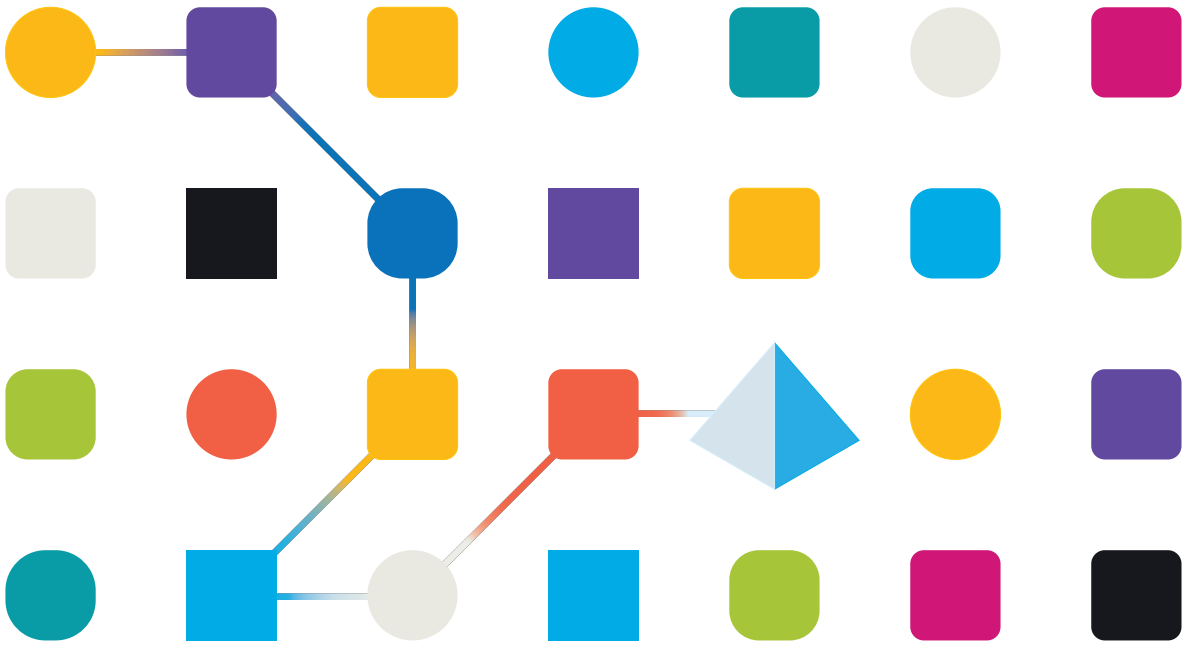
blueprism®

Hub 4.7

インストールガイド

Document Revision: 4.0



商標および著作権

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom。
英国で登録：登録番号4260035。電話：+44 370 879 3000。Web：www.blueprism.com

内容

Hubをインストールする

このガイドでは、Blue Prism® Hubのインストール時に従うプロセスについてのガイダンスと、します。

このガイドにはより詳細なトピックも多数含まれており、インストールのトラブルシューティングや、詳細設定およびオプションの構成に関する情報を提供します。Hubのインストールを実行する担当者は、Blue Prism、SSL証明書の構成、RabbitMQに関する重要な知識または経験を持っていることが前提となります。

本書を利用中にさらにサポートが必要な場合は、Blue Prismアカウントマネージャーまたはテクニカルサポートにお問い合わせください。詳細については、「連絡先」を参照してください。

この情報は、Blue Prism Hubバージョン4.7に関するものです。

Interactをインストールする前に、Blue Prism Hubをインストールする必要があります。

Hubをアップグレードする

以前のバージョンのHub 4からアップグレードする場合、Blue Prismはアップグレードツールを提供します。詳細については、「」「HubとInteractをアップグレードする」を参照してください。

対象者

このガイドは、ネットワーク、サーバー、データベースの構成と管理の経験を持つITの専門家を対象としています。インストールプロセスでは、Webサーバーとデータベースのインストールと構成に精通している必要があります。

動画

このインストールガイドに加えて、インストールプロセスを説明するビデオもご覧いただけます。こちらをクリックしてHubのインストールビデオを参照してください。

関連ガイダンス

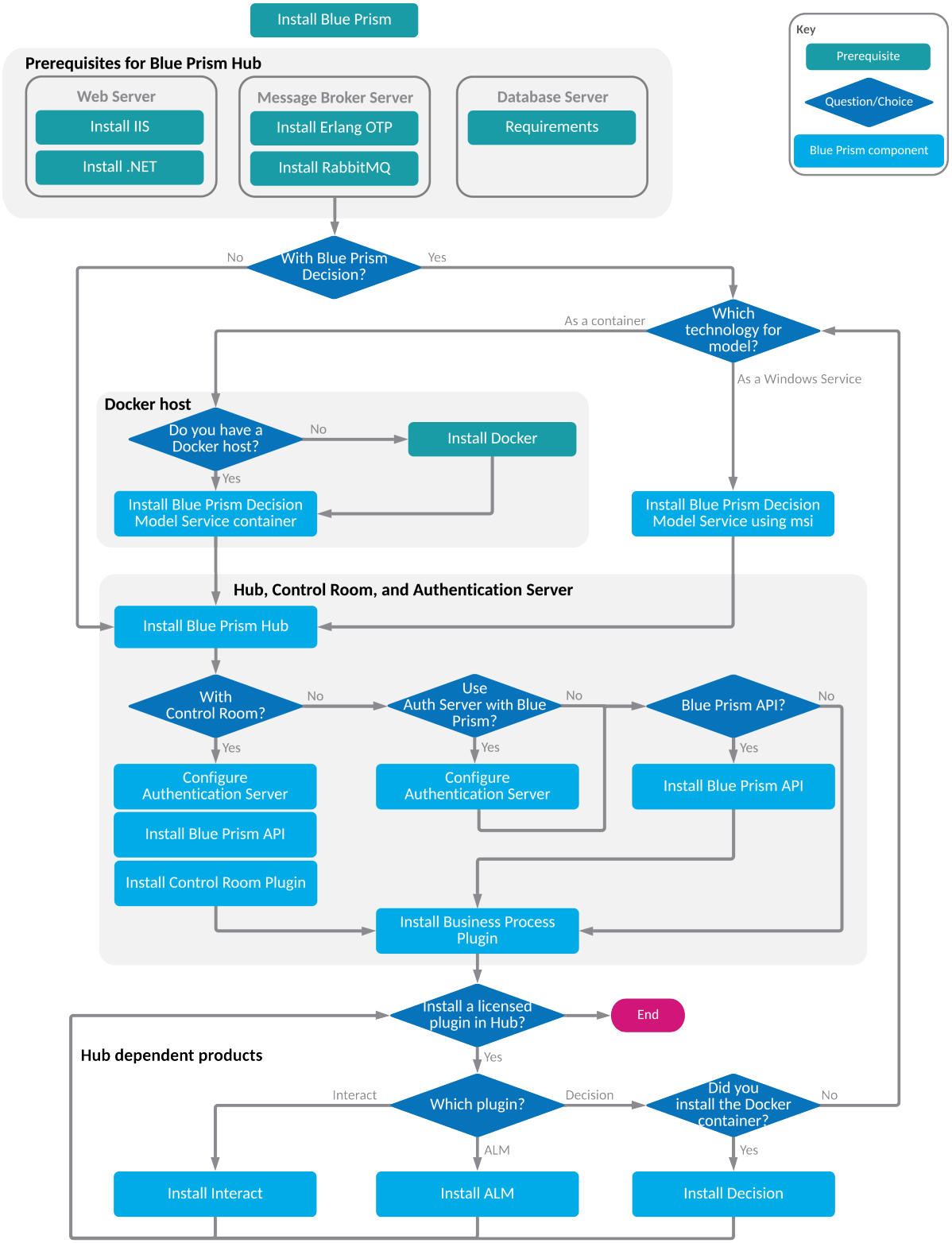
次の文書はHubとそのプラグインの実装の特定面に関する詳細情報を提供します。

文書タイトル	説明
Hubユーザーガイド	Hubのユーザーを対象に、Hubを最大限に活用する方法を説明する文書。
Hub管理者ガイド	Hub管理者を対象に、ユーザーアクセス、ライセンスプラグイン、Hubのカスタマイズなど、Hubを最大限に活用するための詳細な文書。
Authentication Server構成ガイド	Blue Prism HubおよびBlue Prismユーザー認証用にAuthentication Serverを構成する方法を説明する文書。
Authentication Server SAML 2.0拡張機能4.7インストールガイド	SAML 2.0拡張機能のインストール方法を説明する文書。この拡張機能は組織がSAML 2.0認証を使用する場合に必要です。 このリンクからDigital Exchangeに移動し、PDF形式でガイドにアクセスできます。
ALMユーザーガイド	Automation Lifecycle Management(ALM) プラグインの使用方法を説明する文書。これはライセンス製品です。
Control Roomユーザーガイド	Control Roomプラグインの使用方法を説明する文書。このプラグインは無償で入手可能で、Blue Prism 7.0以降と互換性があります。

文書タイトル	説明
Decisionインストールガイド	Blue Prism Decisionのインストールに必要な手順を説明する文書。これはライセンス製品です。
Decisionユーザーガイド	Decisionプラグインの使用方法を説明する文書。これはライセンス製品です。
Interactインストールガイド	Interactのインストールに必要な手順を説明する文書。これはライセンス製品です。
Interactプラグインユーザーガイド	Interactプラグインを使用してInteract Webアプリケーションにフォームを作成する方法を説明する文書。これはライセンス製品です。
Interact Webアプリケーションユーザーガイド	Interact Webアプリケーションをエンドユーザーとして使用する方法を説明する文書。これはライセンス製品です。
Wireframerユーザーガイド	ALMプラグインの一部であるWireframerオプションの使用方法を説明する文書。これはライセンス製品です。

インストールプロセスの概要

以下は、インストールプロセスを視覚化した図です。



準備

Blue Prism Hubのインストールに着手する前に、アーキテクチャがインストールをサポートするよう構成されていることを確認することが重要です。Hubのインストールをサポートするには、複数のシステムが必要です。

計画

インストール実行前に、以下の条件を満たす必要があります。

- Authentication Server、Hub、AuditなどのBlue Prismコンポーネントデータベースをホストするために、SQL Serverが使用可能である必要があります。インストールプロセス中には管理者レベルのアクセスが必要です。詳細については、「最小限必要なSQLの権限 ページ17」を参照してください。
- RabbitMQメッセージブローカーをホスティングしているメッセージブローカーサーバーが利用可能である必要があります。詳細については「メッセージブローカーサーバーをインストールする ページ23」を参照してください。
- Hubインストール用のWebサーバー。詳細については「前提条件 次のページ」を参照してください。
- Blue Prism Hubをインストールするデバイスへの管理者アクセス権が必要です。すべてのデバイスは最小仕様を満たしている必要があり、デバイスはローカルネットワークを介して互いに通信できる必要があります。これには使用するBlue Prismデータベースとの通信も含まれます。DNSはすべてのコンポーネントで使用可能である必要があります。
- インストールを実行するアカウントは、ホストファイルにアクセスできる必要があります。ファイルは通常、C:\Windows\System32\drivers\etc\hosts、または%SYSTEMROOT%\System32\drivers\etc\hostsに保存されています。

デプロイメントを計画する場合、次の点を考慮する必要があります。

- データベースは既存のデータベースサーバーに追加するのか、それとも新しいデータベースサーバーが運用されるのか?

  Blue Prismでは、データベースを別々のデータベースサーバーに保存することを推奨します。
- 追加するデータベースをホストするのに十分な容量とリソースがあるか?

  十分なディスク領域とコンピューティングリソースが追加の負荷に対応できるかどうかをチェックし、確認してください。
- SQLデータベース(SQL NativeまたはWindows認証) には、どのような認証モードが必要か?

  これはIT組織が決定します。
- メッセージブローカーサーバーは、Hubのインストールをサポートするよう設定および構成されているか?

  Hubのインストールを完了するには、メッセージブローカーサーバーが必要です。
- Blue Prism Hubをインストールするすべてのデバイスが最小要件を満たしているか?

  詳細については、「ソフトウェアの要件および許可 ページ15」を参照してください。

前提条件

ソフトウェア要件と最小限必要なSQLの権限の詳細については、「ソフトウェアの要件および許可 ページ 15」を参照してください。

Hubをインストールするには、以下の前提条件が必要です。

- SQL ServerはSSL暗号化を使用するように構成する必要があります。所属組織がSSL暗号化をまだ使用していない場合(SQL Serverの環境を証明書なしで実行しているか、自己署名証明書を使用している)、組織は信頼できる証明局から証明書を取得し、SQL Serverにインポートして有効にする必要があります。-詳細については、「Microsoftドキュメント」を参照してください。

  証明書をSQL Serverにインポートするには:

  1. Windowsタスクバーから [**SQL Server構成マネージャー**]を開きます。
  2. SQL Server構成マネージャーで [**SQL Serverネットワークの構成**]を展開し、[**<SqlServerInstanceName>のプロトコル**]を右クリックして [**プロパティ**]をクリックします。
  3. [<SqlServerInstanceName>のプロトコルのプロパティ]ダイアログで、 [**証明書**]タブを選択し、必要な証明書を選択またはインポートします。
  4. [**適用**]をクリックします。

  本番環境では、信頼できる証明局からの証明書を使用します。ただし自己署名証明書は概念実証または開発環境に使用できます。重要なのは、SQL Serverが使用するFQDNが証明書で定義されるFQDNと一致することです。**これらが一致しない場合、データベースへの接続が確立されずインストールが正しく機能しません。**自己署名証明書の使用と構成については、Blue Prism Hubインストールガイドの「」「自己署名証明書」。

  Hubインストーラーによってインストールされたデータベースに加え、Blue Prismデータベースでも、信頼できる証明局などのHubサーバーが信頼する証明書を使い、SSL暗号化を使用する必要があります。

- メッセージブローカーサーバーの構築は、RabbitMQメッセージブローカーサービスの汎用セットアップおよびベースインストールです。デフォルトパスワードの変更と、SSL証明書の適用などのセキュリティ要件は、IT部門が完了することを推奨します。

  メッセージブローカーの構築を完了するには、以下をダウンロードする必要があります。

  - Erlang/OTPについての参照先:https://www.rabbitmq.com/which-erlang.html
  - RabbitMQ Server(サポート対象バージョンは3.8.0 ~ 3.8.8)、入手先:https://github.com/rabbitmq/rabbitmq-server/releases/

  インストールのガイダンスの入手先:https://www.rabbitmq.com/install-windows-manual.html

- Blue Prism HubはWebサーバーにインストールされているため、Internet Information Services Manager(IIS).Net Coreコンポーネントをインストールする必要があります。これらは、Blue Prism Hubのインストールを成功させるために、事前にインストールする必要があります。詳細情報については、「Webサーバーのインストールと構成 ページ28」を参照してください。

- 次のウェブサイトを作成します。組織のドメインに基づいてURLを定義します。

IIS内のWebサイト	デフォルトのURL(例のみ)
エンドユーザーが使用するユーザーインターフェイスを備えたWebサイト	
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – Hub	https://hub.local
アプリケーション専用Webサイト(サービス)	
Blue Prism – Emailサービス	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

> ⚠ 上記のデフォルトURLは、テスト環境などのスタンドアロン環境に適しています。インストールでホスト名を選択する場合は、組織のDNSおよびドメイン構造を考慮する必要があります。

- 証明書 – インストールプロセス中に、セットアップするWebサイトのSSL証明書の入力を求められます。インフラストラクチャおよびIT組織のセキュリティ要件に応じて、これは内部で作成されたSSL証明書またはWebサイトを保護する購入済み証明書のいずれかにできます。インストーラーは証明書なしで実行できますが、サイトが動作するには、IIS Webサイトのバインディングに有効なSSL証明書がある必要があります。詳細については、「SSL証明書を構成する ページ28」を参照してください。
- 顧客ID – インストールプロセス中に、顧客IDを入力するよう求められます。これは、Hubで使用するためにALM、Decision、またはInteractを購入したときに送信されたメールに記載されています。

> Control Roomのみをインストールする場合は、顧客IDは必要ありません。顧客IDは、ALM、DecisionまたはInteractでのみ提供され、要求されるものです。

- Windows認証を使用する場合、Blue Prism環境で使用するには、定義済みのWindowsサービスアカウントが必要です。これにより、Hubのインストール中に作成されたWebサイトに対してWindowsサービスとアプリケーションプールが正しく構成されます。詳細については、「Windows認証を使用してをインストールする ページ50」を参照してください。
- デフォルトでは、IISアプリケーションプールが使用されます。アプリケーションプールは、アプリケーションファイルと、データ保護および認証のためにインストール中に作成される証明書にアクセスできる必要があります。これらの証明書は、BluePrismCloud_Data_ProtectionとBluePrismCloud_IMS_JWTで、デフォルトのWindows証明書フォルダー内にあります。Hubのアプリケーションプールは、BPC_SQL_CERTIFICATE証明書にもアクセスする必要があります。Windows認証を使用してSQL Serverにアクセスする場合は、手動で構成する必要があります。詳細については、「デフォルトのアプリケーション情報 ページ17」を参照してください。
- デフォルトでは、「ローカルシステム」アカウントがサービスに使用されます。このアカウントは、アプリケーションファイルへのアクセス権を持っている必要があります。Windows認証を使用してSQL Serverにアクセスする場合は、手動で設定する必要があります。

ソフトウェアダウンロードリスト

Blue Prism Hub

以下に、Hubのインストールに必要なすべてのダウンロードをリストします。これらすべては、後ほどインストールガイドで参照されます。

ソフトウェアと参照リンク	関連ガイダンス
RabbitMQ 3.9.22から3.10.7、3.11.9から3.11.10 詳しくは「「Downloading and Installing RabbitMQ」を参照」を参照してください。	メッセージブローカーサーバーをインストールする ページ23
Erlang/OTP 24.xまたは25.x 必要なErlangのバージョンは、使用するRabbitMQのバージョンによって異なります。詳しくは「「RabbitMQ Erlangのバージョン要件」を参照」を参照してください。	
IIS 10.0 Windows Server 2016、2019、2022に含まれています。	Webサーバーのインストールと構成 ページ28
ASP.NET Core Runtime 6.0.9または6.0.10(Windowsホスティングバンドル) https://dotnet.microsoft.com/download/dotnet/6.0 – 必要なバージョンを選択します。**ASP.NET Core Runtime**で、**ホスティングバンドル**を選択します。	
.NET Desktop Runtime 6.0.9または6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 – 必要なバージョンを選択します。**.NET Desktop Runtime**で、適切なダウンロードを選択します。	
.NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 これはWindows Server 2022にデフォルトでインストールされます。Windows Server 2016 DatacenterまたはWindows Server 2019を使用している場合、.NET Frameworkのみをインストールする必要があります。	
Blue Prism Hub 4.7 Blue Prismポータルの以下の製品ダウンロードページのいずれかからHubをダウンロードします。 • Automation Lifecycle Management • Decision • Interact	
Authentication Server SAML 2.0拡張機能 Digital Exchangeからダウンロード – これはオプションのインストーラーです。SAML 2.0認証を使用する場合にのみ必要です。	Digital Exchangeで「インストールガイド」を参照してください。

Blue Prism Decision

Blue Prism Decisionは、Hubのライセンス管理されたプラグインです。組織がDecisionを使用する予定の場合は、Blue Prism Hub 前のページにリストされているダウンロードに加えて、以下をダウンロードする必要があります。

Decision Model Serviceは、2つの異なるテクノロジーを使用して利用できます。

- Windowsサービスとして
- Linuxコンテナとして

これらのうち1つのみをインストールする必要があります。組織の技術的な観点でのインフラストラクチャに最も適したバージョンをダウンロードします。

ソフトウェアとリンク	関連ガイダンス
OpenSSL https://www.openssl.org/source/ これは、自己署名のSSL証明書を作成するためのオプションのダウンロードです。これは、POC/POV/Dev環境にのみ使用してください。	OpenSSL Webサイトを参照してください。
コンテナを使用してDecision Model Serviceを実行するには:	
Docker Engineは、Decisionコンテナの実行に必要な最小要件です。 https://www.docker.com/products/container-runtime Blue Prismでは、本番環境でLinuxサーバーをホストとして使用することを推奨しています。POCまたはDev環境の場合、WindowsサーバーをDocker Desktopの実行に使用できます。 https://www.docker.com/products/docker-desktop	Dockerのインストールの詳細については、以下を参照してください。 • Linuxサーバーについては、「Dockerヘルプ: Docker Engineのインストール」を参照してください。 • Windowsサーバーについては、「Dockerヘルプ: WindowsにDocker Desktopをインストール」を参照してください。
Blue Prism Decisionモデルサービスコンテナ Docker Hubからダウンロードします。	Blue Prism Decisionをインストールする
WindowsサービスとしてDecision Model Serviceを実行するには:	
Blue Prism Decision Model Service MSI。 Blue Prismポータルからダウンロードします。	Blue Prism Decisionをインストールする
Blue Prism Decisionを使用するには:	
Blue Prism Decision API.bpreleaseファイル Blue Prismポータルからダウンロードします。	Blue Prism Decisionをインストールする

Blue Prism Interact

Blue Prism Interactは、ライセンス管理されたHubのプラグインであり、エンドユーザー向けの追加のWebサイトです。組織がInteractを使用する場合は、Blue Prism Hub ページ11にリストされているダウンロードに加えて、以下をダウンロードする必要があります。

ソフトウェアと参照リンク	関連ガイダンス
Blue Prism Interact 4.7 Blue Prismポータルからダウンロードします。	Blue Prism Interactをインストールする
Blue Prism Interact Remote API.bpreleaseファイル Blue Prismポータルからダウンロードします。	Interact Web APIサービスをインストールし構成する

ハードウェア最小要件

以下の情報は、Hubを効果的にインストールして実行するために推奨される最小ハードウェア要件の詳細です4.7。ソフトウェアの要件については、「ソフトウェアの要件および許可 次のページ」を参照してください。

ランタイムリソース

インストールしたBlue Prismのバージョンのインストールガイドに記載されている最小要件を参照してください。詳細については、Blue Prismのヘルプを参照してください。

データベースサーバー

- インテルQuad Xeonプロセッサ
- 8GB RAM
- SQL Server:
  - 2016、2017または2019(64ビット) – Express、StandardまたはEnterpriseエディション

    SQL Expressエディションは、概念実証の実行のためなど、本番以外の環境でしか使えません。
  - Azure SQL Database – インストール時に100eDTU以上が必要です。インストール後に50eDTUまで下げることができます。
  - Azure仮想マシン上のSQL Server
  - Azure SQL Managed Instance
- 該当のオペレーティングシステムのサポートについては、以下を参照してください。
  - SQL Server 2016または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

メッセージブローカーサーバー

- インテルデュアルXeonプロセッサ
- 8 GB RAM
- Windows Server2016 Datacenterまたは2019もしくは2022

Webサーバー

- インテルデュアルXeonプロセッサ
- 8 GB RAM
- Windows Server2016 Datacenterまたは2019もしくは2022
- 「準備 ページ8」に詳述されている前提条件

ソフトウェアの要件および許可

ソフトウェア要件

ソフトウェアと共に使用するために、以下のテクノロジーをサポートしています。

オペレーティングシステム

バージョン	Webサーバー	メッセージブローカー
Windows Server 2016 Datacenter	✓	✓
Windows Server 2019	✓	✓
Windows Server 2022	✓	✓

Blue Prismコンポーネントが64ビットオペレーティングシステムにインストールされる場合は、32ビットアプリケーションとして実行されます。

Microsoft SQL Server

次のMicrosoft SQL Serverバージョンは、Blue Prismコンポーネントデータベースの場所を特定するためにサポートされています。

バージョン	Express	標準	エンタープライズ
SQL Server 2016	✓	✓	✓
SQL Server 2017	✓	✓	✓
SQL Server 2019(64ビット)	✓	✓	✓

注意:

- SQL Expressは、概念実証の実行のためなど、本番以外の環境でしか使えません。
- SQL ServerはSSL暗号化を使用するように構成する必要があります。所属組織がSSL暗号化をまだ使用していない場合(SQL Serverの環境を証明書なしで実行しているか、自己署名証明書を使用している) 、組織は信頼できる証明局から証明書を取得し、SQL Serverにインポートして有効にする必要があります。-詳細については、「Microsoftドキュメント」を参照してください。

  SQL Serverに証明書をインポートする手順については、「前提条件 ページ9」「」を参照してください。

  本番環境では、信頼できる証明局からの証明書を使用します。ただし自己署名証明書は概念実証または開発環境に使用できます。重要なのは、SQL Serverが使用するFQDNが証明書で定義されるFQDNと一致することです。**これらが一致しない場合、データベースへの接続が確立されずインストールが正しく機能しません。**自己署名証明書の使用と構成については、Blue Prism Hubインストールガイドの「」「自己署名証明書」。

以下もサポートされています。

- Azure SQL Database – インストール時に100eDTU以上が必要です。インストール後に50eDTUまで下げることができます。
- Azure仮想マシン上のSQL Server。
- ただし、Azure SQL Managed Instanceでは、インストール前にデータベースを作成する必要があります。

メッセージブローカーサーバー

メッセージブローカーサーバーには、次のソフトウェアが必要です。

- RabbitMQ 3.9.22から3.10.7、3.11.9から3.11.10
- Erlang/OTP 24.xまたは25.x – 必要なErlangのバージョンは、使用するRabbitMQのバージョンによって異なります。

  適切なErlang/OTPサポートについては、「「RabbitMQ Erlangのバージョン要件」を参照」を参照してください。

  該当オペレーティングシステムのサポートについては、「https://www.rabbitmq.com/platforms.html」を参照してください。

詳細については「メッセージブローカーサーバーをインストールする ページ23」を参照してください。

Blue Prismは、ソフトウェアが一般に利用可能になってから2か月以内に、最新のHubバージョンに対して新しいRabbitMQバージョンを完全にテストすることを目指しています。新しいRabbitMQバージョンをサポートするために以降のHub開発が必要な場合、リリースサイクルで決定されるHubの将来のリリースにアップデートが組み込まれます。

Webサーバー

Webサーバーには、次のソフトウェアが必要です。

- .NET Framework 4.8 – Windows Server 2022にデフォルトでインストールされています。
- IIS 10.0
- ASP.NET Core Runtime 6.0.9または6.0.10(Windowsホスティングバンドル)
- .NET Desktop Runtime 6.0.9または6.0.10

Hub 4.7は、上述のASP.NET Core RuntimeおよびNET Desktop Runtimeのバージョンのみをサポートしています。7.x.xなどの新しいバージョンを使用している場合は、問題が発生する可能性があります。

詳細については「Webサーバーのインストールと構成 ページ28」を参照してください。

クライアントマシンのWebブラウザー

次のWebブラウザーの最新バージョンは、Hubでサポートされています。

- Google Chrome
- Microsoft Edge(Chromiumベース)

Active DirectoryユーザーがChromeまたはEdgeブラウザーを使用してHubにログインするには、ブラウザーが統合Windows認証用に構成されている必要があります。

Microsoft Internet ExplorerおよびMozilla Firefoxはサポートされていません。

Blue Prism

Hub自体についてはBlue Prismが利用可能である必要はありませんが、Hubが付属するコンポーネントまたはプラグインの一部ではBlue Prismが必要であり、たとえば、以下のものがあります。

- Authentication Server – Blue Prism 7.1.2 以降が必要です。
- Blue Prism® Automation Lifecycle Management(ALM) – Blue Prism 6.4.0以降が必要です。
- Control Room – Blue Prism 7.1.0 以降が必要です。
- Blue Prism® Decision – Blue Prism 6.4.0以降が必要です。
- Blue Prism® Interact – Blue Prism 6.4.0以降が必要です。

最小限必要なSQLの権限

インストールプロセス中にデータベースに接続するために必要なユーザーの最小限必要なSQLの権限には、製品内からデータベースを作成または構成するための適切な権限が必要です。したがって、インストールプロセスを実行するときは、適切な管理者アカウントを使用する必要があります。

- データベースを作成する:dbcreator(サーバーの役割) またはsysadmin(サーバーの役割)
- データベースを構成する:sysadmin(サーバーの役割) またはdb_owner(データベースの役割)

通常の運用中にデータベースとの接続に必要なデータベースユーザーは、Hubおよび Authentication Server データベースにアクセスするために最小限必要なSQLの権限を持っている必要があります。必要な権限は次のとおりです。

- db_datareader
- db_datawriter

詳細については以下の「デフォルトのアプリケーション情報 下。

デフォルトのアプリケーション情報

以下の情報は、デフォルト値を使用してインストールによって作成されるアプリケーションを示しています。すべてのアプリケーションには、ローカルマシンの証明書ストアにあるBluePrismCloud_Data_Protection証明書へのフルアクセス権が必要です。また、

- IIS APPPOOL\ Blue Prism – Authentication Server およびIIS APPPOOL\ Blue Prism – SignalRでは BluePrismCloud_IMS_JWT証明書へのアクセス権も必要です。
- IIS APPPOOL\ Blue Prism – HubではBPC_SQL_CERTIFICATE証明書へのアクセス権も必要です。

> Windows認証を使用してSQL Serverで認証する場合、専用のActive Directoryユーザーを IISアプリケーションプールのIDに割り当てることをお勧めします(デフォルト名は以下の表に示されています) 。このアプリケーションプールユーザーが**英語(米国)** の地域を使用するように設定する必要があります。これを行うには、[コントロールパネル] > [時計と地域] > [地域] を開き、アプリケーションプールユーザーの [**形式**] を [**英語(米国)**] に設定します。

HubのWebサイト

アプリケーション名	サービス例 のアカウント名 SQL Windows 認証	SQL Server 許可 中の要求インストール	データベース 許可 中の要求実行中のアプリケーション	デフォルトのデータベース名
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	最初のログインと初期構成の場合： dbcreator / sysadmin 以降のログイン： 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
Blue Prism - License Manager	IIS APPPOOL\ Blue Prism – License Manager	dbcreator / sysadmin	db_owner または db_datawriter / 実行権限のあるdb_datareader(下記参照)	LicenseManagerDB
Blue Prism - SignalR	IIS APPPOOL\ Blue Prism – SignalR	該当なし	該当なし	該当なし

アプリケーションの実行中、License Managerはストアドプロシージャの実行に適切な許可を必要とします。許可レベルとしてdb_ownerを使用しない場合は、db_datawriter/db_datareaderを使用し、次のSQLスクリプトを実行して、必要なレベルをユーザーに提供できます。

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

ここでは、

- [LicenseManagerDB]は、License Managerのデータベース名です。
- 「IIS APPPOOL\Blue Prism - License Manager」はユーザー名です。

Hubのサービス

アプリケーション名	サービス例 のアカウント名 SQL Windows 認証	SQL Server 許可 中の要求インストール	データベース 許可 中の要求実行中のアプリケーション	デフォルトのデータベース名
Blue Prism -監査サービスリスナー	NT AUTHORITY\ SYSTEM	dbcreator / sysadmin	db_datawriter / db_datareader	AuditDB
Blue Prism -ログサービス	NT AUTHORITY\ SYSTEM	該当なし	該当なし	該当なし

マルチデバイスデプロイメントについての考慮事項

マルチデバイスデプロイメントに取りかかるときは、インストールに着手する前に、以下の項目を必ず検討します。

エリア	環境に関する懸念事項(開発/テスト/本番前/本番)
全般的なコネクティビティ	各種デバイス間のコネクティビティを、適切に構成する必要があります。通常は、デバイスがそれぞれのFQDNに基づいて相互に解決できるようにDNSを構成すること、および必要なポート上でデバイスが通信できるように適切なファイアウォール規則を定めることが必要です。
メッセージブローカーサーバー	これは、Blue Prismコンポーネント間でメッセージブローキングサービスを提供することに焦点を当てた単一デバイスです。環境ごとにデバイスを使用することを推奨します。
Webサーバー	複数のBlue Prismコンポーネントをホストできる単一デバイス。このデバイスで環境を共有すること、および環境ごとに別のデバイスを使用することは推奨されません。
データベースサーバーインスタンス	重要性や不可欠性に基づいてBlue Prismのデプロイメントに単一の共有インスタンスを使用する際に、リソースをSQL Serverインスタンスに割り当てる方法が適切かどうかを検討します。(たとえば、本番環境は業務上最も不可欠なものである可能性が高い)。 開発環境、UAT環境、本番環境など、さまざまなタイプの環境には、専用のSQL Serverインスタンスを用意することを推奨します。ただし、同じSQL Serverインスタンスで複数の開発環境を実行することもできます。
Digital Worker証明書	インタラクティブクライアントおよびアプリケーションサーバーから各Digital Workerへの指示通信、およびWebサービスをホストしているDigital Workersが受け取るインバウンド接続に、証明書ベースのセキュリティを適用する必要があるかどうかを判断します。証明書が求められる場合は、証明書を手動で生成し、適用可能な各Digital Workerにインストールする必要があります。証明書の共通名は、デバイスとの通信時に使用するようにBlue Prismコンポーネントが構成するアドレスと一致する必要があります(例:FQDNまたはマシンの短縮名)。さらに、Digital Workersに接続するすべてのデバイスは、手動生成の証明書を発行した証明局を信頼する必要があります。

ネットワークポート

アーキテクチャ内のデバイス間のネットワーク接続を確保するために、該当するサーバー上のWindowsファイアウォールは、次のトラフィックフローを許可する必要があります。

データベースサーバー	Webサーバーからの SQL Server接続を許可するポート1433。 SQL Serverインスタンスが名前付きインスタンスの場合、次の要件も必要です。 • 名前付きインスタンスのTCPポート(これは、デフォルトではエフェメラルポート範囲から動的です)、または静的なポートがWebサーバーからのSQL Server接続を許可する場合は定義済みポート。 • Webサーバーからの SQL Server接続を可能にするための SQL Server Browserサービス用のUDPポート1434。
メッセージブローカーサーバー	RabbitMQ Messaging接続を許可するポート5672。 RabbitMQ管理コンソールの接続を可能にするポート15672。
Webサーバー	HTTPS接続を許可するポート443。
Digital Workers	HTTPS接続を許可するポート443。

ポートを構成する際は、組織のネットワークインフラストラクチャの専門家に相談することをお勧めします。組織内の接続を確保するために、構成する必要があるポートが他にもある場合があります。

の一般的なデプロイメント

本番および本番以外の使用に適した一般的なデプロイメントには、別のマシンにデプロイされているBlue Prism Hubのすべてのコンポーネントが含まれます。

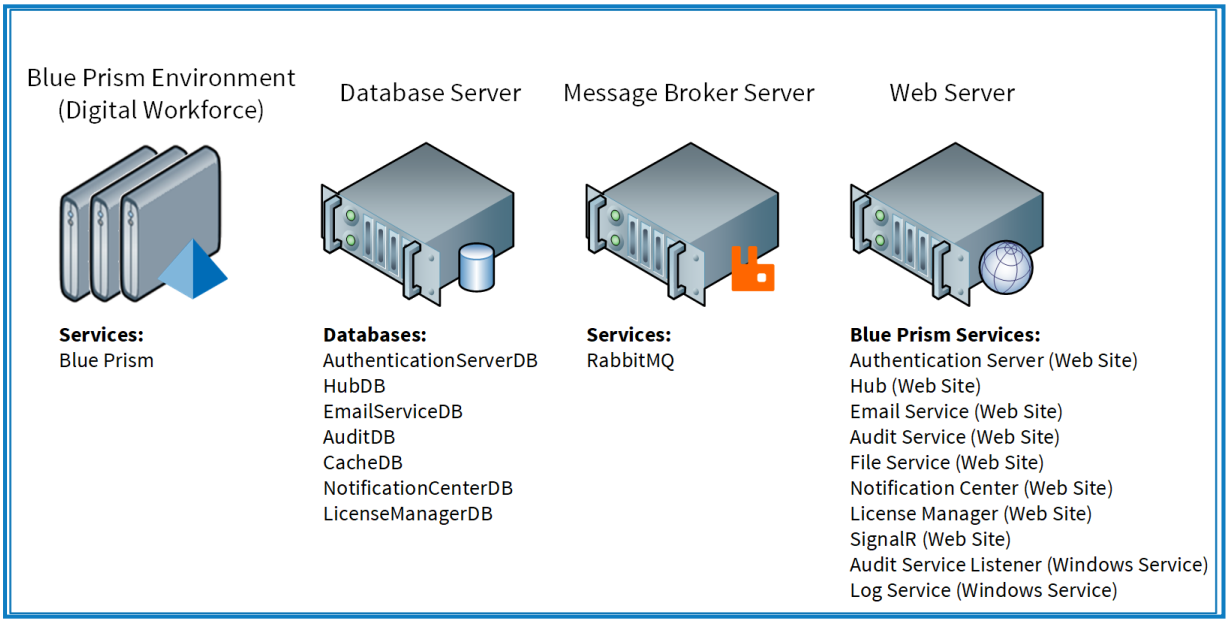
このガイダンスに従う前に、「準備 ページ8」に記載されている情報を十分に検討してください。

本番環境については、少なくとも下の4つのリソースが必要です。

- Blue Prism環境(Digital Workforce)
- データベースサーバー(SQL Server)
- メッセージブローカーサーバー
- Webサーバー

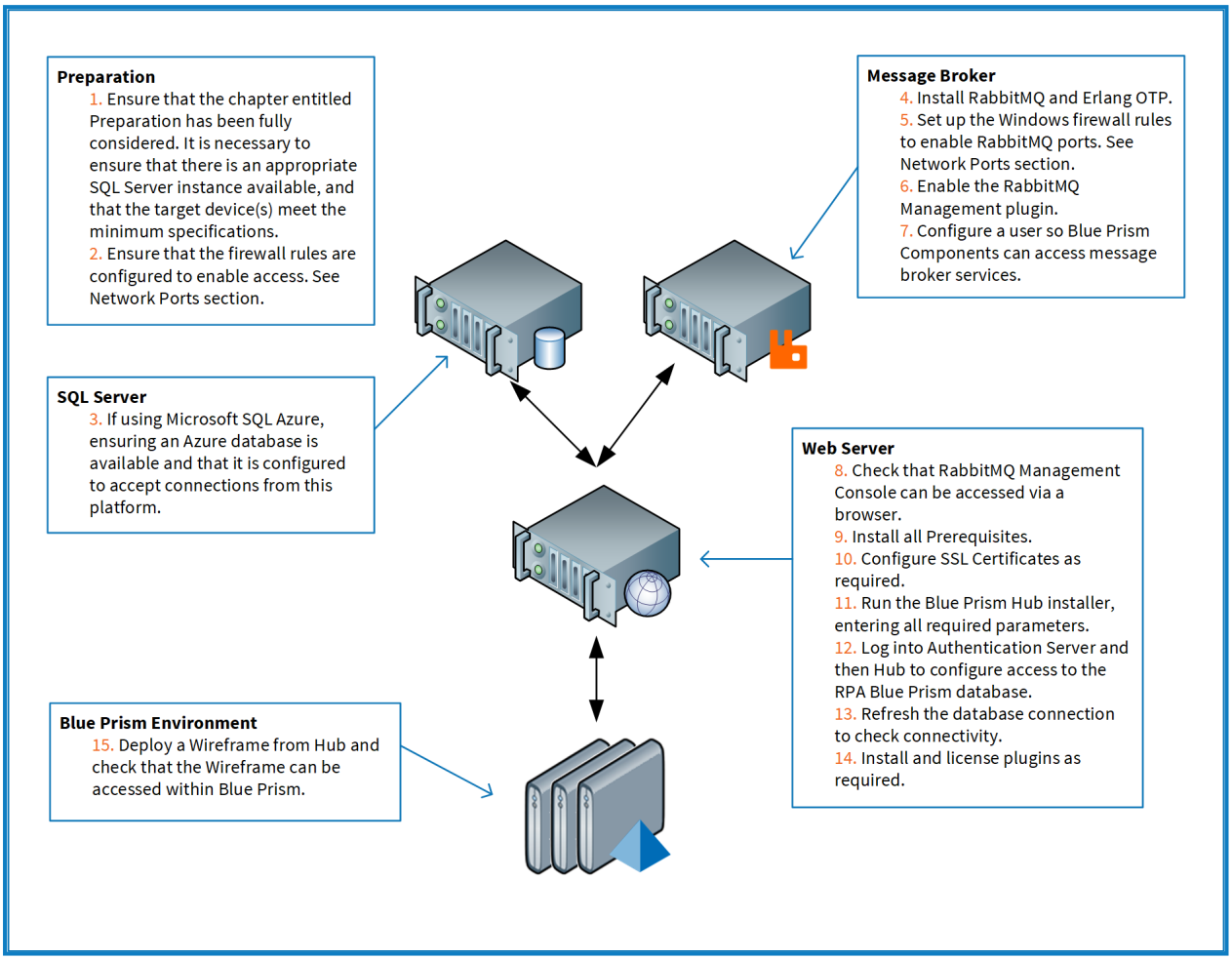
メッセージブローカーサーバーおよびSQL Serverのインスタンスは、Blue Prism Hubのインストールに先立って構成する必要があります。

次の図に、1つの環境に対する一般的なアーキテクチャを示します。



標準インストール手順の概要

一般的なデプロイメントを完了するために必要な手順の概要は、以下のとおりです。



インストール中に問題が発生した場合は、「Hubのインストールのトラブルシューティング ページ63」を参照してください。

メッセージブローカーサーバーをインストールする

メッセージブローカーサーバーをインストールして構成します。これには、ネットワークコネクティビティとRabbitMQ管理コンソールを有効にするWindowsファイアウォールの構成が含まれます。

メッセージブローカーサーバー用のソフトウェアのインストール方法に関するビデオは、https://bpdocs.blueprism.com/video/installation.htmを参照してください。

ソフトウェアのバージョンについては、「ソフトウェア要件 ページ15」を参照してください。

メッセージブローカーがまだインストール、構成されていない場合は、以下の手順に従います。

1. Erlangをダウンロードしてインストールします。インストールウィザードのデフォルト設定をそのまま使用します。

   必要なErlangのバージョンは、使用するRabbitMQのバージョンによって異なります。参考：
   - Erlang/OTPのバージョンおよびサポートについては、「「RabbitMQ Erlangのバージョン要件」を参照」を参照してください。
   - インストール情報については、「Erlang/OTPインストールガイド」を参照してください。
   - ダウンロードについては、「Erlang/OTPのダウンロード」を参照してください。

   このインストール手順については、Erlangのインストールビデオを参照してください。

2. RabbitMQをダウンロードしてインストールし、デフォルト設定を受け入れます。

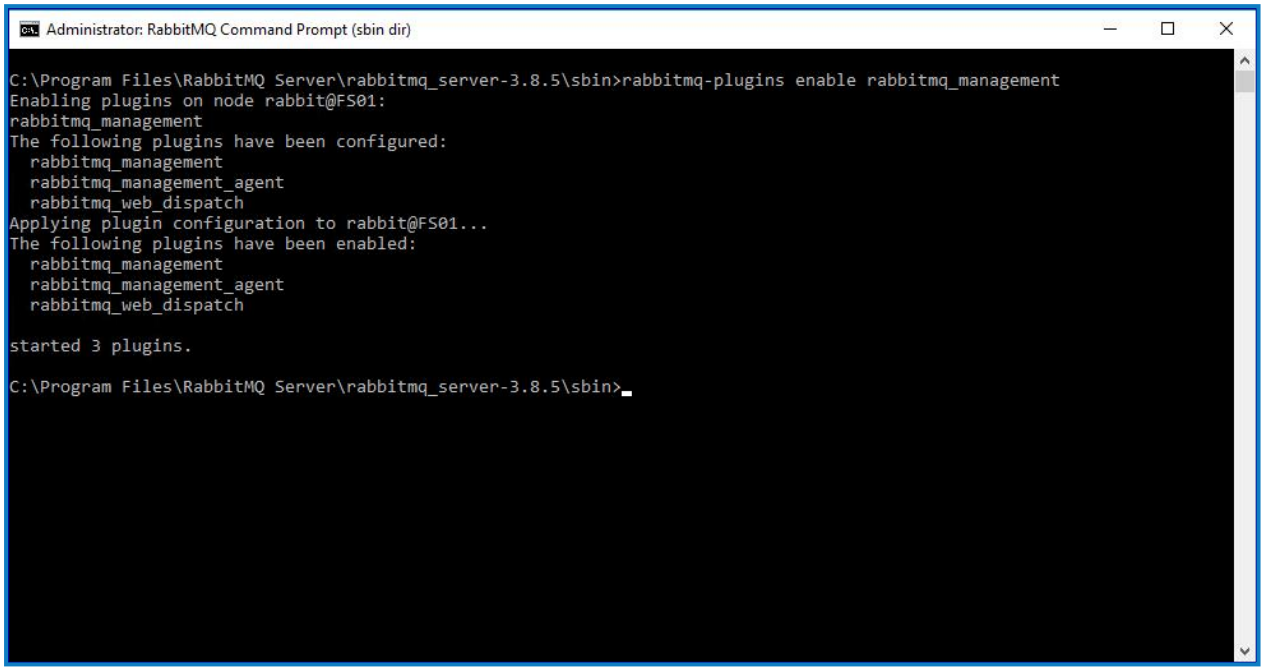
   詳しくは「「Downloading and Installing RabbitMQ」を参照」を参照してください。

   このインストール手順を視聴するには、RabbitMQのインストールビデオを参照してください。

3. Windowsファイアウォールを構成して、ポート5672と15672へのインバウンドトラフィックを有効にします。
4. [スタート]メニューの[RabbitMQ Server]フォルダーで、[RabbitMQ Command Prompt (sbin dir)]を選択します。

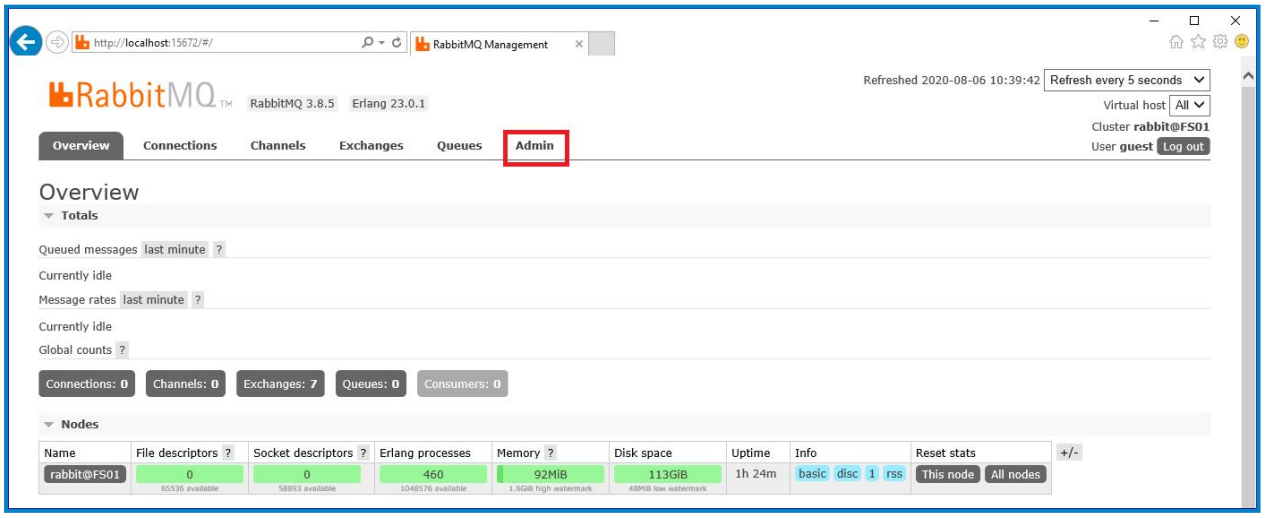
5. [RabbitMQ Command Prompt]ウィンドウで、次のコマンドを入力します。

```
rabbitmq-plugins enable rabbitmq_management
```

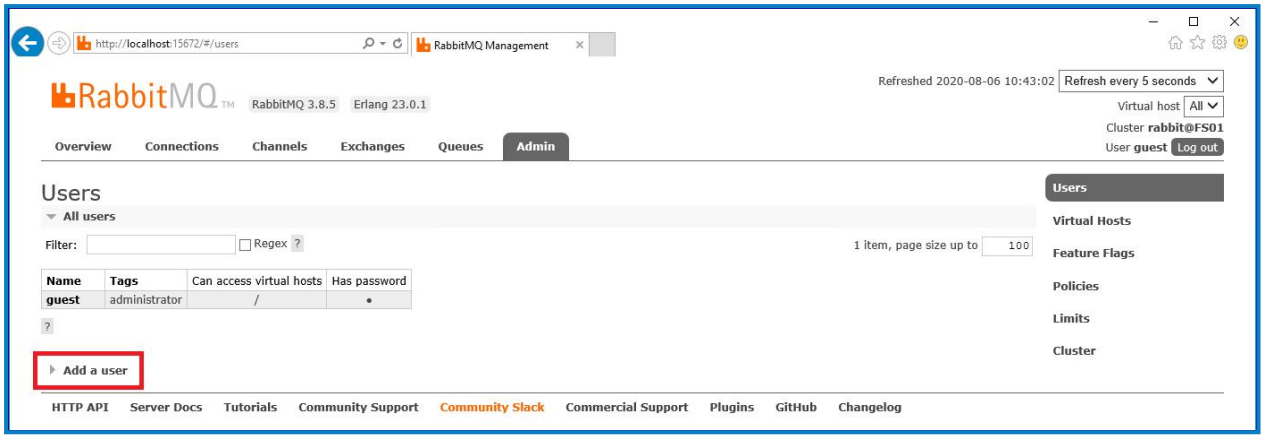


6. ブラウザーを起動し、次のURL：http://localhost:15672に移動します。
7. RabbitMQコンソールで、guest/guestのデフォルト認証情報でログオンします。

8. コンソールで、[Admin]をクリックします。



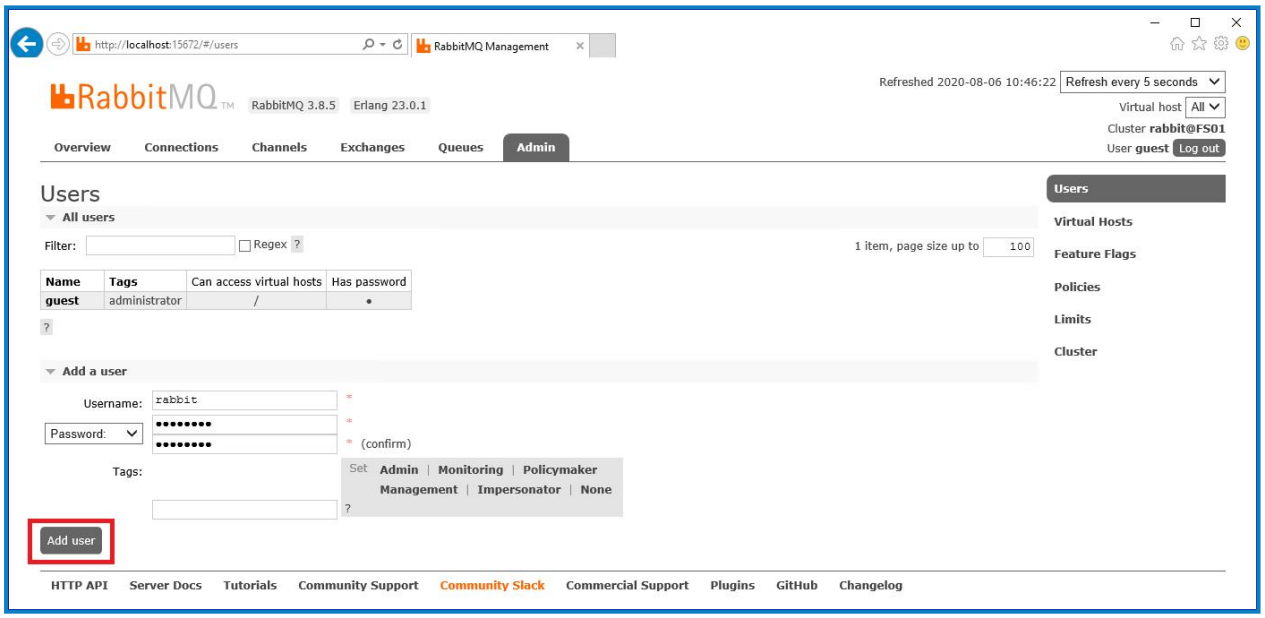
9. [Add a user] をクリックします。



10. ユーザー名とパスワードを入力して、新規ユーザーの詳細を入力します。ユーザーは特別な許可を必要とせず、 [None] のままにしておくことができます。

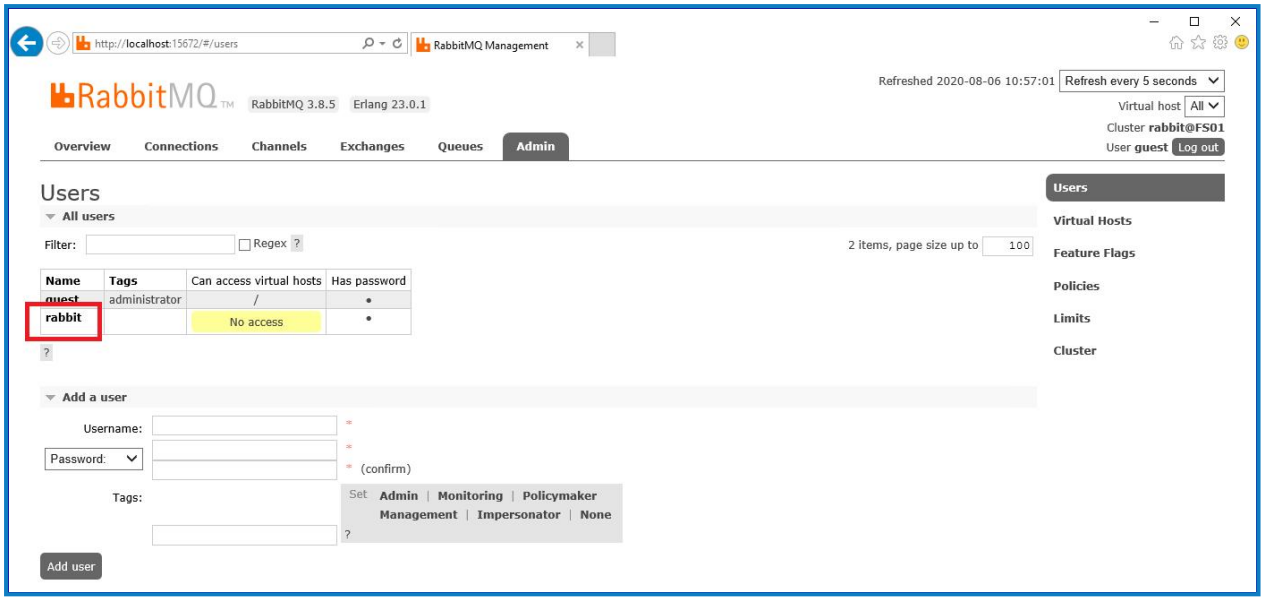
> RabbitMQユーザーを作成する場合、パスワードには、# / : ? @ \ ` " $ 'の文字は使用しないでください。

11. [ユーザーを追加] をクリックします。

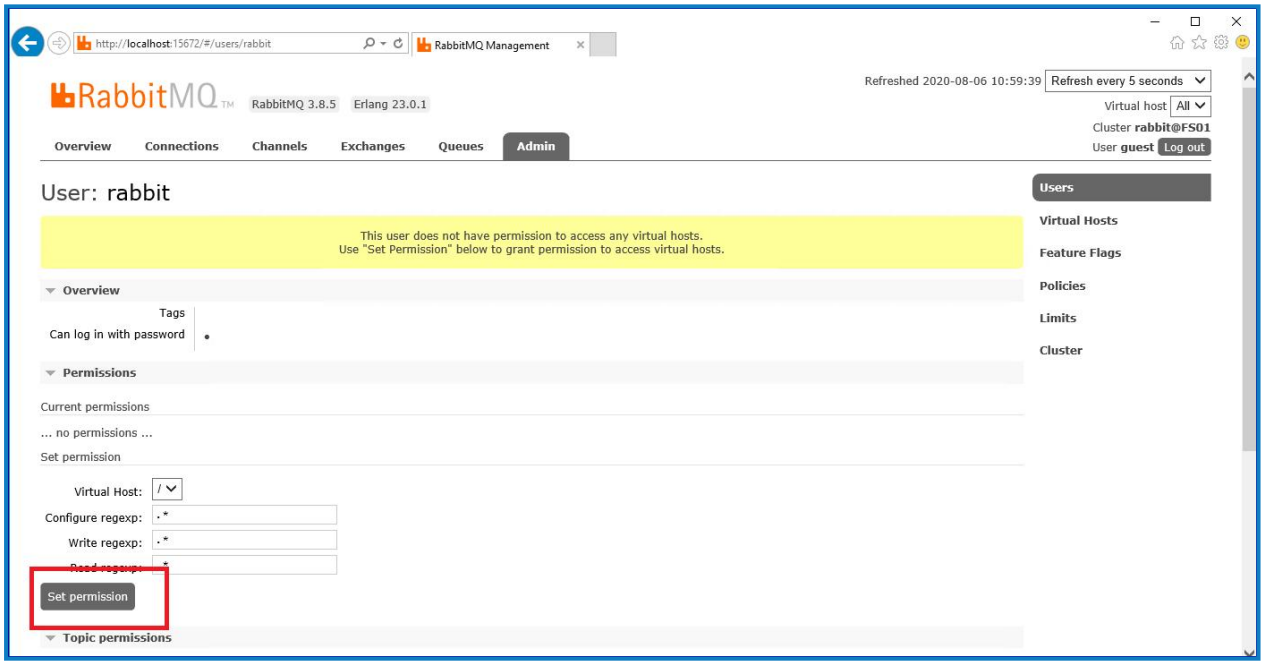


次のステップでは、ユーザーの許可を設定します。

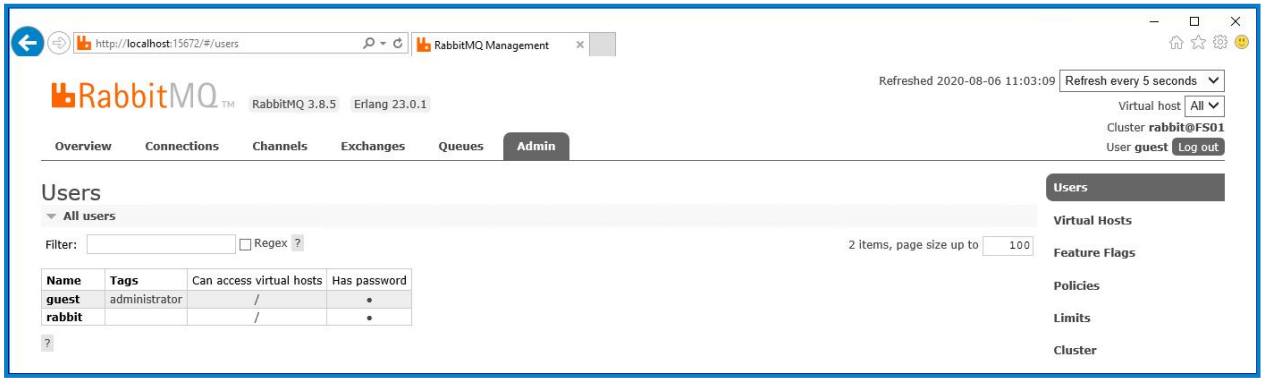
12. 作成したユーザーのユーザー名をクリックします。



13. [Set Permission]をクリックして、デフォルトの許可を割り当てます。



14. 上部の[Admin]タブを選択し、許可が次のように適切に設定されていることを確認します。



このアカウントには管理コンソールへのアクセス権がないため、作成した認証情報を使用してもアクセスは有効になりません。

これは、RabbitMQメッセージブローカーサービスの汎用セットアップおよびベースインストールです。デフォルトパスワードの変更と、SSL証明書の適用などのセキュリティ要件は、IT部門が完了することを推奨します。

新しい管理者アカウントを作成し、デフォルトのゲストアカウントを削除することをお勧めします。デフォルトのゲストアカウントが残っていると、セキュリティリスクが生じる可能性があります。

RabbitMQメッセージブローカーの接続を確認する

ブラウザーを起動し、「http://<Message Broker Hostname>:15672」とURLを入力します。

RabbitMQ管理コンソールの [ログイン] ページが表示されます。

ゲストアカウントはローカルアクセスにのみ制限されており、作成したアカウントは管理コンソールへのアクセスが許可されていないため、管理コンソールにログインできません。

コンソールが表示されない場合は、RabbitMQサービスを再起動してください。それでもコンソールが表示されない場合は、「Hubのインストールのトラブルシューティング ページ63」を参照してください。

Webサーバーのインストールと構成

Hub Webサーバーをインストールする前に、「準備 ページ8」の情報をご一読ください。

Webサーバーをインストールして構成し、システムがRabbitMQメッセージブローカーと通信できることと、。

このプロセスは、以下の手順で構成されます。

1. IISをインストールする
2. SSL証明書を構成する
3. .NET Coreコンポーネントをインストールする
4. Blue Prism Hubをインストールする
5. Authentication Server SAML 2.0拡張機能をインストールする - これはSAML 2.0認証を使用する場合にのみ必要です。

次の手順で説明するデフォルトのホスト名は、テスト環境などのスタンドアロン環境にのみ適しています。インストールでホスト名を選択する場合は、組織のDNSおよびドメイン構造を考慮する必要があります。

前提条件のソフトウェアとBlue Prism Hubのインストール方法に関する動画は、https://bpdocs.blueprism.com/en-us/video/installation.htmを参照してください。

IISをインストールする

システムには、IIS Webサーバーおよび.NET Coreコンポーネントのインストールが必要です。

.NET CoreコンポーネントとBlue Prism Hubをインストールする前に、IISをインストールすることが重要です。IISの機能と役割は、Blue Prism Hubのインストールの一部として自動的にインストールされます。

インストールのスクリプト化

PowerShellコマンドプロンプトを使用して、次のコマンドを実行します。

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

このインストール手順を視聴するには、IISのインストールビデオを参照してください。

デフォルトでは **匿名認証**]が有効に設定され、IISがインストールされます。この設定はHubとその関連サイトで必要です。 **匿名認証**]を無効にした場合は、Hubインストーラーを実行する前に有効にする必要があります。匿名認証の詳細については、「Microsoftの匿名認証のページ」を参照してください。

SSL証明書を構成する

インストールプロセス中に、セットアップするWebサイトのSSL証明書の入力を求められます。インフラストラクチャおよびIT組織のセキュリティ要件に応じて、これは内部で作成されたSSL証明書またはWebサイトを保護する購入済み証明書のいずれかにできます。

証明書を生成する際には、ホスト名を小文字で入力します。すべて小文字のホスト名を使用しないと、Hubインストーラーを使用するときに、証明書の名前とホスト名に名前の不一致が発生することがあります。その結果、証明書が適用されず、インストーラーによってインストールを続行できなくなる可能性があります。

インストーラーは証明書なしで実行できますが、サイトが動作するには、IIS Webサイトのバインディングに有効なSSL証明書がある必要があります。

次の表に必要なSSL証明書の詳細を示します。

IIS内のWebサイト	デフォルトのURL(例のみ)
エンドユーザーが使用するユーザーインターフェイスを備えたWebサイト	
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – Hub	https://hub.local
アプリケーション専用Webサイト(サービス)	
Blue Prism – Emailサービス	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

⚠ 上記のデフォルトURLは、テスト環境などのスタンドアロン環境に適しています。インストールでホスト名を選択する場合は、組織のDNSおよびドメイン構造を考慮する必要があります。

自己署名証明書

自己署名証明書は使用できますが、概念実証(POC)環境、価値実証(POV)環境、開発環境でのみ使用することをお勧めします。本番環境では、組織の認定証明局の証明書を使用します。ITセキュリティチームに連絡して、要件を確認することを推奨します。

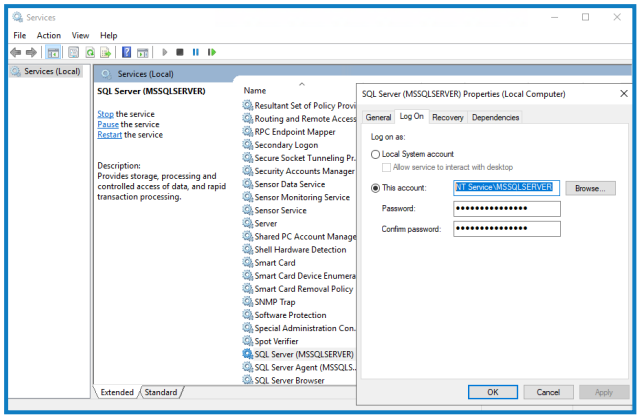
SQL Server用の自己署名証明書を生成して適用するには:

✎ Microsoftが提供するスクリプトを使用して、SQL Server用の自己署名証明書を作成できます。詳細については、「Microsoftドキュメント」を参照してください。その際に重要なのは、SQL Serverが使用するFQDNが証明書で定義されるFQDNと一致することです。**これらが一致しない場合、データベースへの接続が確立されずインストールが正しく機能しません。**

1. 管理者としてPowerShellを実行し、SQL Server用の情報を使用してMicrosoftのスクリプトを実行します。

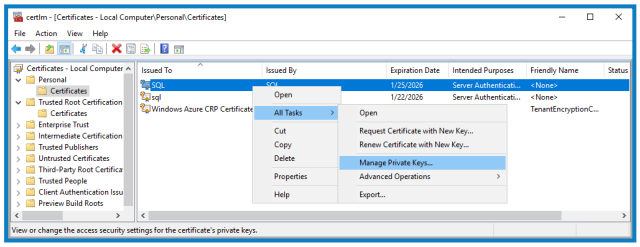
   これにより証明書が生成され、SQL Serverにインストールされます。
2. SQL Serverで以下を行います。
   a. SQL Serverサービスアカウント用証明書で使用する秘密キーへのアクセスを有効にします。これには、以下の操作を行います。

i. SQL Serverサービスアカウントの名前を見つけます(知らない場合)。この情報はSQL ServerのSQL Serverプロパティの[ログオン]タブに表示され、SQL Serverの[サービス]からアクセスできます。

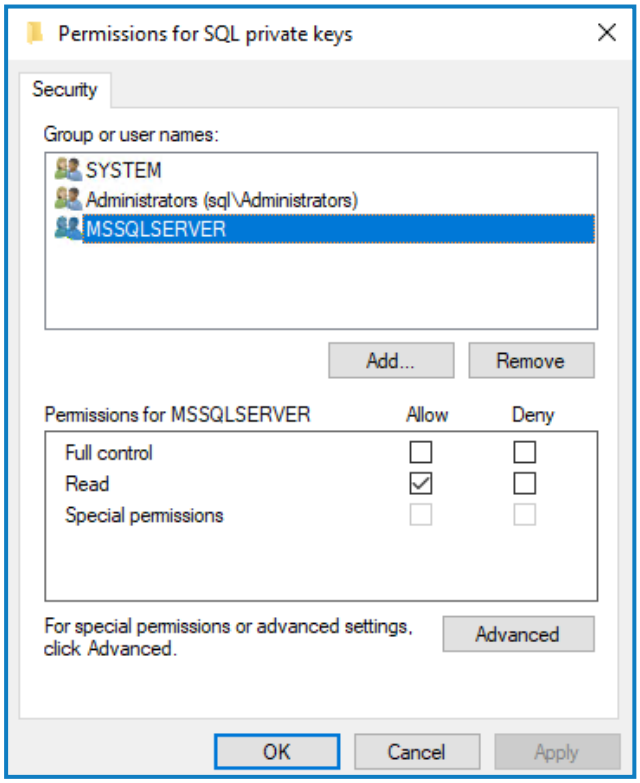


ii. SQL Serverで[証明書マネージャー]を開きます。

iii. [個人]、[証明書]の順に展開し、[SQL]を右クリックし[すべてのタスク]を選択して[秘密キーの管理...]をクリックします。



iv. SQL秘密キーのダイアログの[アクセス許可]で、読み取りアクセス許可を持つSQL Serverサービスアカウントを追加します。例:



v. [OK]をクリックして変更を適用し、ダイアログを閉じます。

b. SQL ServerでSSLを有効にし、証明書を指定します。これには、以下の操作を行います。

i. Windowsタスクバーから[SQL Server構成マネージャー]を開きます。

ii. SQL Server構成マネージャーで[SQL Serverネットワークの構成]を展開し、[<SqlServerInstanceName>のプロトコル]を右クリックして[プロパティ]をクリックします。

iii. [<SqlServerInstanceName>のプロトコルのプロパティ]ダイアログで、[証明書]タブを選択し、必要な証明書を選択またはインポートします。

iv. [適用]をクリックします。

v. [OK]をクリックして[プロパティ]ダイアログを閉じます。

c. SQL Serverサービスを再起動します。

d. 証明書「C:\sqlservercert.cer」をコピーします。これをHubおよびInteract Webサイトのホストサーバーに追加する必要があります。

3. Webサイトのホストサーバー:

a. 「sqlservercert.cer」をHubとInteractのWebサイトホストサーバーに貼り付けます。

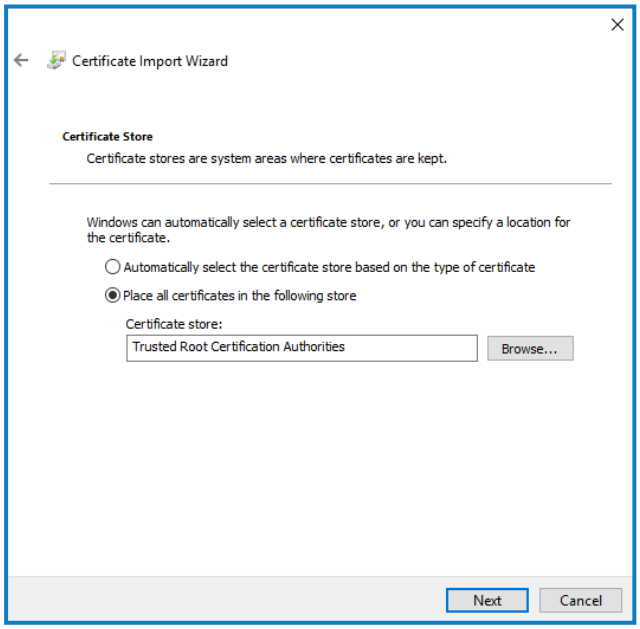
b. 証明書をサーバーの信頼されたルート証明機関の証明書ストアに追加します。これには、以下の操作を行います。

i. 証明書をダブルクリックし[証明書のインストール...]をクリックします。

[証明書のインポートウィザード]が表示されます。

ii. [ウィザードの開始]ページの[保存場所]で[ローカルコンピューター]を選択し、[次へ]をクリックします。

iii. [証明書ストア]ページで[証明書をすべて次のストアに配置する]を選択し、[信頼されたルート証明機関]を選択します。



iv. [次へ]をクリックし、ウィザードに従って手順を完了します。

c. Webサイトのホストサーバーからの SQL Serverへの接続をテストします。

Webサイトの自己署名証明書を生成するには、以下の手順に従います。

1. 管理者としてPowerShellを実行し、次のコマンドを使用して、[Website]および[ExpiryYears]を適切な値に置き換えます。

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

例：

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

この例では、*MySiteCertAuthentication*という自己署名証明書を個人証明書ストアに作成し、*authentication.local*を件名として、作成時点から10年間有効としています。

> 証明書を生成する場合は、ホスト名([Website]) を小文字で入力します。すべて小文字のホスト名を使用しないと、Hubインストーラーを使用するときに、証明書の名前とホスト名に名前の不一致が発生することがあります。その結果、証明書が適用されず、インストーラーによってインストールを続行できなくなる可能性があります。

2. Webサーバーで [コンピューター証明書の管理] アプリケーションを開きます(検索バーに「**コンピューター証明書の管理**」と入力します) 。
3. 証明書を [個人] > [証明書] からコピーして [信頼されたルート証明書] > [証明書] に貼り付けます。
4. Webサイトごとにこのプロセスを繰り返します。

スクリプトによるWebサイトの自己署名証明書の作成

> このプロセスは、本番環境には推奨されません。このプロセスでは、各Webサイトに適用できる証明書を1つ作成します。

次のPowerShellコマンドを実行します。

```
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は、ホストサーバー名に置き換える必要があります。

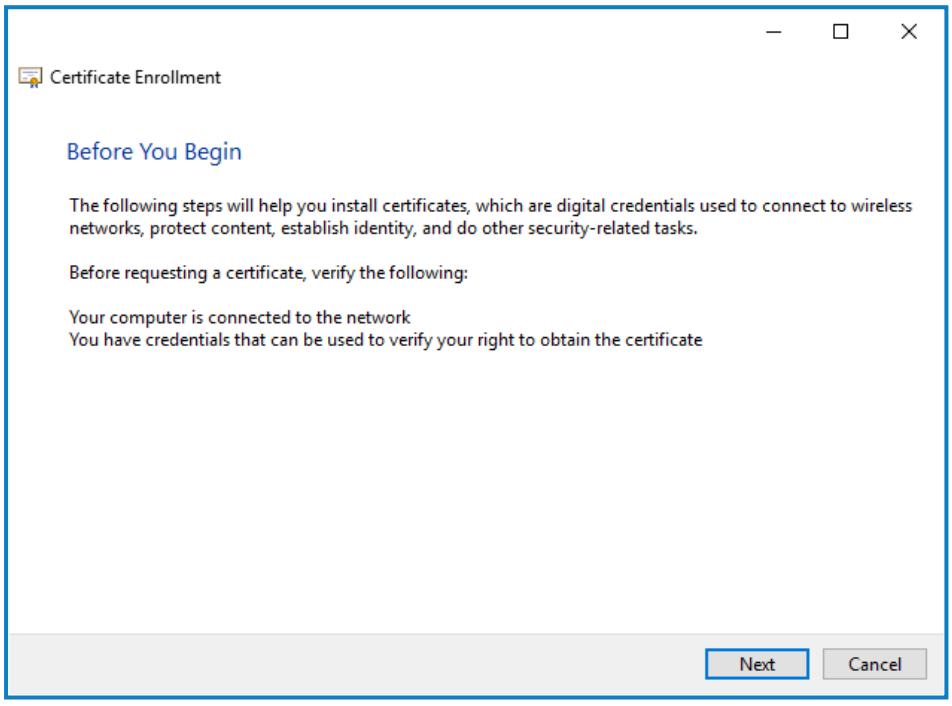
作成したら、ローカルマシンの証明書マネージャー(certlm) を開き、証明をコピーして、信頼されたルート証明書ストアに貼り付けます。

オフライン証明書リクエストを作成する

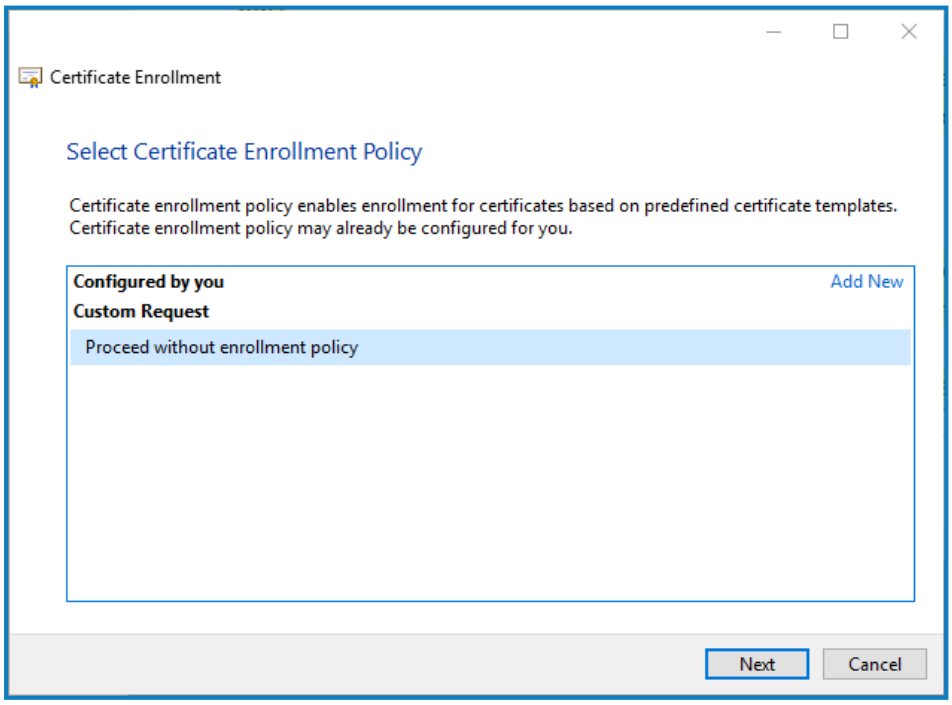
オフライン証明書要求を作成するには、各証明書に対して次の手順に従ってください。

1. Webサーバーで [コンピューター証明書の管理] アプリケーションを開きます (検索バーに「**コンピューター証明書の管理**」と入力します) 。
2. [**個人**] > [**証明書**] を右クリックし、ショートカットメニューから [**すべてのタスク**] > [**詳細設定操作**] > [**カスタム要求の作成**] を選択します。

   [証明書登録] ウィザードが表示されます。

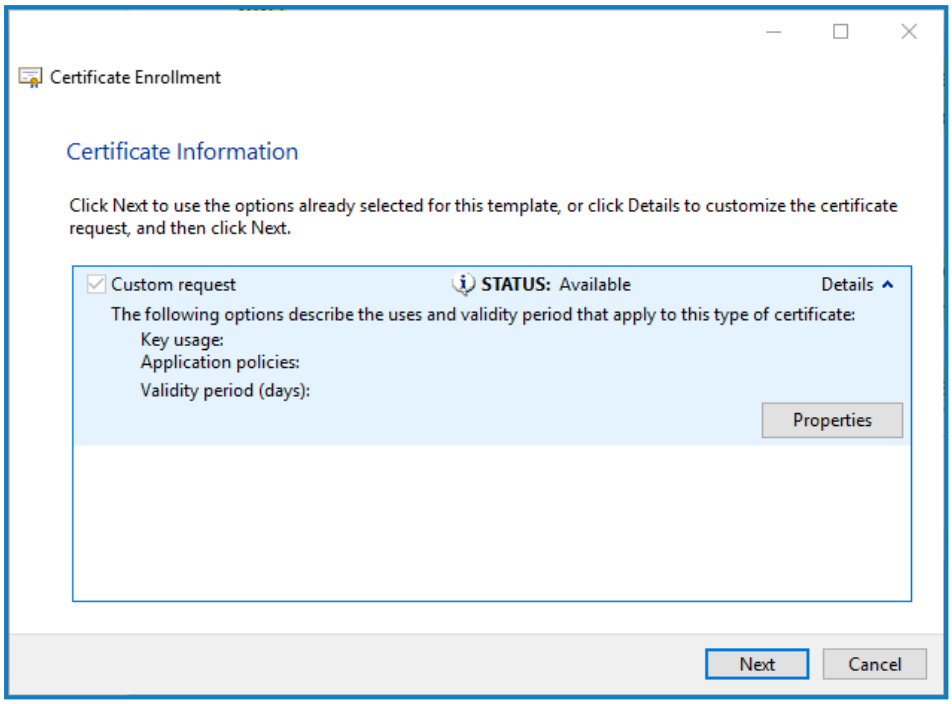


3. [**次へ**] をクリックします。



4. [**登録ポリシーなしで続行する**] を選択し、 [**次へ**] をクリックします。

5. [カスタム要求]画面で、 **[次へ]**をクリックします。
6. [証明書情報]画面で、 **[詳細]**ドロップダウンをクリックし、 **[プロパティ]**をクリックします。



7. [証明書のプロパティ]ダイアログの [全般]タブで、この証明書を適用するWebサイトに基づいてわかりやすい名前と説明を入力します。
8. [サブジェクト]タブで、サブジェクト名の種類を **[共通名]**に変更し、 **[値]**フィールドにWebサイトのURLを入力して **[追加]**をクリックします。

   CN(共通名)が右側のパネルに表示されます。
9. [拡張機能]タブで、 **[拡張キー使用法]**をクリックし、 **[サーバー認証]**を選択して **[追加]**をクリックします。
10. [秘密キー]タブで、 **[キーのオプション]**をクリックし、任意のキーサイズを選択して、 **[秘密キーをエクスポート可能にする]**を選択します。
11. [秘密キー]タブで、 **[ハッシュアルゴリズム]**をクリックし、適切なハッシュを選択します(任意)。
12. **[OK]**をクリックします。

    [証明書の登録]画面に戻ります。
13. **[次へ]**をクリックします。
14. ファイル名とパスを追加し、 **[終了]**をクリックします。

証明書要求を作成した後、証明局に送信する必要があります。証明局がリクエストを処理し証明書を発行します。証明書要求はテキストファイルです。通常は、ファイルからテキストをコピーし、証明局のWebサイトでオンライン提出フォームに入力する必要があります。証明書要求の送信プロセスの説明については、証明局に直接お問い合わせください。

.NET Coreコンポーネントをインストールする

.NET Coreコンポーネントをダウンロードしてインストールする必要があります。

ステップ	詳細
1	次のコンポーネントをダウンロードし、C:\\tempなどの一時的な場所に保管します。 • ASP.NET Core Runtime 6.0.9または6.0.10(Windowsホスティングバンドル) https://dotnet.microsoft.com/download/dotnet/6.0 – 必要なバージョンを選択します。**ASP.NET Core Runtime**で、**ホスティングバンドル**を選択します。 • .NET Desktop Runtime 6.0.9または6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 – 必要なバージョンを選択します。**.NET Desktop Runtime**で、適切なダウンロードを選択します。 • .NET Framework 4.8 https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0 これはWindows Server 2022にデフォルトでインストールされます。Windows Server 2016 DatacenterまたはWindows Server 2019を使用している場合、.NET Frameworkのみをインストールする必要があります。

2	.NET依存関係をインストールするには、PowerShellコマンドプロンプトを使用して次の各コマンドを実行し、各コマンドが完了するまで待機してから、次のコマンドを実行します。
	Windows Server 2016およびWindows Server 2019の場合 :
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	`start-process "C:\temp\ndp48-x86-x64-allos-enu.exe" /q -wait`
	Windows Server 2022の場合 :
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	ファイル名とファイルパスが、手順1で保存したファイルと一致していることを確認します。

3	Blue Prism Hubをインストールする前にサーバーを再起動し、コンポーネントが完全にインストールされ、登録されていることを確認します。

このインストール手順を視聴するには、.NETのインストールビデオを参照してください。

Blue Prism Hubをインストールする

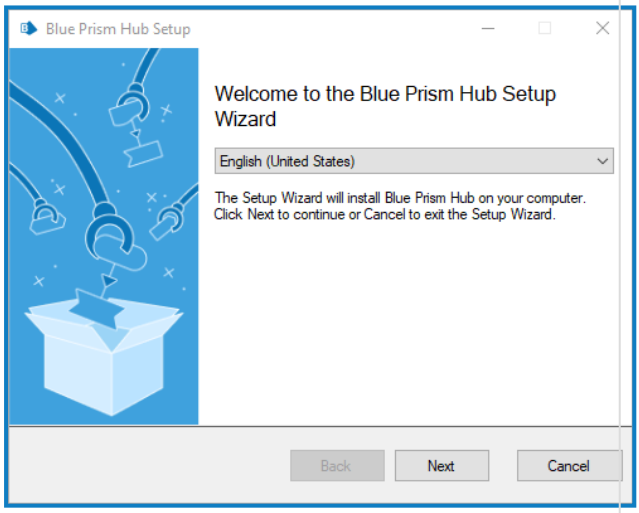
Blue Prism Hubをインストールする前に:

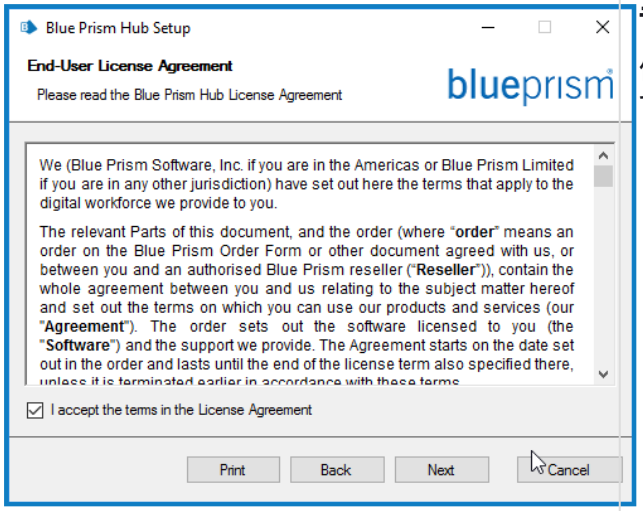
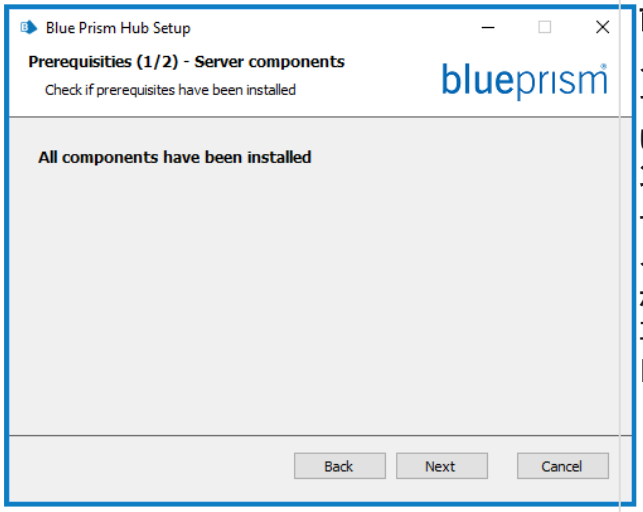
- ALM、Decision、またはInteractを購入した場合は、このHubのインストール中に顧客IDが必要になります。これは、ALM、Decision、またはInteractの購入時に送信されたメールに記載されています。
- HubでBlue Prism Decisionプラグインを使用する場合は、Hubインストールウィザードを実行する前に、Blue Prism Decisionモデルサービスコンテナを Dockerホストにインストールする必要があります。詳しくは、「Blue Prism Decisionをインストールする」を参照してください。
- 以前Blue Prism Hubを使用し削除した後にBlue Prism Hubを再インストールし、同じデータベース名を使用する場合は、データベースを再インストールする前に古いデータを消去することを推奨します。-

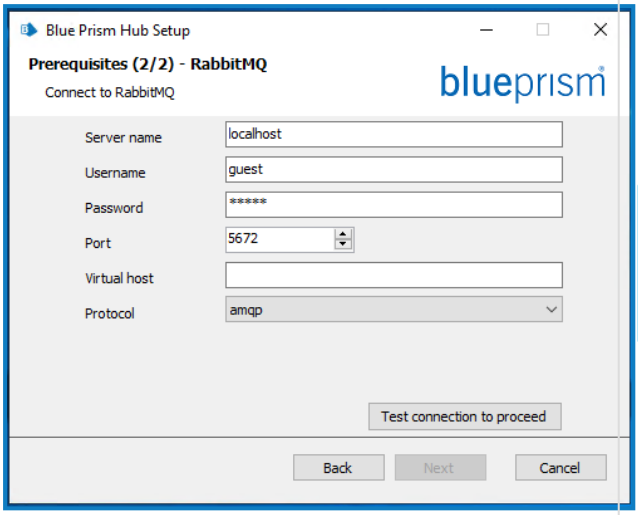
Hubのインストールと構成プロセスを視聴するには、Blue Prism Hubのインストールビデオを参照してください。

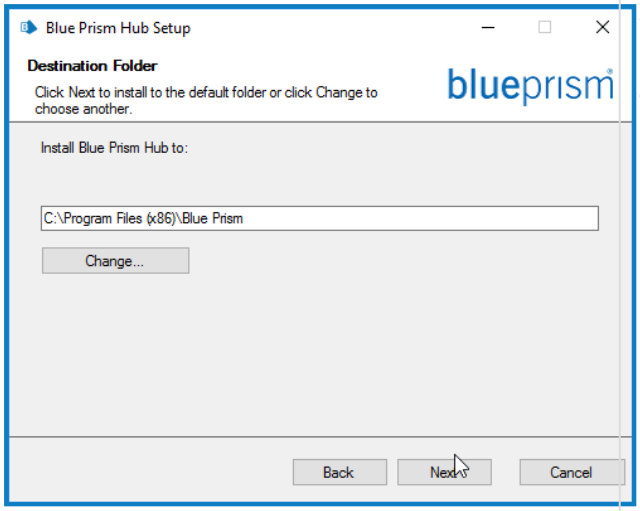
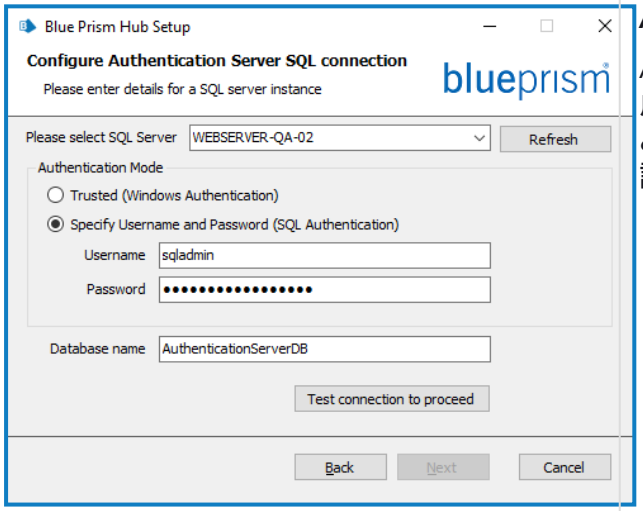
次の手順では、Blue Prism Hubソフトウェアをインストールするプロセスの詳細を説明します。これには、Authentication Server、Hub、その他の関連サービスが含まれます。インストールプロセスによって、必要な新しいデータベースが作成されます。

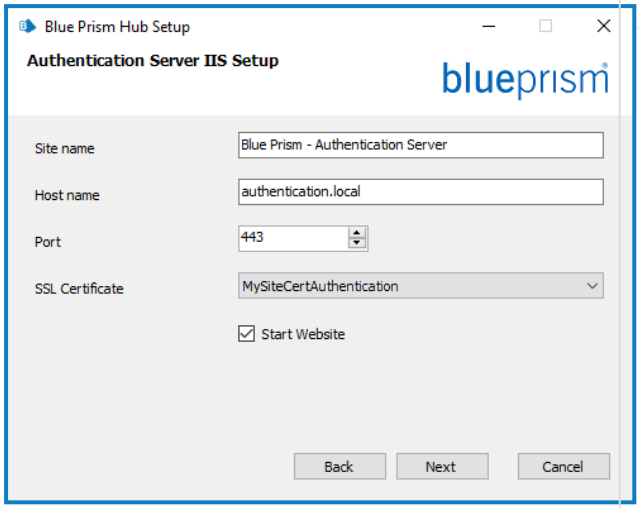
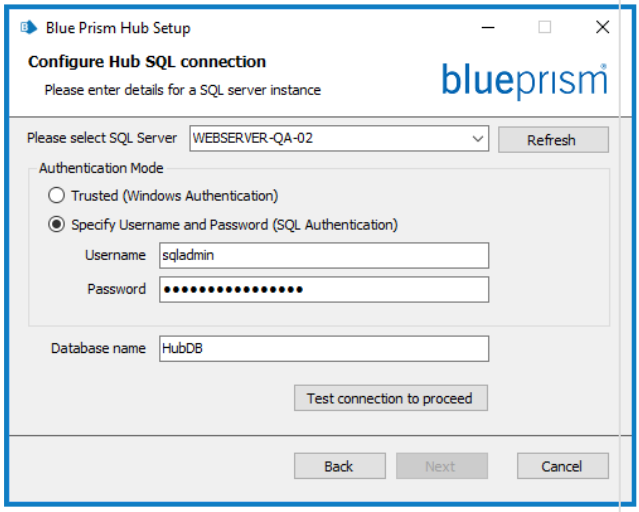
Blue Prismポータルから入手可能なBlue Prism Hubインストーラーをダウンロードして実行し、以下に示すようにインストーラーを進めます。インストーラーは管理者権限で実行する必要があります。

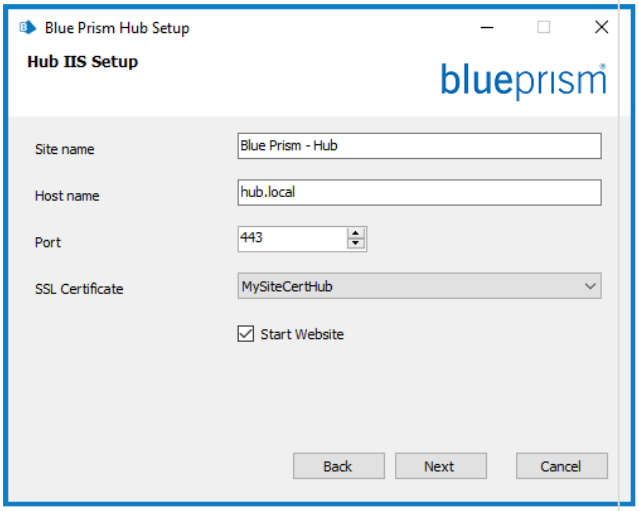
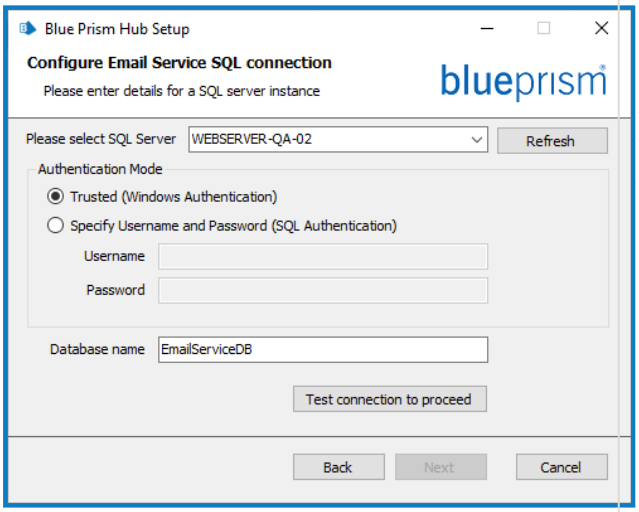
ステップ	インストーラーページ	詳細
1		**ようこそ** 必要に応じて、ドロップダウンリストからインストーラーの言語を変更します。デフォルト言語は英語(米国)です。 [次へ]をクリックします。

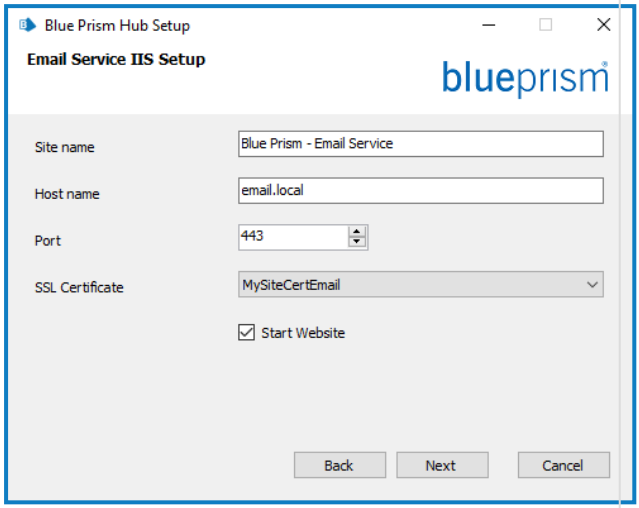
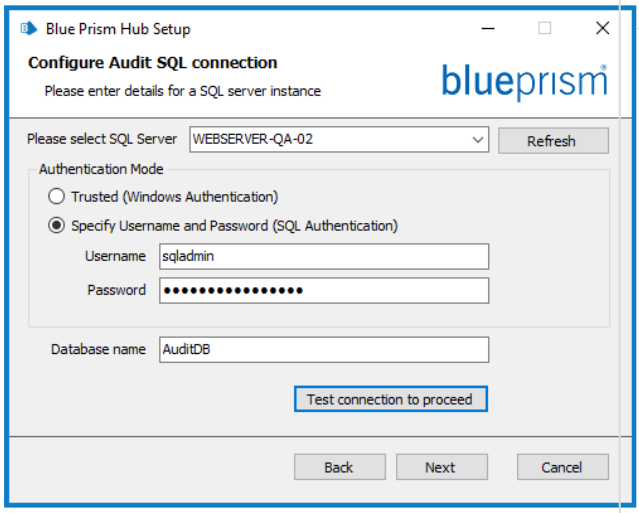
ステップ	インストーラーページ	詳細
2		**ライセンス契約** 使用許諾契約書(EULA)を読み、条件に同意する場合は、チェックボックスを選択します。
3		**前提条件1: サーバーコンポーネント** インストーラーは、前提条件がインストールされていることを確認します。インストールされていないものが特定されます。すべての前提条件がインストールされるまで先に進むことはできません。 アンインストールされた前提条件がある場合は、インストーラーをキャンセルし、不足しているコンポーネントをインストールしてからインストーラーを再起動してください。それ以外の場合、インストールを続行します。

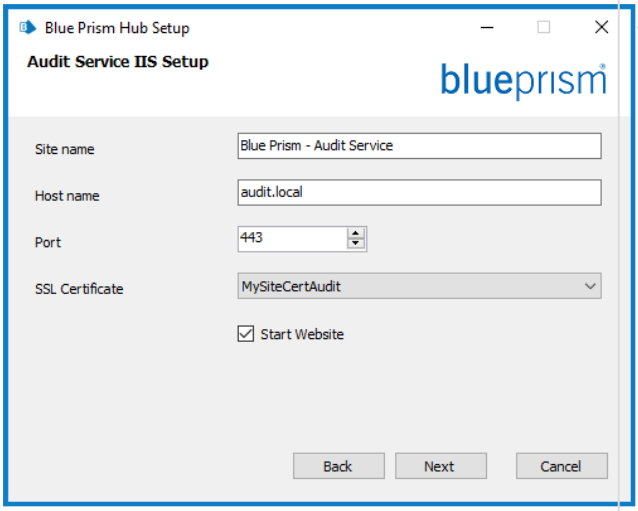
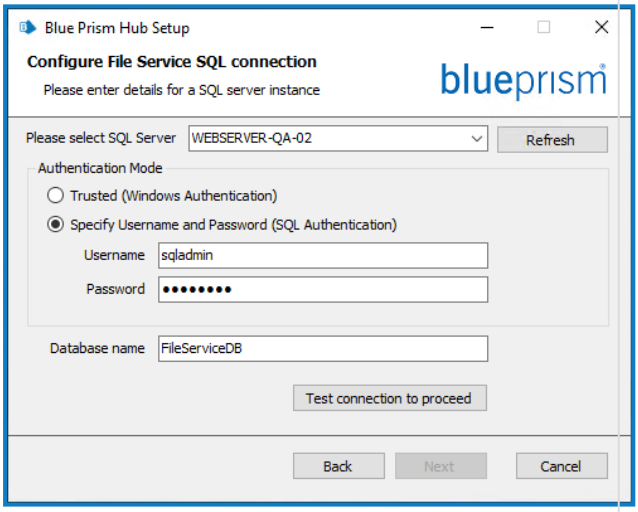
ステップ	インストーラーページ	詳細
4		**前提条件2 – RabbitMQ** メッセージブローカーサーバーのサーバー名またはIPアドレスと、作成したユーザーの認証情報を入力します。 デフォルトのメッセージキューポートは5672です。これは、デフォルトのポートがITサポート組織によって変更された場合にのみ変更する必要があります。 デフォルトでは、 **仮想ホスト**]フィールドは空白です。これを空白にしておくと、RabbitMQルートに接続されます。または、RabbitMQで仮想ホストを設定している場合は、特定のホストに接続できます。 **仮想ホスト**]に、接続するRabbitMQ上の仮想ホストの名前を入力します。仮想ホストはRabbitMQにすでに存在している必要があります。このインストーラーでは新しい仮想ホストは作成されないため、新しい名前を入力することはできません。仮想ホストの詳細については、RabbitMQ Webサイト - 仮想ホストを参照してください。 **プロトコル**]ドロップダウンリストから、使用するプロトコルを選択します。AMQPまたはAMQPSのいずれかを選択できます。 [AMQPS]を選択すると、接続に使用する必要がある証明書を入力するための追加フィールドが表示されます。TLSの設定と証明書の詳細については、RabbitMQウェブサイト - TLSサポートを参照してください。 AMQPSを使用している場合、Blue Prism IISアプリケーションプールにRabbitMQ証明書のフルコントロールを与える必要があります。詳細については、「Hubのインストールのトラブルシューティング ページ63」を参照してください。 **テスト接続**]をクリックして、接続を確認します。テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストが失敗した場合、詳細については「Hubのインストールのトラブルシューティング ページ63」を参照してください。

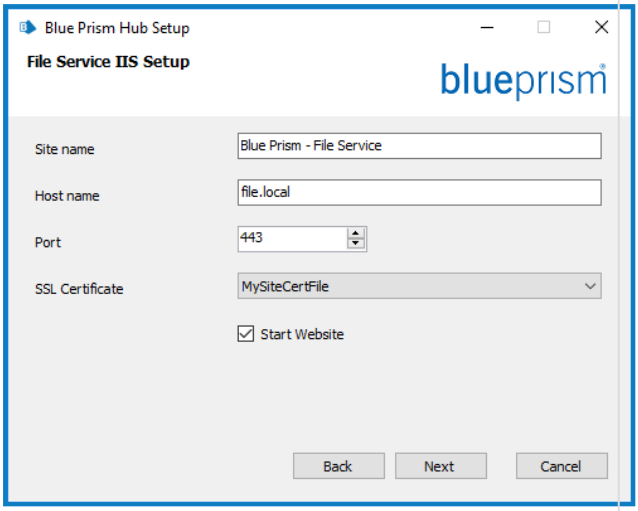
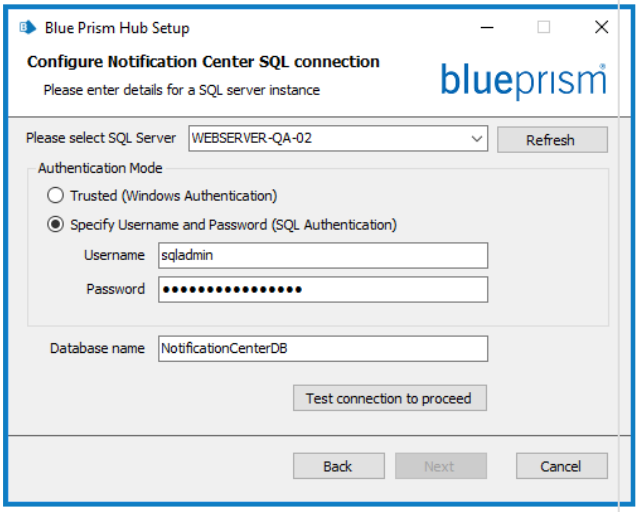
ステップ	インストーラーページ	詳細
5		**インストール先フォルダー** 必要なインストールフォルダーを指定します。デフォルトの場所は、C:\Program Files (x86)\Blue Prismですが、 **[変更]**ボタンを使用して別の場所を選択できます。
6		**Authentication ServerとSQL の接続** Authentication Serverデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • **[Windows認証]**を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • **[SQL認証]**を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 **[接続をテストして続行]**をクリックして、SQL認証情報をテストし、接続を確認します。 テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

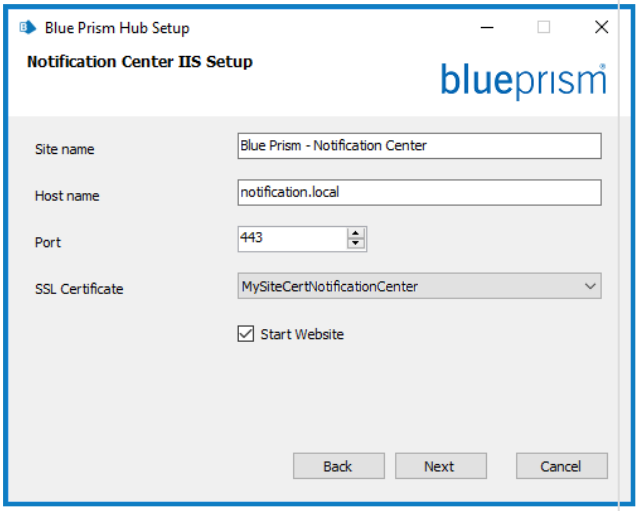
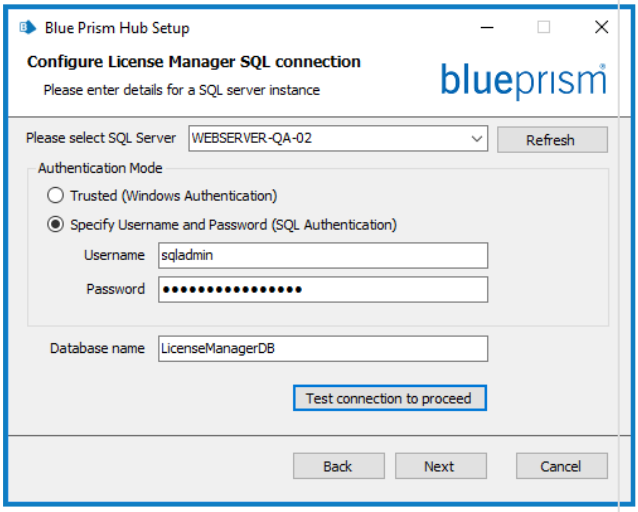
ステップ	インストーラーページ	詳細
7		**Authentication Server IIS のセットアップ** Authentication ServerのWebサイトにIISを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。 インストールが完了すると、Authentication Server Webサイトで IIS機能の**Windows認証**が有効になります。
8		**HubとSQLの接続** Hubデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。 テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

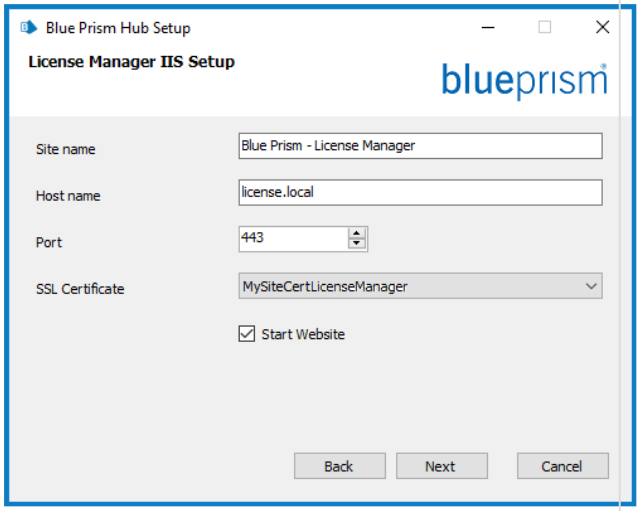
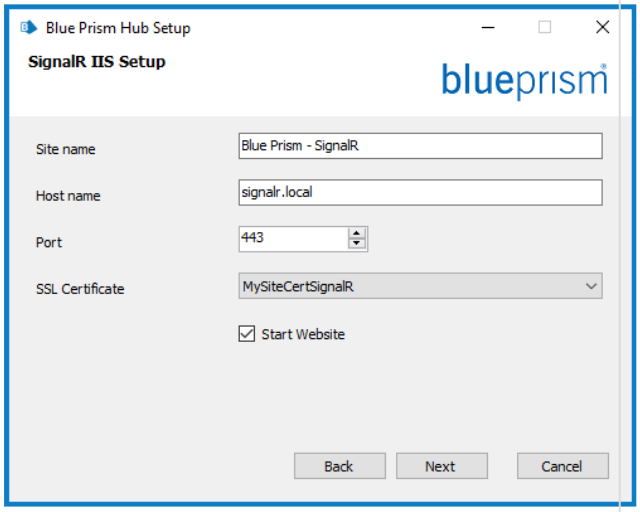
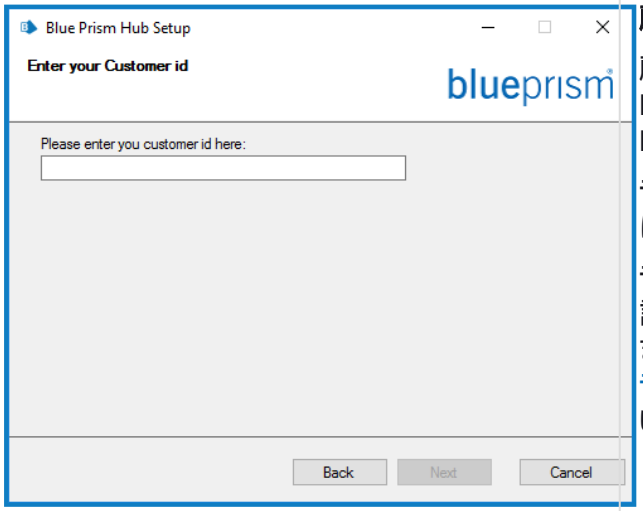
ステップ	インストーラーページ	詳細
9		**Hub IISのセットアップ** HubのWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
10		**Email ServiceとSQLの接続** Email Serviceデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。 テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

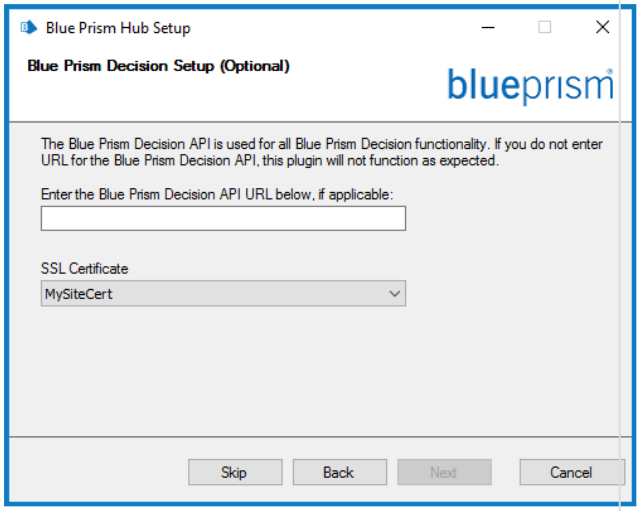
ステップ	インストーラーページ	詳細
11		**Emailサービス IIS のセットアップ** EmailサービスWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
12		**Audit SQL の接続構成** Auditデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

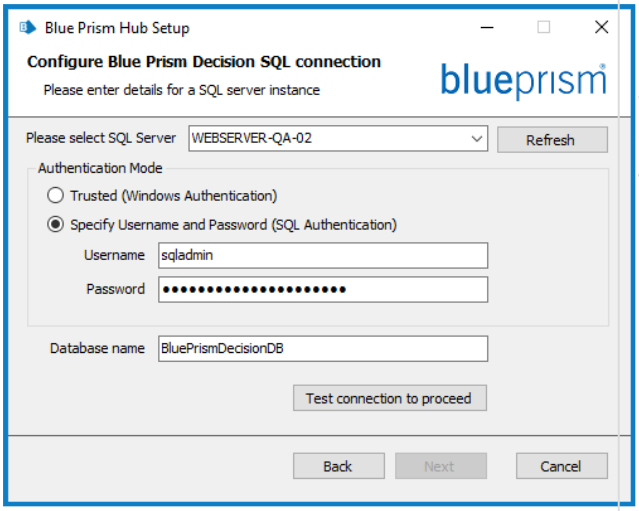
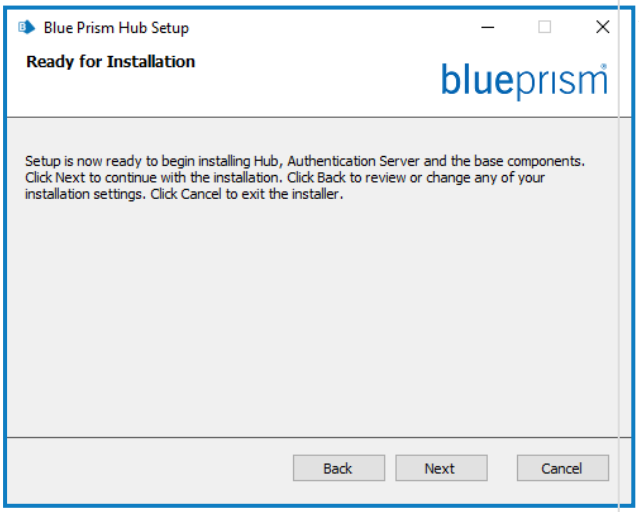
ステップ	インストーラーページ	詳細
13		**Audit Service IIS のセットアップ** Audit ServiceのWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
14		**File Service SQL 接続の構成** File Serviceデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

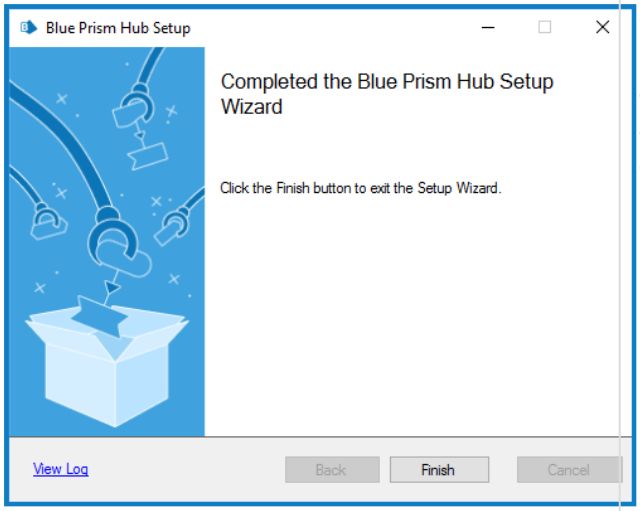
ステップ	インストーラーページ	詳細
15		**File Service IISのセットアップ** File ServiceのWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
16		**通知センターとSQLの接続** 通知センターのデータベース設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

ステップ	インストーラーページ	詳細
17		**Notification Center IISのセットアップ** 通知センターのWebサイトを設定します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**]はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
18		**License ManagerとSQLの接続** License Managerのデータベース設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。

ステップ	インストーラーページ	詳細
19		**License Manager IISのセットアップ** License ManagerのWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**] はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
20		**SignalR IISのセットアップ** SignalRのWebサイトを構成します。以下を行う必要があります。 • サイト名を入力します。 • ホスト名を入力します – これはサイトのURLとして使用されます。ホスト名を選択するときは、DNSとドメイン構造を考慮します。 • ポート番号を入力します。 • 適切なSSL証明書を選択します。 • [**ウェブサイトを開始**] はオンのままにしておきます。ただし、インストールの終了時にWebサイトが自動的に開始されないようにする場合を除きます。
21		**顧客IDを入力** 顧客IDを入力します。このIDは、ALMまたはInteractの製品ライセンスを受け取ったときにBlue Prismから提供されます。 ライセンス済みプラグインを購入していない場合は、独自の値を入力できます。 ライセンス済みプラグを後で購入する場合は、設定ファイル内で顧客IDを変更する必要があります。詳細については、「Hubのインストールのトラブルシューティング ページ63」を参照してください。

ステップ	インストーラーページ	詳細
22		**Blue Prism Decisionの設定 (オプション)** Blue Prism Decisionを使用する場合は、次の操作を行う必要があります。 • Blue Prism Decision Model Serviceコンテナのに続けてポート番号を入力します。URLはhttps://<FQDN>:<ポート番号>の形式にする必要があります。 例：https://decision.blueprism.com:50051。 URLは証明書に指定されたFQDNと一致させる必要があります。ポート番号は、コンテナの実行時に定義したポートと一致させる必要があります。詳しくは、「Blue Prism Decisionをインストールする」を参照してください。 • 適切なSSL証明書を選択します。 Blue Prism Decisionを使用しない場合は、**スキップ**]をクリックします。 [インストール準備完了]画面が表示されます。

ステップ	インストーラーページ	詳細
23		**Blue Prism Decision SQL接続** Blue Prism Decisionデータベースの設定を構成するSQL Serverのホスト名またはIPアドレスと、データベースを作成するためのアカウントの認証情報を指定します。 • [**Windows認証**]を選択した場合、アカウントには適切な許可が必要です。詳細については「」「Windows認証を使用してをインストールする ページ50」を参照してください。 • [**SQL認証**]を選択した場合、ユーザー名とパスワードを入力します。 ⚠ データベースのパスワードには、等号(=)またはセミコロン(;)が使用されていないことを確認します。これらの文字はサポートされておらず、データベースに接続しようとすると問題が発生します。 データベース名は、デフォルト値のままにするか、必要に応じて変更できます。 [**接続をテストして続行**]をクリックして、SQL認証情報をテストし、接続を確認します。 テストの結果を示す通知が表示されます。テストが成功した場合のみ、次のステップに進むことができます。テストに失敗した場合は、「Hubのインストールのトラブルシューティング ページ63」で詳細を確認してください。
24		**インストール準備完了** [**次へ**]をクリックしてHubをインストールします。

ステップ	インストーラーページ	詳細
25		**インストールの完了** インストールに失敗した場合は、**[ログを表示]**オプションに、発生したエラーの詳細が表示されます。詳細については、「Hubのインストールのトラブルシューティング ページ63」を参照してください。

Authentication Server SAML 2.0の拡張機能をインストールする

所属組織がユーザー用にSAML 2.0認証を使用する場合は、HubとAuthentication Serverがインストールされているwebサーバーに Authentication Server SAML 2.0拡張機能をインストールする必要があります。詳細については、Digital Exchangeの「Authentication Server SAML 2.0拡張機能4.7インストールガイド」を参照してください。

所属組織がユーザー用にSAML 2.0 認証を使用しない場合は、他にインストールが必要なものはありません。

Windows認証を使用してをインストールする

インストールの実行時に使用するアカウントには、インストールを実行するために関連SQL Serverの許可が必要です。つまり、sysadminまたはdbcreatorの固定サーバー役割のメンバーシップです。

インストールプロセス中にWindows認証を選択した場合は、通常の操作中にタスクとプロセスを実行するために必要な許可が付与されているアプリケーションプールとサービスのためにWindowsサービスアカウントを使用する必要があります。Windowsサービスアカウントには、以下が必要です。

- SQLデータベースプロセスを実行する機能(「」「最小限必要なSQLの権限 ページ17」「」を参照)。
- 必要な証明書の許可。
- IISアプリケーションプール上の所有権。
- Hubによってインストールされ たWindowsサービスの所有権。

⚠ Hubで環境を作成する前に、Windowsアカウントを使用するアプリケーションプールとサービスを割り当てる必要があります。環境を作成した後にアカウントを割り当てると、パフォーマンスの問題が発生する可能性があります。たとえばInteractプラグインを使用して作成されたフォームがInteractのユーザーに表示されない場合があります。

Windowsサービスアカウントを証明書の所有者として割り当てる

Windowsサービスアカウントには、BluePrismCloud証明書の許可を付与する必要があります。これには、以下の操作を行います。

1. Webサーバーで、 [証明書マネージャー]を開きます。これを行うには、Windowsタスクバーの検索ボックスに [*証明書*]と入力し、 [**コンピューター証明書の管理**]をクリックします。
2. ナビゲーションペインで [**個人**]を展開し、 [**証明書**]をクリックします。
3. BluePrismCloud_Data_Protection証明書とBluePrismCloud_IMS_JWT証明書の両方について、以下の手順に従ってください。
   a. 証明書を右クリックし、 [**すべてのタスク**]を選択して [**プライベートキーの管理...**]をクリックします。
      証明書の許可ダイアログが表示されます。
   b. [**追加**]をクリックし、サービスアカウントを入力して [**OK**]をクリックします。
   c. [**グループまたはユーザー名**]リストでサービスアカウントが選択されている場合、 [**{account name}の許可**]のリストで [**フルコントロール**]が選択されていることを確認します。
   d. [**OK**]をクリックします。
      サービスアカウントが証明書にアクセスできるようになりました。

アプリケーションプールにWindowsサービスアカウントを割り当てる

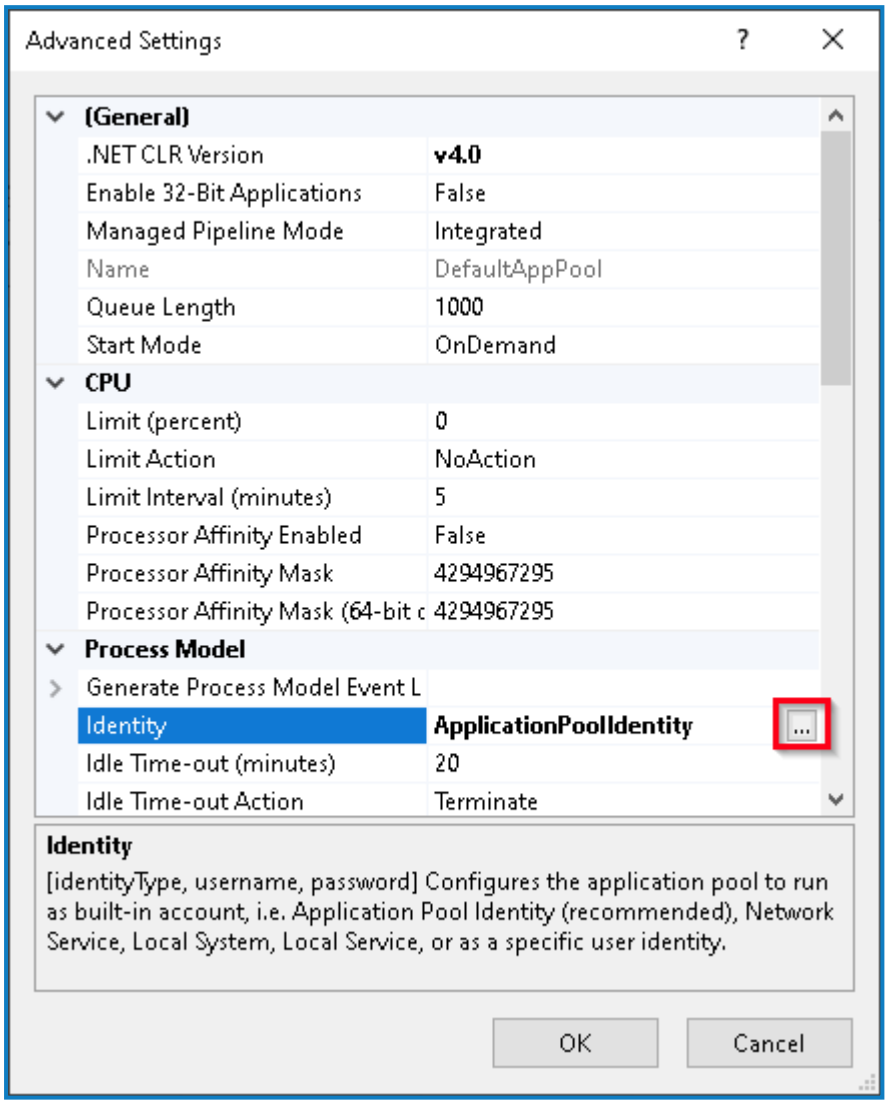
デフォルトでは、アプリケーションプールは「ApplicationPoolIdentity」というIDで作成されます。インストーラーの完了後、アプリケーションプールを管理するためにWindowsサービスアカウントを割り当てる必要があります。これには、以下の操作を行います。

1. WebサーバーでInternet Information Services(IIS)マネージャーを開きます。
2. [接続]パネルでホストを展開し、 [**アプリケーションプール**]を選択します。
3. **ID**列の値を確認します。
   アプリケーションプールのIDは、特定のWindowsサービスアカウントと一致する必要があります。

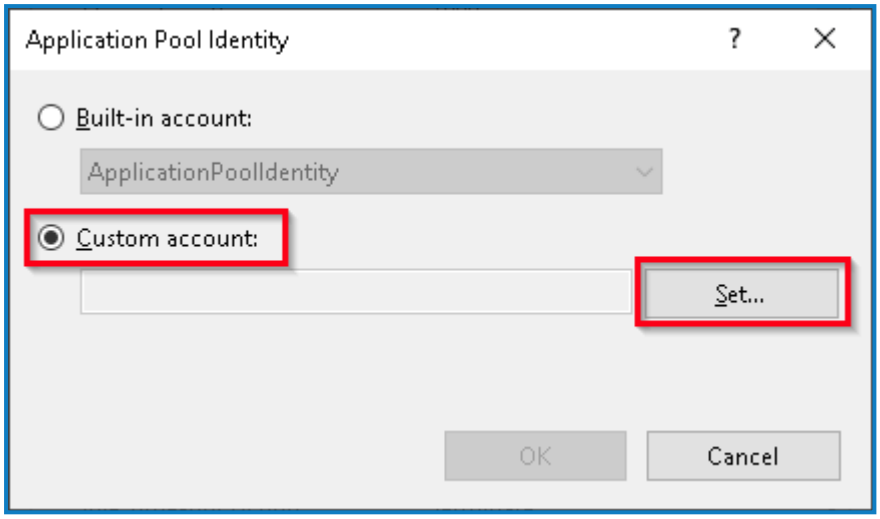
4. ID列にApplicationPoolIdentityがあるアプリケーションプールの場合は、その行を右クリックして **詳細設定...**] を選択します。

   [詳細設定] ダイアログが表示されます。

5. [ID] 設定を選択し、 [...(省略記号)] ボタンをクリックします。



6. [アプリケーションプールID]ダイアログで **[カスタムアカウント]**を選択し、 **[設定...]**をクリックします。



[認証情報の設定]ダイアログが表示されます。

7. 必要なWindowsサービスアカウントの認証情報を入力し、 **[OK]**をクリックします。
8. 変更の必要なアプリケーションプールに対して、この手順を繰り返します。
9. RabbitMQサービスを再起動します。
10. すべてのアプリケーションプールを再起動します。
11. IISを再起動します。

Audit Serviceに問題がある場合は、Windowsサービスアカウントに監査サービスリスナーと監査データベースへのアクセス権があることを確認します。

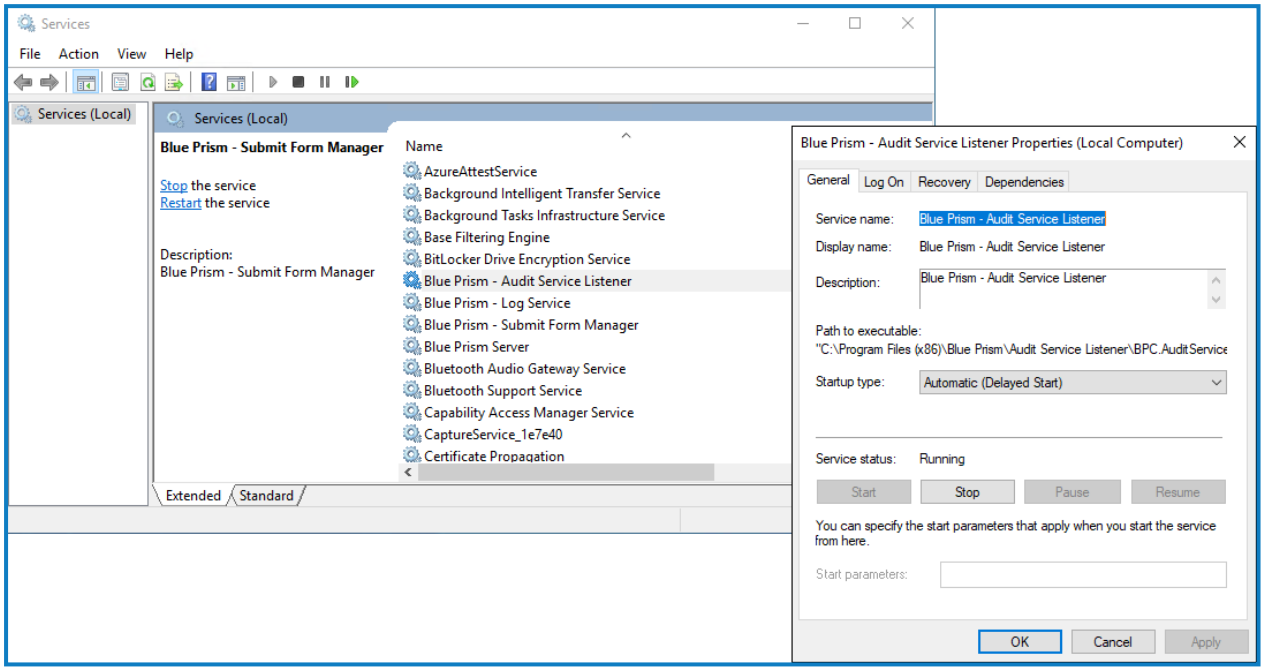
Windowsサービスアカウントをサービスに割り当てる

次のサービスを管理するには、Windowsサービスアカウントを割り当てる必要があります。

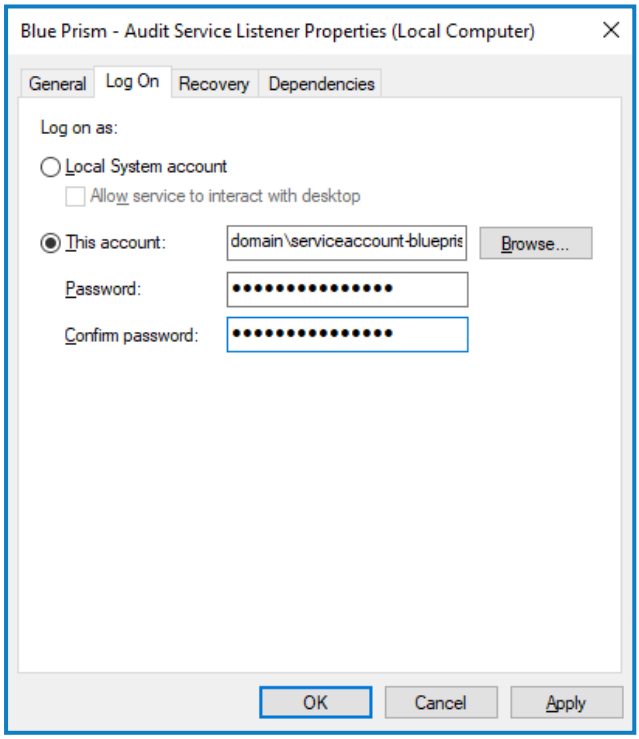
- Blue Prism – 監査サービスリスナー
- Blue Prism - ログサービス

これには、以下の操作を行います。

1. Webサーバーで、 [サービス]を開きます。
2. サービスを右クリックし [**プロパティ**]をクリックします。



3. [ログオン]タブで [**このアカウント**]を選択し、アカウント名を入力するか [**参照**]をクリックして、使用するアカウントを検索します。



4. アカウントのパスワードを入力し、 [OK]をクリックします。
5. [サービス]ウィンドウでサービスを右クリックし、 [**再起動**]をクリックします。
6. 他のBlue Prismサービスについても同じ手順を繰り返します。

初期Hub構成

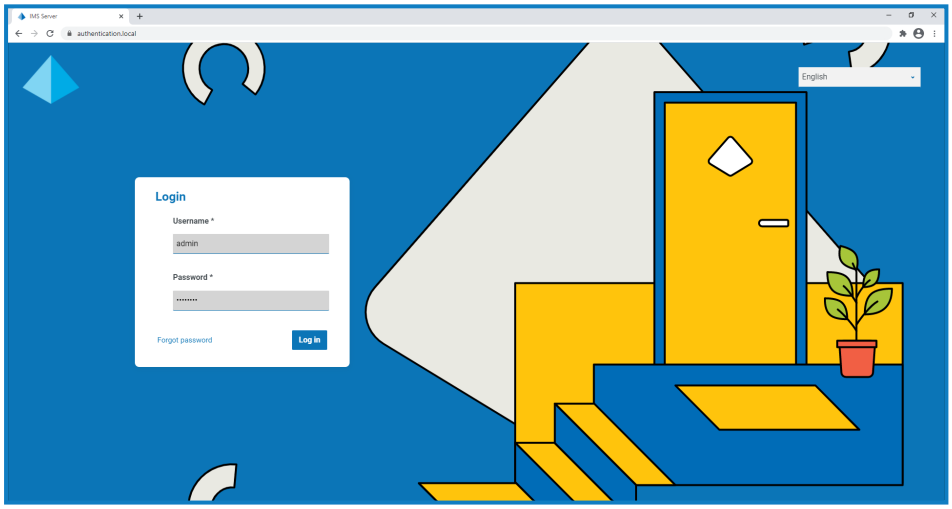
Blue Prism Interactを使用する場合は、この構成を実行する前にInteractをインストールしてください。詳細については、「」「Interactインストールガイド」を参照してください。

これで、初回ログインを行い、システム全体の構成を実行できるようになりました。

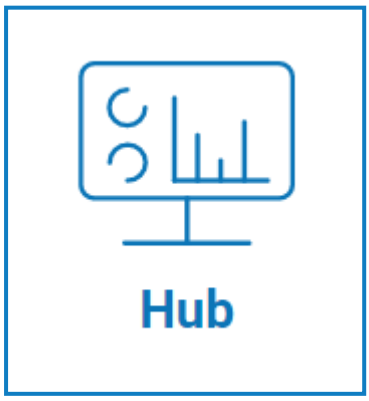
Authentication Serverのログインページを開くと、Webブラウザーからローカリゼーション設定が自動的に適用されます。ログインページとHubは、ブラウザーで設定された言語設定と最も互換性のある言語で表示されます。ブラウザー設定で選択した言語がサポートされていない場合は、英語がデフォルトとして使用されます。必要に応じて、ログインページのドロップダウンリストから使用する言語を手動で変更できます。

Hubのインストールと構成プロセスを視聴するには、Blue Prism Hubのインストールビデオを参照してください。

1. ブラウザーを起動し、Authentication ServerのWebサイトに移動します。この例では、https://authentication.localです。



2. 次のデフォルトの認証情報を使用してログインします。
   - **ユーザー名：**admin
   - **パスワード**：Qq1234!!
3. **[Hub]**をクリックして、HubのWebサイトを起動します。



4. デフォルトのパスワードを新しいセキュアなパスワードに変更します。
   a. Hubで、プロファイルアイコンをクリックして設定ページを開き、 [**プロファイル**] をクリックします。
   b. [**パスワードを更新**] をクリックします。
      [パスワードを更新] ダイアログが表示されます。
   c. 現在の管理者パスワードを入力してから、新しいパスワードを入力し、繰り返します。
   d. [**更新**] をクリックします。
      管理者パスワードが変更されます。

データベース設定

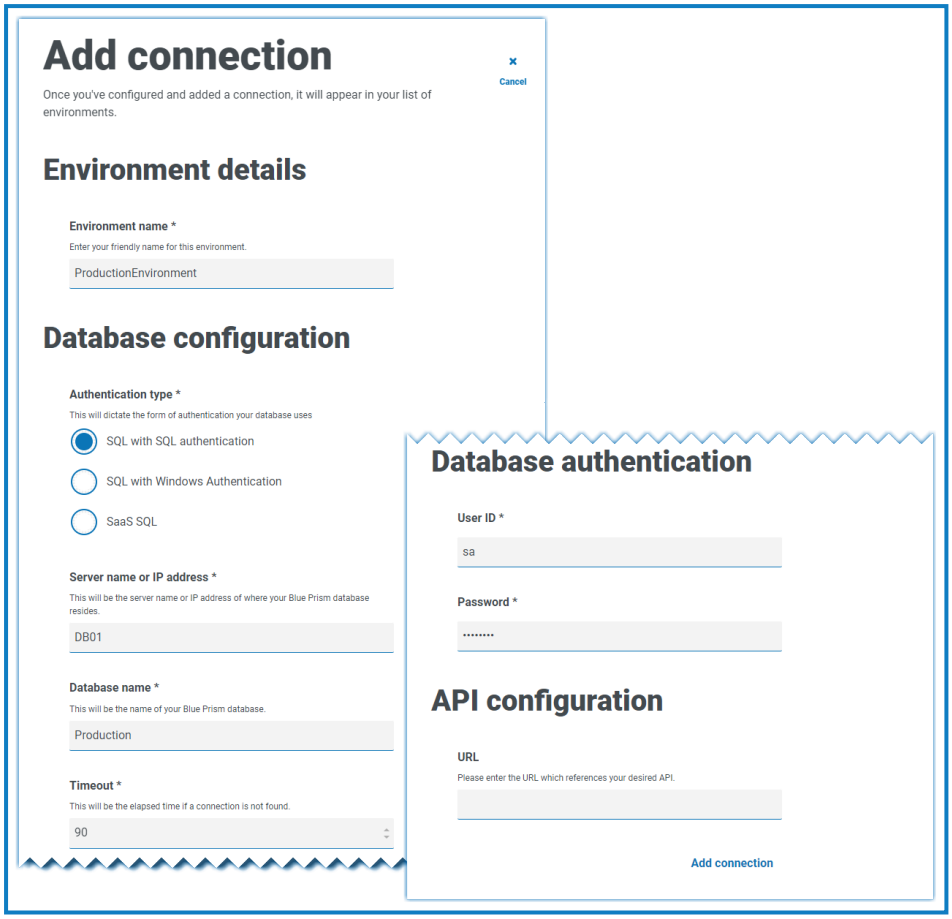
⚠ Windows認証を使用する環境がインストールされている場合は、Windowsアカウントにアプリケーションプールとサービスを事前に割り当ててから、Hubに環境を作成する必要があります。そうしない場合、Interactプラグインを使用して作成されたフォームがInteractユーザーに表示されないなどのパフォーマンスの問題が発生することがあります。詳細については、「」「Windows認証を使用してをインストールするページ50」「」を参照してください。

SSL暗号化は、Hubインストーラーでインストールされるすべてのデータベースで使用されます。HubがBlue Prismデータベースに正常に接続するには、SSL暗号化を使用するようにBlue Prismデータベースも構成する必要があります。詳細については、「前提条件 ページ9」を参照してください。

Blue Prismデータベースへのアクセスを構成するには、

1. プロファイルアイコンをクリックして設定ページを開き、 [**環境マネージャー**] をクリックします。
   [環境管理] ページが表示されます。

2. **接続を追加**]をクリックし、Blue Prismデータベースの詳細を入力します。例を次に示します。



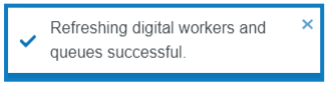
タイムアウト値は秒単位です。

3. **接続を追加**]をクリックして、詳細を保存します。

接続が作成され、環境マネージャーに表示されます。

4. 環境マネージャーで、新しい接続の更新アイコンをクリックします。これにより、Hub内の情報が、データベースに保持されているDigital Workforceとキューで更新されます。

接続が成功すると、Hubのユーザーインターフェイスの右上に次のメッセージが表示され、インストールが検証されます。



メッセージが表示されない場合、詳細については「Hubのインストールのトラブルシューティング ページ63」を参照してください。

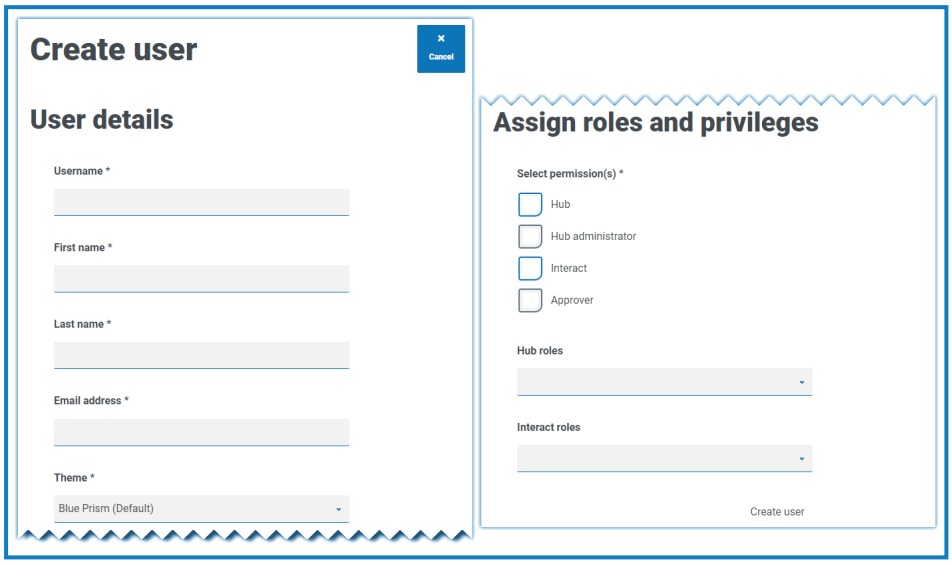
管理者を作成する

Hub構成を完了するには、有効な情報を持つ管理者アカウントを作成する必要があります。汎用管理者アカウントを使用して構成を完了すべきではありません。その理由は次のとおりです。

- メール設定をテストするには、実際のメールアドレスが必要です。
- 完全な監査証跡では、一般アカウントではなく、指定されたユーザーを使用して構成を変更する必要があります。

新しい管理者を作成するには、次の手順に従います。

1. プロファイルアイコンをクリックして設定ページを開き、 **[ユーザー]** をクリックします。
2. **[ユーザー]** ページで、 **[ユーザーを追加]** をクリックします。
   [ユーザーを作成] セクションが表示されます。



3. 次の詳細を入力します。
   - ユーザー名
   - 名
   - 姓
   - メールアドレス
4. **[Hub]** 許可および **[Hub管理者]** 許可を選択します。
5. **[ユーザーを作成]** をクリックします。
   [パスワードを作成] ダイアログが表示されます。
6. **[ユーザーのパスワードを手動で更新]** を選択します。

> パスワードは、Hub内の制限に従う必要があります。

7. **[続行]** をクリックして、画面の指示に従います。
8. 最後に、 **[作成]** をクリックしてユーザーを作成します。
   新しいユーザーがユーザーのリストに表示されます。
9. Hubからログアウトし、新しいアカウントを使用して再度ログインします。

メールの設定

SMTPのセットアップを完了することをお勧めします。これにより、パスワードを忘れたメールなど、システムメールの送信が可能になります。

メールの送信に使用するメールアドレスは、プロファイルの設定時に設定されます。

> メール設定を構成するには、「管理者を作成する前のページ」で作成したユーザーでログインする必要があります。これは、構成プロセスがテストメールを送信するため、有効なメールアドレスを持つユーザーが必要なためです。

次のいずれかの認証方法を使用して、メール設定を構成できます。

- **ユーザー名とパスワード** – この認証方法では、次の情報が必要です。
  - **SMTPホスト** – SMTPホストのアドレス。
  - **ポート番号** – 送信メールサーバーが使用するポート番号。
  - **送信者のメール** – メールを送信するときに使用されるメールアドレス。メールの受信者は、これを差出人のアドレスとして表示します。
  - **暗号化** – メールサーバーがメールを送信するために使用する暗号化方法。
  - **ユーザー名** – SMTP認証のユーザー名。
  - **パスワード** – アカウントのパスワード。
  - **テストメールの受信者** – テストメールがこのメールアドレスに送信されます。これは、変更を行うユーザーのメールアドレスがデフォルトとなり、変更することはできません。
- **Microsoft OAuth 2.0** – この認証方式では、次の情報が必要です。
  - **送信者のメール** – メールを送信するときに使用されるメールアドレス。メールの受信者は、これを差出人のアドレスとして表示します。
  - **アプリケーションID** – この情報は、Azure ADで定義されたアプリケーション(クライアント) IDであり、ITサポートチームによって提供されます。
  - **ディレクトリID** – この情報は、Azure ADで定義されたディレクトリ(テナント) IDであり、ITサポートチームによって提供されます。
  - **クライアントシークレット** - これはAzure ADによって生成されたクライアントシークレットであり、ITサポート チームによって提供され、認証プロセスを制御します。

    > Azure ADでこれらの詳細を見つける方法については、「Microsoftドキュメント」を参照してください。

  - **テストメールの受信者** – テストメールがこのメールアドレスに送信されます。これは、変更を行うユーザーのメールアドレスがデフォルトとなり、変更することはできません。

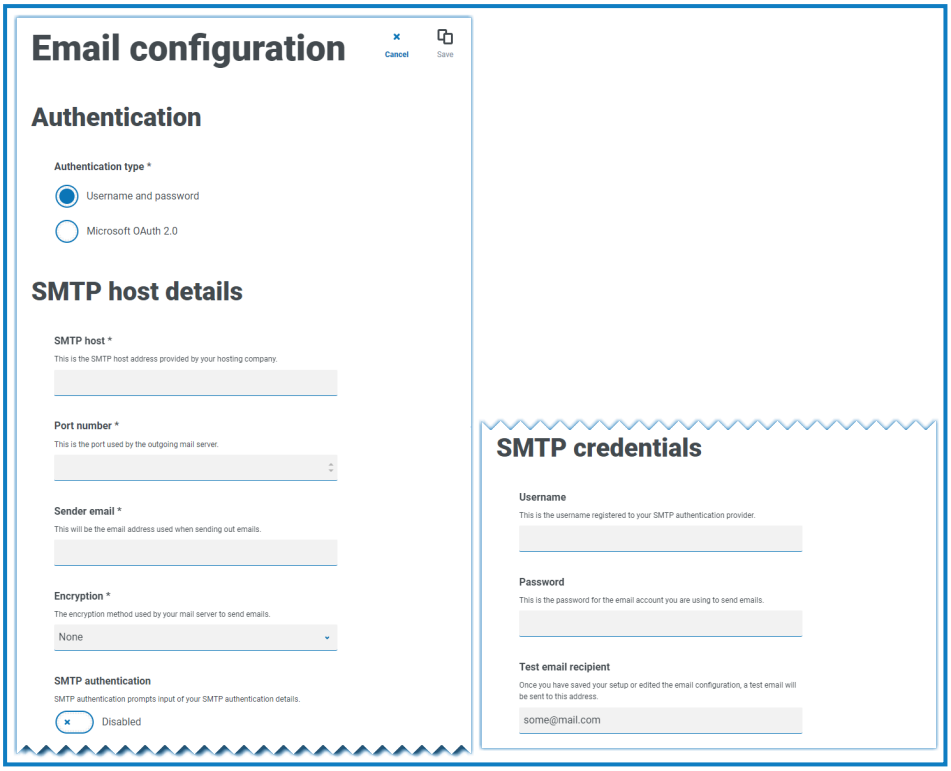
> Microsoft OAuth 2.0を使用している場合は、Azure Active DirectoryのMail.Sendアクセス許可を有効にする必要があります。これは、Azure Active Directoryのアプリケーションプロパティの [APIのアクセス許可] タブにあります。詳細については、「Hubのインストールのトラブルシューティング ページ 63」を参照してください。

メール設定を構成するには:

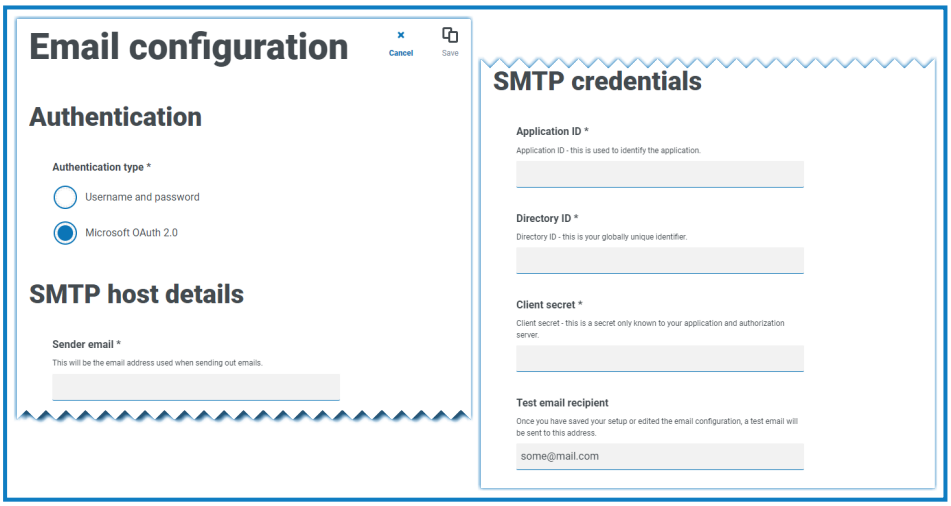
1. プロファイルアイコンをクリックして [設定] ページを開き、 [**メール設定**] をクリックします。
2. [**編集**] をクリックします。
3. 使用する認証タイプを選択します。

   ページ上のフィールドは、上記の選択内容によって異なります。選択したものが以下の場合 :

- [ユーザー名とパスワード]の場合、[メール設定]ページは次のように表示されます。



- [Microsoft OAuth 2.0]の場合、[メール設定]ページは次のように表示されます。



4. 必須情報を入力します。
5. [保存]をクリックします。

メール設定を正しく構成できない場合は、メッセージブローカーサーバーがにアクセスできないことが原因と考えられます。詳細については、「Hubのインストールのトラブルシューティング ページ63」を参照してください。

メール設定の構成の詳細については、「」「」「」「Hub管理者ガイド」を参照してください。

Authentication Serverを構成する

Authentication Serverを使用すると、ユーザーはBlue Prism、Hub、Interactに同じ認証情報でログインできます。Authentication ServerはBlue Prism 7.0以降と互換性があります。

Blue Prism 6の使用

所属組織がBlue Prism 6を使用している場合：

- Authentication Serverを使用してBlue PrismとHub間のユーザーを認証することはできません。ユーザーは、独立したアカウントを使用してBlue PrismとAuthentication Serverにログインできます。
- Hubで認証設定を構成してください。詳細については、「認証設定 次のページ」を参照してください。

Blue Prism 7の使用

所属組織がBlue Prism 7を使用している場合は、ユーザーがBlue Prismの複数のアプリケーションで同じアカウントを使用することを組織が希望するかどうかを検討します。

- 組織が同じユーザーアカウントの使用を希望する場合：
    1. Authentication Serverを構成します。詳細については「Authentication Server構成ガイド」を参照してください。
    2. Hubで認証設定を構成します。詳細については、「認証設定 次のページ」を参照してください。
- 組織が同じユーザーアカウントの使用を希望しない場合は、Hubで認証設定の構成のみを行います。詳細については、「認証設定 次のページ」を参照してください。

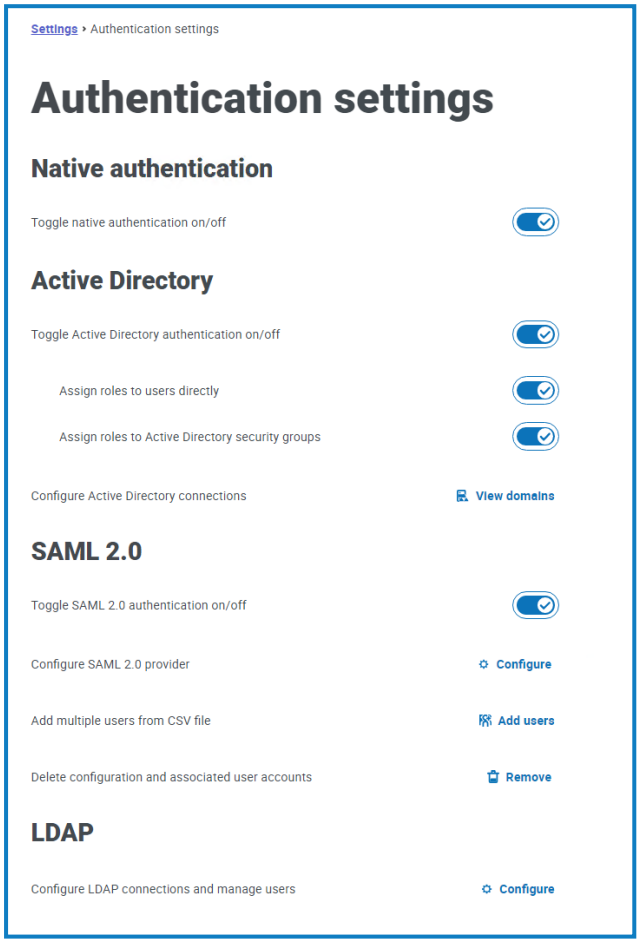
構成手順を視聴するには、Authentication Serverの構成動画を参照してください。

認証設定

Hub環境の認証設定は、 認証設定]ページで構成できます。

認証設定を構成するには:

1. プロファイル]アイコンをクリックして 設定]ページを開き **認証設定**]をクリックします。
   認証設定]ページが表示されます。



2. 使用する認証タイプと、必要に応じて関連するオプションを選択します。
   - **ネイティブ認証** – 新しい環境またはHubをアップグレードするとデフォルトで有効になります。
   - **Active Directory** - Authentication Serverをホストするサーバーがactive Directoryドメインのメンバーである場合にのみ有効にできます。有効にすると、Active Directoryドメインとユーザーの役割管理も構成できます。
   - **SAML 2.0** – このオプションはAuthentication Server SAML 2.0拡張機能が、Authentication Serverがインストールされているホスト Webサーバーにインストールされている場合にのみ、 認証設定]ページに表示されます。
   - **LDAP** – LDAP認証を有効にするには、LDAP接続を少なくとも1つ作成する必要があります。

組織の要件に基づいて、次のオプションがあります。

- すべての認証タイプを有効にします。
- 1つ以上の認証タイプを無効にします。無効にできるのは、無効にされるタイプとは異なる認証タイプでログインするよう設定された管理者ユーザーがシステムに1人以上いる場合に限られます。

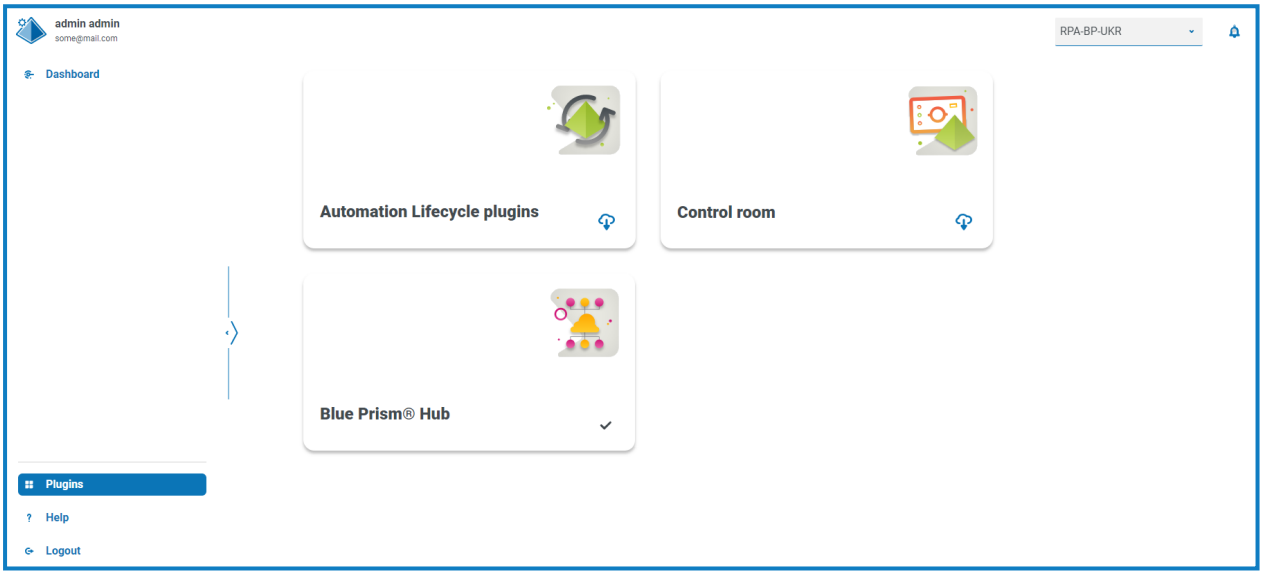
認証設定の構成の詳細については、「」「Hub管理者ガイド」を参照してください。

プラグインをインストールする

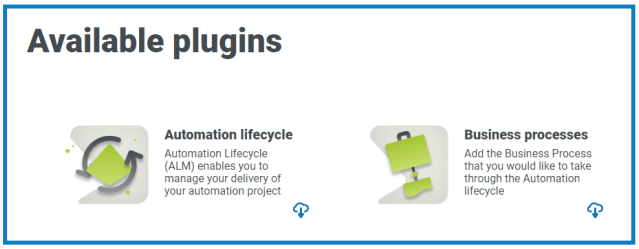
インストールの一部として、HubはHubプラグインを自動的にインストールします。ただし、ALMまたはInteractを使用する場合は、まず無償で入手可能なビジネスプロセスプラグインをインストールする必要があります。

このインストール手順を視聴するには、Business Processプラグインのインストールビデオを参照してください。

1. Hubにログインします。
2. [**プラグイン**]をクリックして、プラグインリポジトリを開きます。



3. [**自動化ライフサイクル**]をクリックします。
使用可能なプラグインコンポーネントが表示されます。



4. [**ビジネスプロセス**]タイルの下隅にあるダウンロードアイコンをクリックして、インストールを開始します。
サイトが再起動します。

Hubのインストールのトラブルシューティング

次のセクションでは、インストール中かインストールが成功したかどうか検証しているときに特定の問題が生じる場合のガイダンスを紹介します。

メッセージブローカーのコネクティビティ

Webサーバーとメッセージブローカー間のコネクティビティを確認するには、RabbitMQ管理コンソールがWebブラウザーからアクセス可能であることを確認します。

接続に失敗する理由はいくつかあります。

- ネットワークコネクティビティを検証する - すべての関連デバイスが同一ネットワークに接続され、通信できることを確認します。
- ファイアウォール - サーバー自体またはネットワーク内のファイアウォールが通信を阻止していないことを確認します。

デフォルトでは、RabbitMQ管理コンソールはポート15672で通信します。メッセージブローカーキューでは、デフォルトで異なるポート、5672が使用されます。すべてのポートでファイアウォールのTCPアクセスを確認する必要があります。これは、特に、IT組織が非デフォルトポートを指定している場合に当てはまります。

データベースコネクティビティ

インストーラー内の **接続をテストして続行**]ボタンで、以下を確認します。

- データベースが存在する場合：
  - 接続できること。
  - データベースをホストするSQL Serverに有効な証明書が適用されていること。
  - アカウントにデータベースの読み取り、書き込み、編集の権限があること。
- データベースが存在しない場合：
  - アカウントにデータベースを作成する権限があること。
  - SQL Serverに有効な証明書が適用されていること。

これらの要件を満たすことができない場合、インストールは停止します。

LANでSQL Serverに接続できない場合、実行できるチェックが多数あります。

- ネットワークコネクティビティを検証する - すべての関連デバイスが同一ネットワークに接続され、通信できることを確認します。
- SSL暗号化 – SQL Serverに有効な証明書があることを確認します。詳細については、「前提条件 ページ9」「」を参照してください。
- SQL認証情報 - SQL認証情報と、ユーザーがSQL Server上で適切な許可を持っていることを検証します。
- ファイアウォール - サーバー自体またはネットワーク内のファイアウォールが通信を阻止していないことを確認します。
- SQL Server Browserサービス - SQLインスタンスを検索できるようにSQL Server上のSQL Server Browserサービスが有効になっていることを確認します。SQL Server Expressの場合、このサービスは通常、デフォルトで無効です。
- TCP/IPコネクティビティを許可 - リモートコネクティビティがSQLに必要な場合、SQLインスタンスに対してTCP/IPコネクティビティが有効になっていることを確認します。Microsoftは、SQLの各バージョンに特化した、SQL Serverに対してTCP/IPネットワークプロトコルを有効にするための手順を提示する記事を用意しています。

インストーラーの実行時に、データベースエラーでインストールプロセスが失敗した場合、以下を参照してください。その後、Webサーバーがデータベースと SQL接続できることを確認します。これは、上記の理由のいずれかが原因である可能性があります。

```
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.
```

失敗の原因のもう1つの可能性は、インストーラー内のデータベースの作成に使用するアカウントが、データベースの作成に必要な権限を持っていないことです。

最後に、ソフトウェアの削除後にインストールが再インストールされた場合です。その後、同じデータベース名が使用されている場合は、元のデータベースをバックアップしてドロップしてから、再インストールする必要があります。

Webサーバー

インストールプロセス中、インストーラーはすべての前提条件が満たされていることを確認します。前提条件がインストールされていない場合は、インストーラーをキャンセルし、前提条件がインストールされてから、インストーラープロセスを再開することをお勧めします。

詳細については、「」「前提条件 ページ9」「」を参照してください。

RabbitMQをAMQPSと使用する

RabbitMQでAMQPS(Advanced Message Queuing Protocol - Secure) を使用している場合、Hubインストールの一部として作成されたアプリケーションプールにRabbitMQ証明書の許可を付与する必要があります。これには、以下の操作を行います。

1. Webサーバーで、 [**証明書マネージャー**] を開きます。これを行うには、Windowsタスクバーの検索ボックスに *[証明書]* と入力し、 [**コンピューター証明書の管理**] をクリックします。
2. Hubのインストール中にRabbitMQ AMQPSで使用するために特定された証明書に移動して右クリックし、 [**すべてのタスク**] を選択して [**プライベートキーの管理...**] をクリックします。
   証明書の許可ダイアログが表示されます。
3. [**追加**] をクリックし、次のアプリケーションプールを [**オブジェクト名を入力して選択**] フィールドに入力します。

   ```
   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;
   ```

   これらはデフォルトのアプリケーションプール名です。インストール中に異なる名前を入力した場合は、使用している名前がリストに反映されていることを確認してください。
4. Windows認証を使用している場合は、次のWindowsサービスに使用されるサービスアカウントの名前も追加します。
   - Blue Prism – 監査サービスリスナー
   - Blue Prism - ログサービス

5. **名前の確認**]をクリックします。

   名前を検証します。検証されない場合は、使用しようとしているアプリケーションプールまたはサービスアカウントと名前が一致することを確認し、必要に応じて修正します。

6. **OK**]をクリックします。
7. **グループまたはユーザー名**リストで各アプリケーションプールを順番に選択し、**{account name}の許可**]のリストで**フルコントロール**]が選択されていることを確認します。
8. **OK**]をクリックします。

   これで、アプリケーションプールは証明書にアクセスできるようになりました。

Interactもインストールする場合は、Interactのインストール中に作成されたアプリケーションプールに対してもこれを実行する必要があります。詳細については、「Interactインストールガイド」を参照してください。

File Service

File ServiceがAuthentication ServerおよびHubのイメージを検索できない場合、これはBlue Prism製品のアンインストールと再インストールが原因です。この問題は、初回インストールでは発生しません。

削除処理中は、データベースは削除されないため、再インストールで同じデータベース名が使用されている場合は、File ServiceとURLへの元のパスが使用されます。

これを回避するには、削除プロセスの実行後にデータベースを削除またはクリーンアップして以前のパスを削除するか、再インストール時に代替のデータベース名を使用します。

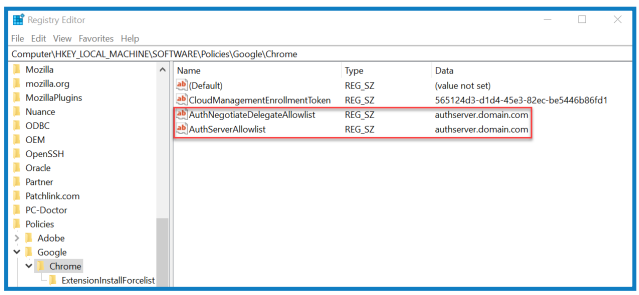
統合Windows認証用にブラウザーを構成する

インストール後にActive Directoryユーザーが Blue Prism Hubにログインできない場合、クライアントマシンが現在ログインしているユーザーを取得できるように、統合Windows認証をサポートするWebブラウザーが構成されていることを確認してください。構成手順は、Hubがサポートする各Webブラウザーによって異なります。

Google Chromeを構成する

1. Chromeで開いているインスタンスを閉じます。
2. レジストリエディターを開き、トップバーに以下を入力します。

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
3. Chromeフォルダーを右クリックし、**新規**] > **文字列値**]を選択します。
4. 文字列値を追加：`AuthNegotiateDelegateAllowlist`および`AuthServerAllowlist`。
5. 各文字列値を順番に右クリックし、**修正**]を選択します。
6. 2つの文字列値の**値のデータ**]フィールドにAuthentication Server Webサイトのホスト名(authserver.domain.comなど)を入力し、**OK**]をクリックします。

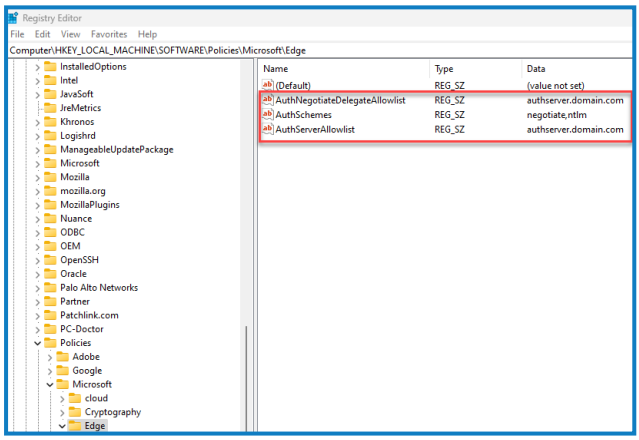


Microsoft Edgeを構成する

1. Edgeで開いているインスタンスを閉じます。
2. レジストリエディターを開き、トップバーに以下を入力します。

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Edgeフォルダーを右クリックし、 **新規**] > **文字列値**]を選択します。
4. 文字列値を追加：`AuthNegotiateDelegateAllowlist`、`AuthServerAllowlist`、`AuthSchemes`。
5. 各文字列値を順番に右クリックし、 **修正**]を選択します。
6. `AuthNegotiateDelegateAllowlist`と`AuthServerAllowlist`の **データ値**]フィールドに Authentication Server Webサイトのホスト名 (authserver.domain.comなど) を入力し、 **OK**]をクリックします。
7. `AuthSchemes`の **データ値**]フィールドに、「`negotiate, ntlm`」と入力し、 **OK**]をクリックします。詳細については、「Microsoft Edgeポリシーに関するMicrosoftドキュメント」を参照してください。

> この文字列値は、組織がKerberos認証のみに設定されている場合は必須ではありません。詳細については、以下を参照してください。

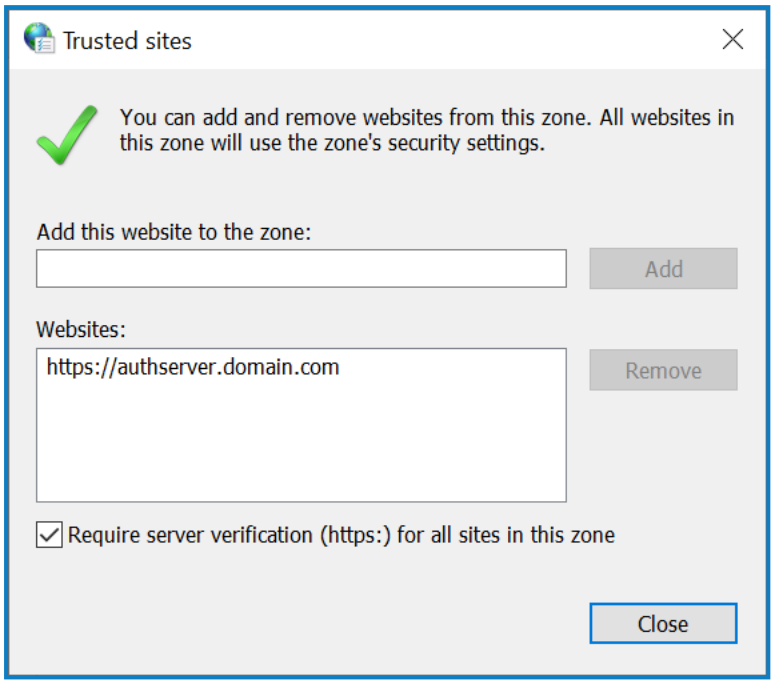


または、Microsoft Edgeの以下の手順に従ってください。

1. Edgeで開いているインスタンスを閉じます。
2. **コントロールパネル**] > **ネットワークとインターネット**] > **インターネットオプション**]に移動します。
3. **詳細**]タブの **セキュリティ**]で、 **統合Windows認証を有効化**]を選択します。
4. **セキュリティ**]タブで、 **信頼済みサイト**] > **サイト**]をクリックします。

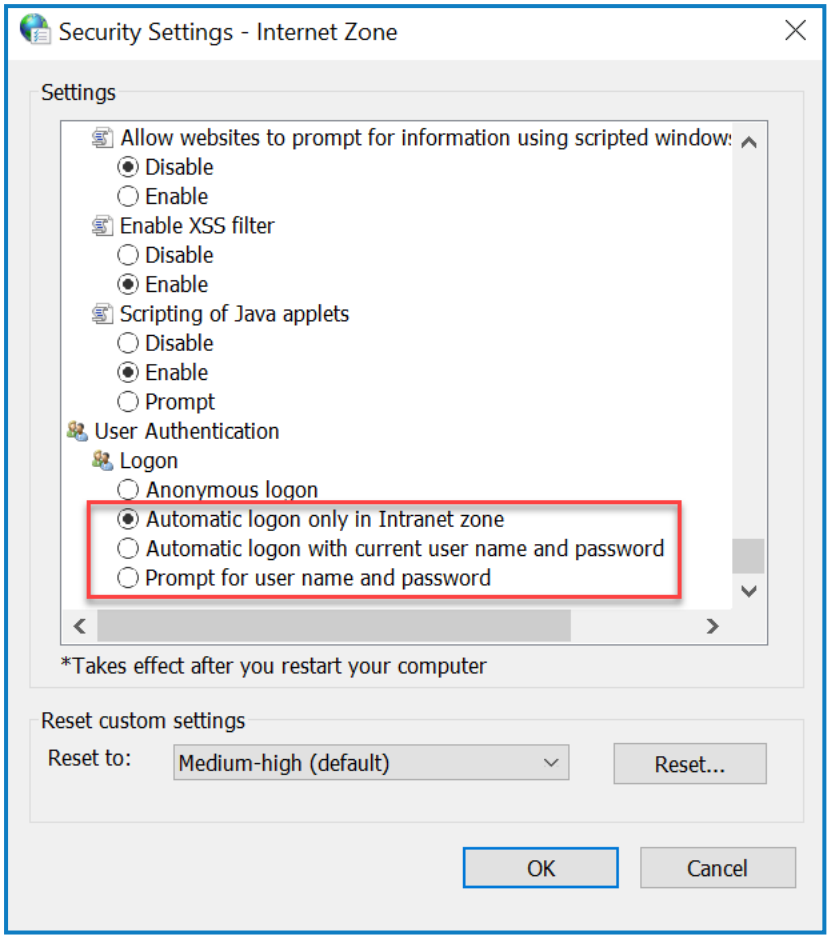
5. [信頼済みサイト]ダイアログで、 **[このWebサイトをゾーンに追加する]**フィールドにAuthentication ServerのURL(https://authserver.domain.comなど) を入力し、 **[追加]**をクリックします。

   URLが **[Webサイト]**フィールドに表示されます。



6. **[閉じる]**をクリックします。
7. [インターネットオプション]ダイアログの [セキュリティ]タブで、 **[信頼済みサイト]** > **[カスタムレベル]**をクリックします。

8. [ユーザー認証] > [ログオン] で、 [匿名ログオン] が選択されていないことを確認します。代わりに、以下に示すように、ブラウザーがユーザー認証情報を取得できるいずれかの設定を使用します。



9. [OK] をクリックします。

Kerberos認証を構成する

Windows New Technology LAN Manager(NTLM) 認証が環境で無効になっている場合、上述の手順だけでは不十分です。この場合、Kerberos認証とサービスプリンシパル名 (SPN) も構成する必要があります。組織の設定によっては、Microsoft Edge WebView2レジストリキーの追加が必要になる場合もあります。詳細については、NTLMおよびKerberos認証に関するMicrosoftドキュメントを参照してください。

1. Webサーバーで Internet Information Services(IIS) マネージャーを開きます。
2. 接続のリストで、 [Blue Prism - Authentication Server] を選択します。
   これはデフォルトのサイト名です。カスタムサイト名を使用している場合は、適切な接続を選択します。
3. [IS] で、 [認証] をダブルクリックします。
   [認証] ページが表示されます。
4. [Windows認証] を選択し(*有効*] に設定されていることを確認) 、 [プロバイダー...] をクリックします。
   [プロバイダー] ダイアログが表示されます。
5. 組織の設定に基づいて、利用可能なプロバイダーのリストから1つ以上のプロバイダーを追加し、 [OK] をクリックします。

サービスプリンシパル名 (SPN) を構成する

Kerberos認証が正しく機能するようにするには、サービスプリンシパル名 (SPN) を構成してAuthentication Server URLに登録する必要もあります。必要な許可を含む詳細については、このトピックに関するMicrosoftドキュメントを参照してください。これは、アカウントの許可がないことでSetspnコマンドの実行に失敗しないようにするために、組織のITチームと確認すべき重要なステップです。

1. Webサーバーの管理者としてコマンドプロンプトを開き、該当するコマンドを実行します。

   Blue Prism - Authentication Serverアプリケーションプールがローカルシステムアカウントとして実行されている場合は、次を使用します。

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

   Blue Prism - Authentication Serverアプリケーションプールがサービスアカウントとして実行されている場合は、次を使用します。

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

   > HTTPはHTTPとHTTPSの両方に対応します。HTTPSを含むようにコマンドを変更すると、構成に失敗するので、変更しないでください。

2. `Klist purge`を実行してKerberosチケットを更新します。
3. Authentication Serverにログインして、Kerberos認証が正しく機能していることを確認します。

Microsoft Edge WebView2レジストリキーを追加する

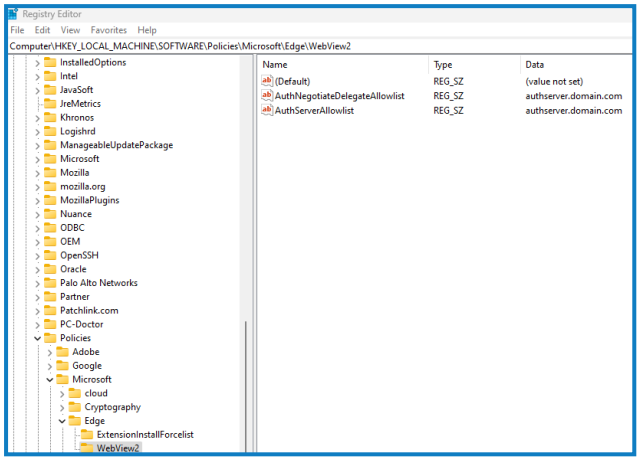
組織がKerberos認証のみに設定されており、Authentication Serverも使用してBlue Prism Enterpriseにもログインする場合、以下の手順でMicrosoft Edge WebView2ブラウザーのレジストリキーを追加する必要があります。

1. Edgeで開いているインスタンスを閉じます。
2. レジストリエディターを開き、トップバーに以下を入力します。

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge

3. Edgeフォルダーを右クリックし、 **新規**] > **キー**]を選択します。
4. 新しいキーに「**WebView2**」という名前を付けます。
5. WebView2フォルダーを右クリックして、文字列値を追加 : `AuthNegotiateDelegateAllowlist`および`AuthServerAllowlist`。
6. 各文字列値を順番に右クリックし、 **修正**]を選択します。

7. AuthNegotiateDelegateAllowlistとAuthServerAllowlistの [データ値] フィールドに Authentication Server Webサイトのホスト名 (authserver.domain.comなど) を入力し、 [OK] をクリックします。



開始時にHubにエラーが表示される

ユーザーがAuthentication Serverにログインしてを選択すると、次のメッセージが表示されます。

アプリケーションの起動中にエラーが発生しました

これは、IIS サイトを再起動する必要があることを意味します。このエラーは、単一のサーバーにインストールされているシステムに影響を与え、IISサイトの後にRabbitMQが起動すると発生します。そのため、IISサイトには、RabbitMQを最初に起動できるように起動遅延を設定することをお勧めします。

このエラーが発生した場合は、次の方法で解決できます。

1. サーバーで、Internet Information Services(IIS) Managerを開き、すべてのBlue Prismサイトを停止します。リストについては、「」「HubのWebサイト ページ18」「」を参照してください。
2. RabbitMQサービスを再起動します。
3. すべてのBlue Prismアプリケーションプールを再起動します。
4. 手順1で停止したBlue Prismサイトを起動します。

IISサイトサービスの起動を遅らせるには、次の手順に従います。

1. サーバーで、 [サービス] を開きます。
2. [**World Wide Web Publishing Service**] を右クリックし、 [**プロパティ**] を選択します。
3. [全般] タブで、 [**スタートアップの種類**] を [**自動 (遅延起動)**] に設定します。
4. [OK] をクリックして [サービス] ウィンドウを閉じます。

HubでSMTP設定が構成できない

HubでSMTP設定を構成できない場合、これは通常、サービスの起動順序に関連しています。

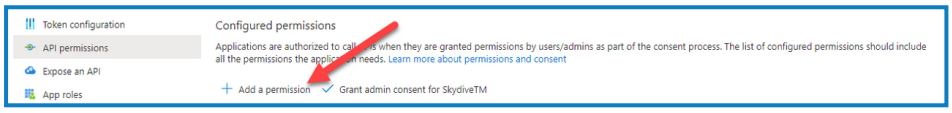
RabbitMQサービスがすべて起動した後、Webサーバーを起動する必要があります。RabbitMQサービスの準備が整う前にWebサーバーサービスが開始した場合、HubのSMTP設定に進むと「問題が発生しました」というメッセージが表示されます。

SMTP設定を保存すると、OAuth 2.0の使用している場合エラーが返されます。

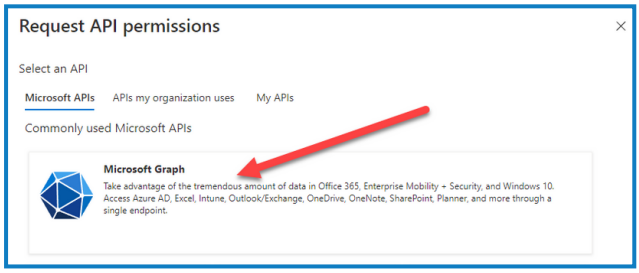
OAuth 2.0を使用してメール構成を保存するとエラーが発生する場合は、Azure Active Directoryでアプリケーションに Mail.Sendアクセス許可が設定されていることを確認してください。

Mail.Sendアクセス許可を追加するには:

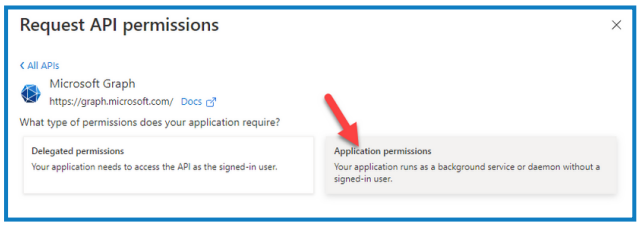
1. Azure Active Directoryで、Hubをリンクしているアプリケーションのアプリケーションプロパティを開きます。
2. [**APIのアクセス許可**]をクリックします。
3. [**アクセス許可の追加**]をクリックします。



4. Microsoft APIの [APIを選択します]で、**Microsoft Graph**を選択します。

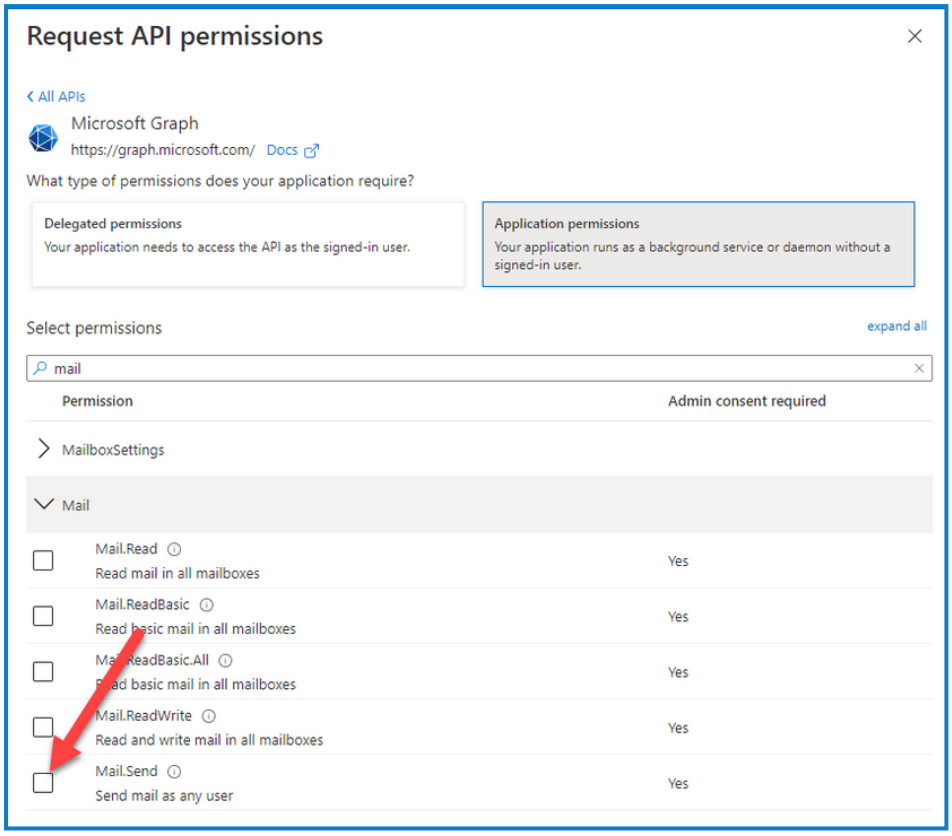


5. Microsoft Graphで、 [**アプリケーションのアクセス許可**]をクリックします。

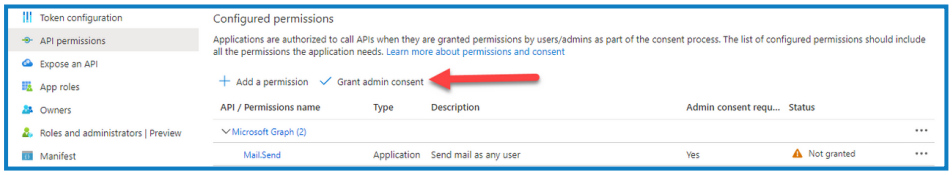


6. 検索フィールドに「Mail」と入力し、Enterを押します。

7. 表示されるメールリストで、 **[Mail.Send]**を選択し、 **[アクセス許可の追加]**をクリックします。



8. **[アプリケーションのアクセス許可]**ページで、 **[管理者の同意の付与]**をクリックします。



インストール後に顧客IDを更新する

インストール後に顧客IDを入力または更新する必要がある場合は、License Managerのappsettings.json構成ファイルを更新する必要があります。構成ファイルが更新されたら、License ManagerをInternet Information Services(IIS) マネージャーで再起動する必要があります。

appsetting.jsonファイルで顧客IDを更新するには:

1. Windows Explorerを開き、`C:\Programs (x86)\Blue Prism\LicenseManager\appsettings.json`に移動します。

   これはデフォルトのインストール場所です。カスタムの場所を使用した場合はその場所に移動します。

2. appsettings.jsonファイルをテキストエディターで開きます。

3. ファイルの`License:CustomerId`セクションを見つけて、新しい顧客IDを入力します。例:

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

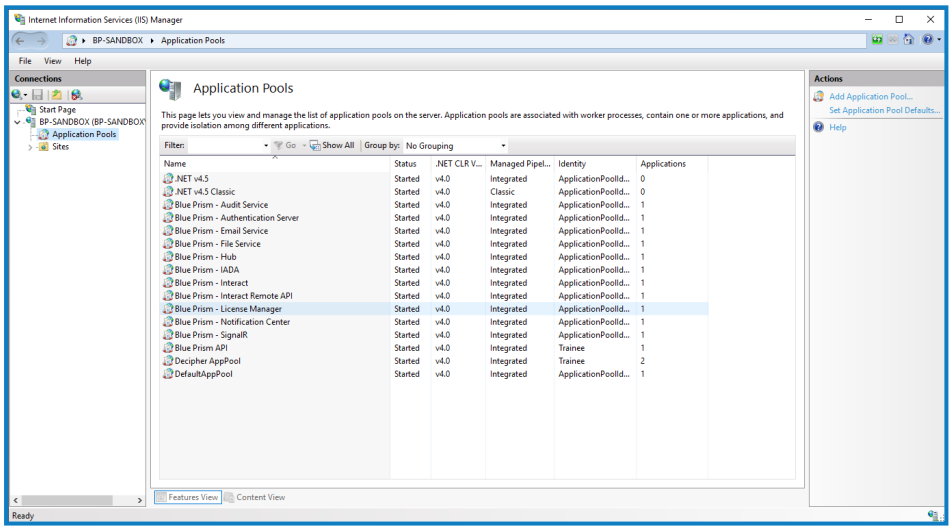
4. ファイルを保存します。

License Managerを再起動するには:

1. Internet Information Services(IIS) マネージャーを開きます。
2. 接続のリストで、**Blue Prism - License Manager**を選択します。

> これはデフォルトのサイト名です。カスタムサイト名を使用している場合は、適切な接続を選択します。

3. [Webサイトの管理]コントロールで **再起動**]をクリックします。



License Managerが再起動します。

ログ

診断ロギングの目的は、アプリケーションの実行時に利用可能な情報を増やすことです。ログに記録されたエラーと警告は、エンドユーザーにすぐには明らかにならない可能性があるシステム内の障害を特定するのに役立ちます。より詳細なロギングを一時的に有効にすると、問題のトラブルシューティング時にアプリケーションがどのように動作しているかをわかりやすく図で示すことができます。

Blue PrismはNLogと呼ばれる、実績があり信頼できるライブラリを利用して、ログ情報を出力し記録します。管理者は、グローバルまたはアプリケーションの特定の領域に記録される情報量を微調整できます。

ロギングレベル

ログエントリはレベル別に分類されます。*情報*レベル以上のエントリは通常、標準として記録されます。 [デバッグ] や [*トレース*] など、より詳細な下位レベルでは、より詳細な情報が提供されますが、有効にする必要があります。

NLogは、次のレベルを定義します。

- **トレース** – 非常に詳細なログ。プロトコルペイロードなどの大量の情報が含まれることがあります。このログレベルは、通常は開発中にのみ有効になります。
- **デバッグ** – トレースよりも詳細度の低いデバッグ情報は通常、パフォーマンスに影響する可能性があるため、本番環境では有効になりません。
- **情報** – 情報メッセージ。通常は本番環境で有効になっています。
- **警告** – 警告メッセージ。通常は、復旧可能な重要でない問題、または一時的な障害に関するものです。
- **エラー** – エラーメッセージ – ほとんどの場合、これらは例外です。
- **致命的** – 非常に重大なエラー。

標準ロギング構成

ロギングレベルは、各Webサイトとサービスのインストールフォルダー内のappsettings.jsonファイル内で定義されます。デフォルトのインストールでは、これらのフォルダーはC:\\Program Files (x86)\\Blue Prism\\にあります。

Blue Prismを普通に使っている間は、自分でappsettings.jsonファイルのログ構成設定に変更を加える必要はありません。製品の問題を調査する場合は、Blue Prismカスタマーサポートから別のログ構成設定が提供されます。appsettings.jsonファイルでロギング設定を変更した場合は、サイトをIIS内で再起動する必要があります。

ロギング構成に変更を加えるとアプリケーションの性能に影響を及ぼす可能性があるため、本番環境内を修正する場合は特に注意する必要があります。

デフォルトの構成では、情報レベル以上 (警告、エラー、致命的なエラーを含む) のログエントリをログファイルに書き込みます。ログファイルは、appsettings.jsonファイルのLogsFolder設定で指定されたディレクトリに書き込まれます。通常は、./Logs_{Application}に設定されます。例 ./Logs_Hubまたは./Logs_Interact。

デフォルトでは、appsettings.jsonファイルのロギング構成設定は次のようになります。

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

ログレベルと日付に基づいて個別のログファイルが生成され、これらは、warns.2021-05-07やinfos.2021-05-07などのログファイル名に反映されます。

情報ログファイルからの行の例を次に示します。

```
[08:58:11.4549] Connect.Core.Actions.UpdateCacheAction - ウィジェットのキャッシュが更新されました
```

このテキストの形式には、以下の要素が含まれています。

- 時刻(サーバーで設定されたタイムゾーンを使用) – 日付がファイル名に反映されます。
- ロガー名 – これは通常、ログエントリの起点となるクラスと名前空間を識別します。
- ログメッセージ。
- エラー情報 - 例外情報がログされている場合のみ使用可能です。完全な詳細は、ログメッセージの下の別の行に記録されます。

追加のログ構成

Blue Prismは、特定のコンポーネントによるアクティビティをキャプチャするために、適切なappsettings.jsonファイルに追加できるログ構成設定を開発しました。

LDAPのデバッグ

ロギングを構成して、HubをLDAPと同期する際に発生する可能性のあるさまざまな問題をデバッグできます。Hub UIでユーザーを同期する前に、Authentication Serverのappsettings.jsonファイルでログインを設定する必要があります。

1. サーバーで、Authentication Serverフォルダーに移動します。デフォルトでは、これはC:\Program Files (x86)\Blue Prism\にあります。
2. appsettings.jsonファイルをテキストエディターで開きます。
3. Loggingセクションを見つけて、LogLevelセクションに`"ImsServer.IntegrationServices.Services.LdapConnectionService": "Debug"`を追加し、上の行の最後にカンマを挿入します。以下のようになります。

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

4. ファイルを保存します。
5. IISアプリケーションプールでAuthentication Serverプールをリサイクルします。

   4.3より前のバージョンからアップグレードした場合は、IMSプールをリサイクルする必要があります。

6. IISサイトでAuthentication Serverサイトを再起動します。

これにより、Logs_AuthenticationServerディレクトリにプレフィックス「デバッグ」と適切な日付を持つファイルが作成されます。

デバッグ情報を使用して問題を解決したら、追加された行とカンマを削除してファイルを保存し、手順5と6を繰り返す必要があります。これを行わないと、ログファイルのサイズは大幅に増加し、メモリがいっぱいになる可能性があります。

ログ収集サービス

このWindowsサービスは、各Webサーバーコンポーネント(Hub、Interact、 Authentication Server 、Audit Service、監査サービスリスナー、Emailサービス、ログ収集サービス、IADA、Interact Remote API、SignalR、送信フォームマネージャー) から古い製品ログを削除します。このサービスは毎月7日に実行されるスケジュールとなっており、ログはC:\Program Files (x86)\Blue Prism\ArchivedLogsに移動されます。

apppsettings.json内で、アーカイブされたログフォルダーのパスとスケジューラーの日付を変更できます。C:\Program Files (x86)\Blue Prism\Log Service(デフォルト) の「ArchivedFolder」ではアーカイブパスを、「DayOfMonth」ではスケジューラーの日付を変更できます。

詳細情報

以下のリンクから、役立つ詳細情報を参照できます。

- NLog Githubリポジトリ - 基本のチュートリアル
- NLogオフィシャルWebサイト - 構成オプション

Hubをアンインストールする

Blue Prism Hubをアンインストールするには、システム管理者である必要があります。

Hub 4.7を完全にアンインストールするには、以下を行う必要があります。

1. IISを使用してアプリケーションプールを停止する。
2. [プログラムと機能]アプリケーションを使用してHubを削除する。
3. IIS Webサイトおよびアプリケーションプールを削除する。
4. ホストを削除する。
5. データベースを削除する。
6. RabbitMQデータを削除する。
7. 証明書を削除する。
8. 残りのファイルすべて削除する。

IISを使用してアプリケーションプールを停止する

1. Internet Information Services(IIS)マネージャーを開きます。これを行うには、Windowsタスクバーの[検索]ボックスに「*IIS*」と入力し、**[Internet Information Services(IIS)マネージャー]**をクリックします。
2. **接続**ペインで、**[アプリケーションプール]**をクリックします。
3. Blue Prismサイトに関連付けられているすべてのアプリケーションプールを停止します。それぞれを順番に選択し、**[停止]**をクリックします。リストについては、「HubのWebサイト ページ18」を参照してください。

[プログラムと機能]を使用してHubを削除する

> Interactもインストールしている場合は、手順3でBlue Prism Interactを選択して、これらの手順を使用して先にアンインストールする必要があります。

1. [コントロールパネル]を開きます。これを行うには、Windowsタスクバーの[検索]ボックスに「*コントロールパネル*」と入力し、**[コントロールパネル]**をクリックします。
2. **[プログラム]**をクリックし、**[プログラムと機能]**をクリックします。
3. [Blue Prism Hub]を選択します。
4. **[アンインストール]**をクリックします。
5. アンインストールを続行することを確認します。

IIS Webサイトおよびアプリケーションプールを削除する

1. Internet Information Services(IIS)マネージャーを開きます。これを行うには、Windowsタスクバーの[検索]ボックスに「*IIS*」と入力し、**[Internet Information Services(IIS)マネージャー]**をクリックします。
2. **[接続]**ペインで、**[サイト]**ノードを展開し、Hubを削除した後も残っている次のサイトを削除します。
   - Blue Prism - License Manager。
   - Blue Prism - Notification Center。

3. [接続]ペインで、[アプリケーションプール]ノードを展開し、Hubを削除した後も残っているプールを削除します。
   - Blue Prism - License Manager。
   - Blue Prism - Notification Center。

ホストを削除する

1. `C:\Windows\System32\drivers\etc\hosts`ファイルをテキストエディターで開きます。
2. License Managerのドメインの行を削除します。この行は、テキスト「*licensemanager*」を検索することで見つけることができます。
3. 通知センターのドメインの行を削除します。この行は、テキスト「*notificationcenter*」を検索することで見つけることができます。
4. ファイルを保存します。

データベースを削除する

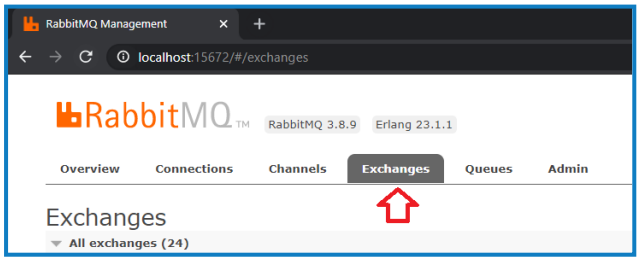
テストシステムのデータベースのみを削除してください。本番稼働中のシステムのデータベースを削除しようとしている場合は、そのデータを組織でアーカイブする必要があるか、監査目的で使用する必要があるかを検討する必要があります。

> Hubのアンインストール後、同じデータベースを使用して後日再インストールする場合は、再インストールする前にデータベースからデータを消去する必要があります。

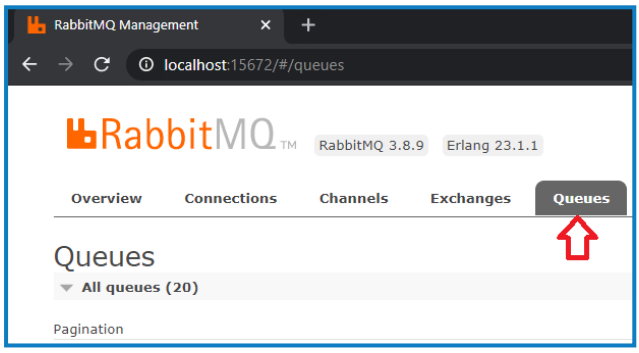
1. HubおよびInteract(インストールされている場合)アプリケーションのデータベースを削除またはアーカイブします。

RabbitMQデータを削除する

1. RabbitMQ adminページを開きます。デフォルトでは、URLはローカルコンピューター上の http://localhost:15672です。
2. [Exchanges]をクリックします。



3. 次のアイテムを検索して削除します。
   - bpc.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*
4. **Queues**]をクリックします。



5. 次のアイテムを検索して削除します。
   - bpc.audit.*
   - bpc.email-service.*
   - bpc-hub.*
   - bpc.iada.*
   - bpc.ims.*
   - bpc.interact.*
   - bpc.notification-center.*
   - bpc.signalr.*
   - bpc.submissions.*

証明書を削除する

1. 証明書マネージャーを開きます。これを行うには、Windowsタスクバーの検索ボックスに *[証明書]*と入力し、 **[コンピューター証明書の管理]**をクリックします。
2. ナビゲーションペインで **[信頼されたルート証明書]**を展開し、 **[証明書]**をクリックします。
3. Blue Prismサイト用に作成された証明書を選択し、削除します。また、以下も選択します。
   - BluePrismCloud_Data_Protection
   - BluePrismCloud_IMS_JWT
   - BPC_SQL_CERTIFICATE

残りのファイルすべて削除する

1. エクスプローラーで、Hubインストールの親フォルダーを開きます。デフォルトでは、これは`C:\Program Files (x86)\Blue Prism`ですが、Hubのインストール中に変更されている場合もあります。
2. Hubフォルダーを削除します。