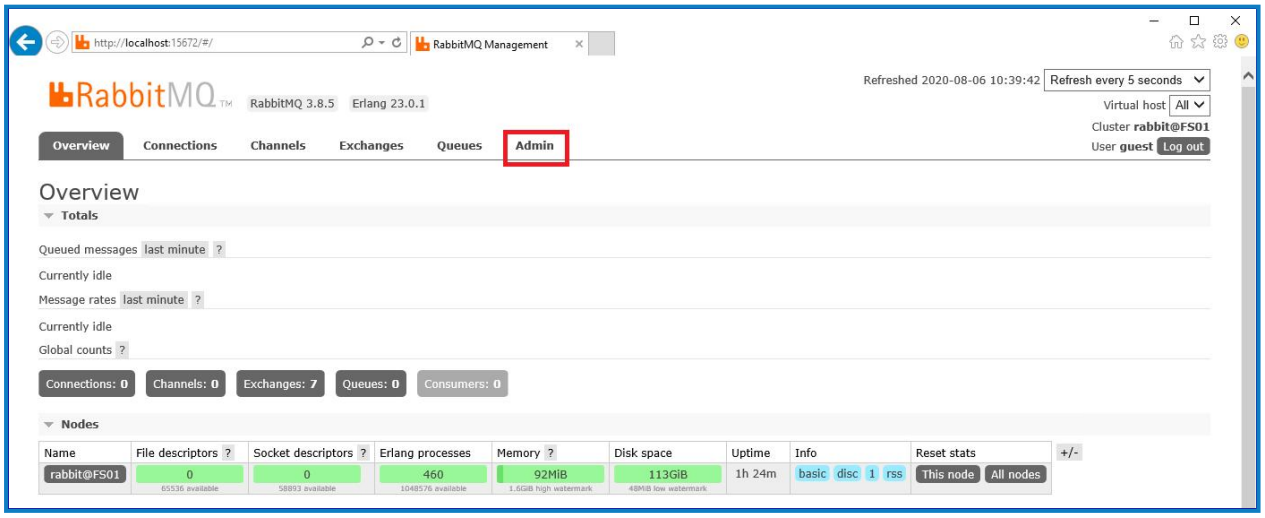
5. Geben Sie im Fenster „RabbitMQ Command Prompt“ den folgenden Befehl ein:

```
rabbitmq-plugins enable rabbitmq_management
```

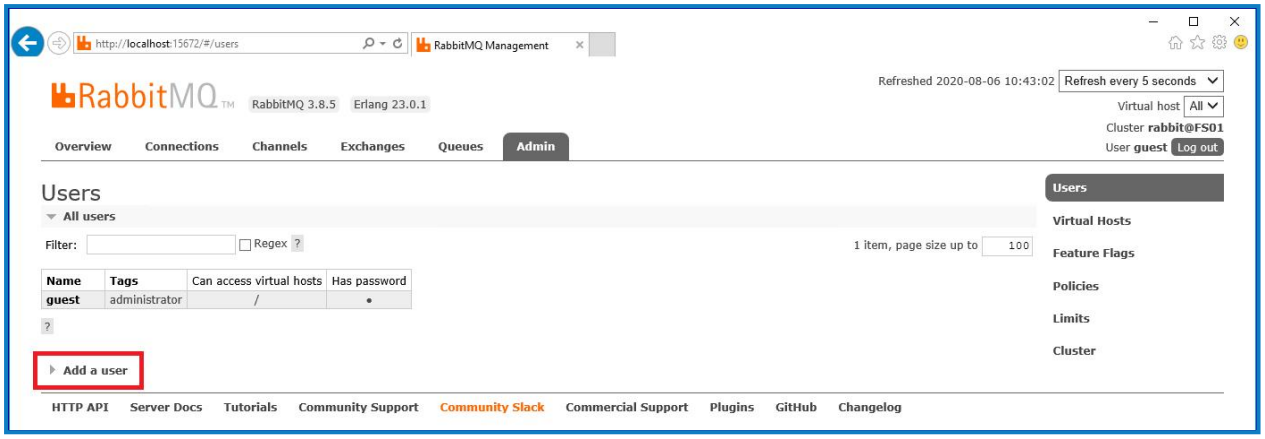


6. Starten Sie einen Browser und navigieren Sie zur folgenden URL: http://localhost:15672
7. Melden Sie sich in der RabbitMQ-Konsole mit den Standard-Anmeldedaten „guest/guest“ an.

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



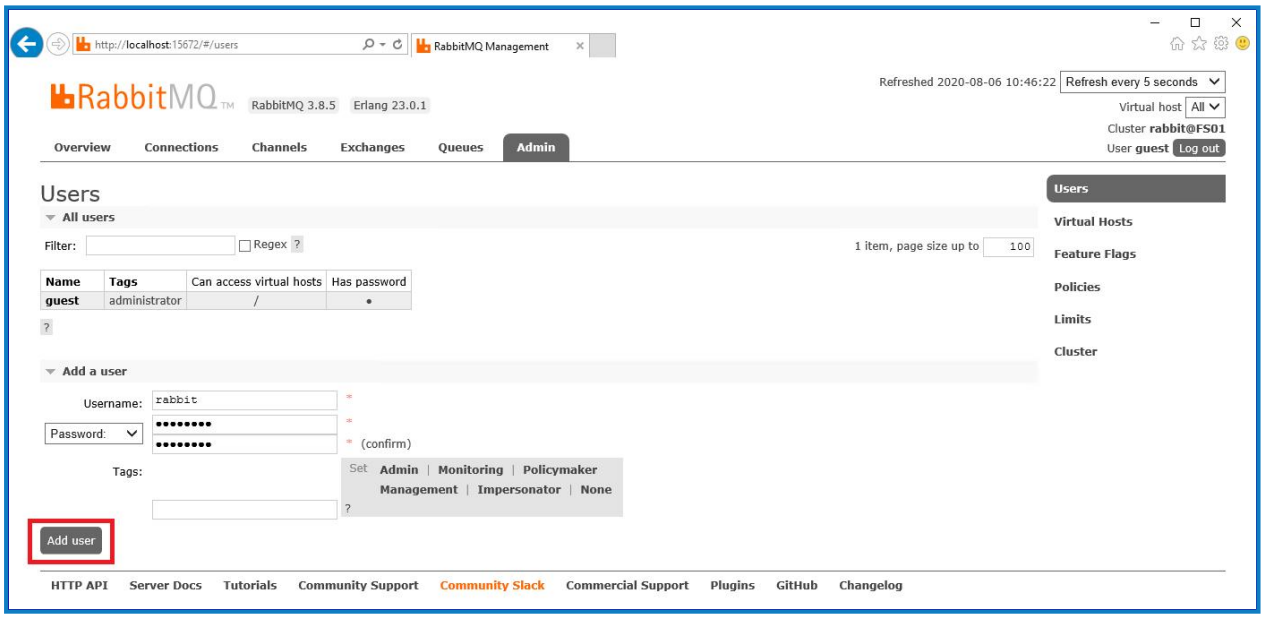
9. Klicken Sie auf **Add a user** (Einen Benutzer hinzufügen).



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.

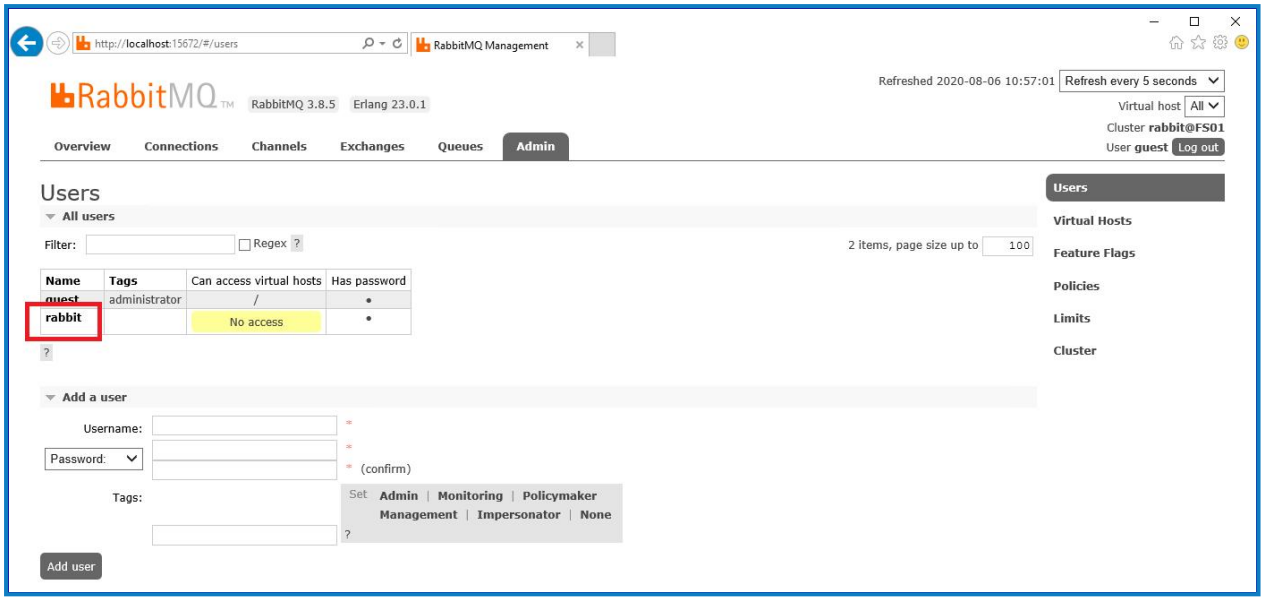
> Die folgenden Zeichen dürfen bei der Erstellung des RabbitMQ-Benutzers nicht für das Passwort verwendet werden: **# / : ? @ \ ` " $ '**.

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

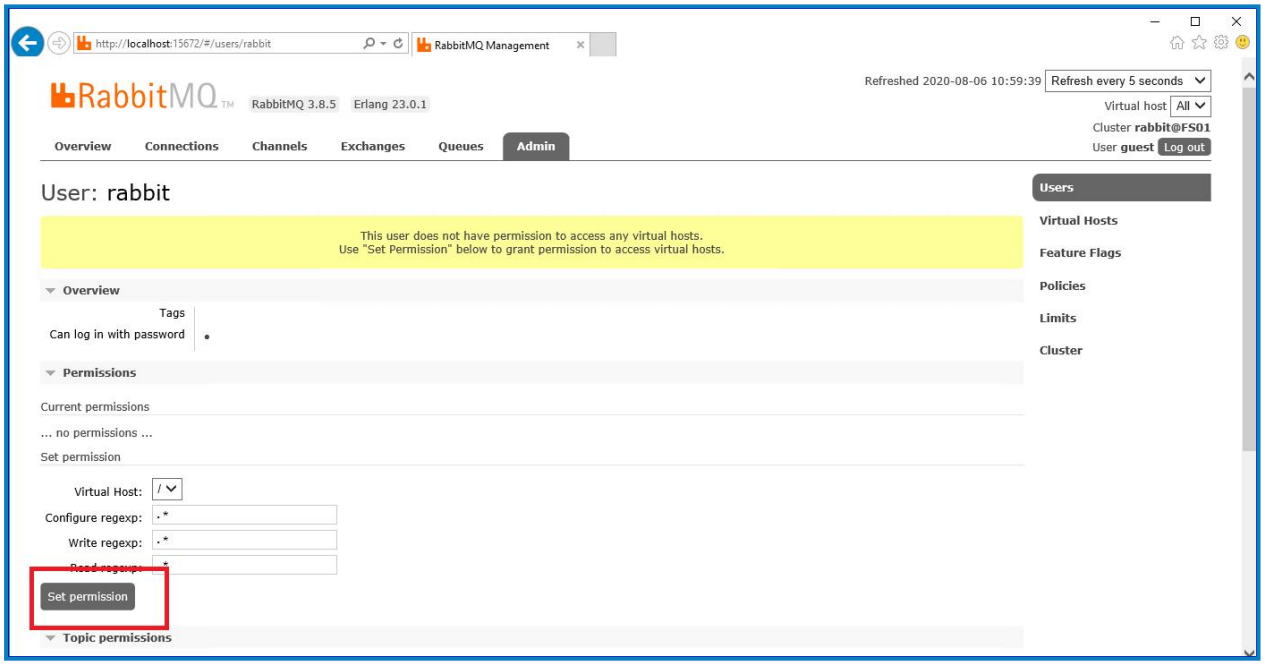


Als Nächstes werden die Berechtigungen des Benutzers festgelegt.

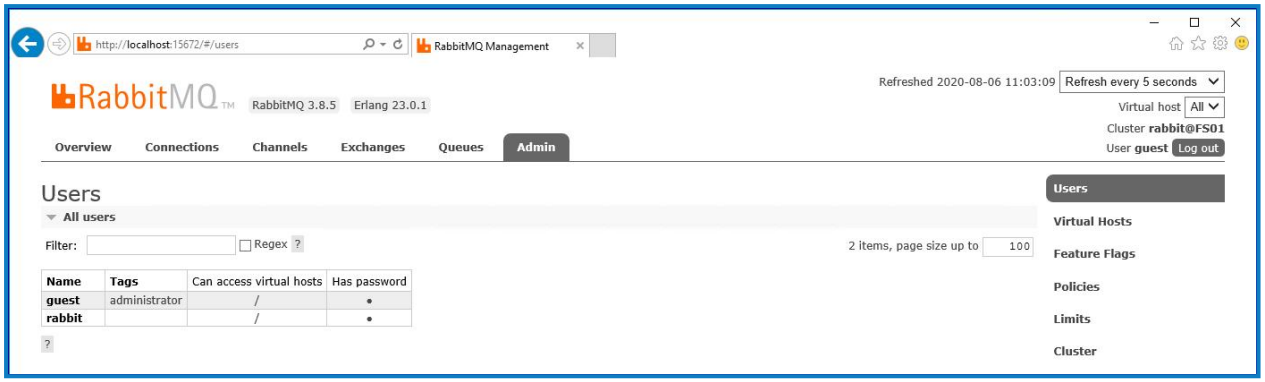
12. Klicken Sie auf den Benutzernamen des Benutzers, den Sie gerade erstellt haben.



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 67.

Webserver installieren und konfigurieren

Lesen Sie vor dem Installieren des Hub Webservers die Informationen unter Vorbereiten auf Seite 8.

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. Anwendungspool-Recycling konfigurieren

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.

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 der folgenden Tabelle sind die erforderlichen SSL-Zertifikate aufgeführt.

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

⚠ 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 Sie ein selbstsigniertes Zertifikat:

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.
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 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 -FriendlyName "TheOneCert" -NotAfter (Get-Date).AddYears(10)
```

> XXXXXXXXXX muss durch den Host-Servernamen ersetzt werden.

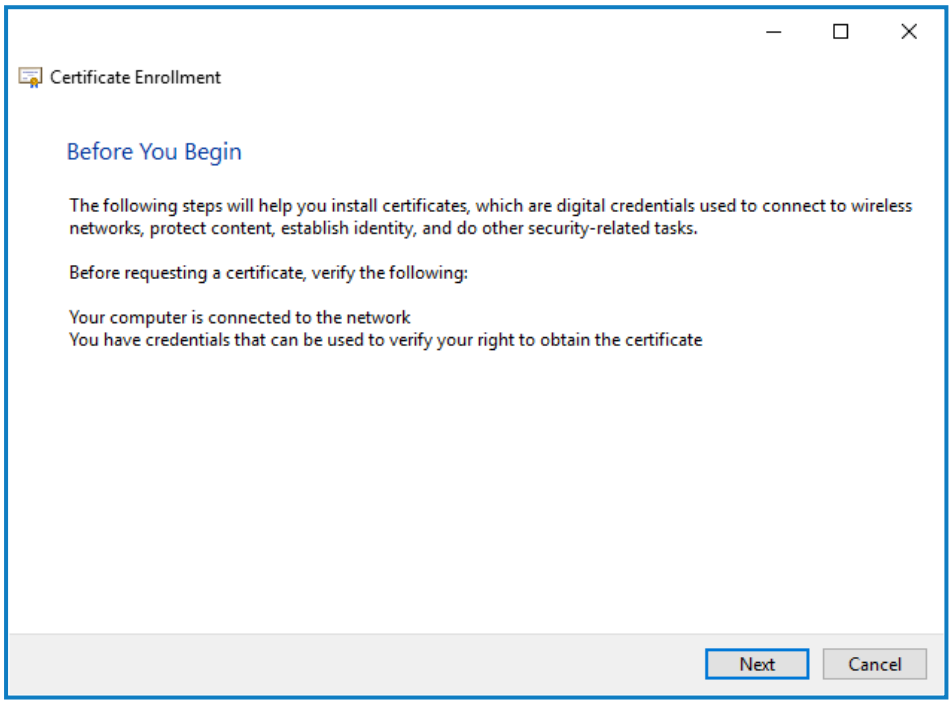
Öffnen Sie nach der Erstellung den Zertifikat-Manager des lokalen Computers (certlm) und kopieren Sie die Zertifikate in den Zertifikatspeicher für vertrauenswürdige Root-Zertifikate.

Offline-Zertifikatanforderung erstellen

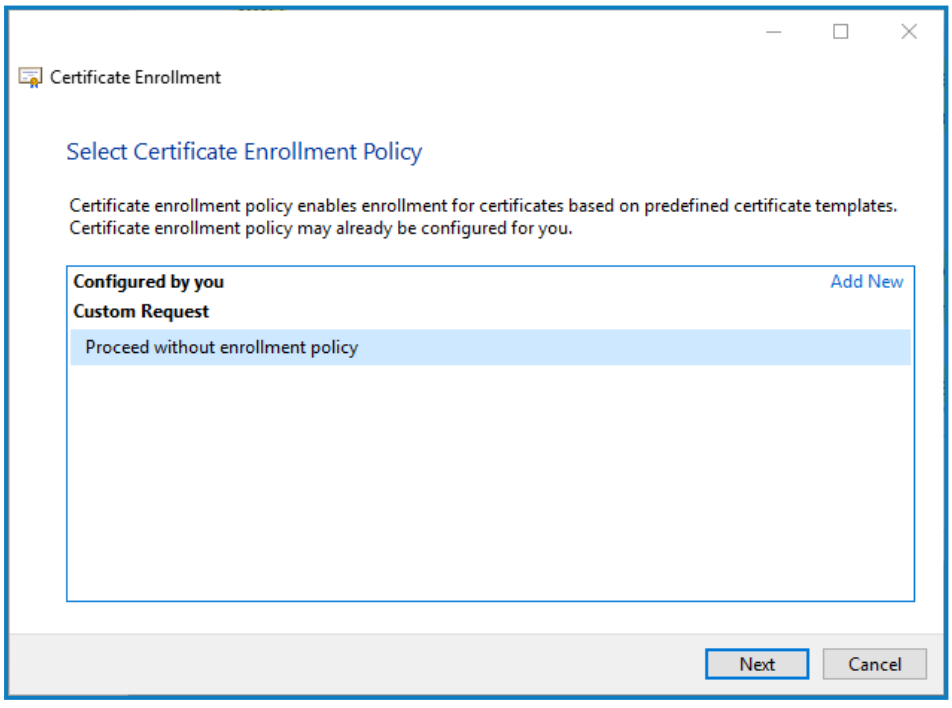
Um eine Offline-Zertifikatanforderung zu erstellen, führen Sie für jedes Zertifikat dieses Verfahren aus:

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.

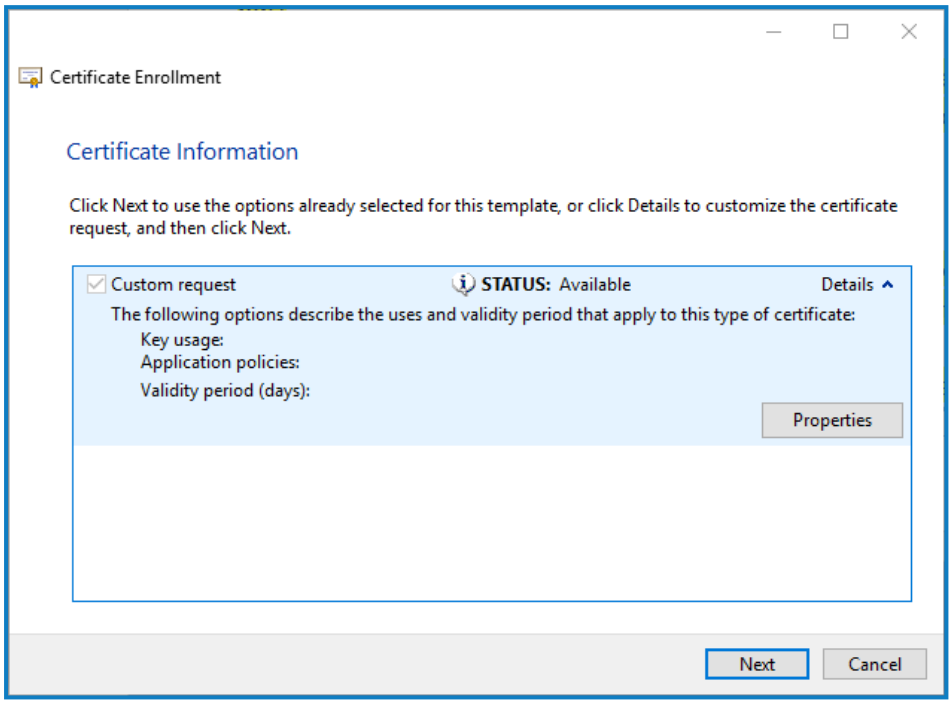


3. Klicken Sie auf **Weiter**.



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: • .NET Core Windows Server Hosting 3.1.11 oder höhere Versionen von 3.1 https://dotnet.microsoft.com/download/dotnet/3.1 – Wählen Sie die benötigte Version aus. Wählen Sie unter **ASP.NET Core Runtime** die Option **Hosting-Paket** aus. • .NET Core Windows Desktop Runtime 3.1.11 oder höhere Versionen von 3.1 https://dotnet.microsoft.com/download/dotnet/3.1 – Wählen Sie die benötigte Version aus. Wählen Sie unter **.NET Desktop Runtime** den benötigten Download aus. • Visual C++ Redistributable 2012 (x64) https://download.microsoft.com/download/1/6/B/16B06F60-3B20-4FF2-B699-5E9B7962F9AE/VSU_4/vcredist_x64.exe • .NET Framework 4.7.2 https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net472-web-installer Unter Windows Server 2019 wird dies standardmäßig installiert. Sie müssen .NET Framework nur installieren, wenn Sie Windows Server 2016 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:
	`start-process "C:\temp\dotnet-hosting-3.1.11-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-3.1.11-win-x64.exe" /q -wait`
	`start-process "C:\temp\vcredist_x64.exe" /q -wait`
	`start-process "C:\temp\NDP472-KB4054531-Web.exe" /q -wait`
	Für Windows Server 2019:
	`start-process "C:\temp\dotnet-hosting-3.1.11-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-3.1.11-win-x64.exe" /q -wait`
	`start-process "C:\temp\vcredist_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

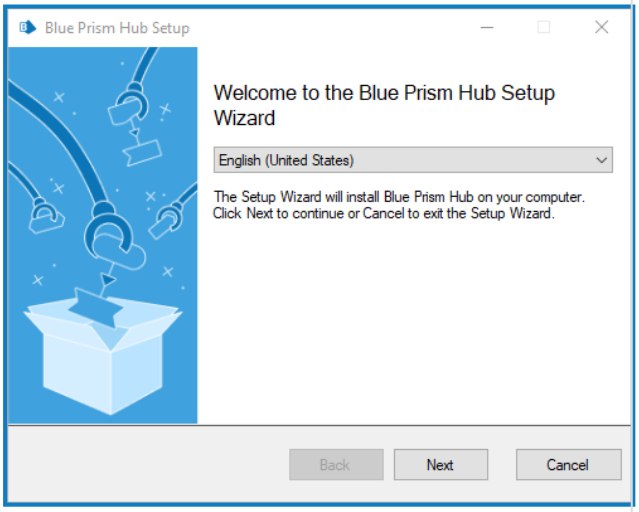
Bevor Sie Blue Prism Hub installieren:

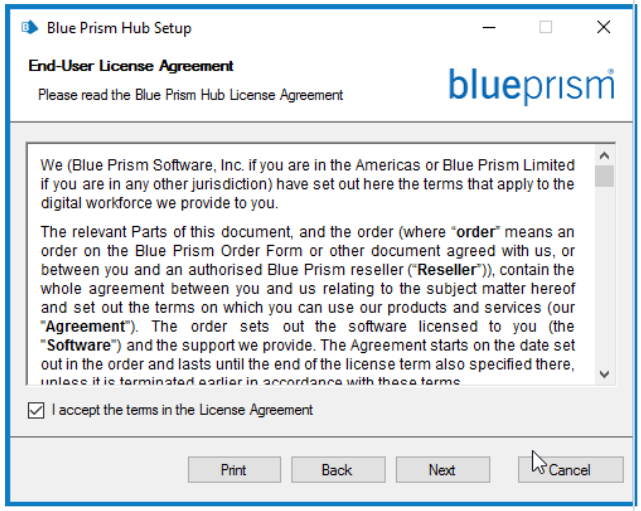
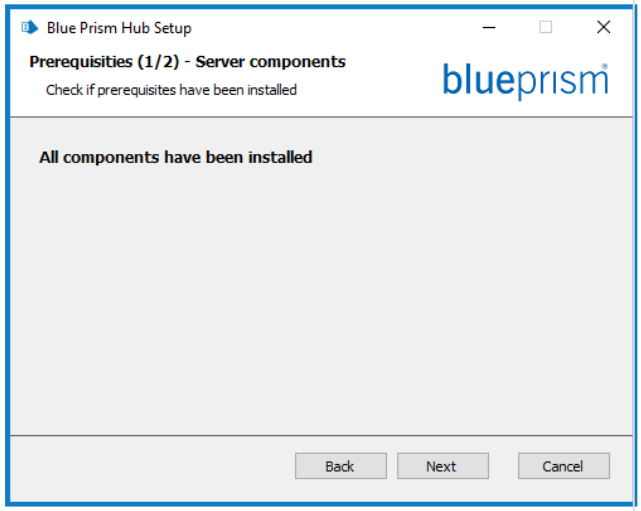
- Wenn Sie ALM, Decision oder Interact gekauft haben, benötigen Sie während der Installation von Hub Ihre Kunden-ID. Diese finden Sie in der E-Mail, die Ihnen beim Kauf von ALM, Decision oder Interact zugesandt wurde.
- Wenn Sie das Blue Prism Decision Plug-in in Hub verwenden möchten, müssen Sie den 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.

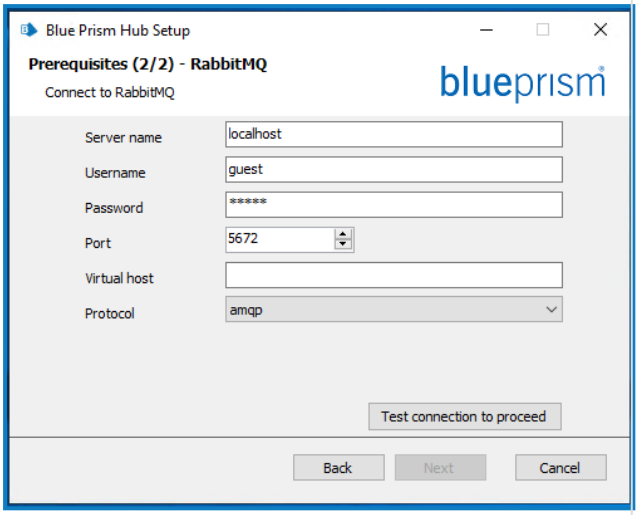
Sehen Sie sich das Blue Prism Hub Installationsvideo für die Installation und Konfiguration von Hub an.

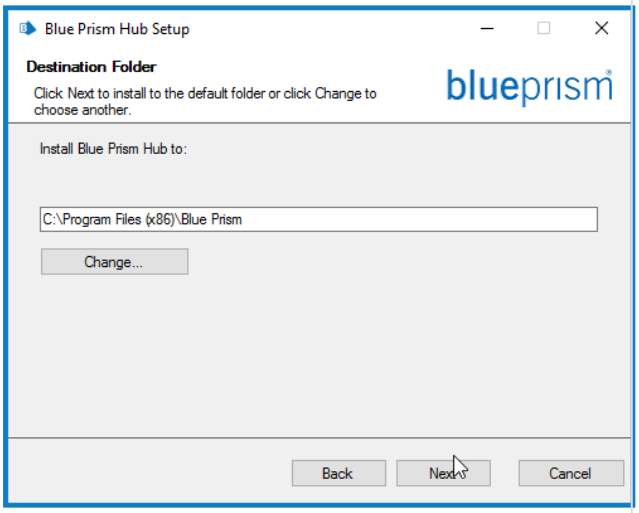
Die folgenden Schritte beschreiben den Prozess zur Installation der Blue Prism Hub Software. Dazu gehören Authentication Server, Hub und andere zugehörige Dienste. Der Installationsprozess wird alle neuen Datenbanken erstellen, die erforderlich sind.

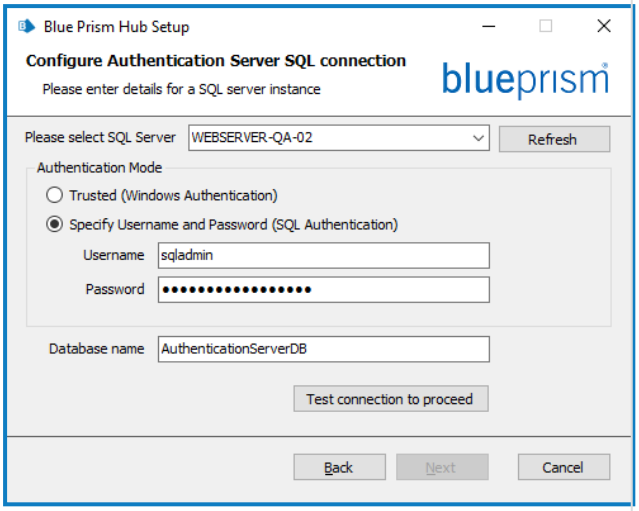
Laden Sie das Blue Prism Hub Installationsprogramm aus dem Blue Prism Portal herunter, führen Sie es aus und gehen Sie wie folgt vor. Das Installationsprogramm muss mit Administratorrechten ausgeführt werden.

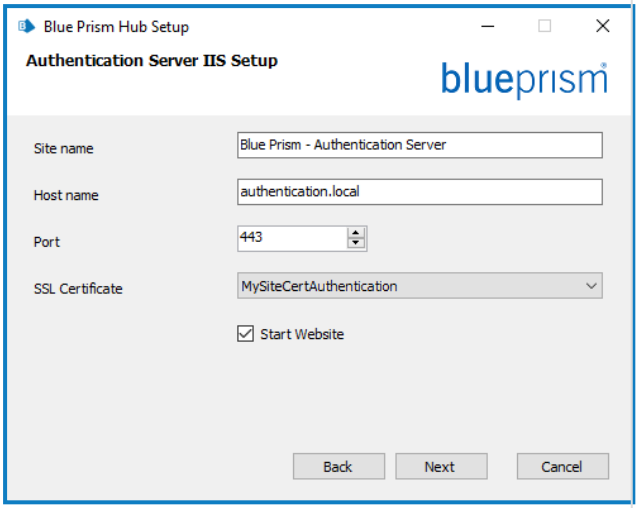
Schritt	Seite des Installationsprogramms	Details
1		**Willkommen** Falls erforderlich, wählen Sie für das Installationsprogramm eine andere Sprache in der Dropdown-Liste aus. Die Standardsprache ist Englisch (USA). Klicken Sie auf **Weiter**.

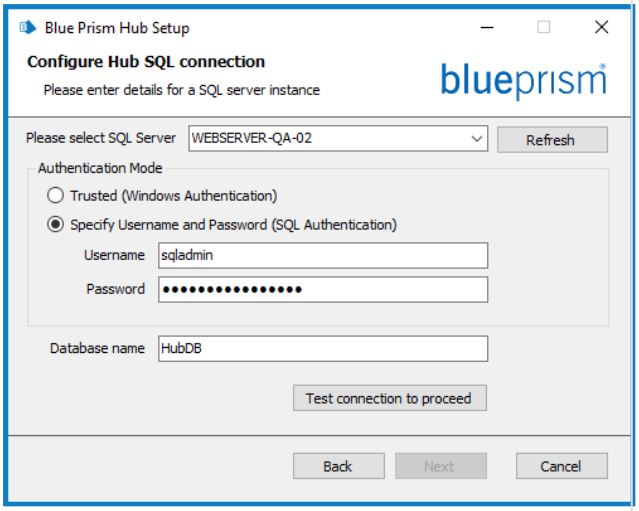
Schritt	Seite des Installationsprogramms	Details
2		**Lizenzvereinbarung** Lesen Sie die Endbenutzer-Lizenzvereinbarung. Wenn Sie den Bedingungen zustimmen, aktivieren Sie das Kontrollkästchen.
3		**Voraussetzungen 1 – Serverkomponenten** Das Installationsprogramm überprüft, ob die Voraussetzungen installiert 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.

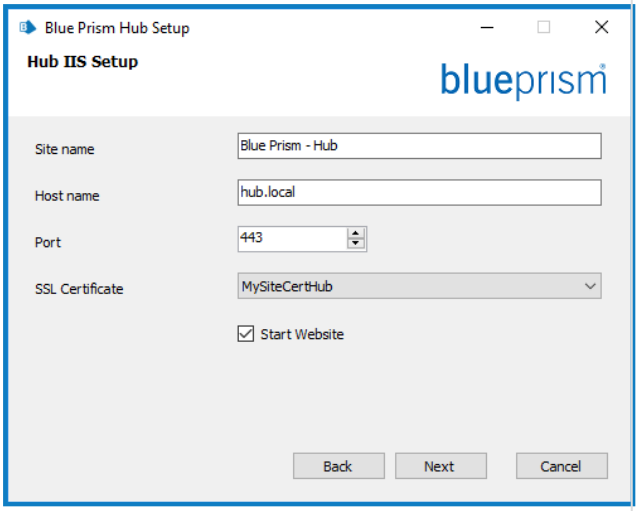
Schritt	Seite des Installationsprogramms	Details
4		**Voraussetzungen 2 – RabbitMQ** Geben Sie den Servernamen oder die IP-Adresse des Message-Broker-Servers und die Anmeldeinformationen des von Ihnen erstellten Benutzers ein. Der Standard-Port für Nachrichtenwarteschlangen ist 5672. Dies sollte nur 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.

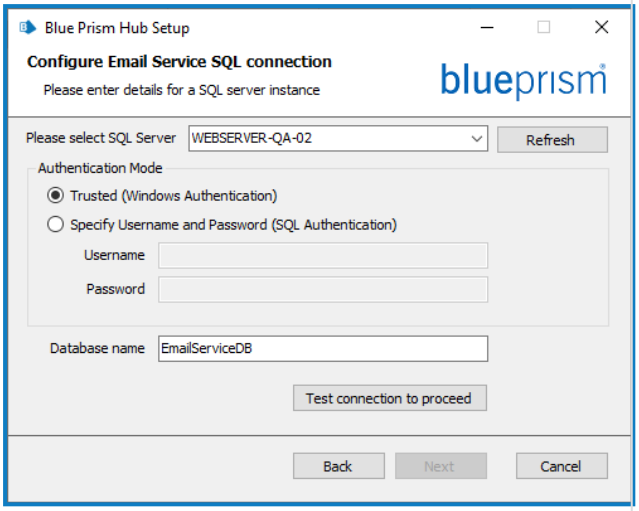
Schritt	Seite des Installationsprogramms	Details
		Wenn Sie AMQPS verwenden, müssen Sie den Blue Prism IIS-Anwendungspools die volle Kontrolle über das RabbitMQ-Zertifikat geben. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 67. Klicken Sie auf **Verbindung testen**, 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 67.
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.

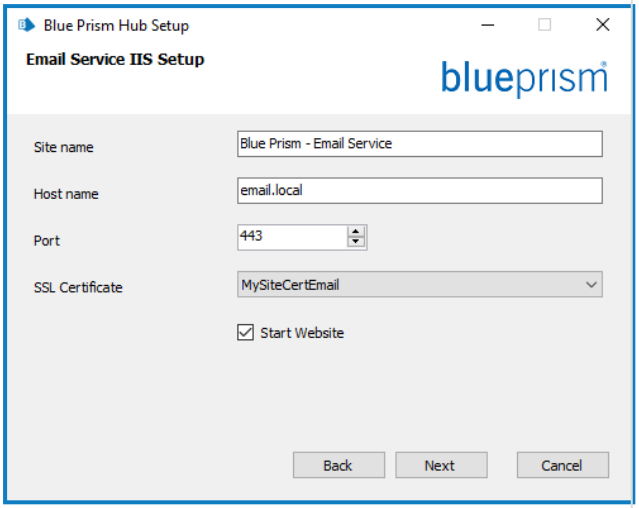
Schritt	Seite des Installationsprogramms	Details
6		**Authentication Server SQL-Verbindung** Einstellungen für die Authentication Server Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

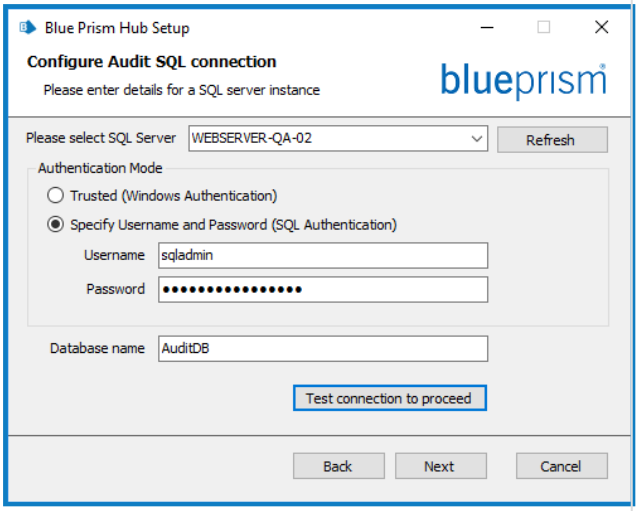
Schritt	Seite des Installationsprogramms	Details
7		**Authentication Server IIS-Einrichtung** Konfigurieren Sie IIS für die Authentication Server Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen 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.

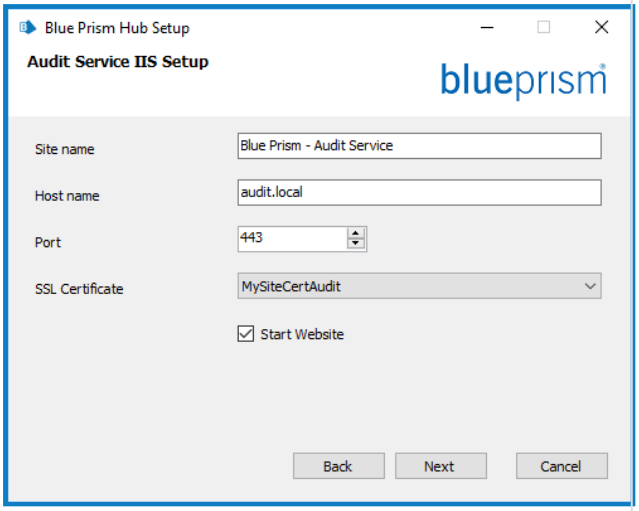
Schritt	Seite des Installationsprogramms	Details
8		**Hub SQL-Verbindung** Einstellungen für die Hub Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

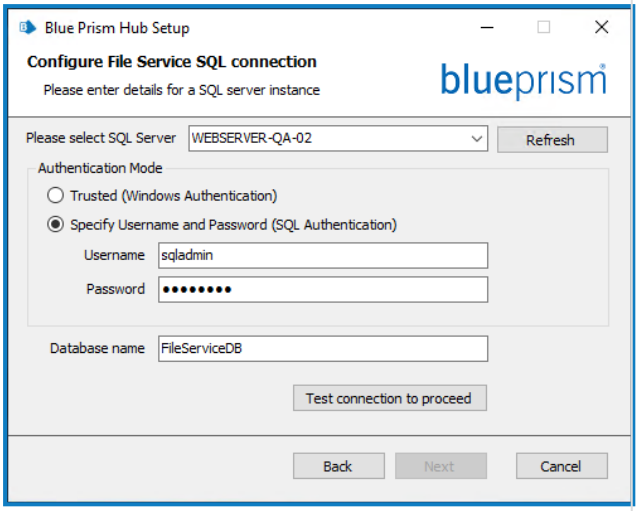
Schritt	Seite des Installationsprogramms	Details
9		**Hub IIS-Setup** Konfigurieren Sie die Hub Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der Auswahl eines Hostnamens 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.

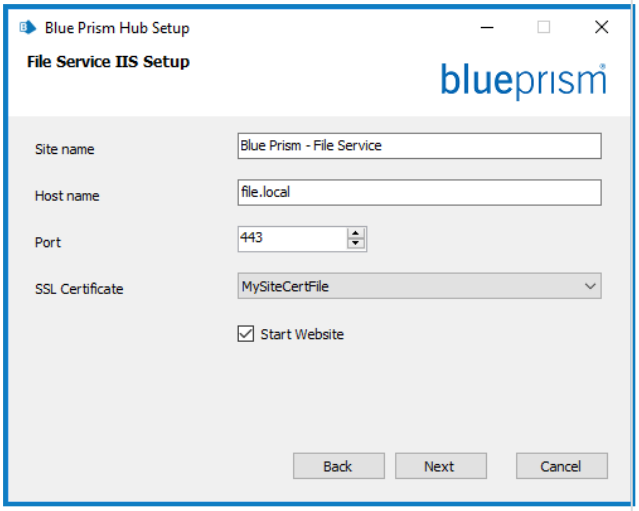
Schritt	Seite des Installationsprogramms	Details
10		**Email Service SQL-Verbindung** Einstellungen für die Email Service Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

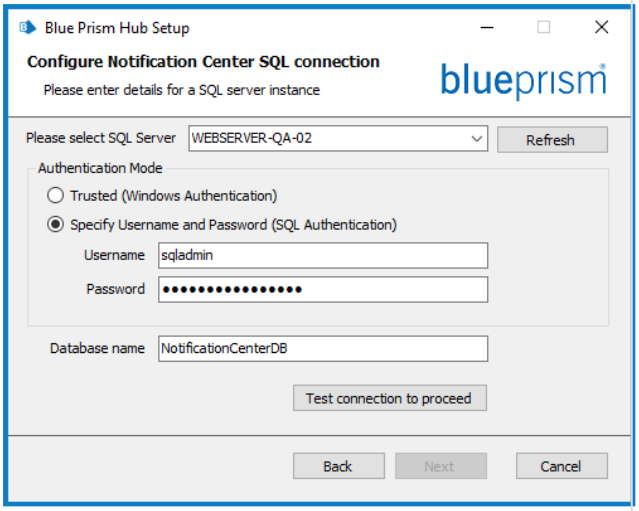
Schritt	Seite des Installationsprogramms	Details
11		**Email Service IIS-Einrichtung** Konfigurieren Sie die Email Service-Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie 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.

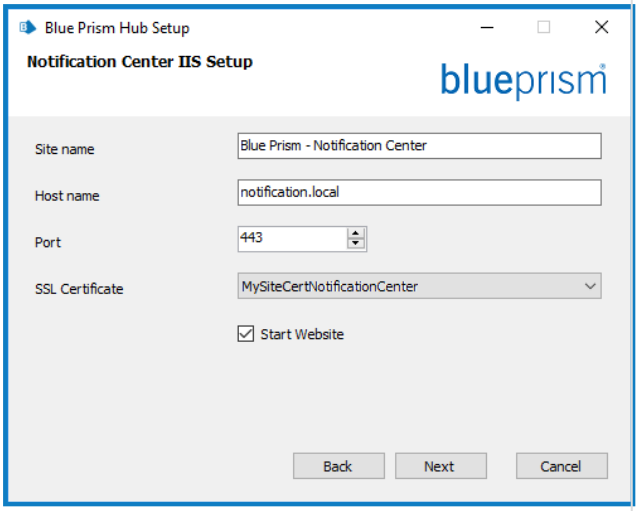
Schritt	Seite des Installationsprogramms	Details
12		**Audit SQL-Verbindung konfigurieren** Einstellungen für die Audit Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

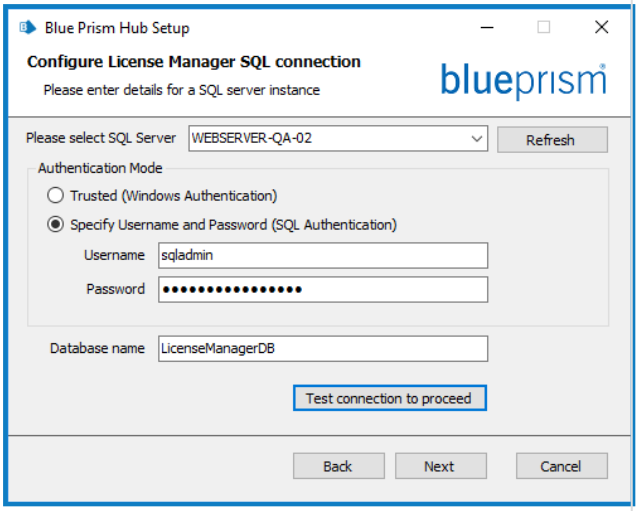
Schritt	Seite des Installationsprogramms	Details
13		**Audit Service IIS-Einrichtung** Konfigurieren Sie die Audit Service Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie 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.

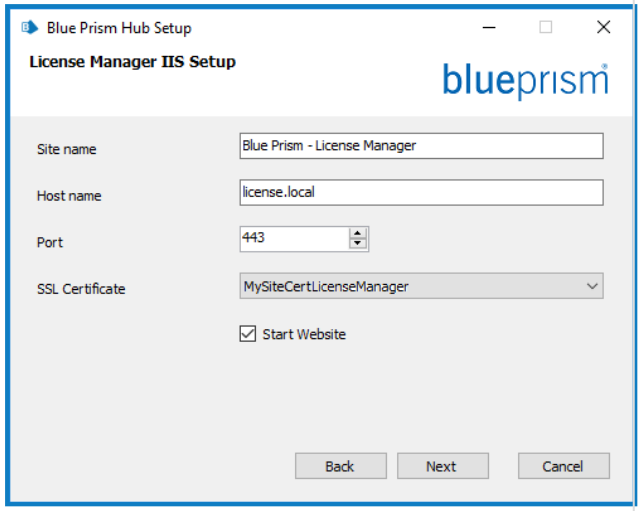
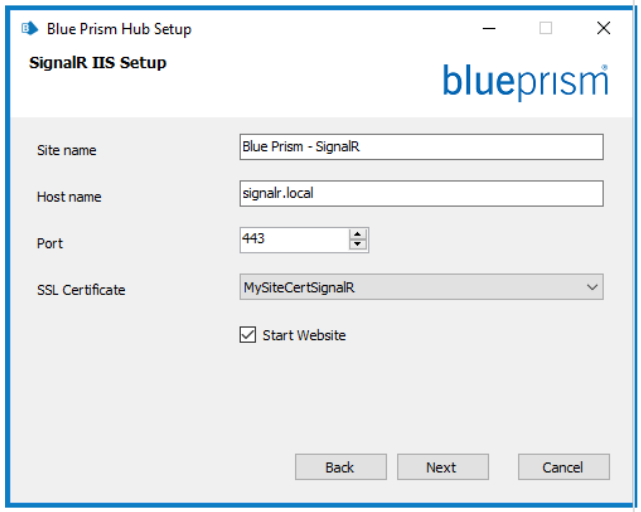
Schritt	Seite des Installationsprogramms	Details
14		**File Service SQL-Verbindung konfigurieren** Einstellungen für die File Service Datenbank konfigurieren durch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

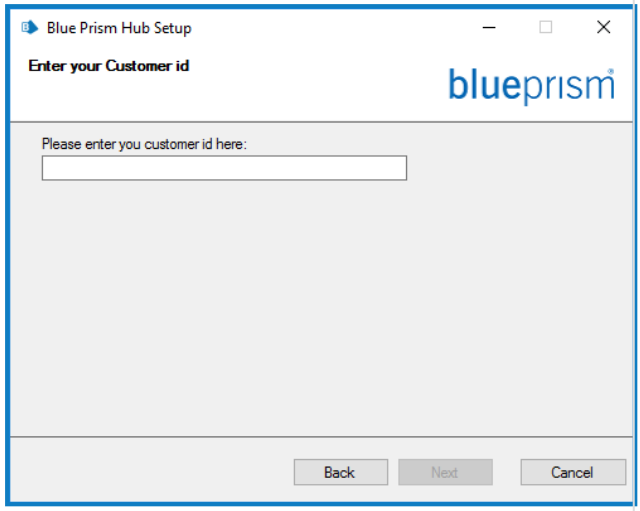
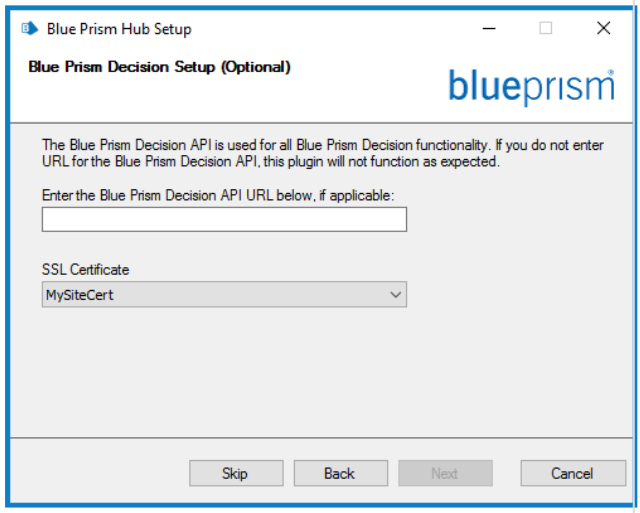
Schritt	Seite des Installationsprogramms	Details
15		**File Service IIS-Setup** Konfigurieren Sie die File Service Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, dass Sie bei der 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.

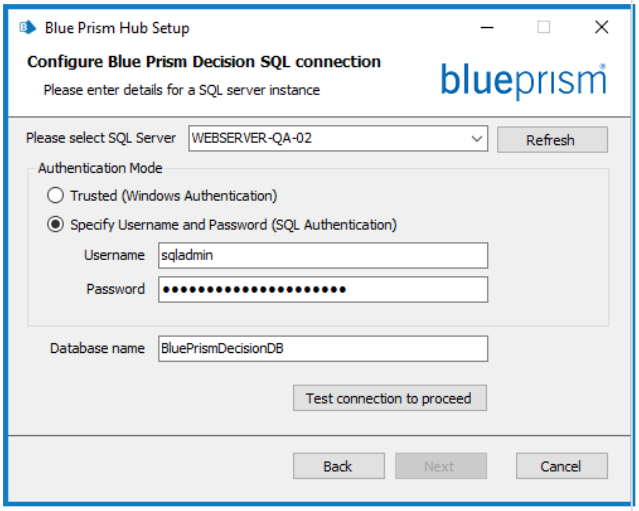
Schritt	Seite des Installationsprogramms	Details
16		**Notification Center SQL-Verbindung** Einstellungen für die Notification Center Datenbank konfigurierendurch Angabe des SQL Server-Hostnamens oder der IP-Adresse und der Anmeldedaten für das Konto zur Erstellung der Datenbank: • Wenn **Windows-Authentifizierung** ausgewählt ist, muss das Konto über die entsprechenden Berechtigungen verfügen. Weitere Informationen erhalten Sie unter mit Windows-Authentifizierung installieren auf Seite 54. • 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 67 weitere Details.

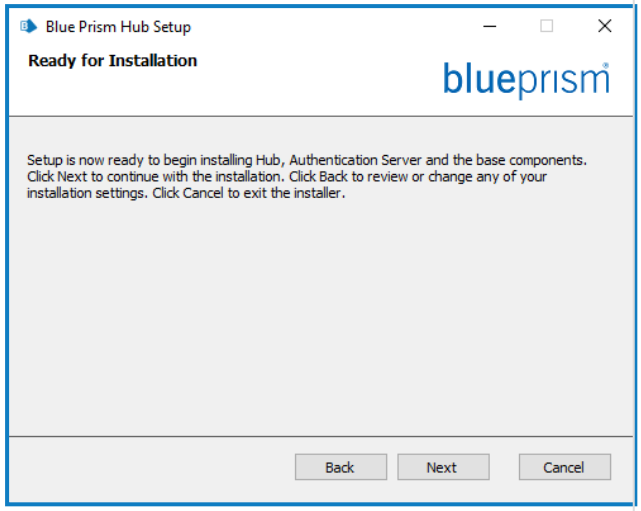
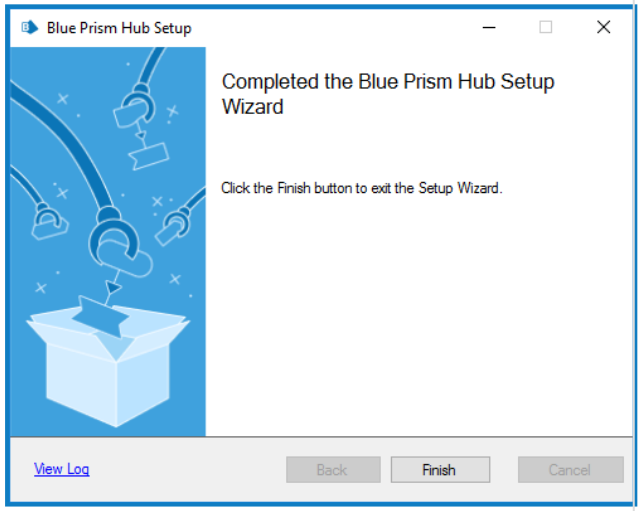
Schritt	Seite des Installationsprogramms	Details
17		**Notification Center IIS-Setup** Konfigurieren Sie die Notification Center Website. Erforderliche Schritte: • Geben Sie den Namen einer Site ein. • Geben Sie einen Hostnamen ein – dieser wird als URL für die Website verwendet. Stellen Sie sicher, 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 54. • 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 67 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 67.
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 54. • 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 67 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 67.

Anwendungspool-Recycling konfigurieren

Die Anwendungspools für Authentication Server und Hub sollten so eingestellt werden, dass sie nacheinander recycelt werden, wobei Authentication Server zuerst recycelt wird. Sie sollten die Anwendungspools so konfigurieren, dass sie zu einem bestimmten Zeitpunkt außerhalb der Arbeitszeit oder in Zeiten geringer Nutzung recycelt werden. Der Anwendungspool für Authentication Server sollte so eingestellt werden, dass er mindestens 10 Minuten vor dem Hub Anwendungspool recycelt wird.

Es gibt verschiedene Methoden, mit denen Sie die Recycling-Informationen einstellen können. Im Folgenden wird der Internet Information Services (IIS) Manager verwendet:

1. Klicken Sie im IIS-Manager (Internet Information Services) mit der rechten Maustaste auf den betroffenen Anwendungspool und wählen Sie **Recyceln ...**.
2. Deaktivieren Sie die Option **Regelmäßige Zeitintervalle (in Minuten)**.
3. Wählen Sie die Option **Spezifische Zeit(en)** und geben Sie eine Zeit in das Feld ein:
   - Stellen Sie für den Blue Prism – Hub Anwendungspool eine bestimmte Zeit außerhalb der Arbeitszeit oder in Zeiträumen mit geringer Nutzung ein.
   - Stellen Sie für den Blue Prism – Authentication Server Anwendungspool ein, dass er mindestens 10 Minuten vor dem Hub Anwendungspool recycelt wird.
4. Klicken Sie auf **Weiter** und dann 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 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.

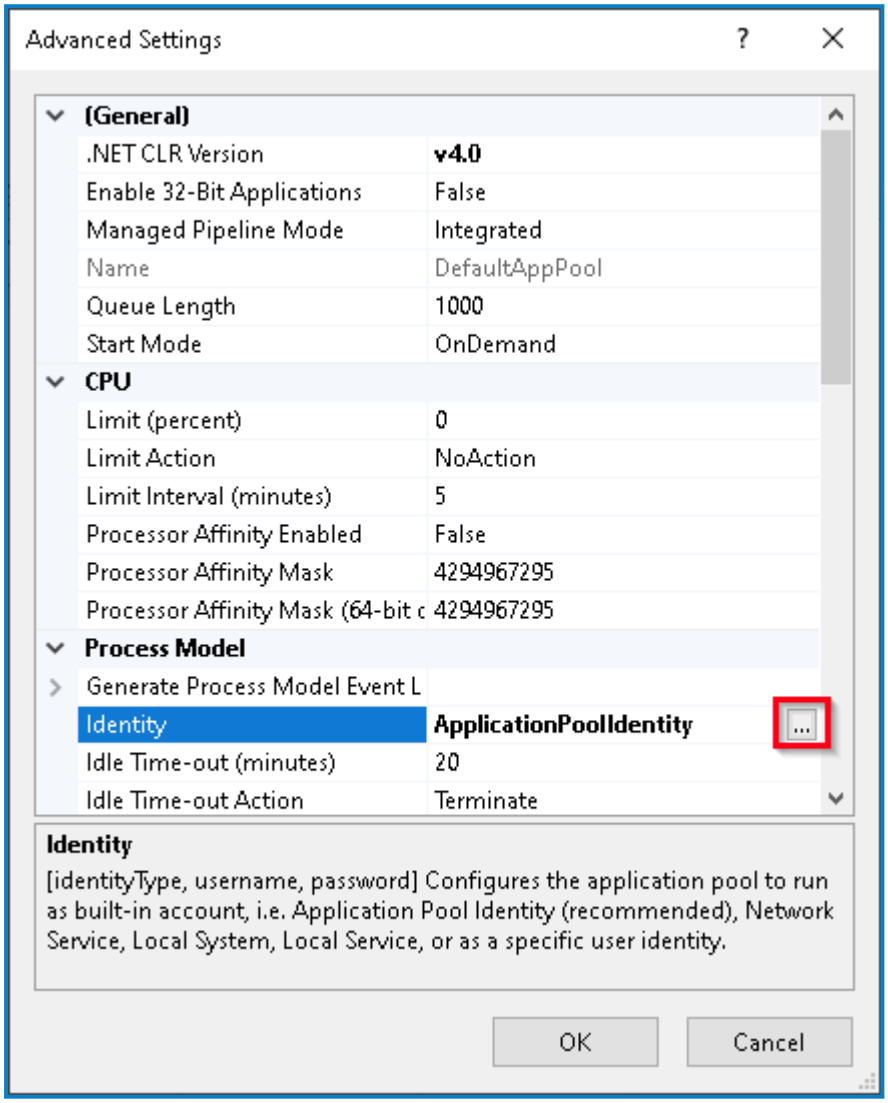
3. Überprüfen Sie die Werte in der Spalte **Identität**.

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

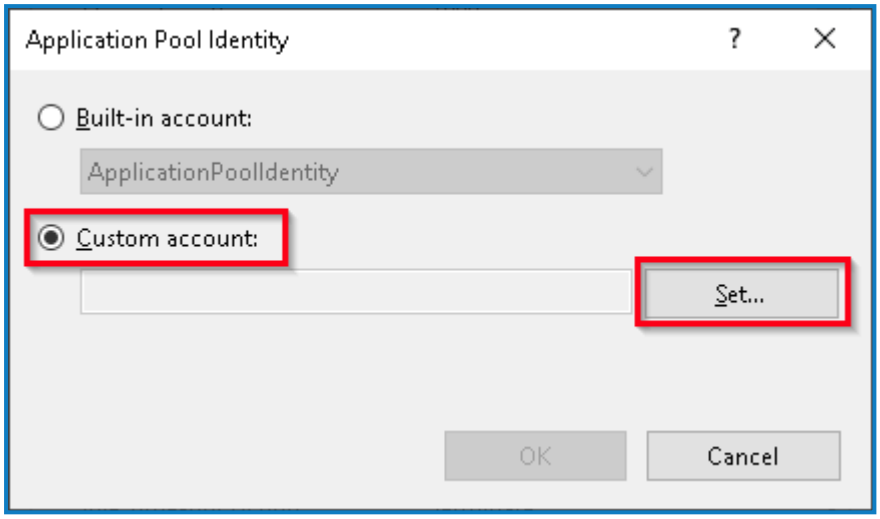
4. Bei Anwendungspools, bei denen *ApplicationPoolIdentity* in der Spalte **Identität** steht, klicken Sie mit der rechten Maustaste auf die Zeile und wählen **Erweiterte Einstellungen...** aus.

   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.

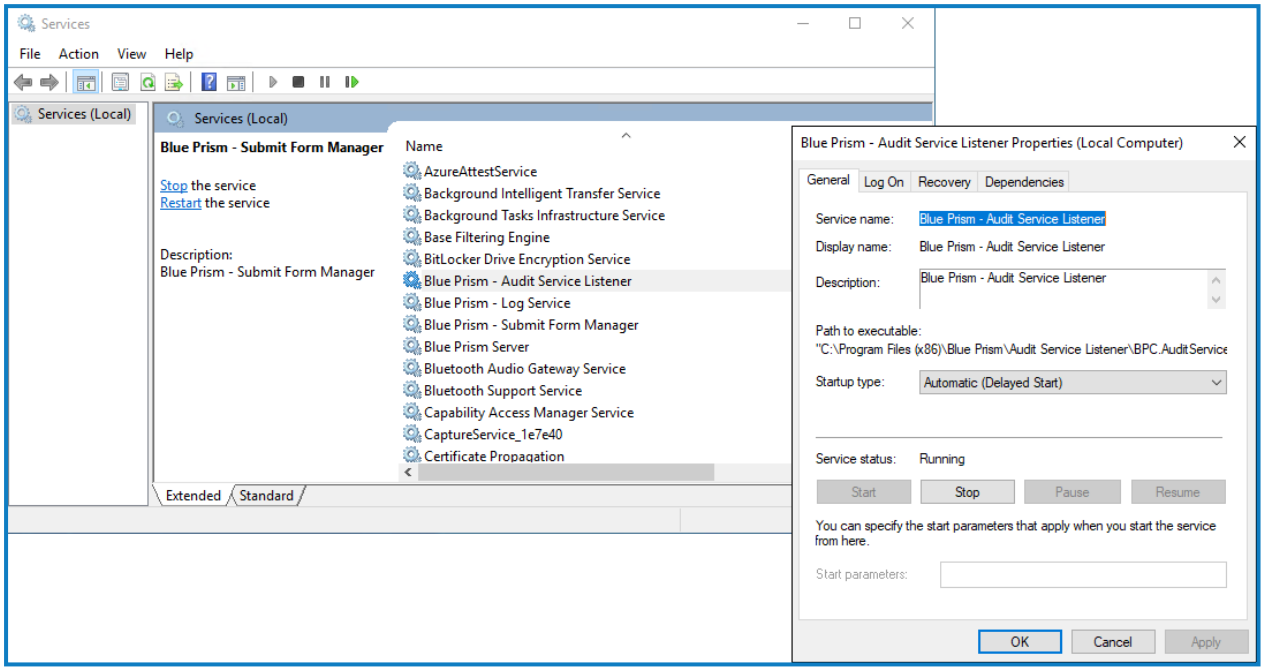
Zuweisen eines Windows-Dienstkontos zu einem Dienst

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

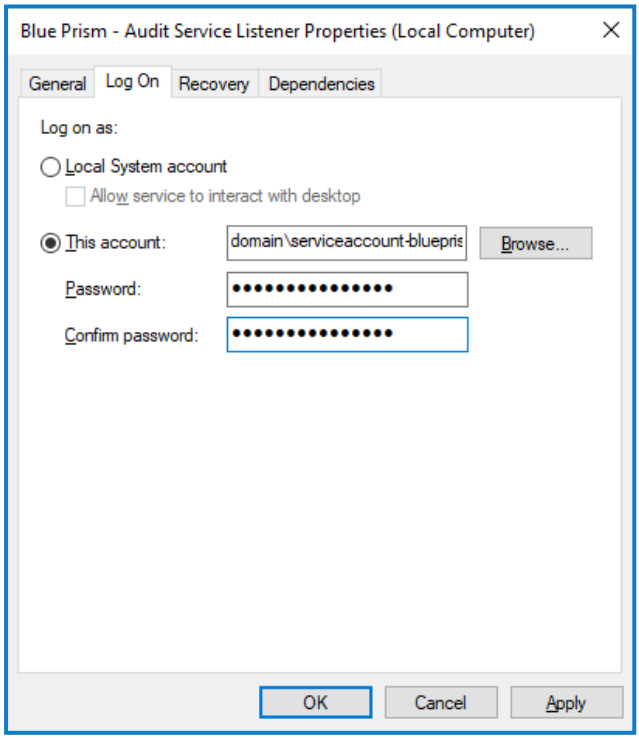
- Blue Prism – Audit-Dienst-Listener
- Blue Prism – Log Service

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

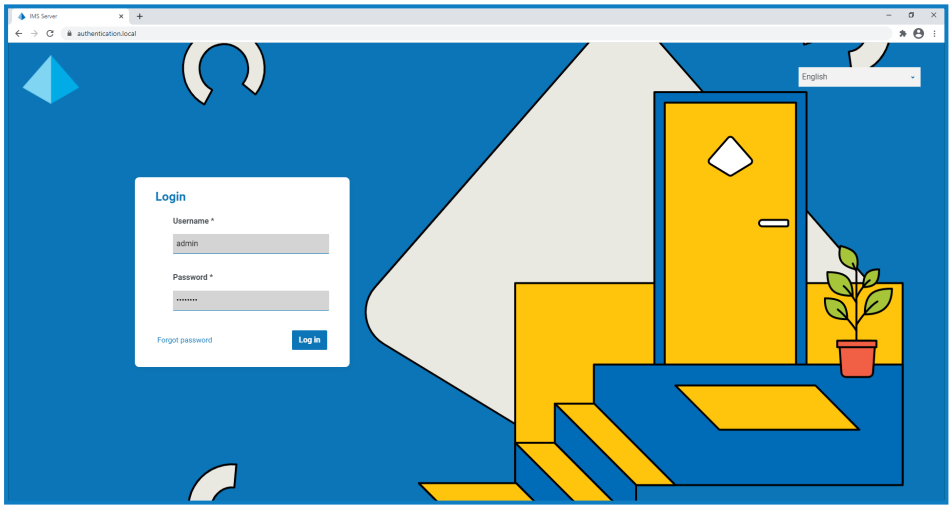
Wenn Sie Blue Prism Interact verwenden möchten, installieren Sie Interact, bevor Sie diese Konfiguration ausführen. Mehr erfahren Sie im Interact Installationshandbuch.

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

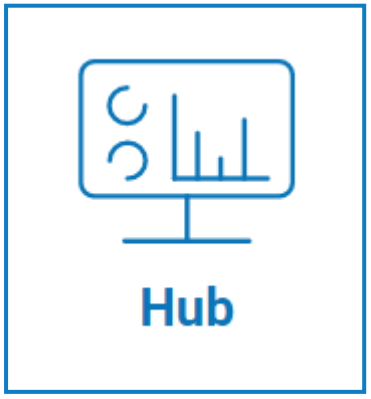
Wenn Sie die Anmeldeseite für Authentication Server öffnen, wendet ihr Webbrowser automatisch Lokalisierungseinstellungen an. Die Anmeldeseite und Hub werden in der Sprache angezeigt, die am besten zu den im Browser festgelegten Spracheinstellungen passt. Wenn die in den Einstellungen Ihres Browsers 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

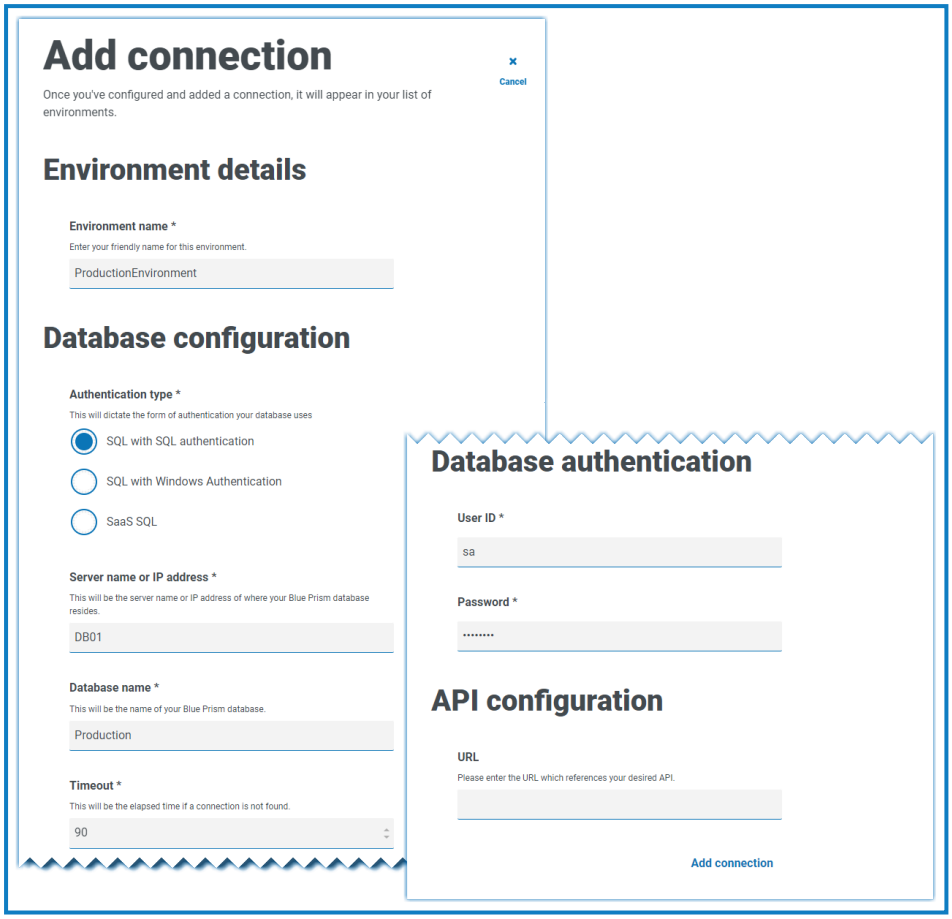
⚠ Wenn Sie Ihre Umgebung so installiert haben, dass Windows-Authentifizierung verwendet wird, müssen Sie die Anwendungspools und -dienste zur Verwendung von Windows-Konten zuweisen, bevor Sie eine Umgebung in Hub erstellen. Wenn dies nicht der Fall ist, können Leistungsprobleme auftreten, z. B. werden 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 54.

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:



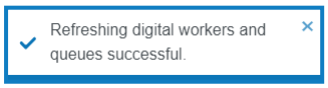
Der Timeout-Wert ist in Sekunden angegeben.

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 67 weitere Informationen.

Einen Administrator erstellen

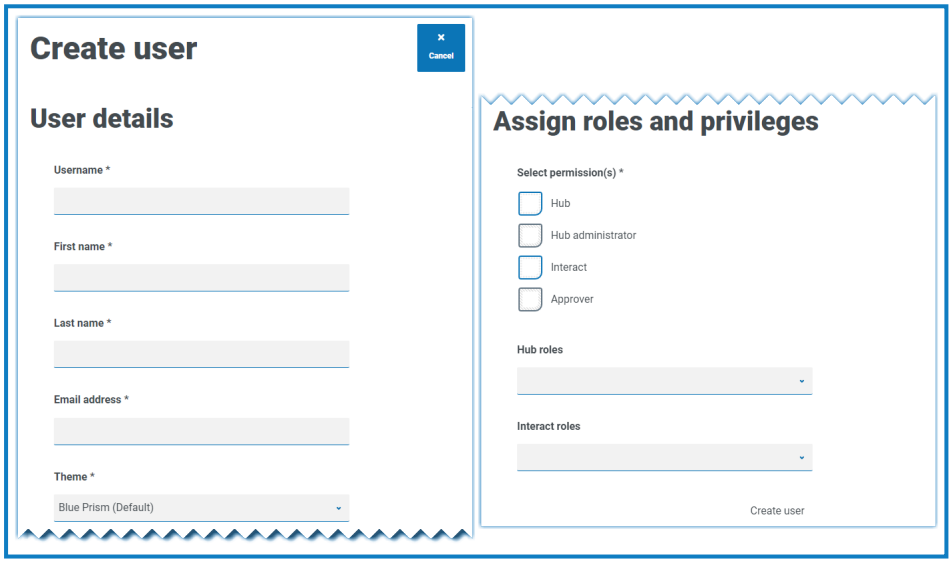
Sie müssen ein Administratorkonto mit gültigen Informationen erstellen, um die Hub Konfiguration abzuschließen. Sie sollten das generische Administratorkonto nicht verwenden, um die Konfiguration abzuschließen. Der Grund:

- 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 60 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.

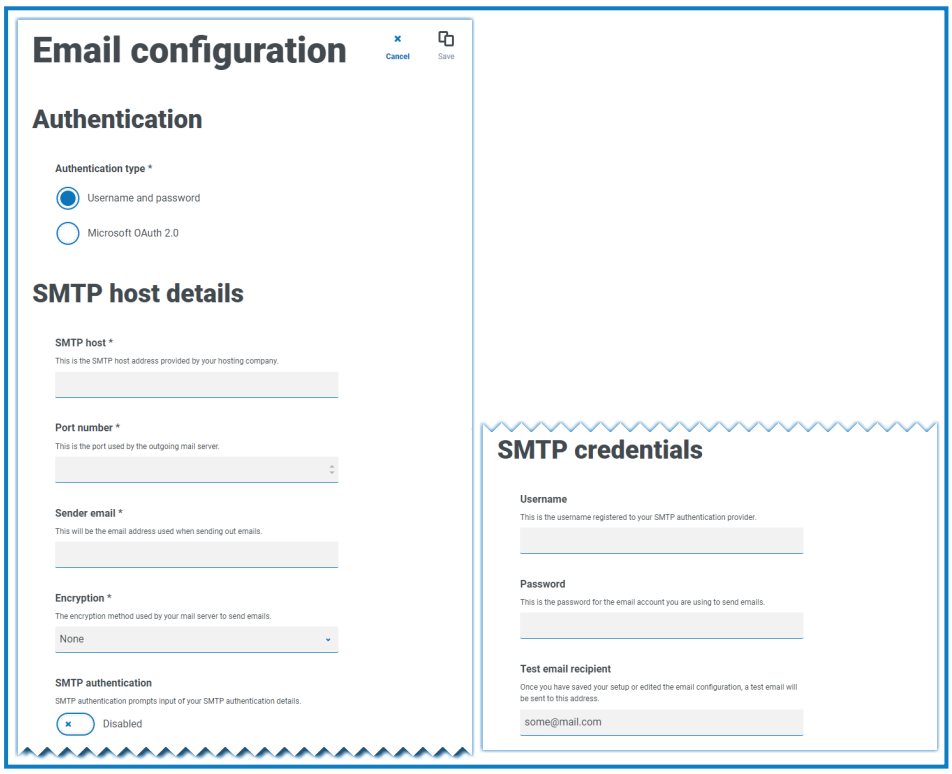
> Wenn Sie Microsoft OAuth 2.0 verwenden, muss die Berechtigung „Mail.Send“ in Azure Active Directory aktiviert sein. Dies finden Sie auf der Registerkarte „API-Berechtigung“ unter den Anwendungseigenschaften in Azure Active Directory. Weitere Informationen finden Sie unter Fehlerbehebung einer Hub Installation auf Seite 67.

So konfigurieren Sie E-Mail-Einstellungen:

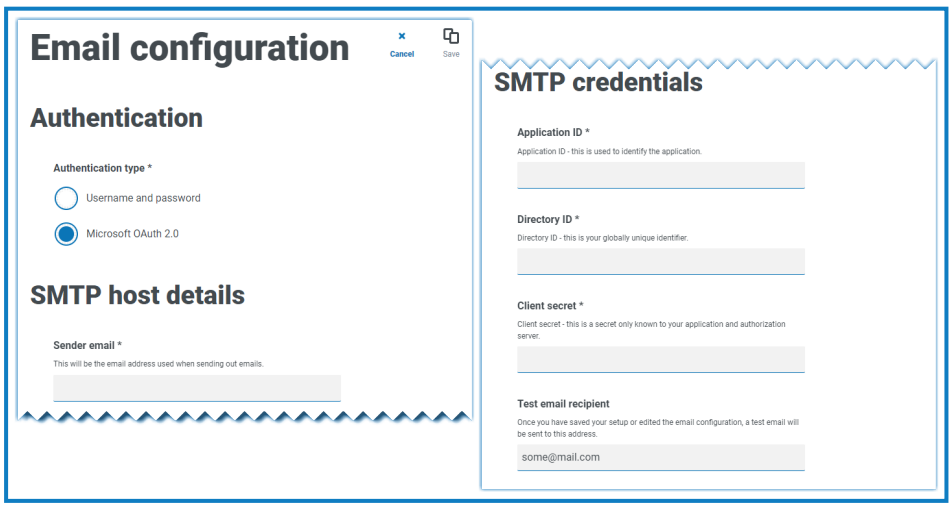
1. Klicken Sie auf Ihr Profilsymbol, um die Seite „Einstellungen“ zu öffnen. Klicken Sie dann auf **E-Mail-Konfiguration**.
2. Klicken Sie auf **Bearbeiten**.
3. Wählen Sie den Authentifizierungstyp aus, den Sie verwenden möchten.

   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 67 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.

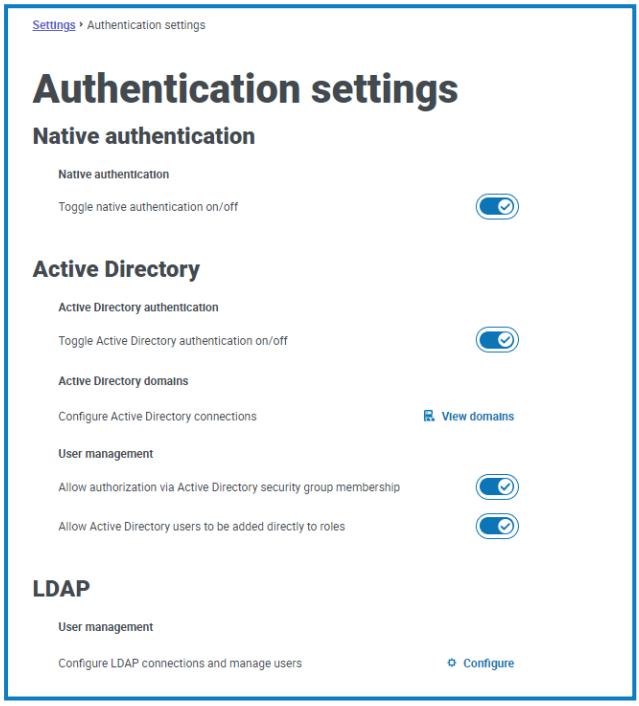
Authentifizierungseinstellungen

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.
   - **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 die native Authentifizierung, wenn mindestens ein Hub Administrator im System vorhanden ist, der sich über LDAP- oder Active Directory-Authentifizierung anmelden kann.
- Deaktivieren Sie die native und Active Directory-Authentifizierung, wenn mindestens ein Hub Administrator im System vorhanden ist, der sich über LDAP anmelden kann.
- Wenn es keine LDAP-Benutzer im System gibt, muss entweder die native oder Active Directory-Authentifizierung aktiviert sein, und mindestens ein Hub Administrator, der für die Verwendung des aktivierten Authentifizierungstyps konfiguriert ist, muss im System beibehalten werden. Eine Warnung wird angezeigt, wenn kein Administrator für die Anmeldung über den/die aktuell aktivierten Authentifizierungstyp(en) konfiguriert ist.

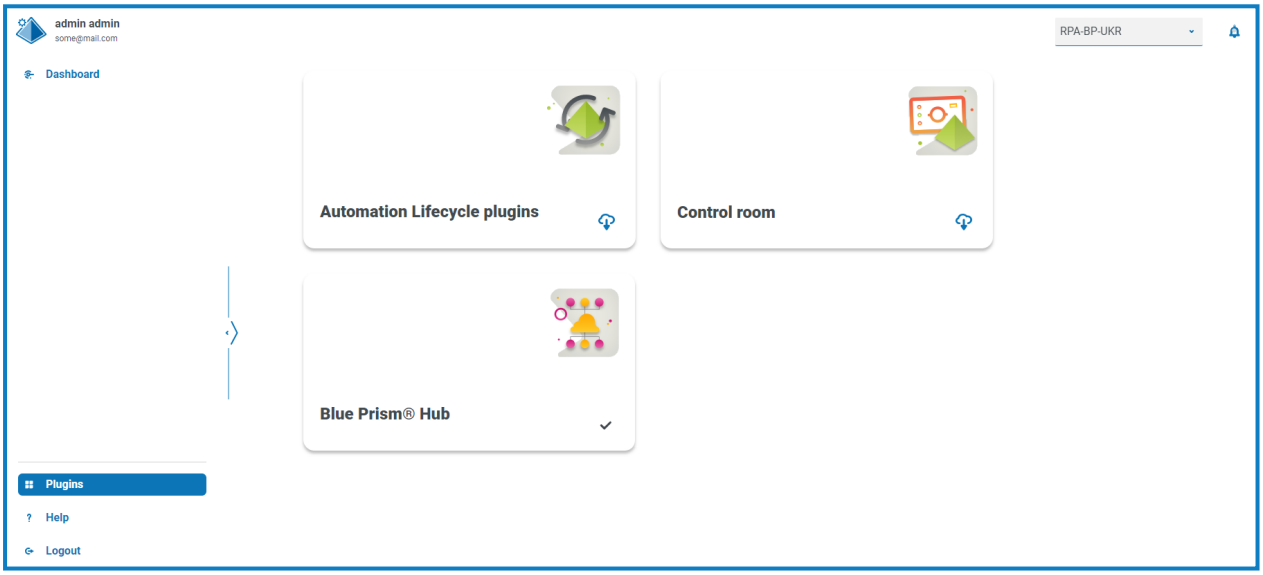
Weitere Informationen zur Konfiguration von Authentifizierungseinstellungen finden Sie im Hub Administratorhandbuch.

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.

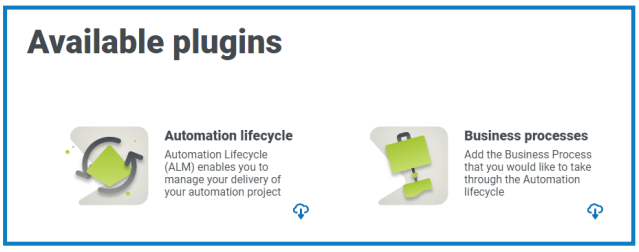
Diesen Installationsschritt können Sie auch im Geschäftsprozess-Plug-in-Installationsvideo sehen.

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.

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 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.

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.
- 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 9.

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:

```
iis apppool\Blue Prism - Audit Service;
iis apppool\Blue Prism - Authentication Server;
iis apppool\Blue Prism - Email Service;
iis apppool\Blue Prism - File Service;
iis apppool\Blue Prism - Hub;
iis apppool\Blue Prism - License Manager;
iis apppool\Blue Prism - Notification Center;
iis apppool\Blue Prism - SignalR;
```

> 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.

Wenn Sie auch Interact installieren, müssen Sie dies auch für die Anwendungspools tun, die während der Interact Installation erstellt wurden. Mehr erfahren Sie im Interact Installationshandbuch.

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

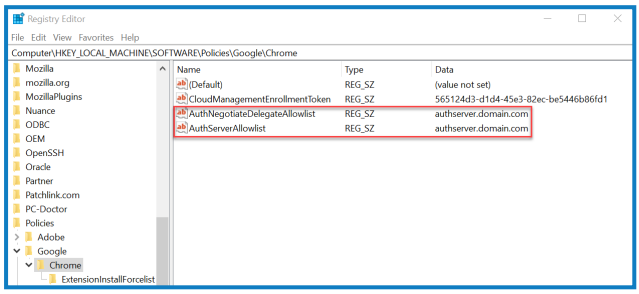
Falls sich Active Directory-Benutzer nach der Installation nicht bei Blue Prism Hub anmelden können, überprüfen Sie, ob Sie die unterstützten Webbrowser für die integrierte Windows-Authentifizierung konfiguriert haben, damit die derzeit angemeldeten Benutzer vom Client-Computer abgerufen werden können.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

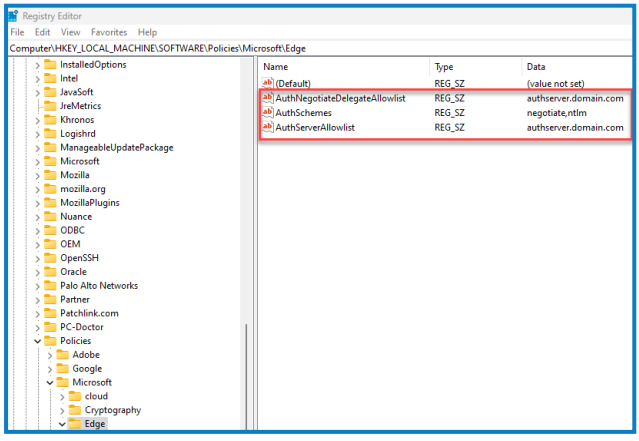


Microsoft Edge konfigurieren

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.

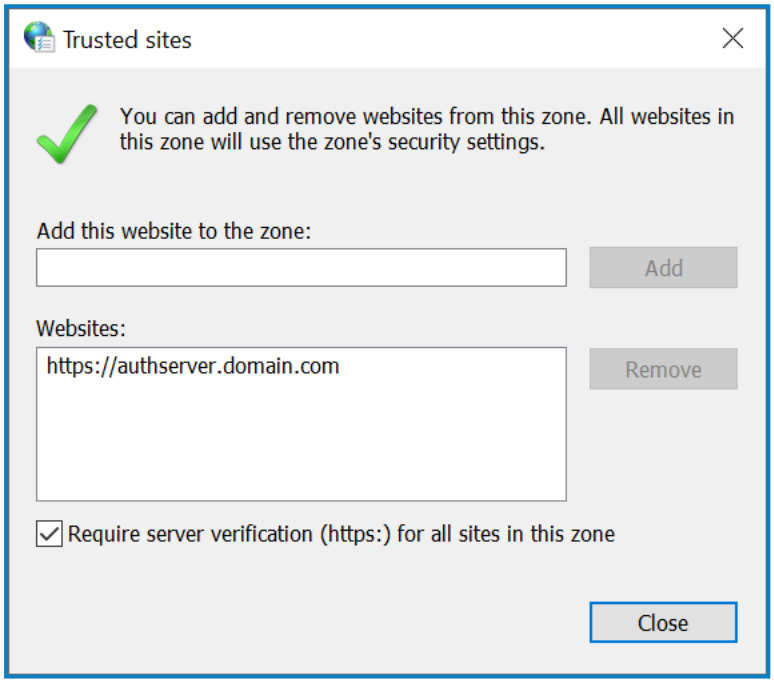
> Dieser Zeichenfolgenwert ist nicht erforderlich, wenn in Ihrer Organisation nur die Kerberos-Authentifizierung eingerichtet ist. Unten finden Sie weitere Informationen.



Alternativ können Sie die folgenden Schritte für Microsoft Edge ausführen:

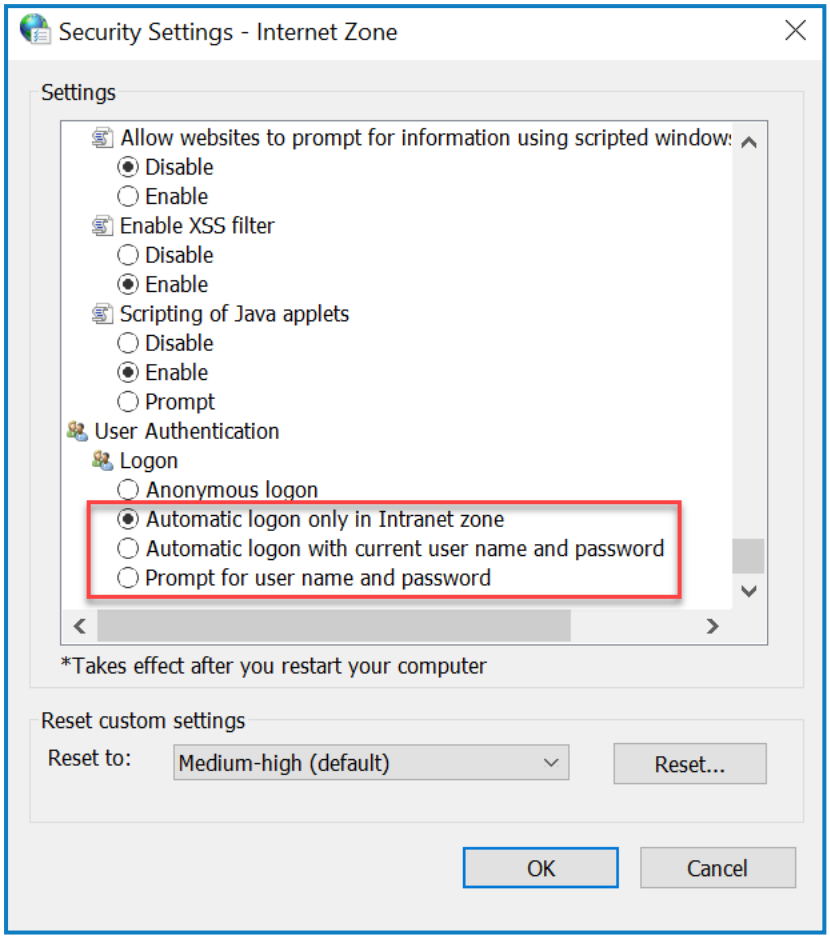
1. Schließen Sie alle offenen Instanzen von Edge.
2. Navigieren Sie zu **Systemsteuerung** > **Netzwerk und Internet** > **Internetoptionen**.
3. Wählen Sie auf der Registerkarte „Erweitert“ unter „Sicherheit“ die Option **Integrierte Windows-Authentifizierung aktivieren**.
4. Klicken Sie auf der Registerkarte „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.

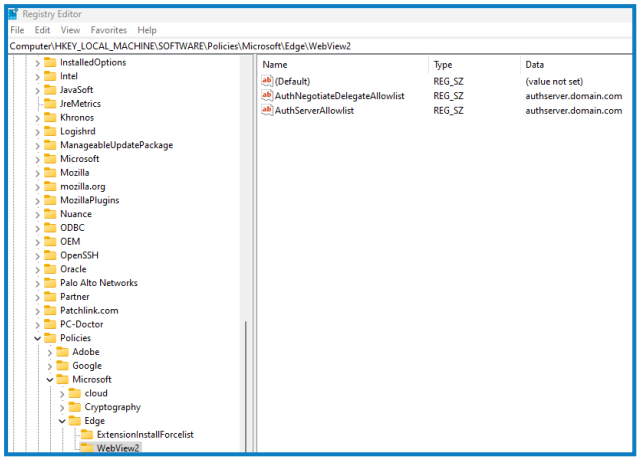
Microsoft Edge WebView2-Registrierungsschlüssel hinzufügen

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 auf Seite 16.
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.

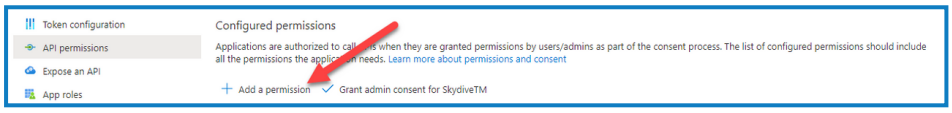
Der Webserver muss nach dem Start der RabbitMQ-Dienste gestartet werden. Wenn die Webserver-Dienste starten, bevor der RabbitMQ-Dienst bereit ist, dann führt das beim Öffnen der SMTP-Einstellungen in Hub zu einer Fehlermeldung.

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

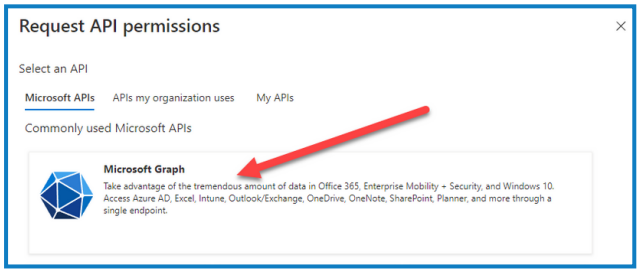
Wenn Sie beim Speichern einer E-Mail-Konfiguration mit OAuth 2.0 einen Fehler erhalten, überprüfen Sie, ob die Berechtigung Mail.Send für die Anwendung in Azure Active Directory konfiguriert ist.

So fügen Sie die Berechtigung Mail.Send hinzu:

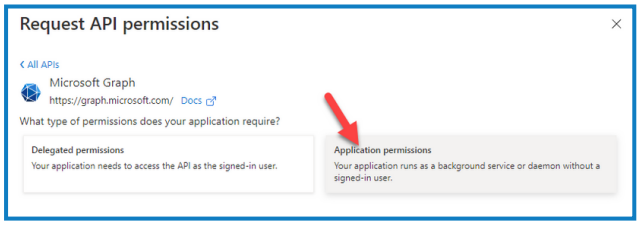
1. Öffnen Sie in Azure Active Directory die Anwendungseigenschaften der Anwendung, mit der Sie Hub verknüpfen.
2. Klicken Sie auf **API-Berechtigungen**.
3. Klicken Sie auf **Berechtigung hinzufügen**.



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

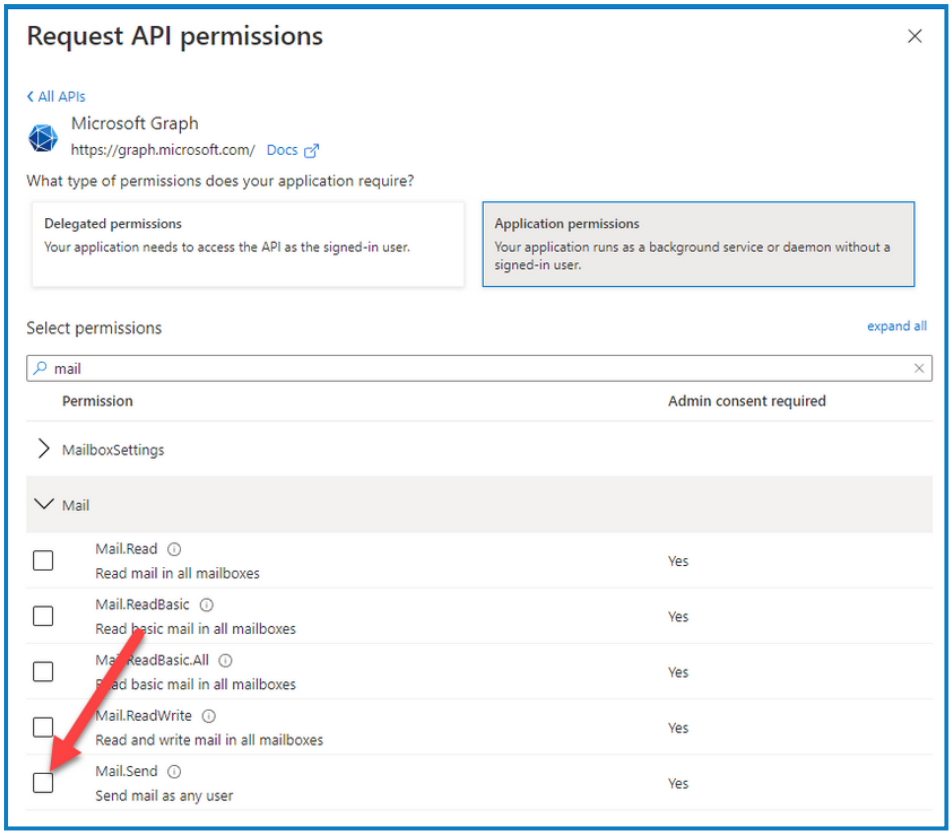


5. Klicken Sie unter Microsoft Graph auf **Anwendungsberechtigungen**.

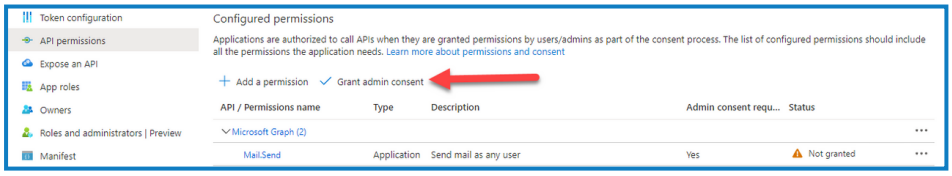


6. Geben Sie *Mail* in das Suchfeld ein und drücken Sie die Eingabetaste.

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"
}
```

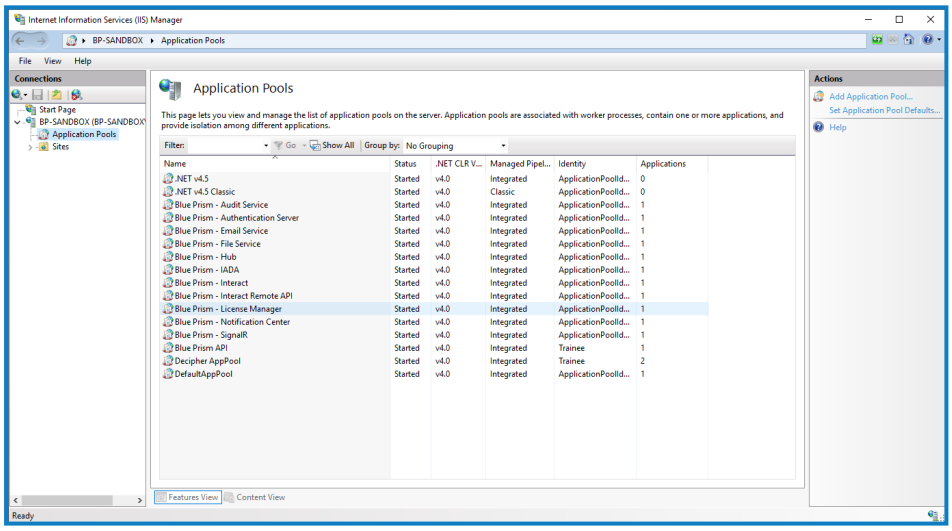
4. Speichern Sie die Datei.

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.

Logging

Der Zweck diagnostischen Loggings besteht darin, während der Ausführung der Anwendung mehr Informationen zur Verfügung zu stellen. Geloggte Fehler und Warnungen können helfen, Fehler innerhalb des Systems, die für einen Endbenutzer womöglich nicht sofort offensichtlich sind, genau zu ermitteln. Temporär kann ausführlicheres Logging aktiviert werden, um bei der Behebung eines Fehlers einen hilfreichen Einblick in das Verhalten der Anwendung zu gewinnen.

Zum Ausgeben und Aufzeichnen von Loginformationen verwendet Blue Prism eine bewährte und zuverlässige Bibliothek namens NLog. Ein Administrator kann die Menge der protokollierten Informationen entweder global oder in bestimmten Bereichen der Anwendung anpassen.

Logging-Stufen

Logeinträge werden in Stufen kategorisiert. Einträge mit der Stufe *Information* oder höher werden in der Regel standardmäßig aufgezeichnet. Niedrigere, detailliertere Stufen, wie *Debug* und *Trace*, liefern ausführlichere Informationen, müssen jedoch aktiviert werden.

NLog definiert die folgenden Stufen:

- **Trace** – Sehr detaillierte Logs, die große Informationsmengen wie Protokollnutzlasten, enthalten können. Diese Logstufe wird typischerweise nur während der Entwicklung aktiviert.
- **Debuggen**– Debugging-Informationen mit weniger Details als Trace, normalerweise in Produktionsumgebungen aufgrund möglicher Auswirkungen auf die Leistung nicht aktiviert.
- **Information** – Informationsmeldungen, die normalerweise in Produktionsumgebungen aktiviert sind.
- **Warning** – Warnhinweise, typischerweise für nicht kritische Probleme, die gelöst werden können, oder für vorübergehende Fehler.
- **Error** – Fehlermeldungen – meist sind dies Ausnahmen.
- **Fatal** – Sehr schwerwiegende Fehler.

Standard-Logging-Konfiguration

Die Logging-Stufen werden in der „appsettings.json“-Datei im Installationsordner für jede Website und jeden Dienst definiert. Bei Standardinstallationen finden Sie diese Ordner unter C:\Programme (x86)\Blue Prism\.

Sie sollten die Logkonfigurationseinstellungen in der „appsettings.json“-Datei bei normaler Verwendung nicht eigenständig ändern müssen. Der Blue Prism Kundensupport stellt bei der Untersuchung eines Problems mit dem Produkt alternative Logkonfigurationseinstellungen bereit. Wenn die Logging-Einstellungen in der „appsettings.json“-Datei geändert werden, muss die Site in IIS neu gestartet werden.

Das Ändern der Logging-Konfiguration kann sich auf die Performance der Anwendung auswirken und bei Änderungen in einer Produktionsumgebung ist besondere Vorsicht geboten.

Die Standardkonfiguration schreibt Logeinträge der Stufe „Information“ und höher (einschließlich „Warning“, „Error“ und „Fatal“) in eine Logdatei. Logdateien werden in das Verzeichnis geschrieben, das für die „LogsFolder“-Einstellung in der „appsettings.json“-Datei angegeben ist. Typischerweise ist dies festgelegt auf „./Logs_{Anwendung}“, beispielsweise „./Logs_Hub“ oder „./Logs_Interact“.

Die standardmäßigen Logging-Konfigurationseinstellungen in der Datei appsettings.json sind:

```
"Logging": {
      "LogsFolder": "./Logs_{Application}",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning"
      }
    },
```

Separate Logdateien werden basierend auf der Logstufe und dem Datum generiert und diese werden in die Logdateinamen aufgenommen, zum Beispiel „warns.2021-05-07“ oder „infos.2021-05-07“.

Es folgt ein Beispiel für eine Zeile in einer Information-Logdatei:

```
[08:58:11.4549] Connect.Core.Actions.UpdateCacheAction - Cache für Widgets wurde aktualisiert
```

Das Format dieses Texts enthält die folgenden Elemente:

- Zeit (unter Verwendung der auf dem Server eingestellten Zeitzone) – Das Datum ist im Dateinamen enthalten.
- Logger-Name – Identifiziert normalerweise die Klasse und den Namespace, aus dem der Logeintrag stammt.
- Die Lognachricht.
- Fehlerinformationen – nur verfügbar, wenn Ausnahmeinformationen protokolliert werden. Die vollständigen Details werden in einer separaten Zeile unter der Lognachricht protokolliert.

Zusätzliche Logging-Konfiguration

Blue Prism hat zusätzliche Logging-Konfigurationseinstellungen entwickelt, die der jeweiligen „appsettings.json“-Datei hinzugefügt werden können, um Aktivitäten bestimmter Komponenten zu erfassen.

Debugging von LDAP

Sie können das Logging so konfigurieren, dass es beim Debugging von Problemen hilft, die bei der Synchronisierung von Hub mit LDAP auftreten können. Sie müssen das Logging in der Datei appsettings.json von Authentication Server einrichten, bevor Sie die Benutzer in der Hub Benutzeroberfläche synchronisieren.

1. Navigieren Sie auf dem Server zum Ordner „Authentication Server“. Standardmäßig befindet er sich in C:\Programme (x86)\Blue Prism\.
2. Öffnen Sie die Datei „appsettings.json“ in einem Texteditor.
3. Suchen Sie den Abschnitt „Logging“ und fügen Sie `"ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"` zum Abschnitt „LogLevel“ hinzu und setzen Sie am Ende der obigen Zeile ein Komma ein. Zum Beispiel:

```
"Logging": {
      "LogsFolder": "./Logs_AuthenticationServer",
      "LogLevel": {
        "Default": "Information",
        "System": "Warning",
        "Microsoft": "Warning",
        "ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"
      }
    },
```

4. Speichern Sie die Datei.
5. Recyceln Sie den Authentication Server Pool in den IIS-Anwendungspools.

   Wenn Sie ein Upgrade von einer Version vor 4.3 durchgeführt haben, müssen Sie den IMS-Pool recyceln.

6. Starten Sie die Authentication Server Site in den IIS-Sites neu.

Dadurch wird eine Datei mit dem Präfix „debug“ und dem entsprechenden Datum im Verzeichnis „Logs_AuthenticationServer“ erstellt.

Nachdem Sie mit den Debugging-Informationen die Probleme erfolgreich gelöst haben, müssen Sie die hinzugefügte Zeile und das Komma entfernen, die Datei speichern und die Schritte 5 und 6 wiederholen. Andernfalls wird die Größe der Logdatei deutlich zunehmen und möglicherweise den Speicher füllen.

Log-Gatherer-Service

Dieser Windows-Dienst entfernt alte Produktlogs von der jeweiligen Webserver-Komponente (Hub, Interact, Authentication Server , Audit Service, Audit Service Listener, Email Service, Log-Gatherer-Service, IADA, Interact Remote API, SignalR, Manager für die Formularübermittlung). Dies geschieht jeweils am 7. des Monats und die Logs werden in C:\Programme (x86)\Blue Prism\ArchivedLogs verschoben.

Sie können den Pfad für archivierte Logdaten und das Zeitplanerdatum in apppsettings.json ändern – unter „ArchivedFolder“ in C:\Programme (x86)\Blue Prism\Log Service (Standard) können Sie den Archivpfad und unter „DayOfMonth“ das Zeitplanerdatum ändern.

Weitere Informationen

Die folgenden Links können weitere nützliche Informationen liefern:

- NLog GitHub Repository – Basis-Tutorial
- Offizielle Website von NLog – Konfigurationsoptionen

Hub deinstallieren

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

Gehen Sie wie folgt vor, um Hub 4.6 vollständig zu deinstallieren:

1. Stoppen Sie die Anwendungspools mit IIS.
2. Entfernen Sie Hub über „Programme und Features“.
3. Entfernen Sie die IIS-Websites und Anwendungspools.
4. Entfernen Sie die Hosts.
5. Entfernen Sie die Datenbanken.
6. Entfernen Sie die RabbitMQ-Daten.
7. Entfernen Sie die Zertifikate.
8. 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 Hub Websites auf Seite 16.

Hub über „Programme und Features“ entfernen

Wenn Sie auch Interact installiert haben, müssen Sie es zunächst mithilfe dieser Schritte deinstallieren, indem Sie in Schritt 3 Blue Prism Interact auswählen.

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 Hub aus.
4. Klicken Sie auf **Deinstallieren**.
5. Bestätigen Sie, dass Sie mit der Deinstallation fortfahren möchten.

IIS-Websites und Anwendungspools entfernen

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. Erweitern Sie im Bereich **Verbindungen** den Knoten **Websites** und entfernen Sie die Websites, die beim Entfernen von Hub übrig geblieben sind:
   - Blue Prism – License Manager.
   - Blue Prism – Notification Center.

3. Erweitern Sie im Bereich **Verbindungen** den Knoten **Anwendungspools** und entfernen Sie die Pools, die beim Entfernen von Hub übrig geblieben sind:
   - Blue Prism – License Manager.
   - Blue Prism – Notification Center.

Hosts entfernen

1. Öffnen Sie die Datei `C:\Windows\System32\drivers\etc\hosts` in einem Texteditor.
2. Löschen Sie die Zeile mit der Domäne „License Manager“. Sie können diese Zeile finden, indem Sie nach dem Text *licensemanager* suchen.
3. Löschen Sie die Zeile mit der Domäne „Notification Center“. Sie können diese Zeile finden, indem Sie nach dem Text *notificationcenter* suchen.
4. Speichern Sie die Datei.

Datenbanken entfernen

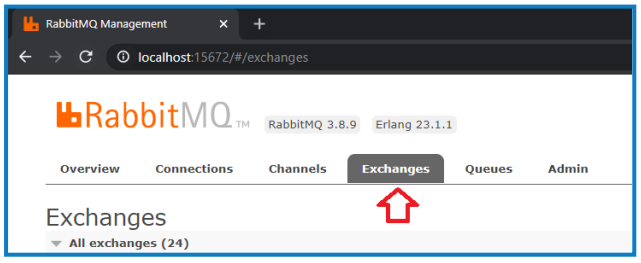
Sie sollten nur Datenbanken für Testsysteme entfernen. Wenn Sie eine Datenbank für ein System, das sich in der Produktion befand, entfernen möchten, sollten Sie überlegen, ob die Daten von Ihrem Unternehmen archiviert oder für Audit-Zwecke genutzt werden sollen.

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

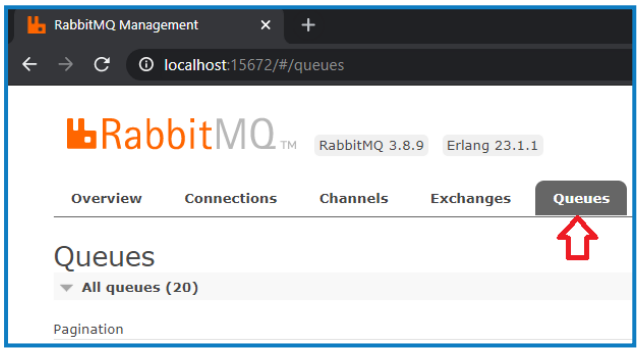
1. Löschen oder archivieren Sie die Datenbanken für die Hub Anwendung und die Interact Anwendung (falls diese installiert wurde).

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.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*
4. Klicken Sie auf **Queues** (Warteschlangen).



5. Suchen und entfernen Sie die folgenden Elemente:
   - bpc.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*

Zertifikate entfernen

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
   - BPC_SQL_CERTIFICATE

Alle verbleibenden Dateien entfernen

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