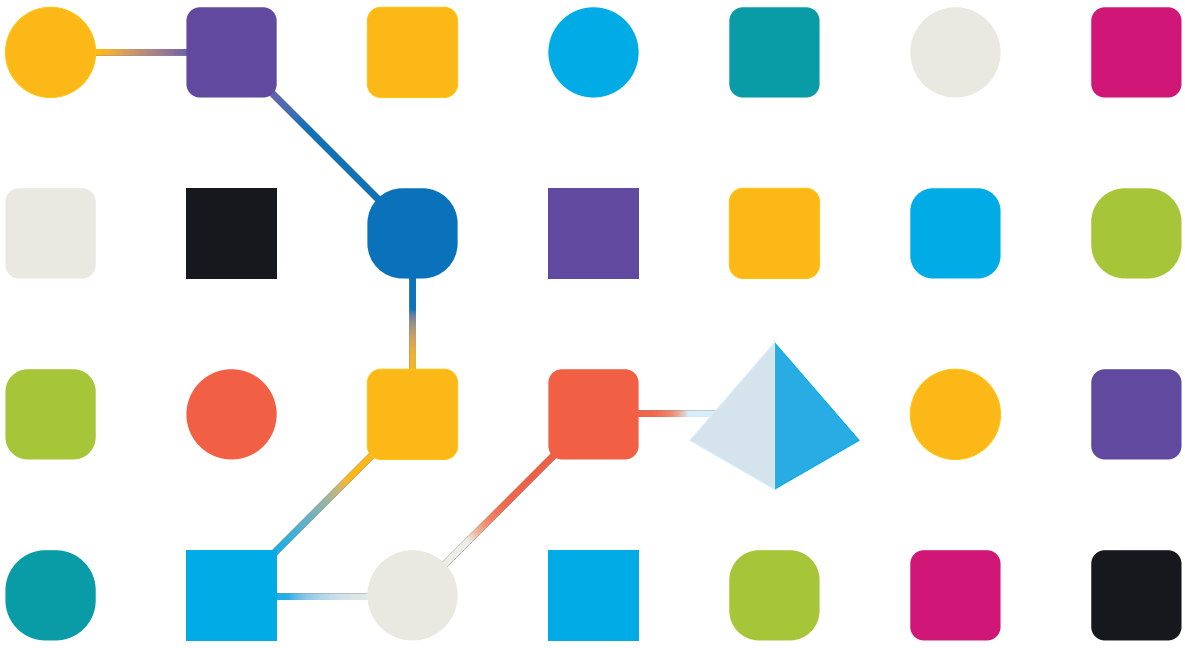
blueprism®

Interact 4.7

Guide d'installation

Révision des documents : 3.0



Marques déposées et droits d'auteur

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Enregistré en Angleterre : numéro d'enregistrement 4260035. Tél. : +44 370 879 3000. Web : www.blueprism.com

Contenu

Introduction

Ce guide fournit des conseils relatifs au processus à suivre lors de l'installation de Blue Prism® Interact et contient des informations sur la façon de vérifier que l'installation a réussie.

Blue Prism Interact est uniquement pris en charge dans un déploiement sur plusieurs appareils. C'est là que les composants Blue Prism sont déployés sur un certain nombre d'appareils. Les raisons sont les suivantes :

- Cela fournit un déploiement extensible des composants Blue Prism adapté à un large éventail de scénarios.
- Les techniques avancées liées au déploiement de services additionnels ou à la sécurisation et au renforcement de l'environnement nécessiteront généralement ce type de déploiement.

Un certain nombre de sujets plus avancés sont également inclus dans ce guide pour fournir des informations sur la résolution de problèmes liés aux installations et la configuration des réglages avancés et des options.

Si vous avez besoin d'aide supplémentaire même en suivant les instructions ce document, veuillez contacter votre responsable de compte Blue Prism ou votre service d'assistance technique. Pour plus d'informations, voir Nous contacter.

Ces informations se rapportent uniquement à la version 4.7 de Blue Prism Interact.

Blue Prism Hub doit être installé avant d'essayer d'installer Interact.

Mise à niveau d'Interact

En cas de mise à niveau à partir d'une version antérieure d'Interact 4, Blue Prism fournit une mise à niveau. Pour plus d'informations, voir Mettre à niveau Hub et Interact.

Public visé

Ce guide s'adresse aux professionnels de l'informatique expérimentés dans la configuration et la gestion des réseaux, des serveurs et des bases de données. Le processus d'installation nécessite une bonne connaissance de l'installation et de la configuration des serveurs Web et des bases de données.

Vidéos

En plus de ce guide d'installation, vous pouvez regarder nos vidéos illustrant le processus d'installation. Cliquez ici pour regarder les vidéos relatives à l'installation d'Interact.

Documents associés

Les documents suivants fournissent des informations supplémentaires sur des aspects spécifiques de l'implémentation de Hub et d'Interact.

Titre du document	Description
Guide de l'utilisateur de Hub	Document destiné aux utilisateurs Hub expliquant comment tirer le meilleur parti de Hub.
Guide de l'administrateur de Hub	Document détaillé destiné aux administrateurs Hub expliquant comment tirer le meilleur parti de Hub, dont l'accès utilisateur, la mise sous licence des plug-ins et la personnalisation de Hub.

Titre du document	Description
Guide de l'utilisateur du plug-in Interact	Un document détaillé expliquant comment tirer le meilleur parti d'Interact, dont la création de formulaires et leur attribution à des rôles.
le guide de l'utilisateur Interact	Document détaillé expliquant comment utiliser Interact pour soumettre et approuver des formulaires.
Guide de l'utilisateur du service API Web Interact	Un document fournissant des informations détaillées sur la façon d'utiliser le service API Web Interact et l'objet Blue Prism associé.

Préparation

Avant d'entreprendre l'installation de Blue Prism Interact, il est important de s'assurer que l'architecture est configurée pour prendre en charge l'installation. Plusieurs systèmes sont nécessaires pour prendre en charge l'installation d'Interact.

Planification

Avant d'effectuer l'installation, les conditions suivantes doivent être remplies :

- Un serveur SQL doit être disponible pour héberger les bases de données des composants Blue Prism, telles que Authentication Server , Hub, Audit, Interact, InteractCache, etc. L'accès de niveau administrateur est requis pendant le processus d'installation. Voir Permissions SQL minimales pour en savoir plus.
- Un serveur de l'agent de messages doit être disponible pour héberger l'agent de messages RabbitMQ.
- Un serveur Web pour les installations Hub (voir Prérequis sur la page suivante) et Interact co-existantes.
- L'accès administrateur aux appareils où Blue Prism Interact sera installé doit être disponible. Tous les appareils doivent répondre aux spécifications minimales et les appareils doivent pouvoir communiquer entre eux sur le réseau local, y compris avec votre base de données Blue Prism.
- Le compte effectuant l'installation doit avoir accès au fichier d'hôtes. Il est généralement stocké dans C:\Windows\System32\drivers\etc\hosts ou %SYSTEMROOT%\System32\drivers\etc\hosts.

Lors de la planification de votre déploiement, les points suivants doivent être pris en compte :

- La base de données sera-t-elle ajoutée à un serveur de base de données existant ou un nouveau sera-t-il mis en service ?

  Blue Prism recommande que les bases de données soient conservées sur des serveurs de base de données distincts.
- Y a-t-il suffisamment d'espace et de ressources pour héberger les bases de données ajoutées ?

  Vous devez vérifier et vous assurer qu'un espace disque et des ressources de calcul suffisants peuvent supporter la charge supplémentaire.
- Quel mode d'authentification est requis pour la base de données SQL (SQL natif ou Windows Authentication) ?

  C'est la décision de votre organisation informatique.
- Le serveur de l'agent de messages a-t-il été configuré pour prendre en charge l'installation de Hub ?

  Un serveur de l'agent de messages est nécessaire pour terminer l'installation de Hub.
- Tous les appareils où Blue Prism Hub sera installé répondent-ils aux exigences minimales ?

  Voir Exigences et permissions du logiciel pour en savoir plus.

Prérequis

Voir Exigences et permissions du logiciel pour en savoir plus sur les exigences et permissions SQL minimales du logiciel.

L'installation d'Interact nécessite les prérequis suivants :

- SQL Server doit être configuré pour utiliser le cryptage SSL. Si votre entreprise n'utilise pas déjà le cryptage SSL (vous avez exécuté votre environnement sans certificat pour votre serveur SQL Server ou vous avez utilisé un certificat autosigné), elle doit obtenir un certificat auprès d'une autorité de certification approuvée et l'importer dans SQL Server pour activer le cryptage. Voir la documentation Google pour en savoir plus.

  Pour importer le certificat dans SQL Server :

  1. Dans la barre des tâches Windows, ouvrez **SQL Server Configuration Manager**.
  2. Dans SQL Server Configuration Manager, développez **Configuration réseau SQL Server** et cliquez avec le bouton droit sur **Protocoles pour <SqlServerInstanceName>**, puis cliquez sur **Propriétés**.
  3. Dans la boîte de dialogue Protocoles pour les propriétés <SqlServerInstanceName>, sélectionnez l'onglet **Certificat**, puis sélectionnez ou importez le certificat requis.
  4. Cliquez sur **Appliquer**.

  ⚠ Les certificats d'autorités de certification approuvées doivent être utilisés pour les environnements de production. Cependant, un certificat autosigné peut être utilisé pour les environnements de preuve de concept ou de développement. Il est important que le nom de domaine explicite (FQDN) utilisé par SQL Server corresponde au FQDN défini dans le certificat. **S'ils ne correspondent pas, la connexion à la base de données ne sera pas établie et votre installation ne fonctionnera pas correctement.** Pour plus d'informations sur l'utilisation et la configuration des certificats autosignés, voir Certificats autosignés dans le guide d'installation de Blue Prism Hub.

  En plus des bases de données installées par l'installateur Hub, votre base de données Blue Prism doit également utiliser le cryptage SSL, à l'aide d'un certificat auquel le serveur Hub fait confiance, par exemple d'une autorité de certification de confiance.

- Blue Prism Hub nécessite qu'un serveur de l'agent de messages soit installé et configuré.
- Le build du serveur de l'agent de messages est une configuration générique et une installation de base d'un service d'agent de messages RabbitMQ. Il est recommandé que les mots de passe par défaut soient modifiés et que les exigences en matière de sécurité, telles que l'application des certifications SSL, soient remplies par votre service informatique.

  Pour terminer la création de l'agent de messages, les éléments suivants doivent être téléchargés :

  - Erlang/OTP, voir : https://www.rabbitmq.com/which-erlang.html
  - RabbitMQ Server (les versions prises en charge sont 3.8.0 à 3.8.8), disponible ici : https://github.com/rabbitmq/rabbitmq-server/releases/

  Les conseils d'installation sont fournis ici : https://www.rabbitmq.com/install-windows-manual.html

- Blue Prism Hub est installé sur le serveur Web et nécessite donc l'installation du gestionnaire d'Internet Information Services (IIS), et des composants .Net Core. Ceux-ci doivent être installés au préalable pour permettre une installation réussie de Blue Prism Hub. Voir Installer et configurer le serveur Web sur la page 26 pour plus d'informations.

- Le système Interact est un serveur Web et nécessite par conséquent que le serveur Web IIS et les composants .NET Core soient installés. Tous ces éléments sont installés dans le cadre d'une installation réussie de Blue Prism Interact à l'aide de Blue Prism Hub et du support d'installation de Blue Prism Interact.
- Vous allez créer les sites Web suivants avec l'assistant d'installation de Interact. Vous devez définir les URL en fonction du domaine de votre organisation :

Site Web dans IIS	URL par défaut
Sites Web avec une interface utilisateur destinée à être utilisée par les utilisateurs finaux	
Blue Prism – Interact	https://interact.local
Sites Web destinés à être utilisés uniquement par l'application (services)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

⚠ Les URL par défaut indiquées ci-dessus conviennent à un environnement autonome, tel qu'un environnement de test. Les structures DNS et de domaine de votre organisation doivent être prises en compte lors du choix des noms d'hôte pour votre installation.

Elles s'ajoutent aux sites Web créés par le programme d'installation de Hub, voir Configurer les certificats SSL sur la page 27 pour une liste.

- Certificats : pendant le processus d'installation, vous serez invité à fournir les certificats SSL pour les sites Web en cours de configuration. Selon les exigences de sécurité de votre infrastructure et de votre organisation informatique, il peut s'agir d'un certificat SSL créé en interne ou d'un certificat acheté pour protéger les sites Web. Le programme d'installation peut être exécuté sans que les certificats soient présents, bien que pour que les sites fonctionnent, les liaisons des sites Web IIS devront avoir des certificats SSL valides présents. Voir Configurer les certificats SSL pour en savoir plus.
- Par défaut, les pools d'applications IIS sont utilisés. Les pools d'applications doivent avoir accès aux fichiers d'application et aux certificats créés pendant l'installation pour la protection et l'autorisation des données. Ces certificats, BluePrismCloud_Data_Protection et BluePrismCloud_IMS_JWT, sont situés dans le dossier de certificats Windows par défaut. Si vous utilisez l'autorisation Windows pour accéder à SQL Server, celle-ci devra être configurée manuellement. Pour plus d'informations, voir Informations d'application par défaut sur la page 15.
- Par défaut, le compte « Système local » est utilisé pour les services. Ce compte doit avoir accès aux fichiers d'application. Si vous utilisez l'autorisation Windows pour accéder à SQL Server, celle-ci devra être configurée manuellement.

Liste de téléchargement de logiciels

Blue Prism Hub

Cela répertorie tous les téléchargements requis pour installer Hub. Tous ces éléments apparaissent plus tard dans le guide d'installation :

Logiciel et lien de référence	Conseils connexes
RabbitMQ 3.9.22 à 3.10.7 ou 3.11.9 à 3.11.10 Pour plus d'informations, voir voir Téléchargement et installation de RabbitMQ..	Installer le serveur de l'agent de messages sur la page 21
Erlang/OTP 24.x ou 25.x La version d'Erlang dont vous avez besoin dépend de la version de RabbitMQ que vous avez l'intention d'utiliser. Pour plus d'informations, voir voir Configuration requise pour la version Erlang de RabbitMQ..	
IIS 10.0 Inclus avec Windows Server 2016, 2019 et 2022.	Installer et configurer le serveur Web sur la page 26
ASP.NET Core Runtime 6.0.9 ou 6.0.10 (bundle d'hébergement Windows) https://dotnet.microsoft.com/download/dotnet/6.0 : sélectionnez la version dont vous avez besoin. Sous **ASP.NET Core Runtime**, sélectionnez **Bundle d'hébergement**.	
.NET Desktop Runtime 6.0.9 ou 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 : sélectionnez la version dont vous avez besoin. Sous **.NET Desktop Runtime**, sélectionnez le téléchargement approprié.	
.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 Il est installé par défaut sur Windows Server 2022. Vous n'avez besoin d'installer .NET Framework que si vous utilisez Windows Server 2016 Datacenter ou Windows Server 2019.	
Blue Prism Hub 4.7 Téléchargez Hub à partir de l'une des pages de téléchargement de produit suivantes sur le portail Blue Prism : • Automation Lifecycle Management • Decision • Interact	

Logiciel et lien de référence	Conseils connexes
Extension Authentication Server SAML 2.0 Télécharger à partir de Digital Exchange – Il s'agit d'un assistant d'installation facultatif. Il n'est requis que si vous avez l'intention d'utiliser l'authentification SAML 2.0.	Consultez le guide d'installation sur Digital Exchange..

Blue Prism Interact

Blue Prism Interact est un plug-in contrôlé par licence dans Hub et un site Web supplémentaire pour les utilisateurs finaux. Si votre organisation a l'intention d'utiliser Interact, vous devrez télécharger les éléments suivants en plus des téléchargements répertoriés dans Blue Prism Hub sur la page précédente.

Logiciel et lien de référence	Conseils connexes
Blue Prism Interact 4.7 Téléchargez à partir du portail Blue Prism.	Installer Blue Prism Interact
Fichier Remote API.bprelease de Blue Prism Interact Téléchargez à partir du portail Blue Prism.	Installer et configurer le service API Web Interact

Configuration matérielle minimale

Les informations ci-dessous détaillent la configuration matérielle minimale recommandée pour installer et exécuter efficacement Hub et Interact 4.7. Pour les exigences logicielles, voir Exigences et permissions du logiciel sur la page suivante.

Ressource d'exécution

Veuillez vous reporter aux exigences minimales du guide d'installation pour la version de Blue Prism que vous avez installée. Consultez l'aide Blue Prism pour plus d'informations.

Serveur de la base de données

- Processeur Intel Xeon à quatre cœurs
- 8 Go de RAM
- SQL Server :
  - 2016, 2017 ou 2019 (64 bits) – Éditions Express, Standard ou Entreprise

    Les éditions de SQL Express ne conviennent qu'aux environnements hors production, comme pour les exercices de preuve de concept.
  - Base de données Azure SQL : un minimum de 100 eDTU est requis pendant l'installation. Ce chiffre peut être abaissé à 50 eDTU après l'installation.
  - SQL Server sur les machines virtuelles Azure
  - Instance gérée par Azure SQL
- Pour une prise en charge appropriée du système d'exploitation, voir :
  - SQL Server 2016 ou 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

Serveur de l'agent de messages

- Processeur Intel Dual Xeon
- RAM 8 Go
- Windows Server 2016 Datacenter, 2019 ou 2022

Serveur Web

- Processeur Intel Dual Xeon
- RAM 8 Go
- Windows Server 2016 Datacenter, 2019 ou 2022
- Les prérequis sont détaillés dans Préparation sur la page 7

Exigences et permissions du logiciel

Configuration logicielle

Les technologies suivantes sont prises en charge pour une utilisation avec le logiciel :

Système d'exploitation

Version	Serveur Web	Agent de messages
Windows Server 2016 Datacenter	✓	✓
Windows Server 2019	✓	✓
Windows Server 2022	✓	✓

Lorsque les composants Blue Prism sont installés sur un système d'exploitation 64 bits, il fonctionnera comme une application 32 bits.

Microsoft SQL Server

Les versions suivantes de Microsoft SQL Server sont prises en charge pour localiser les bases de données de composants Blue Prism :

Version	Express	Standard	Entreprise
SQL Server 2016	✓	✓	✓
SQL Server 2017	✓	✓	✓
SQL Server 2019 (64 bits)	✓	✓	✓

Remarque :

- SQL Express ne convient qu'aux environnements hors production, comme pour les exercices de preuve de concept.
- SQL Server doit être configuré pour utiliser le cryptage SSL. Si votre entreprise n'utilise pas déjà le cryptage SSL (vous avez exécuté votre environnement sans certificat pour votre serveur SQL Server ou vous avez utilisé un certificat autosigné), elle doit obtenir un certificat auprès d'une autorité de certification approuvée et l'importer dans SQL Server pour activer le cryptage. Voir la documentation Google pour en savoir plus.

  Pour connaître les étapes d'importation de certificats dans SQL Server, consultez Prérequis sur la page 8.

  Les certificats d'autorités de certification approuvées doivent être utilisés pour les environnements de production. Cependant, un certificat autosigné peut être utilisé pour les environnements de preuve de concept ou de développement. Il est important que le nom de domaine explicite (FQDN) utilisé par SQL Server corresponde au FQDN défini dans le certificat. **S'ils ne correspondent pas, la connexion à la base de données ne sera pas établie et votre installation ne fonctionnera pas correctement.** Pour plus d'informations sur l'utilisation et la configuration des certificats autosignés, voir Certificats autosignés.

Les éléments suivants sont également pris en charge :

- Base de données Azure SQL : un minimum de 100 eDTU est requis pendant l'installation. Ce chiffre peut être abaissé à 50 eDTU après l'installation.
- SQL Server sur les machines virtuelles Azure.
- Instance gérée SQL Azure, cependant, les bases de données doivent être créées avant l'installation.

Serveur de l'agent de messages

Le logiciel suivant est requis sur le serveur de l'agent de messages :

- RabbitMQ 3.9.22 à 3.10.7 ou 3.11.9 à 3.11.10
- rlang/OTP 24.x ou 25.x : la version d'Erlang dont vous avez besoin dépend de la version de RabbitMQ que vous avez l'intention d'utiliser.

  Pour une prise en charge appropriée d'Erlang/OTP, voir Configuration requise pour la version Erlang de RabbitMQ..

  Pour une prise en charge appropriée du système d'exploitation, voir https://www.rabbitmq.com/platforms.html.

Voir Installer le serveur de l'agent de messages sur la page 21 pour en savoir plus.

Blue Prism vise à tester entièrement toutes les nouvelles versions de RabbitMQ par rapport à la dernière version de Hub dans les deux mois suivant la disponibilité générale de ce logiciel. Si un développement ultérieur de Hub est nécessaire pour prendre en charge une nouvelle version de RabbitMQ, toutes les mises à jour seront intégrées dans une version future de Hub, tel que déterminé par notre cycle de publication.

Serveur Web

Le logiciel suivant est requis sur le serveur Web :

- .NET Framework 4.8 : installé par défaut sur Windows Server 2022.
- IIS 10.0
- ASP.NET Core Runtime 6.0.9 ou 6.0.10 (bundle d'hébergement Windows)
- .NET Desktop Runtime 6.0.9 ou 6.0.10

Interact 4.7 ne prend en charge que les versions de ASP.NET Core Runtime et .NET Desktop Runtime indiquées ci-dessus. Si vous utilisez une version ultérieure, telle que 7.x.x, vous pourriez rencontrer des problèmes.

Voir Installer et configurer le serveur Web sur la page 26 pour en savoir plus.

Navigateur Web sur les machines clientes

Les dernières versions des navigateurs Web suivants sont prises en charge par Interact :

- Google Chrome
- Microsoft Edge (basé sur Chromium)

Pour permettre aux utilisateurs Active Directory de se connecter à Interact à l'aide d'un navigateur Chrome ou Edge, les navigateurs doivent être configurés pour l'authentification Windows intégrée.

Microsoft Internet Explorer et Mozilla Firefox ne sont pas pris en charge.

Blue Prism

Blue Prism 6.4.0 ou une version ultérieure est requis pour l'utilisation avec Interact.

Permissions SQL minimales

Les permissions SQL minimales pour l'utilisateur requises pour se connecter à la base de données pendant le processus d'installation doivent disposer des privilèges appropriés pour créer ou configurer la base de données à partir du produit. Par conséquent, un compte administrateur approprié devra être utilisé lors de l'exécution du processus d'installation :

- Créer la base de données : dbcreator (rôle serveur) ou sysadmin (rôle serveur)
- Configurer la base de données : sysadmin (rôle de serveur) ou db_owner (rôle de base de données)

L'utilisateur de base de données requis pour se connecter aux bases de données pendant le fonctionnement normal doit disposer des permissions SQL minimales pour accéder aux bases de données Interact et Interact Cache. Les permissions requises sont :

- db_datareader
- db_datawriter

Un utilisateur disposant d'un accès db_owner à la base de données doit être utilisé pendant le processus d'installation et lors de la première exécution de l'application. Une fois terminé, l'accès à la base de données pour cet utilisateur peut être modifié par db_datareader et db_datawriter.

Pour plus d'informations, voir Informations d'application par défaut en dessous.

Informations d'application par défaut

Les informations ci-dessous montrent les applications qui sont créées par l'installation Interact, en utilisant les valeurs par défaut. Toutes les applications doivent avoir un accès complet au certificat BluePrismCloud_Data_Protection situé dans le magasin de certificats sur la machine locale. IIS APPPOOL\ Blue Prism – IADA aura également besoin d'accéder au certificat BPC_SQL_CERTIFICATE.

Pour plus d'informations sur les applications Hub, voir Exigences et permissions du logiciel Hub.

Sites Web Interact

Nom de l'application	Exemple de service nom de compte pour SQL Windows Authentification	SQL Server permissions requis pendant installation	Base de données permissions requis pendant application en cours d'exécution	Nom de la base de données par défaut
Blue Prism - Interact	IIS APPPOOL\ Blue Prism – Interact	dbcreator / sysadmin	db_datawriter / db_datareader	InteractDB, InteractCacheDB
Blue Prism - Interact Remote API	IIS APPPOOL\ Blue Prism – Interact Remote API	dbcreator / sysadmin	db_datawriter / db_datareader	AuthenticationServerDB, InteractDB
Blue Prism - IADA	IIS APPPOOL\ Blue Prism – IADA	dbcreator / sysadmin	db_datawriter / db_datareader	IadaDB

Services Interact

Nom de l'application	Exemple de service nom de compte pour SQL Windows Authentification	SQL Server permissions requis pendant installation	Base de données permissions requis pendant application en cours d'exécution	Nom de la base de données par défaut
Blue Prism - Submit Form Manager	NT AUTHORITY\ SYSTÈME	Indisponible	db_datawriter / db_datareader	InteractDB

Informations sur le déploiement multi-appareils

Lors d'un déploiement multi-appareils, les éléments suivants doit être pris en compte avant l'installation.

Zone	Préoccupations environnementales (développement/test/préproduction/production)
Connectivité générale	La connectivité entre les différents appareils doit être configurée de façon appropriée. Cela nécessite généralement que le DNS soit configuré pour permettre aux appareils de s'identifier mutuellement en fonction de leur nom de domaine explicite et que des règles de pare-feu appropriées soient mises en place pour permettre aux appareils de communiquer sur les ports requis.
Serveur de l'agent de messages	Il s'agit d'un appareil unique axé sur la fourniture de services d'agent de messages entre les composants Blue Prism. Un appareil par environnement est recommandé.
Serveur Web	Un appareil unique pouvant héberger plusieurs composants Blue Prism. Il n'est pas recommandé que les environnements soient partagés sur cet appareil et qu'un appareil distinct soit utilisé par environnement.
Instance de serveur de base de données	Déterminer si la façon dont les ressources sont affectées aux instances de SQL Server permet d'utiliser une seule instance partagée pour les déploiements de Blue Prism en fonction de leur importance et de leur criticité. (Par exemple, les environnements de production sont susceptibles d'être les plus critiques pour l'entreprise.) Il est recommandé que différents types d'environnements, tels que les environnements de développement, UAT et de production, disposent de leur propre instance SQL Server dédiée. Toutefois, vous pouvez exécuter plusieurs environnements de développement sur la même instance SQL Server.
Certificats de Digital Worker	Décider s'il y a une exigence supplémentaire d'appliquer une sécurité basée sur un certificat aux communications d'instruction des clients interactifs et des serveurs d'applications à chaque Digital Worker et aux communications entrantes reçues par les Digital Workers s'ils hébergent des services Web. Si un certificat est requis, il doit être généré manuellement et installé sur chaque Digital Worker applicable. Le nom commun figurant sur le certificat doit correspondre à l'adresse à laquelle les composants Blue Prism seront configurés pour communiquer avec les appareils (par exemple, le nom de domaine explicite ou le nom de machine court). De plus, tous les appareils qui se connecteront aux Digital Workers doivent faire confiance à l'autorité de certification qui délivre le(s) certificat(s) généré(s) manuellement.

Ports réseau

Pour garantir la connectivité réseau entre les appareils de l'architecture, le pare-feu Windows sur les serveurs applicables devra autoriser les flux de trafic suivants :

Serveur de la base de données	Port 1433 pour permettre la connectivité SQL Server à partir du serveur Web. Si l'instance SQL Server est une instance nommée, ce qui suit sera également requis : • Le port TCP pour l'instance nommée (dynamique par défaut à partir de la plage éphémère) ou le port défini s'il s'agit d'un port statique pour permettre la connectivité SQL Server à partir du serveur Web. • Port UDP 1434 pour le service de navigateur SQL Server afin d'autoriser la connectivité SQL Server à partir du serveur Web.
Serveur de l'agent de messages	Port 5672 pour permettre la connectivité de la messagerie RabbitMQ. Port 15672 pour permettre la connectivité de la console de gestion RabbitMQ.
Serveur Web	Port 443 pour permettre la connectivité HTTPS.
Digital Workers	Port 443 pour permettre la connectivité HTTPS.

Il est recommandé de consulter l'expert en infrastructure réseau de votre organisation lors de la configuration des ports. D'autres ports peuvent devoir être configurés pour assurer la connectivité dans votre organisation.

Déploiement typique

Adapté à la production et à une utilisation hors production, un déploiement typique contient tous les composants de Blue Prism Interact déployés sur des machines distinctes.

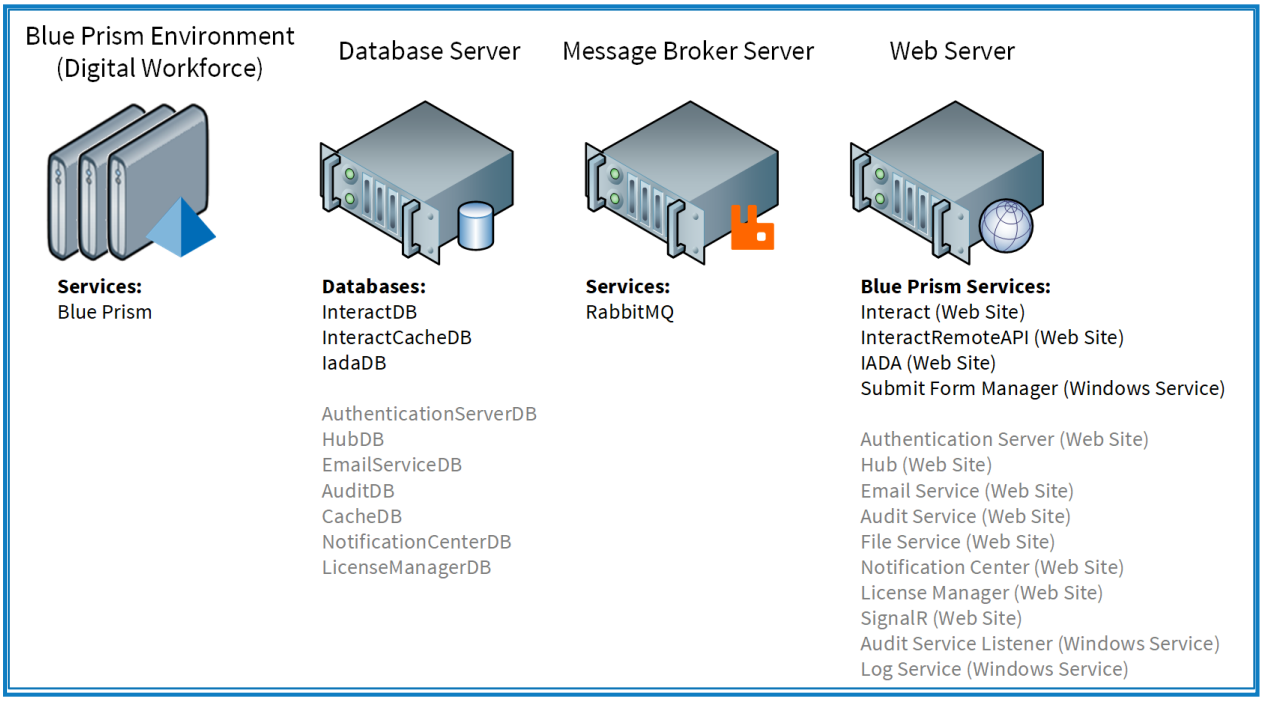
Avant de suivre ce guide, assurez-vous d'avoir complètement pris en compte les informations dans Préparation.

Pour les environnements de production, au moins quatre ressources sont nécessaires :

- Serveur Web
- Serveur de l'agent de messages
- Digital Workers
- SQL Server

Le serveur de l'agent de messages et les instances SQL Server doivent être préconfigurés avant l'installation de Blue Prism Interact.

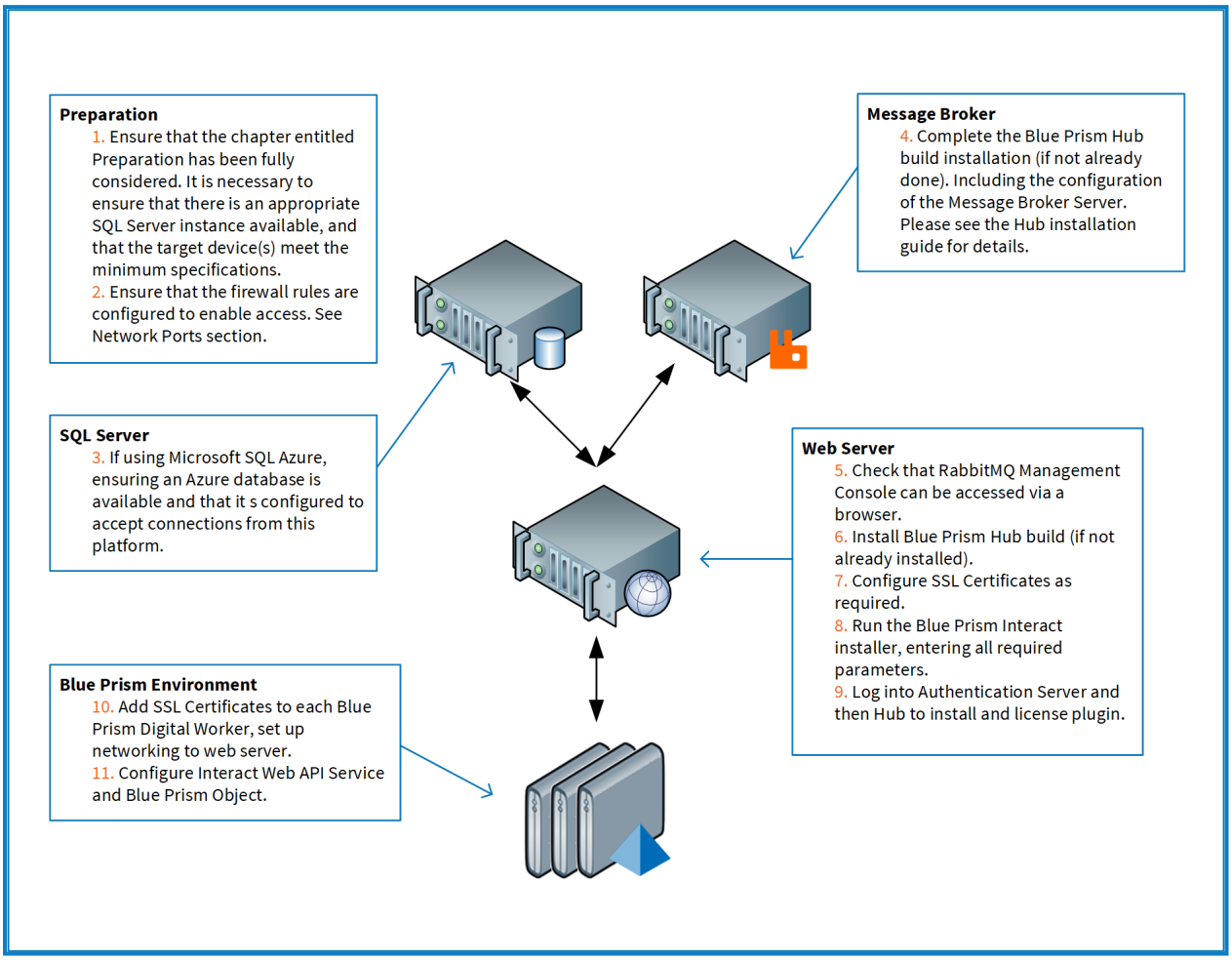
Le diagramme ci-dessous illustre l'architecture typique d'un environnement.



Les éléments en gris sont déployés dans le cadre de l'installation de Blue Prism Hub.

Aperçu des étapes d'installation typiques

Un aperçu des étapes généralement requises pour réaliser un déploiement typique est fourni ci-dessous.



Si vous rencontrez des problèmes pendant l'installation, voir Dépanner une installation.

Installer le serveur de l'agent de messages

Installez et configurez le serveur de l'agent de messages, y compris la configuration du pare-feu Windows pour activer la connectivité réseau et la console de gestion RabbitMQ.

Des vidéos explicatives sur la manière d'installer le logiciel pour le serveur de l'agent de messages sont disponibles sur : https://bpdocs.blueprism.com/video/installation.htm.

Pour les versions logicielles, voir Configuration logicielle sur la page 13.

Si l'agent de messages n'est pas déjà installé et configuré, suivez les étapes ci-dessous :

1. Téléchargez et installez Erlang, et acceptez les réglages par défaut dans l'assistant d'installation.

   La version d'Erlang dont vous avez besoin dépend de la version de RabbitMQ que vous avez l'intention d'utiliser. Pour :

   - Version d'Erlang/OTP et support : voir voir Configuration requise pour la version Erlang de RabbitMQ..
   - Informations d'installation, consultez le guide d'installation d'Erlang/OTP.
   - Téléchargements : voir Télécharger Erlang/OTP.

   Pour regarder cette étape d'installation, accédez à notre vidéo d'installation d'Erlang.

2. Téléchargez et installez RabbitMQ, et acceptez les réglages par défaut.

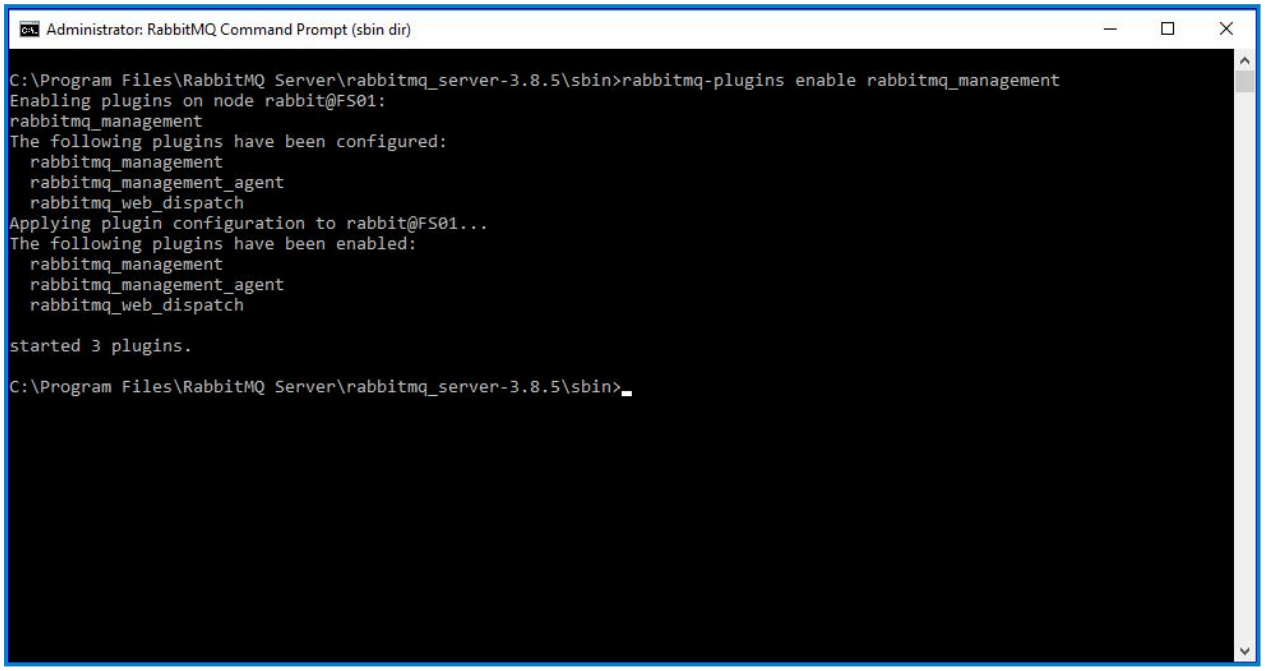
   Pour plus d'informations, voir voir Téléchargement et installation de RabbitMQ..

   Pour regarder cette étape d'installation, accédez à notre vidéo d'installation de RabbitMQ.

3. Configurez le pare-feu Windows pour activer le trafic entrant vers les ports 5672 et 15672.
4. Dans le menu Démarrer, sous le dossier du serveur RabbitMQ, sélectionnez l'invite de commande RabbitMQ (sbin dir).

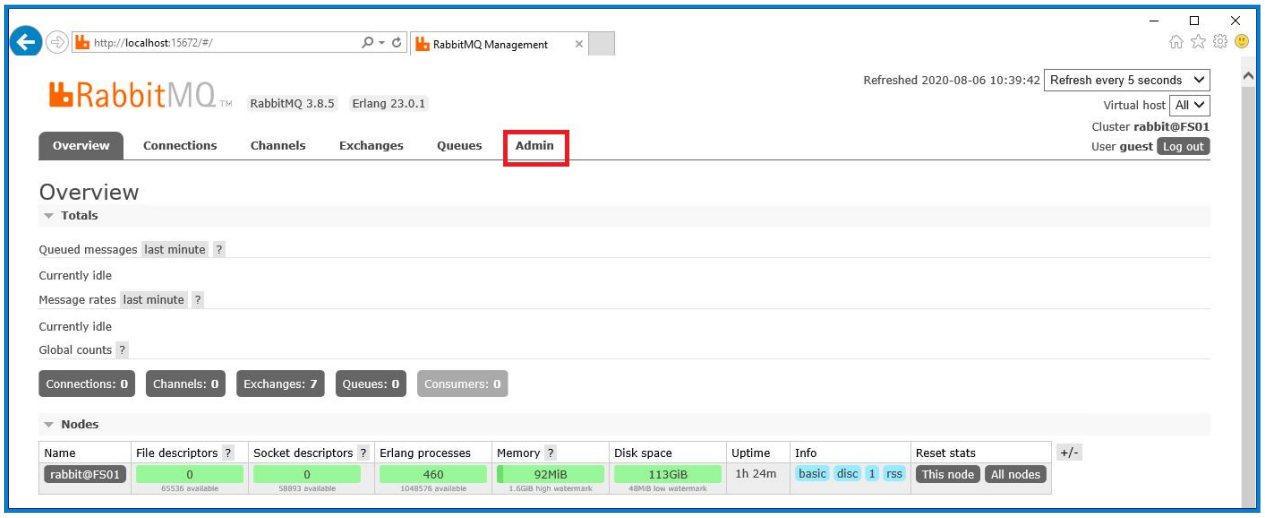
5. Dans la fenêtre d'invite de commande RabbitMQ, tapez la commande suivante :

```
rabbitmq-plugins enable rabbitmq_management
```

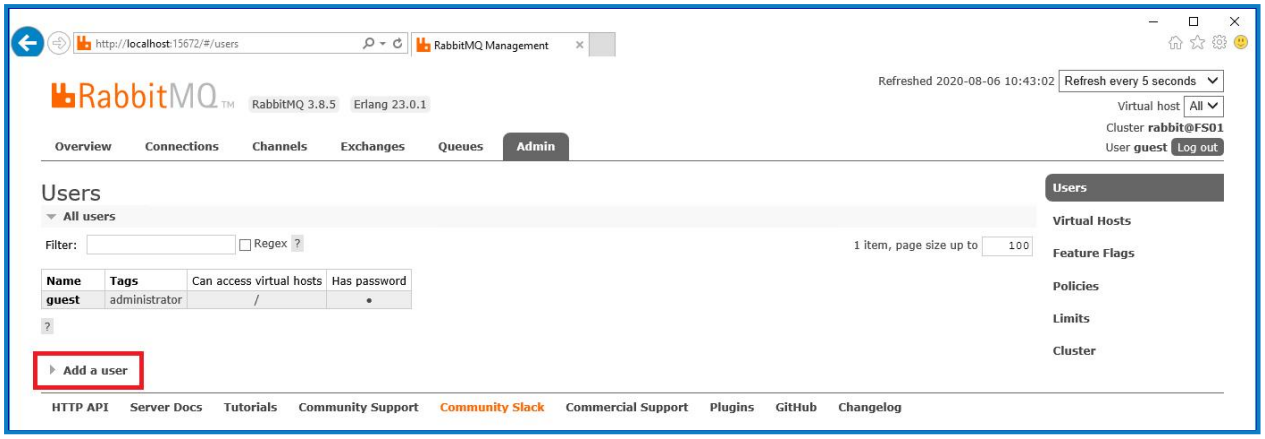


6. Lancez un navigateur et naviguez jusqu'à l'URL suivante : http://localhost:15672
7. Dans la console RabbitMQ, connectez-vous avec les identifiants par défaut de invité/invité.

8. Dans la console, cliquez sur **Admin**.



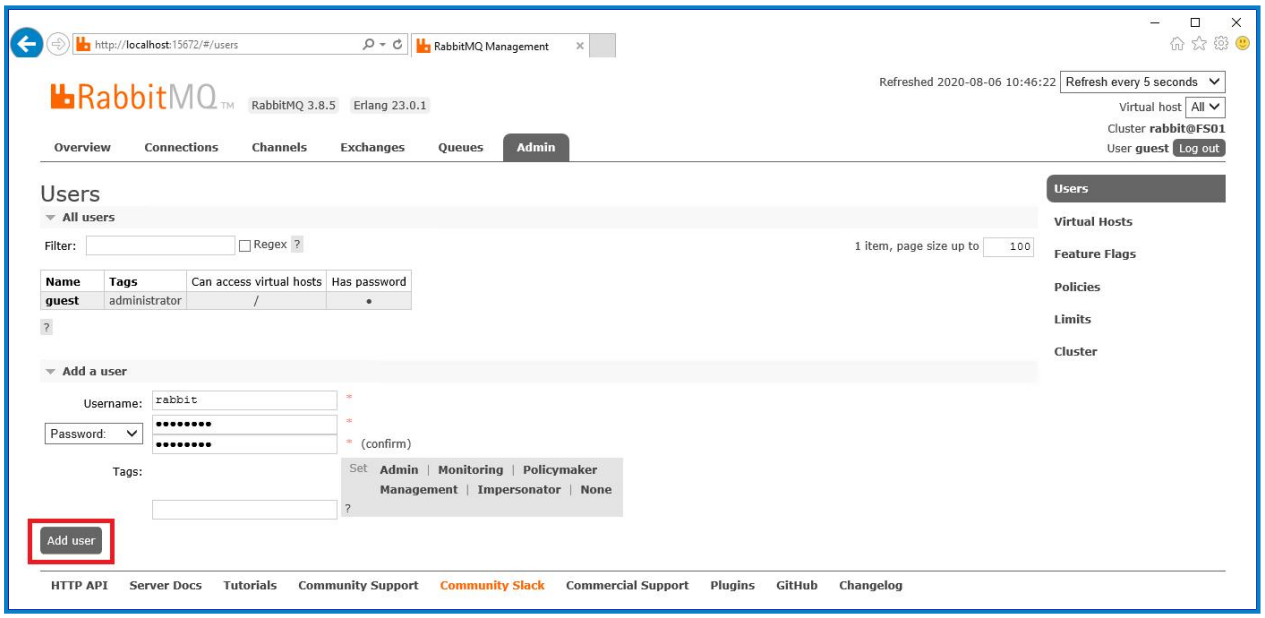
9. Cliquez sur **Ajouter un utilisateur**.



10. Saisissez les détails d'un nouvel utilisateur, en fournissant le nom d'utilisateur et le mot de passe. L'utilisateur ne nécessite aucune permission spéciale et le champ peut être laissé sur Aucun.

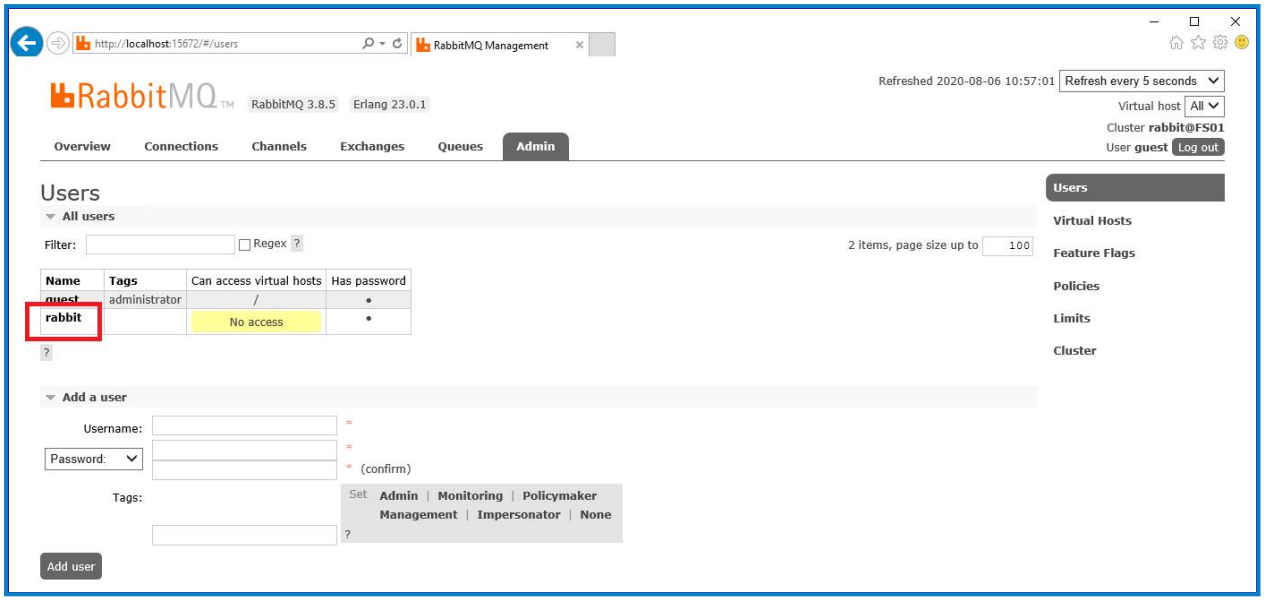
> Les caractères suivants ne doivent pas être utilisés pour le mot de passe lors de la création de l'utilisateur RabbitMQ **# / : ? @ \ ` " $ '**.

11. Cliquez sur **Ajouter l'utilisateur**.

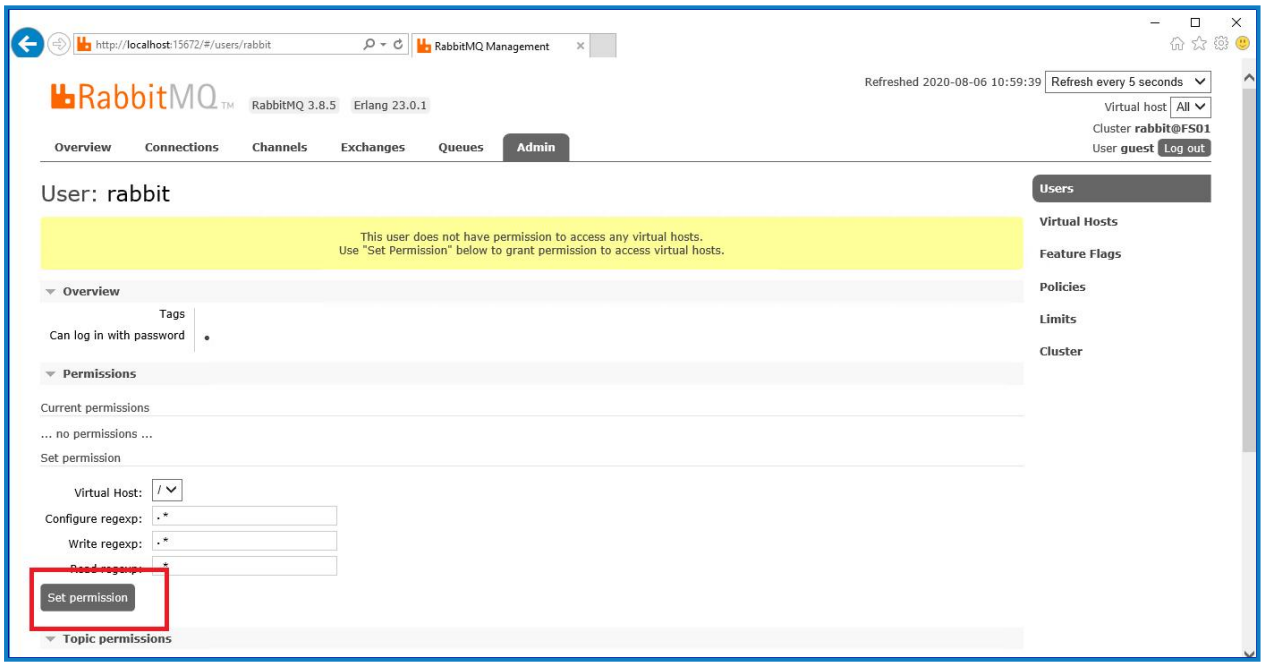


L'étape suivante consiste à définir les permissions pour l'utilisateur.

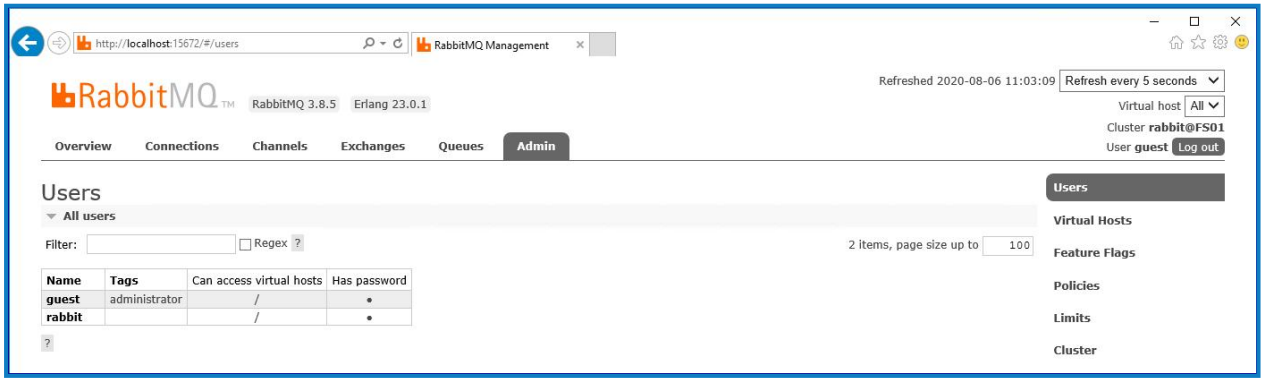
12. Cliquez sur le nom d'utilisateur de l'utilisateur que vous venez de créer.



13. Cliquez sur **Définir les permissions** pour attribuer les permissions par défaut.



14. Sélectionnez l'onglet **Admin** en haut et vérifiez que les permissions ont été correctement définies, comme indiqué ci-dessous.



Ce compte n'a pas d'accès à la console de gestion, donc l'utilisation des identifiants que vous venez de créer n'activera aucun accès.

Il s'agit d'une configuration générique et d'une installation de base d'un service d'agent de messages RabbitMQ. Il est recommandé que les mots de passe par défaut soient modifiés et que les exigences de sécurité, telles que l'application des certificats SSL, soient satisfaites par votre service informatique.

Il est recommandé de créer un compte administrateur et de supprimer le compte invité par défaut. Laisser le compte invité par défaut disponible peut présenter un risque de sécurité.

Vérifier la connectivité de l'agent de messages RabbitMQ

Lancez un navigateur et tapez l'URL suivante : http://<Nom d'hôte de l'agent de messages>:15672

La page de connexion de la console de gestion RabbitMQ doit s'afficher.

Vous ne pourrez pas vous connecter à la console de gestion, car le compte invité est limité à l'accès local et le compte que vous avez créé n'est pas autorisé à accéder à la console de gestion.

Si la console n'apparaît pas, redémarrez le service RabbitMQ. Si la console n'apparaît toujours pas, voir Dépanner une installation Hub sur la page 99.

Installer et configurer le serveur Web

Avant d'installer le serveur Web Hub, assurez-vous d'avoir lu les informations dans Préparation sur la page 7.

Installez et configurez le serveur Web en veillant à ce que le système puisse communiquer avec l'agent de messages RabbitMQ.

Le processus comprend les étapes suivantes :

1. Installer IIS
2. Configurer les certificats SSL
3. Installer les composants .NET Core
4. Installer Blue Prism Hub
5. Installer l'extension Authentication Server SAML 2.0 : cette action n'est requise que si vous avez l'intention d'utiliser l'authentification SAML 2.0.

Les noms d'hôte par défaut fournis dans les procédures ci-dessous ne sont adaptés qu'à un environnement autonome, tel qu'un environnement de test. Les structures DNS et de domaine de votre organisation doivent être prises en compte lors du choix des noms d'hôte dans votre installation.

Des vidéos explicatives sur la manière d'installer le logiciel de prérequis et Blue Prism Hub sont disponibles sur : https://bpdocs.blueprism.com/fr-fr/video/installation.htm.

Installer IIS

Le système requiert que le serveur Web IIS et les composants .NET Core soient installés.

Il est important qu'IIS soit installé avant d'installer les composants .NET Core et Blue Prism Hub. Les fonctionnalités et les rôles IIS sont automatiquement installés dans le cadre de l'installation de Blue Prism Hub.

Installation scriptée

Exécutez la commande ci-dessous à l'aide de l'invite de commande PowerShell :

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

Pour regarder cette étape d'installation, accédez à notre vidéo d'installation d'IIS.

Par défaut, IIS est installé avec le réglage **Authentification anonyme** activé. Ce réglage est requis par Hub et ses sites associés. Si vous avez désactivé l'**authentification anonyme**, vous devez l'activer avant d'exécuter l'assistant d'installation de Hub. Pour plus d'informations sur l'authentification anonyme, consultez la page Authentification anonyme de Microsoft.

Configurer les certificats SSL

Pendant le processus d'installation, vous serez invité à fournir les certificats SSL pour les sites Web en cours de configuration. Selon les exigences de sécurité de votre infrastructure et de votre organisation informatique, il peut s'agir d'un certificat SSL créé en interne ou d'un certificat acheté pour protéger les sites Web.

Lors de la génération d'un certificat, saisissez le nom d'hôte en minuscules. Si vous n'utilisez pas exclusivement des minuscules, vous risquez de rencontrer un problème de correspondance entre le nom du certificat et le nom de l'hôte lorsque vous utiliserez le programme d'installation de Hub. Cela pourrait entraîner l'échec de l'application du certificat et empêcher le programme d'installation de poursuivre la procédure.

Le programme d'installation peut être exécuté sans que les certificats soient présents, bien que pour que les sites fonctionnent, les liaisons des sites Web IIS devront avoir des certificats SSL valides présents.

Les tableaux ci-dessous détaillent les certificats SSL requis.

Sites Web de Hub :

Site Web dans IIS	URL par défaut (exemple uniquement)
Sites Web dotés d'une interface utilisateur destinée à être utilisée par les utilisateurs finaux	
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – Hub	https://hub.local
Sites Web destinés à être utilisés uniquement par l'application (services)	
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

Sites Web Interact :

Site Web dans IIS	URL par défaut
Sites Web avec une interface utilisateur destinée à être utilisée par les utilisateurs finaux	
Blue Prism – Interact	https://interact.local
Sites Web destinés à être utilisés uniquement par l'application (services)	
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local

Les URL par défaut indiquées ci-dessus conviennent à un environnement autonome, tel qu'un environnement de test. Les structures DNS et de domaine de votre organisation doivent être prises en compte lors du choix des noms d'hôte pour votre installation.

Certificats autosignés

Les certificats autosignés peuvent être utilisés, mais ne sont recommandés que pour les environnements de preuve de concept (POC), de preuve de valeur (POV) et de développement (Dev). Pour les environnements de production, utilisez les certificats de l'autorité de certification approuvée de votre organisation. Il est recommandé de contacter votre équipe de sécurité informatique pour vérifier leurs exigences.

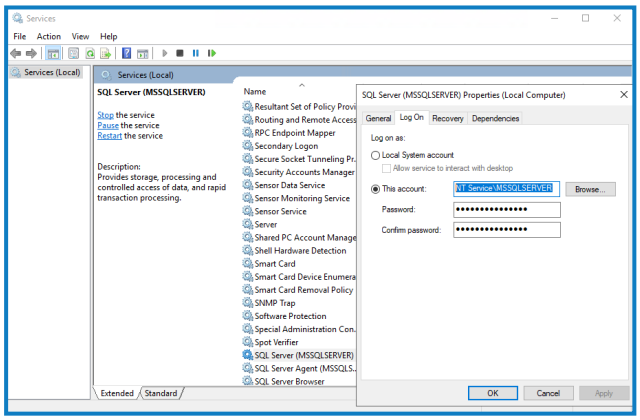
Pour générer et appliquer un certificat autosigné pour SQL Server :

> Microsoft fournit un script qui peut être utilisé pour générer un certificat autosigné pour SQL Server. Voir la documentation Google pour en savoir plus. Il est important que le nom de domaine explicite (FQDN) utilisé par SQL Server corresponde au FQDN défini dans le certificat. **S'ils ne correspondent pas, la connexion à la base de données ne sera pas établie et votre installation ne fonctionnera pas correctement.**

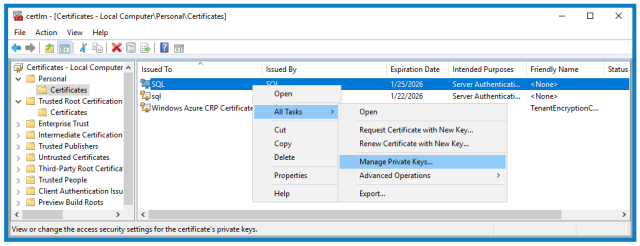
1. Exécutez PowerShell en tant qu'administrateur et exécutez le script Microsoft avec les informations de votre serveur SQL :

   Cela génère le certificat et l'installe sur SQL Server.

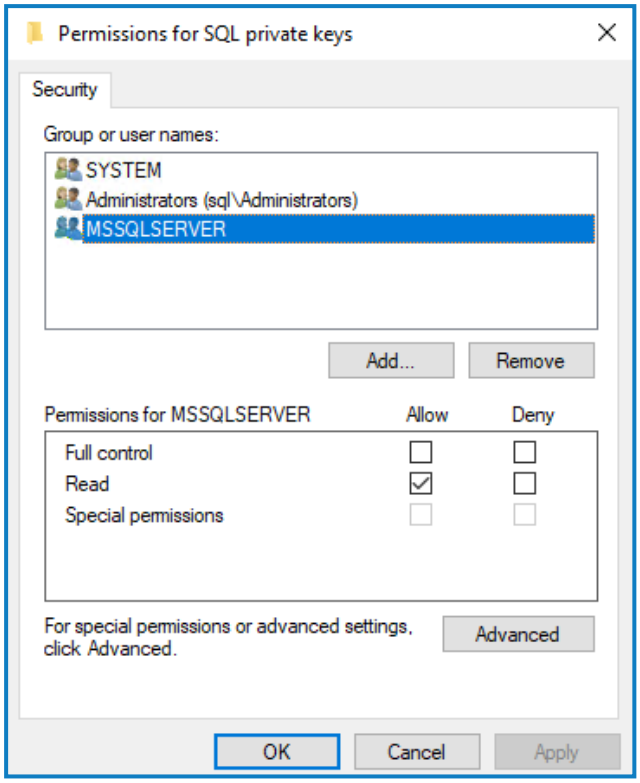
2. Sur votre serveur SQL :
   a. Activez l'accès à la clé privée du certificat pour le compte de service SQL Server. Pour ce faire :
      i. Si vous ne le connaissez pas déjà, recherchez le nom de votre compte de service pour votre serveur SQL. Vous le trouverez dans l'onglet Connexion des propriétés SQL Server, accessible dans les services de votre serveur SQL.



      ii. Ouvrez le gestionnaire de certificats sur votre serveur SQL.
      iii. Développez **Personnel**, puis **Certificats**, cliquez avec le bouton droit sur **SQL**, puis sélectionnez **Toutes les tâches** et cliquez sur **Gérer les clés privées...**



iv. Dans la boîte de dialogue Permissions pour les clés privées SQL, ajoutez votre compte de service SQL Server avec les permissions de lecture. Par exemple :



v. Cliquez sur **OK** pour appliquer les modifications et fermer la boîte de dialogue.

b. Activez SSL sur votre serveur SQL et spécifiez le certificat. Pour ce faire :

i. Dans la barre des tâches Windows, ouvrez **SQL Server Configuration Manager**.

ii. Dans SQL Server Configuration Manager, développez **Configuration réseau SQL Server** et cliquez avec le bouton droit sur **Protocoles pour <SqlServerInstanceName>**, puis cliquez sur **Propriétés**.

iii. Dans la boîte de dialogue Protocoles pour les propriétés <SqlServerInstanceName>, sélectionnez l'onglet **Certificat**, puis sélectionnez ou importez le certificat requis.

iv. Cliquez sur **Appliquer**.

v. Cliquez sur **OK** pour fermer la boîte de dialogue Propriétés.

c. Redémarrez le service SQL Server.

d. Copiez le certificat C:\sqlservercert.cer. Vous devrez l'ajouter aux serveurs hôtes du site Web Hub et Interact.

3. Sur les serveurs hôtes du site Web :

a. Collez sqlservercert.cer dans les serveurs hôtes du site Web pour Hub et Interact.

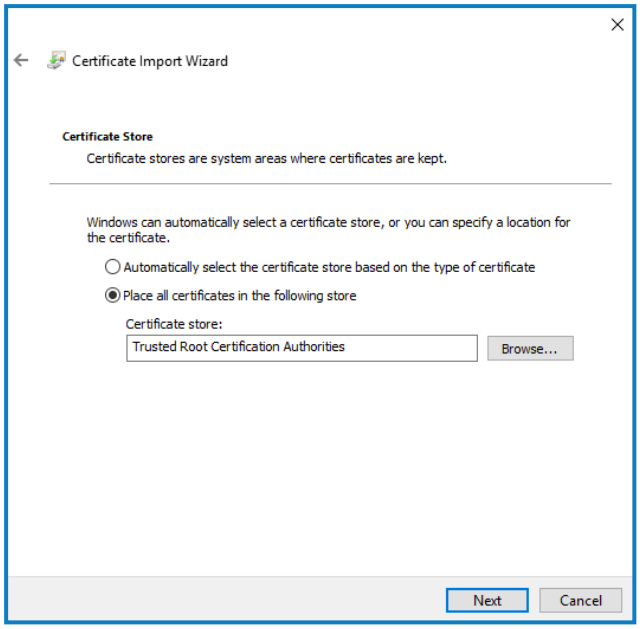
b. Ajoutez le certificat au magasin de certificats des autorités de certification racine de confiance du serveur. Pour ce faire :

i. Double-cliquez sur le certificat et cliquez sur **Installer le certificat...**.

L'assistant d'importation du certificat s'affiche.

ii. Sur la page d'accueil, sélectionnez **Machine locale** sous **Emplacement du magasin** et cliquez sur **Suivant**.

iii. Sur la page Magasin de certificats, sélectionnez **Placer tous les certificats dans le magasin suivant** et saisissez **Autorités de certification racine de confiance**.



iv. Cliquez sur **Suivant** et suivez l'assistant jusqu'à la fin.

c. Testez la connexion entre le serveur hôte du site Web et SQL Server.

Pour générer un certificat autosigné pour un site Web :

1. Exécutez PowerShell en tant qu'administrateur et utilisez la commande suivante, en remplaçant `[Website]` et `[ExpiryYears]` par les valeurs appropriées :

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

Par exemple :

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

Cet exemple crée un certificat autosigné appelé *MySiteCertAuthentication* dans le magasin de certificats personnels, avec *authentication.local* comme objet. Ce certificat est valide pendant 10 ans à compter de la création.

> Lors de la génération d'un certificat, saisissez le nom d'hôte (`[Website]`) en minuscules. Si vous n'utilisez pas exclusivement des minuscules, vous risquez de rencontrer un problème de correspondance entre le nom du certificat et le nom de l'hôte lorsque vous utiliserez le programme d'installation de Hub. Cela pourrait entraîner l'échec de l'application du certificat et empêcher le programme d'installation de poursuivre la procédure.

2. Ouvrez l'application Gérer les certificats de l'ordinateur sur votre serveur Web (saisissez **gérer l'ordinateur** dans la barre de recherche).

3. Copiez et collez le certificat depuis Personnel > Certificats vers Certification racine de confiance > Certificats.
4. Répétez ce processus pour chaque site Web.

Création scriptée des certificats autosignés du site Web

> Ce processus n'est pas recommandé pour les environnements de production. Ce processus créera un certificat unique qui peut être appliqué à chaque site Web.

Exécutez les commandes PowerShell suivante :

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

> XXXXXXXXXX doit être remplacé par le nom du serveur hôte.

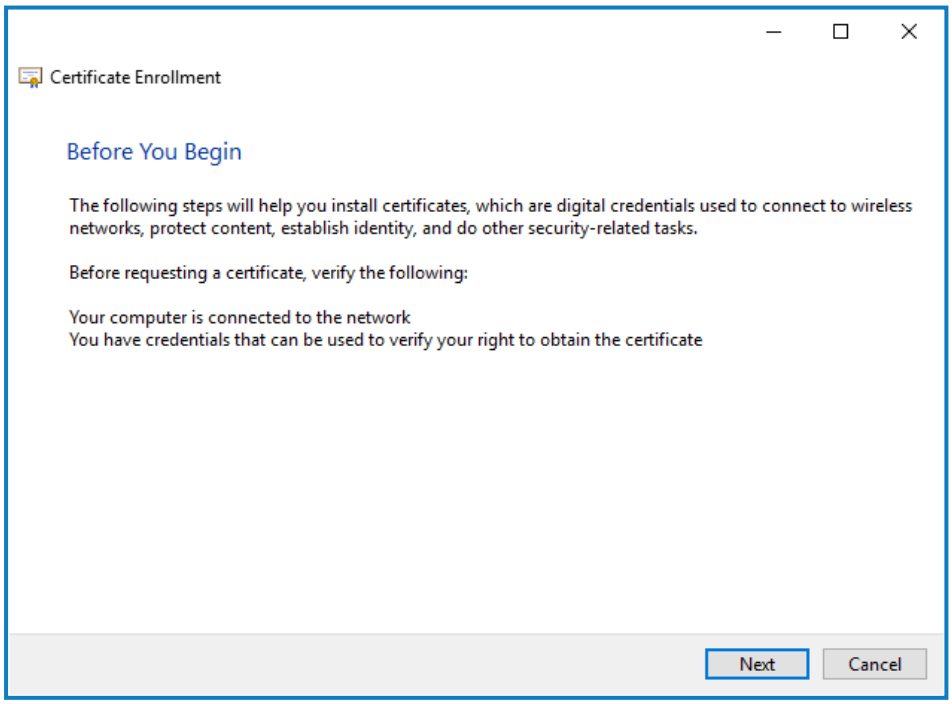
Une fois les certificats créés, ouvrez le gestionnaire de certificats de la machine locale (certlm) et copiez-collez-le dans le magasin de certificats racine de confiance.

Créer une requête de certificat hors ligne

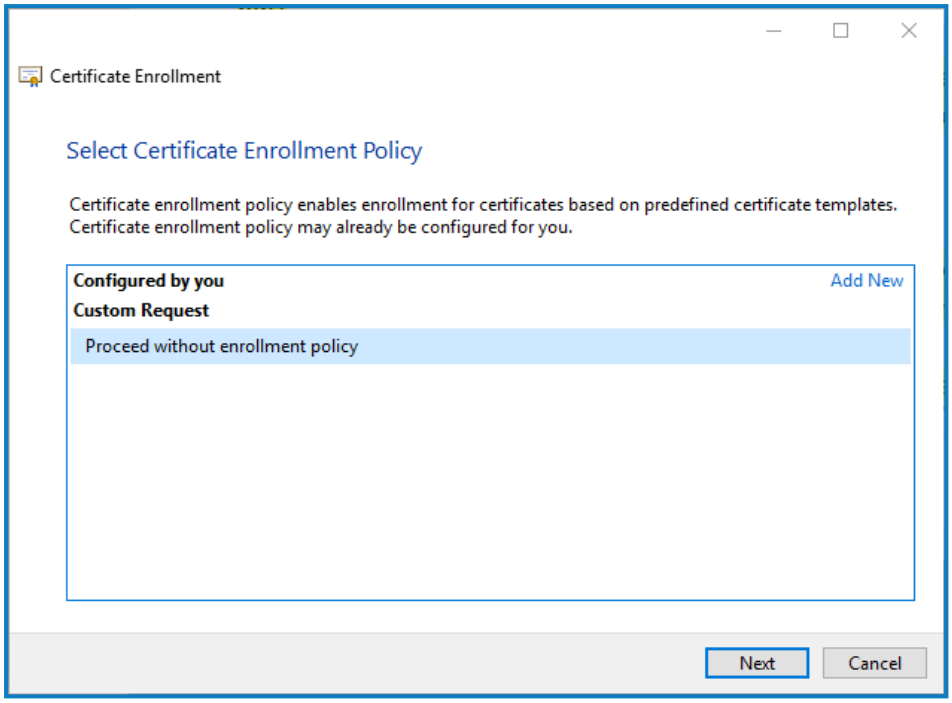
Pour créer une requête de certificat hors ligne, suivez la procédure suivante pour chaque certificat :

1. Ouvrez l'application Gérer les certificats de l'ordinateur sur votre serveur Web (saisissez **ordinateur géré** dans la barre de recherche).
2. Cliquez avec le bouton droit sur **Personnel** > **Certificats** et sélectionnez **Toutes les tâches** > **Opérations avancées** > **Créer une requête personnalisée** dans le menu contextuel.

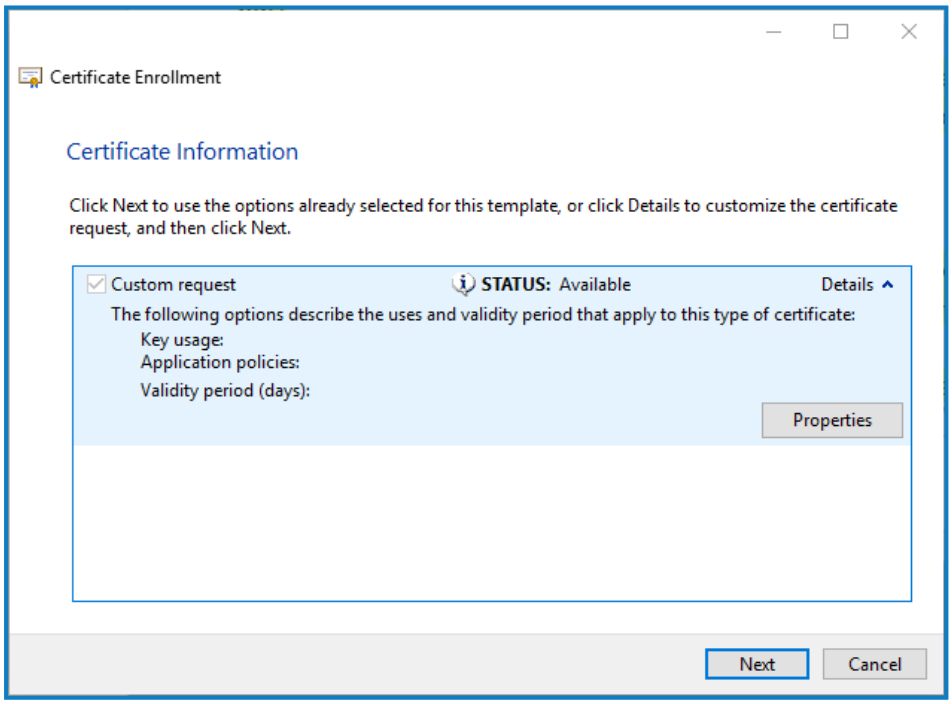
   L'assistant Inscription de certificat s'affiche.



3. Cliquez sur **Suivant**.



4. Sélectionnez **Continuer sans politique d'inscription** et cliquez sur **Suivant**.
5. Sur l'écran Requête personnalisée, cliquez sur **Suivant**.
6. Sur l'écran Informations du certificat, cliquez sur le menu déroulant **Détails** et sur **Propriétés**.



7. Dans l'onglet Général de la boîte de dialogue Propriétés du certificat, saisissez un nom convivial et une description basée sur le site Web auquel ce certificat sera appliqué.
8. Dans l'onglet Objet, remplacez le type de nom de l'objet par **Nom commun**, saisissez l'URL du site Web dans le champ **Valeur** et cliquez sur **Ajouter**.

   Le CN (nom commun) s'affichera dans le panneau de droite.

9. Dans l'onglet Extensions, cliquez sur **Utilisation étendue des clés**, sélectionnez **Authentification du serveur** et cliquez sur **Ajouter**.
10. Dans l'onglet Clé privée, cliquez sur **Options de clé**, sélectionnez la taille de clé de votre choix et sélectionnez **Rendre la clé privée exportable**.
11. Toujours dans l'onglet Clé privée, cliquez sur **Algorithme de hachage** et sélectionnez un hachage approprié (facultatif).
12. Cliquez sur **OK**.

    Vous êtes renvoyé à l'écran Inscription au certificat.
13. Cliquez sur **Suivant**.
14. Ajoutez un nom de fichier et un chemin d'accès, et cliquez sur **Terminer**.

Après avoir créé votre requête de certificat, vous devrez la soumettre à une autorité de certification afin que cette dernière puisse la traiter et émettre un certificat. La requête de certificat est un fichier texte. Généralement, vous devez copier le texte du fichier et le saisir dans un formulaire de soumission en ligne sur le site Web de l'autorité de certification. Vous devrez contacter votre autorité de certification directement pour obtenir des instructions sur le processus de soumission de votre requête de certificat.

Installer les composants .NET Core

Les composants .NET Core doivent être téléchargés et installés.

Étape	Détails
1	Téléchargez les composants suivants et stockez-les dans un emplacement temporaire, par exemple, C:\temp : • ASP.NET Core Runtime 6.0.9 ou 6.0.10 (bundle d'hébergement Windows) https://dotnet.microsoft.com/download/dotnet/6.0 : sélectionnez la version dont vous avez besoin. Sous **ASP.NET Core Runtime**, sélectionnez **Bundle d'hébergement**. • .NET Desktop Runtime 6.0.9 ou 6.0.10 https://dotnet.microsoft.com/download/dotnet/6.0 : sélectionnez la version dont vous avez besoin. Sous **.NET Desktop Runtime**, sélectionnez le téléchargement approprié. • .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 Il est installé par défaut sur Windows Server 2022. Vous n'avez besoin d'installer .NET Framework que si vous utilisez Windows Server 2016 Datacenter ou Windows Server 2019.

2	Pour installer les dépendances .NET, exécutez chacune des commandes suivantes à l'aide de l'invite de commande PowerShell, en veillant à attendre que chacune se termine avant d'exécuter la commande suivante :
	Pour Windows Server 2016 et Windows Server 2019 :
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	`start-process "C:\temp\ndp48-x86-x64-allos-enu.exe" /q -wait`
	Pour Windows Server 2022 :
	`start-process "C:\temp\dotnet-hosting-6.0.0-win.exe" /q -wait`
	`start-process "C:\temp\windowsdesktop-runtime-6.0.0-win-x64.exe" /q -wait`
	Assurez-vous que le nom du fichier et le chemin d'accès correspondent aux fichiers qui ont été stockés à l'étape 1.

3	Redémarrez votre serveur avant d'installer Blue Prism Hub pour vous assurer que les composants sont entièrement installés et enregistrés.

Pour regarder cette étape d'installation, accédez à notre vidéo d'installation de .NET.

Installer Blue Prism Hub

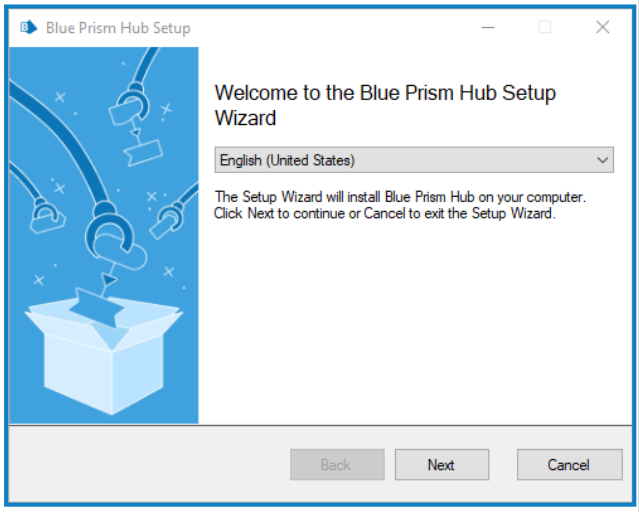
Avant d'installer Blue Prism Hub :

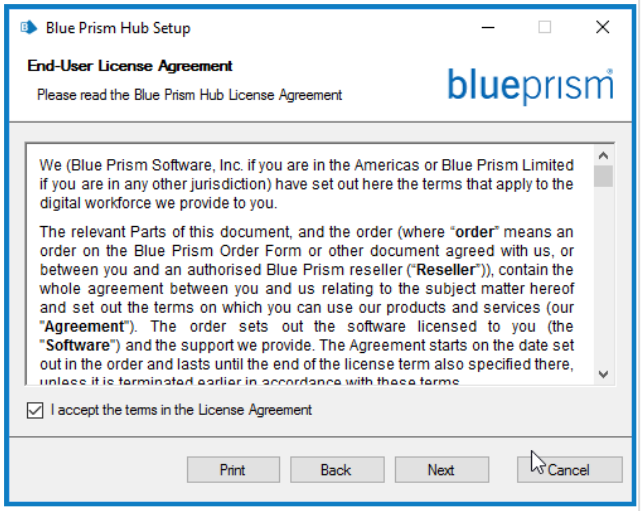
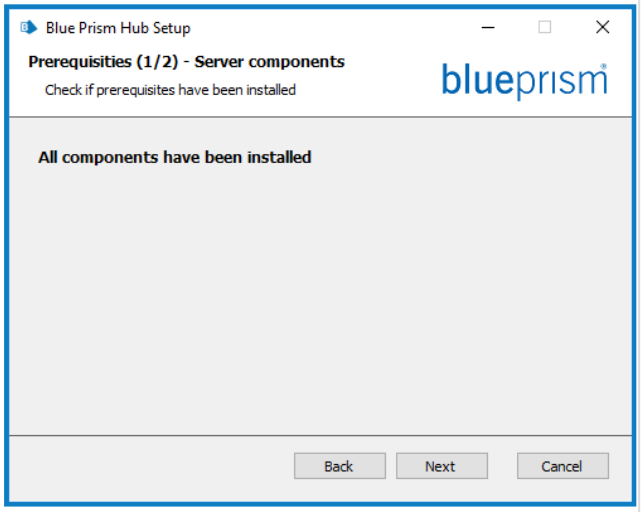
- Si vous avez acheté ALM, Decision ou Interact, vous aurez besoin de votre ID client pendant l'installation de Hub. Vous le trouverez dans l'e-mail qui vous a été envoyé lorsque vous avez acheté ALM, Decision ou Interact.
- Si vous souhaitez utiliser le plug-in Blue Prism Decision dans Hub, vous devrez installer le conteneur de Blue Prism Decision Model Service sur un hôte Docker avant d'exécuter l'assistant d'installation de Hub. Pour plus d'informations, voir Installer Blue Prism Decision.
- Si vous réinstallez Blue Prism Hub après l'avoir utilisé et l'avoir supprimé, et que les mêmes noms de base de données doivent être utilisés, il est recommandé d'effacer toutes les anciennes données des bases de données avant la réinstallation.

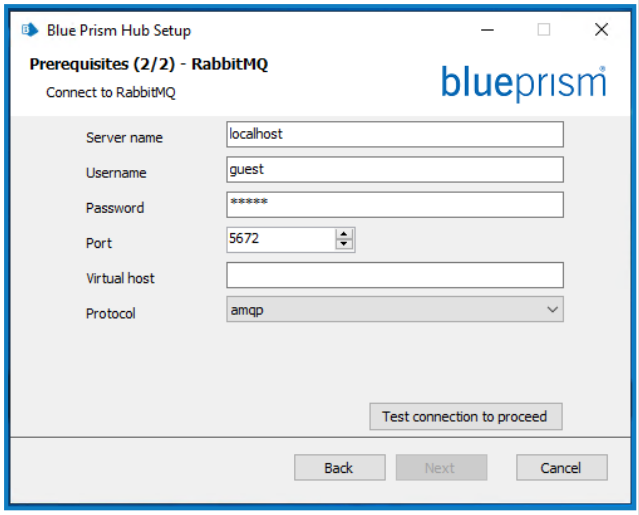
Pour regarder le processus d'installation et de configuration de Hub, accédez à notre vidéo d'installation de Blue Prism Hub.

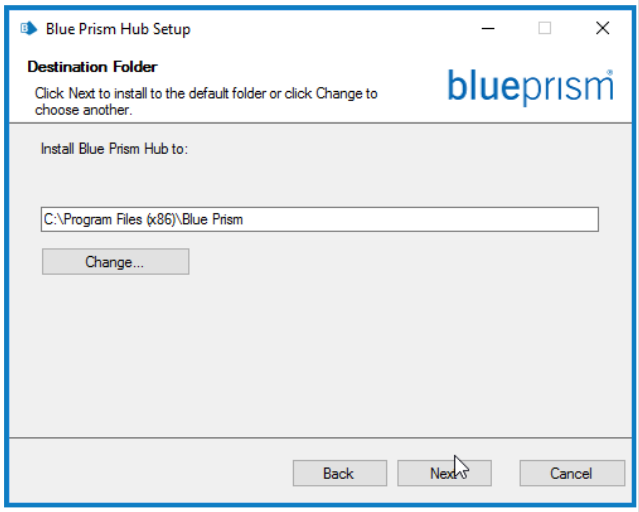
Les étapes ci-dessous détaillent le processus d'installation du logiciel Blue Prism Hub. Cela inclut Authentication Server, Hub et les autres services associés. Le processus d'installation créera toutes les bases de données requis.

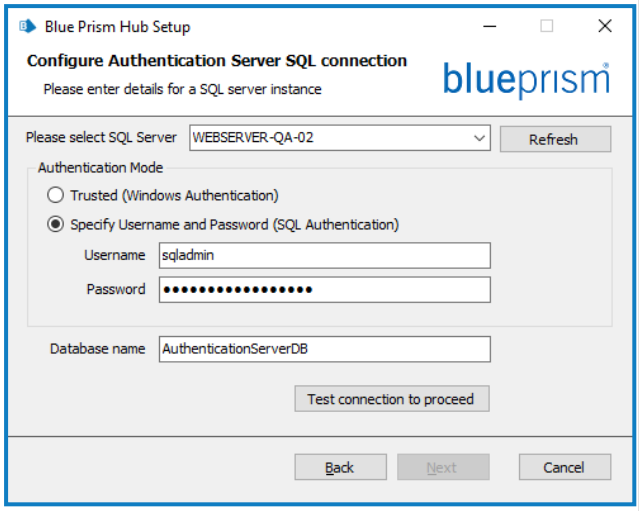
Téléchargez et exécutez le programme d'installation de Blue Prism Hub, disponible sur le portail Blue Prism, et progressez dans l'assistant d'installation comme indiqué ci-dessous. L'assistant d'installation doit être exécuté avec des droits d'administrateur.

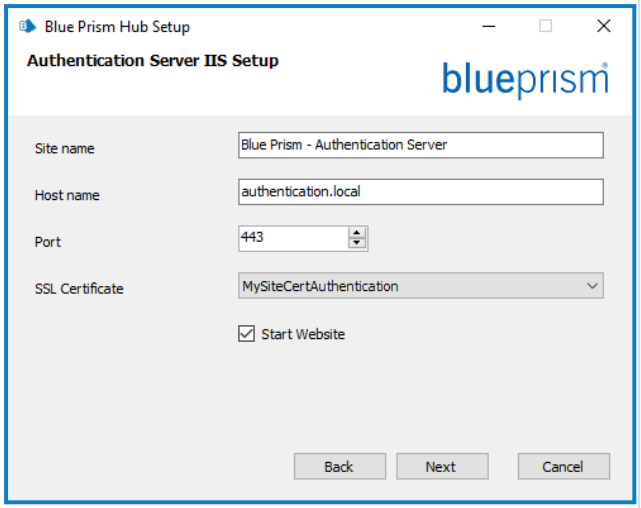
Étape	Page du programme d'installation	Détails
1		**Bienvenue** Si nécessaire, sélectionnez une autre langue pour l'assistant d'installation dans la liste déroulante. La langue par défaut est l'anglais (États-Unis). Cliquez sur **Suivant**.

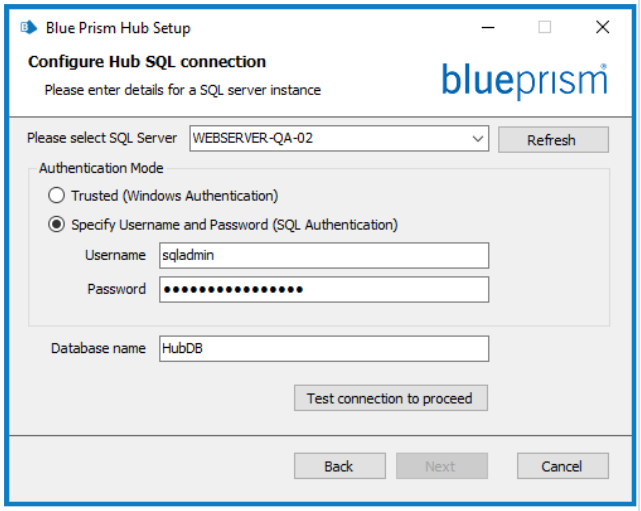
Étape	Page du programme d'installation	Détails
2		**Contrat de licence** Lisez le contrat de licence de l'utilisateur final et, si vous acceptez les conditions, cochez la case.
3		**Prérequis 1 – Composants du serveur** Le programme d'installation vérifie que les prérequis ont été installés. Ceux qui ne sont pas installés sont identifiés. Vous ne pouvez pas continuer tant que tous les prérequis n'ont pas été installés. Si des prérequis ne sont pas installés, annulez le programme d'installation et installez les composants manquants avant de redémarrer le programme d'installation. Sinon, procédez à l'installation.

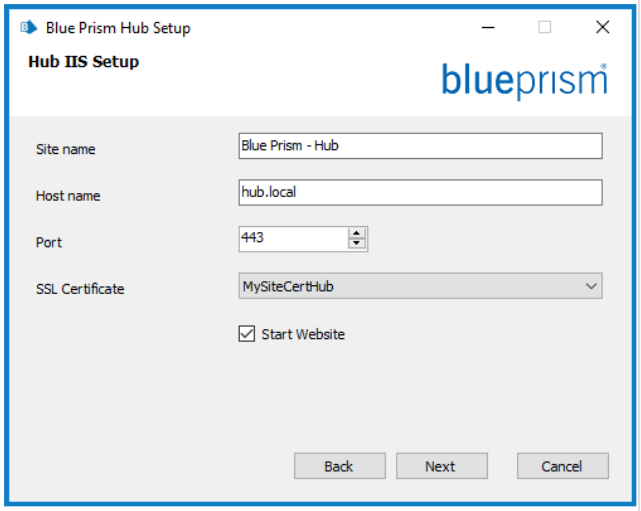
Étape	Page du programme d'installation	Détails
4		**Prérequis 2 – RabbitMQ** Saisissez le nom du serveur ou l'adresse IP du serveur de l'agent de messages et les identifiants de l'utilisateur que vous avez créé. Le port de mise en file d'attente des messages par défaut est 5672. Il ne doit être modifié que si les ports par défaut ont été modifiés par votre service de support informatique. Par défaut, le champ **Hôte virtuel** est vide. Vous pouvez laisser ce champ vide et la connexion sera établie à la racine de RabbitMQ. Sinon, si vous avez des hôtes virtuels configurés dans RabbitMQ, vous pouvez vous connecter à un hôte spécifique. Dans **Hôte virtuel**, saisissez le nom de l'hôte virtuel sur RabbitMQ auquel vous souhaitez vous connecter. L'hôte virtuel doit déjà exister sur RabbitMQ. Vous ne pouvez pas saisir un nouveau nom, car ce programme d'installation ne créera pas d'hôte virtuel. Des informations supplémentaires sur les hôtes virtuels sont disponibles sur le site Web RabbitMQ - Hôtes virtuels. Dans la liste déroulante **Protocole**, sélectionnez le protocole que vous souhaitez utiliser. Vous pouvez sélectionner AMQP ou AMQPS. Si vous sélectionnez AMQPS, un champ supplémentaire s'affiche pour vous permettre d'entrer le certificat qui doit être utilisé pour la connexion. Pour plus d'informations sur la configuration et les certificats TLS, consultez le site Web RabbitMQ - Prise en charge de TLS. Si vous utilisez AMQPS, vous devrez donner aux pools d'applications Blue Prism IIS le contrôle total du certificat RabbitMQ. Pour plus d'informations, voir Dépanner une installation Hub sur la page 99. Cliquez sur **Tester la connexion** pour vérifier la connectivité. Une notification

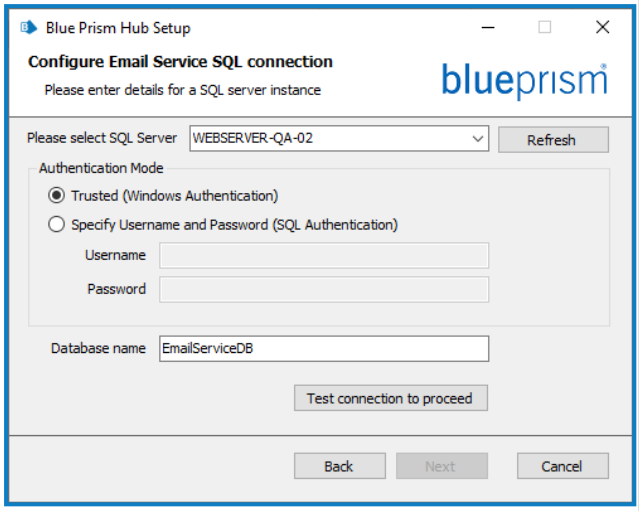
Étape	Page du programme d'installation	Détails
		affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. En cas d'échec du test, voir Dépanner une installation Hub sur la page 99 pour en savoir plus.
5		**Dossier de destination** Spécifiez le dossier d'installation requis. L'emplacement par défaut est C:\Program Files (x86)\Blue Prism, mais vous pouvez choisir un autre emplacement à l'aide du bouton **Modifier**.

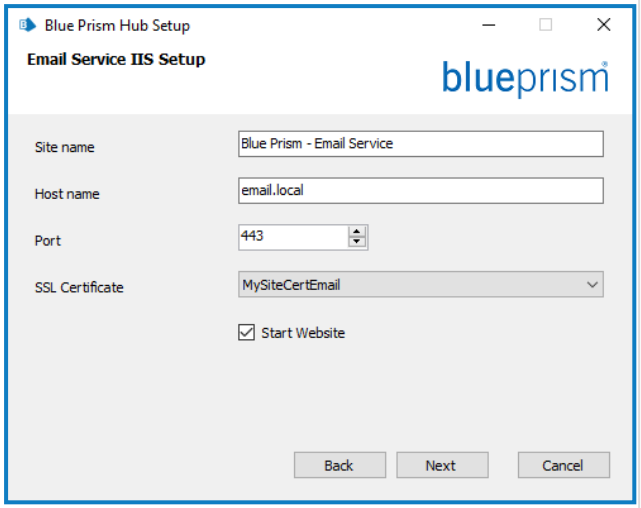
Étape	Page du programme d'installation	Détails
6		**Connexion SQL d'Authentication Server** Configurer les réglages de la base de données Authentication Serveren fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

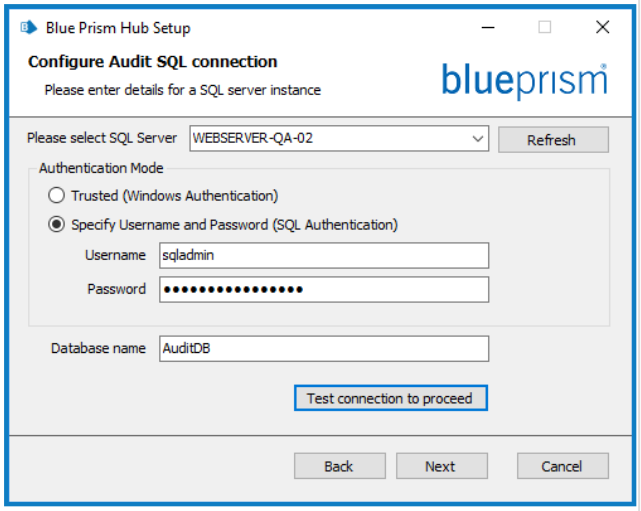
Étape	Page du programme d'installation	Détails
7		**Configuration IIS d'Authentication Server** Configurez IIS pour le site Web Authentication Server. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation. Une fois l'installation terminée, la fonctionnalité IIS **Authentification Windows** est activée sur le site Web d'Authentication Server.

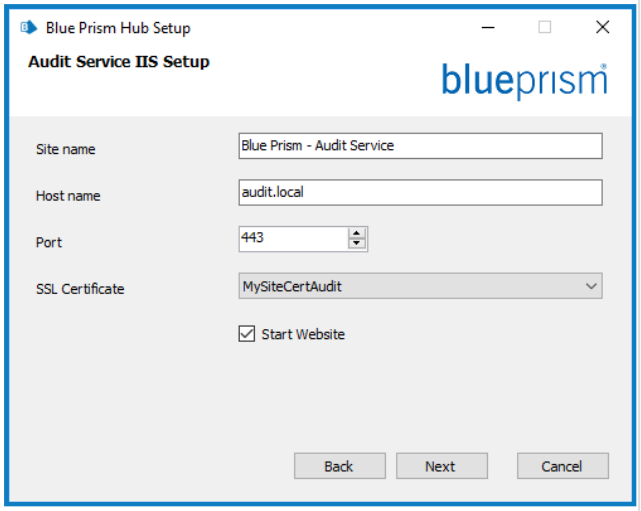
Étape	Page du programme d'installation	Détails
8		**Connexion SQL de Hub** Configurer les réglages de la base de données Huben fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

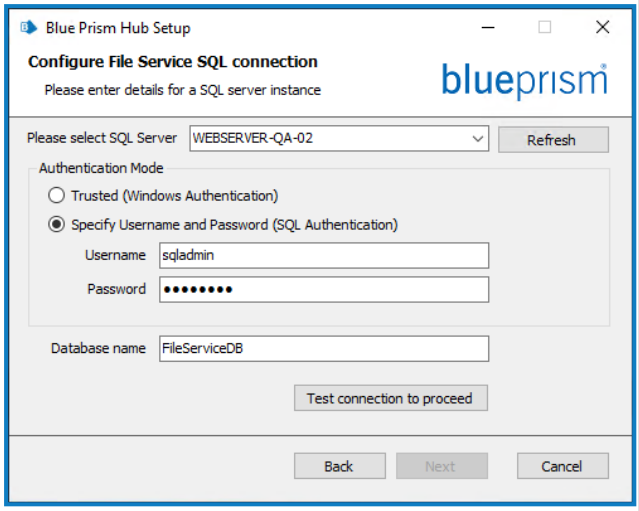
Étape	Page du programme d'installation	Détails
9		**Configuration IIS de Hub** Configurez le site Web de Hub. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

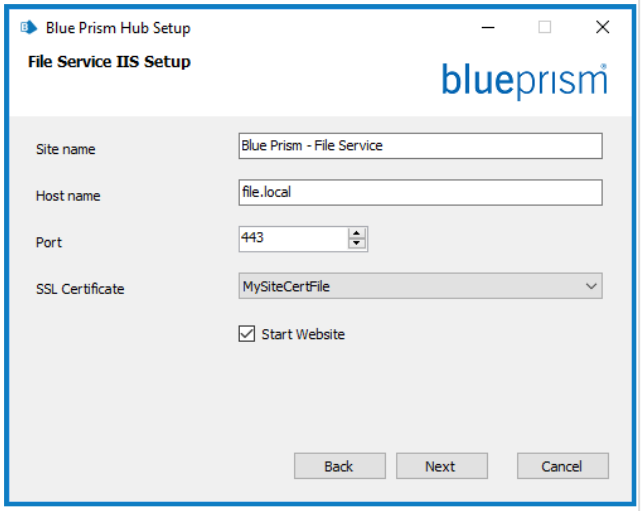
Étape	Page du programme d'installation	Détails
10		**Connexion SQL d'Email Service** Configurer les réglages de la base de données Email Service en fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

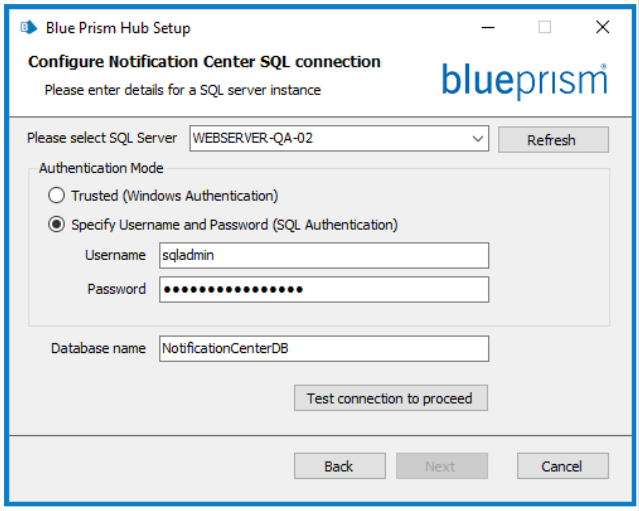
Étape	Page du programme d'installation	Détails
11		**Email Service Configuration IIS** Configurez le site Web Email Service. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

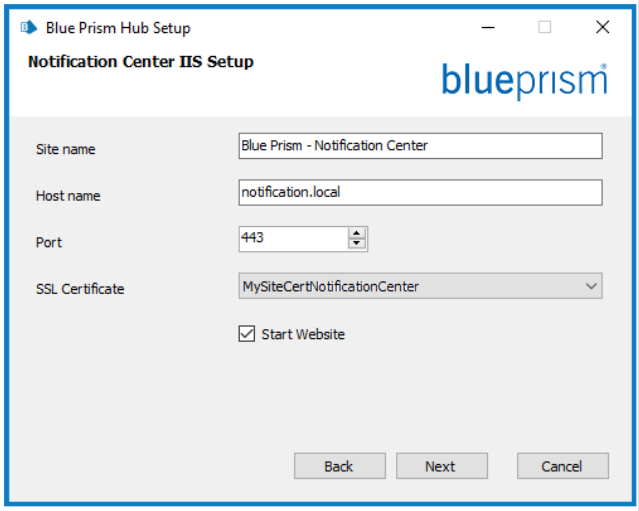
Étape	Page du programme d'installation	Détails
12		**Configuration d'une connexion SQL d'Audit** Configurer les réglages de la base de données Audit en fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

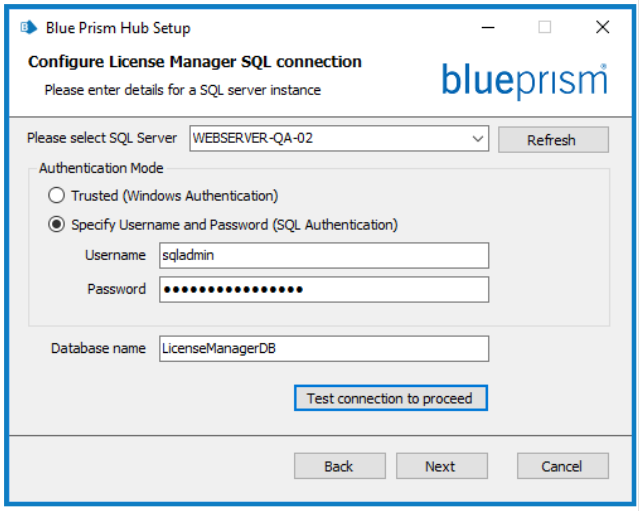
Étape	Page du programme d'installation	Détails
13		**Configuration IIS d'Audit Service** Configurez le site Web d'Audit Service. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

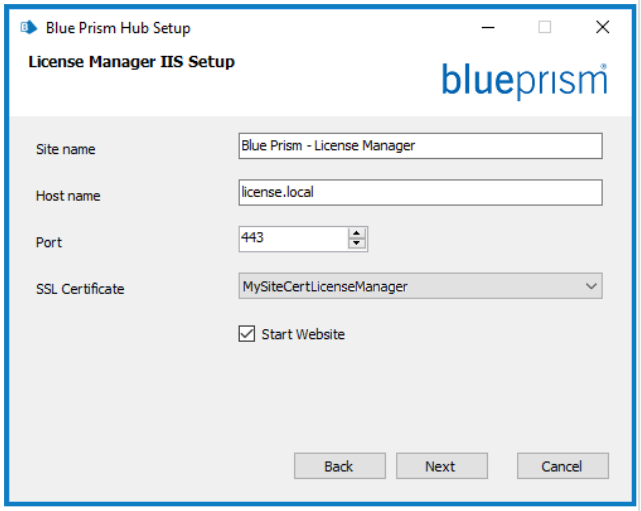
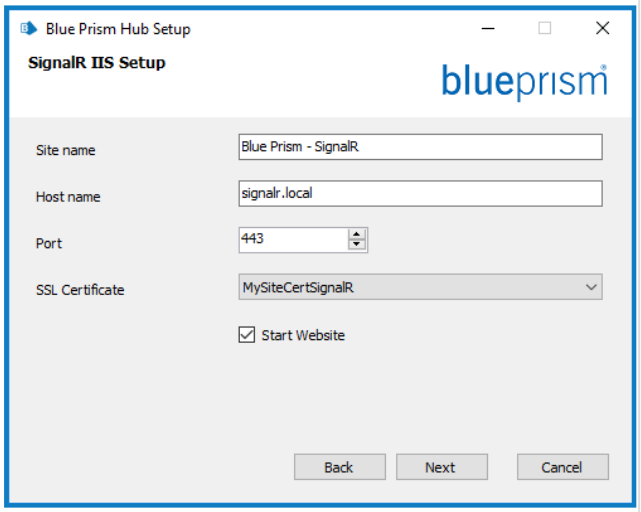
Étape	Page du programme d'installation	Détails
14		**Configuration de la connexion SQL de File Service** Configurer les réglages de la base de données File Service en fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

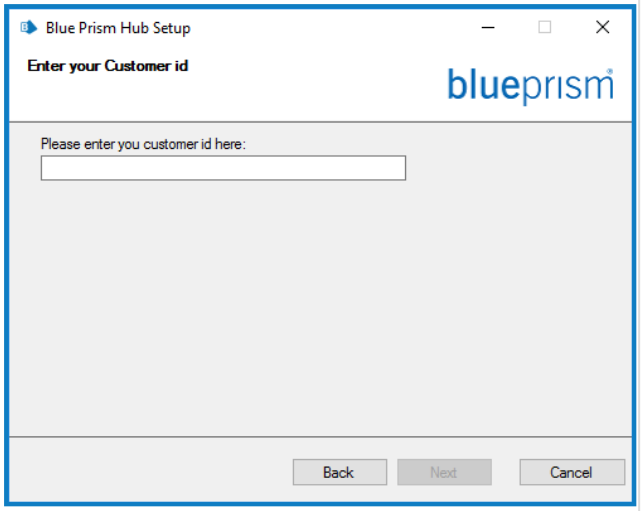
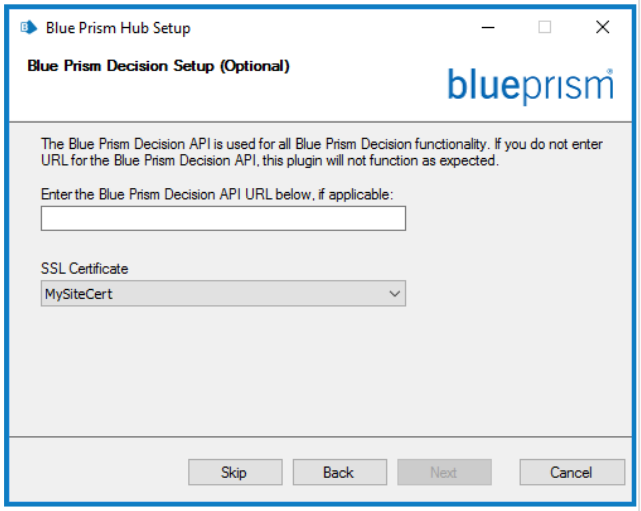
Étape	Page du programme d'installation	Détails
15		**Configuration IIS de File Service** Configurez le site Web de File Service. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

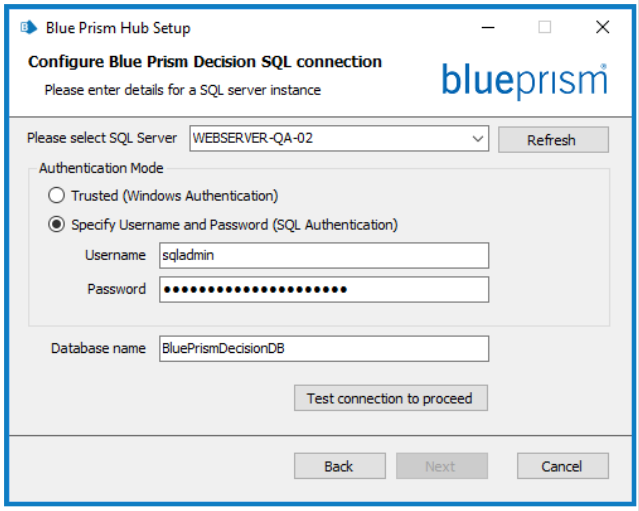
Étape	Page du programme d'installation	Détails
16		**Connexion SQL de Notification Center** Configurer les réglages de la base de données Notification Centeren fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

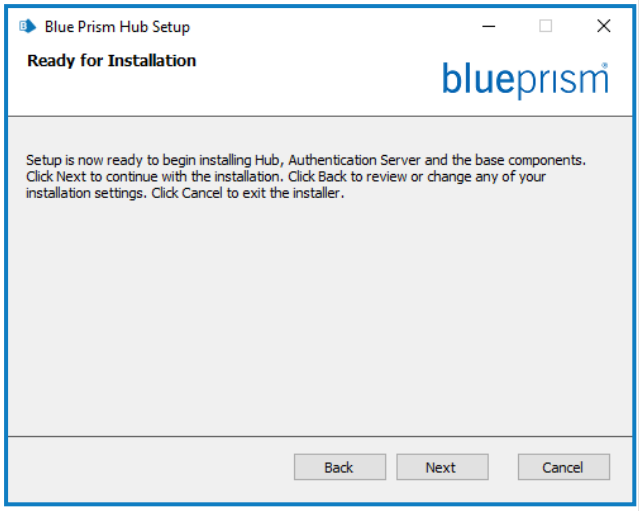
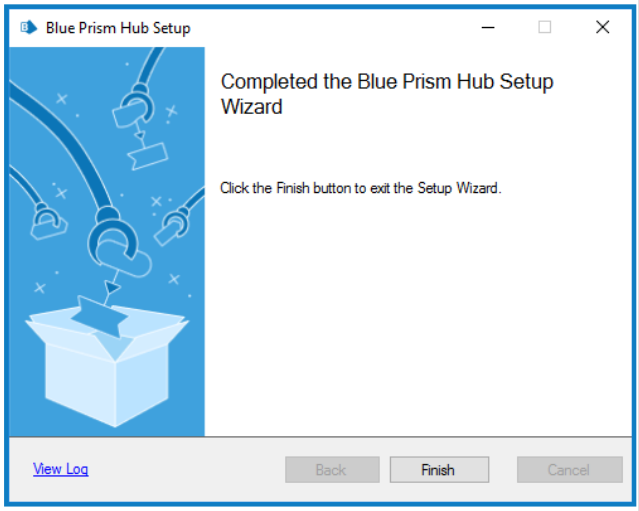
Étape	Page du programme d'installation	Détails
17		**Configuration IIS de Notification Center** Configurez le site Web de Notification Center. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

Étape	Page du programme d'installation	Détails
18		**Connexion SQL de License Manager** Configurer les réglages de la base de données License Manageren fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

Étape	Page du programme d'installation	Détails
19		**Configuration IIS de License Manager** Configurez le site Web de License Manager. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.
20		**Configuration IIS de SignalR** Configurez le site Web de SignalR. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

Étape	Page du programme d'installation	Détails
21		**Saisir votre ID client** Saisissez votre identifiant client. Cet identifiant vous est fourni par Blue Prism lorsque vous recevez votre licence produit pour ALM ou Interact. Si vous n'avez pas acheté de plug-in sous licence, vous pouvez saisir votre propre valeur. Si vous achetez ultérieurement un plug-in sous licence, votre ID client devra être modifié dans le fichier de configuration. Pour plus d'informations, voir Dépanner une installation Hub sur la page 99.
22		**Configuration de Blue Prism Decision (facultatif)** Si vous souhaitez utiliser Blue Prism Decision, vous devez : • Saisissez l'URL du conteneur de Blue Prism Decision Model Service, suivie du numéro de port. L'URL doit être au format https://<FQDN>:<numéro port>, par exemple, https://decision.blueprism.com:50051. L'URL doit correspondre au nom de domaine explicite (FQDN) spécifié dans le certificat. Le numéro de port doit correspondre au port qui a été défini lorsque le conteneur a été défini pour s'exécuter. Pour plus d'informations, voir Installer Blue Prism Decision. • Sélectionnez le certificat SSL approprié. Si vous ne souhaitez pas utiliser Blue Prism Decision, cliquez sur **Ignorer**. L'écran Prêt pour l'installation s'affiche.

Étape	Page du programme d'installation	Détails
23		**Connexion SQL de Blue Prism Decision** Configurer les réglages de la base de données Blue Prism Decisionen fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Hub sur la page 99 pour plus de détails.

Étape	Page du programme d'installation	Détails
24		**Prêt pour l'installation** Cliquez sur **Suivant** pour installer Hub.
25		**Installation terminée** Si l'installation échoue, l'option **Afficher le log** donne des détails sur l'erreur qui s'est produite. Voir Dépanner une installation Hub sur la page 99 pour en savoir plus.

Installer l'extension Authentication Server SAML 2.0

Si votre entreprise a l'intention d'utiliser l'authentification SAML 2.0 pour vos utilisateurs, vous devez installer l'extension Authentication Server SAML 2.0 sur votre serveur Web où Hub et Authentication Server sont installés. Pour plus d'informations, consultez le guide d'installation de l'extension 4.7 Authentication Server SAML 2.0 sur Digital Exchange.

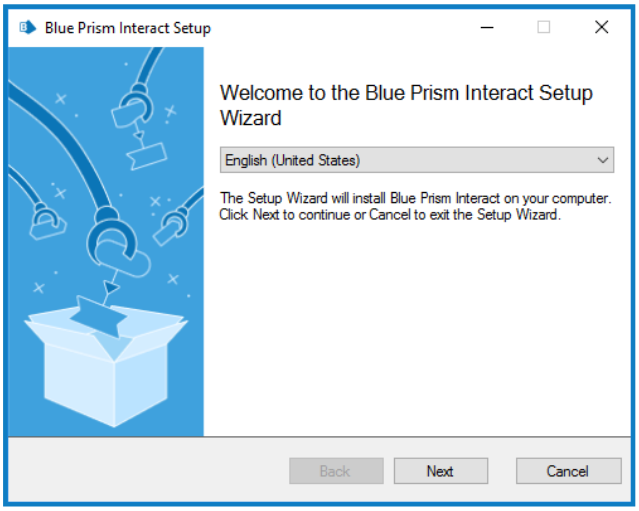
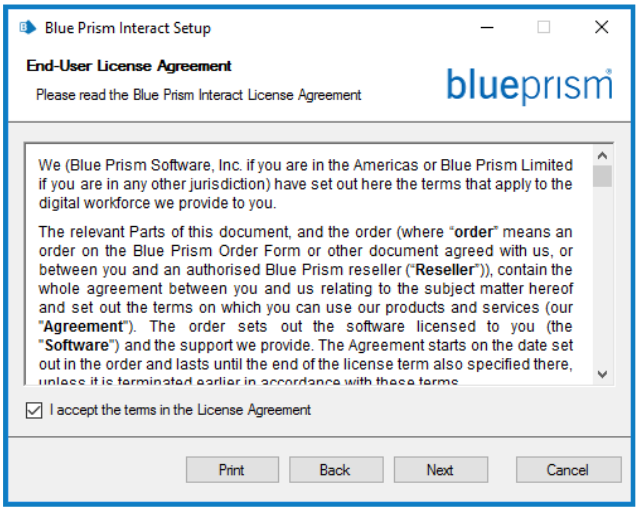
Si votre entreprise n'a pas l'intention d'utiliser l'authentification SAML 2.0 pour vos utilisateurs, vous n'avez rien d'autre à installer.

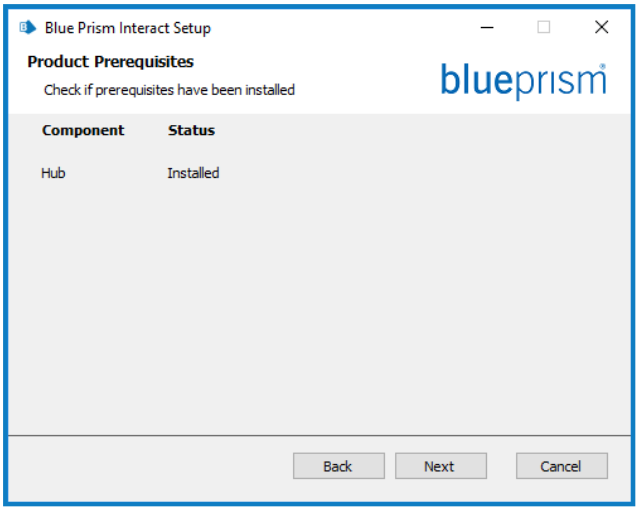
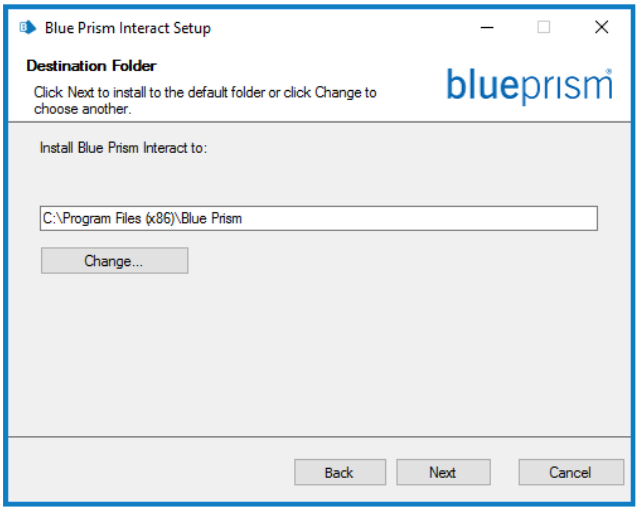
Installer Blue Prism Interact

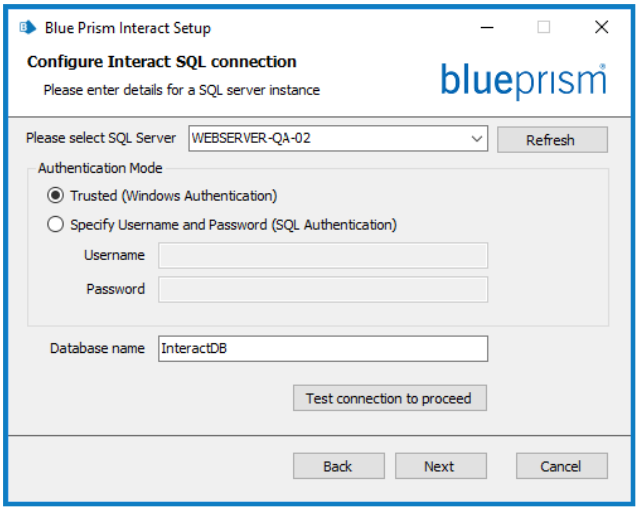
Les étapes ci-dessous détaillent le processus d'installation du logiciel Blue Prism Interact. Cela suppose que Blue Prism Hub a été installé, ce qui inclut Authentication Server, Hub et d'autres services associés.

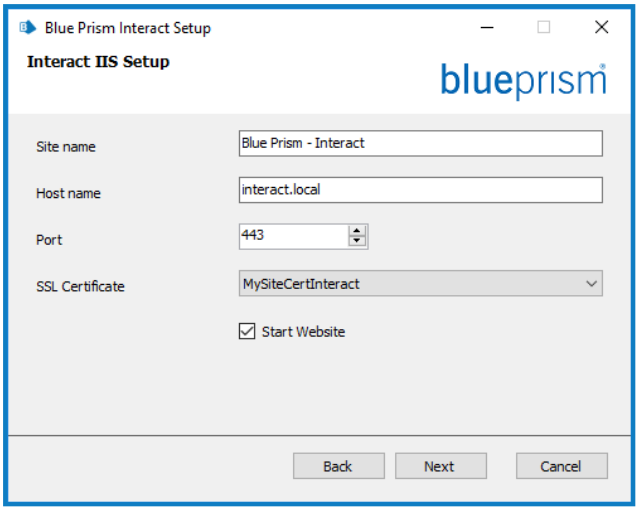
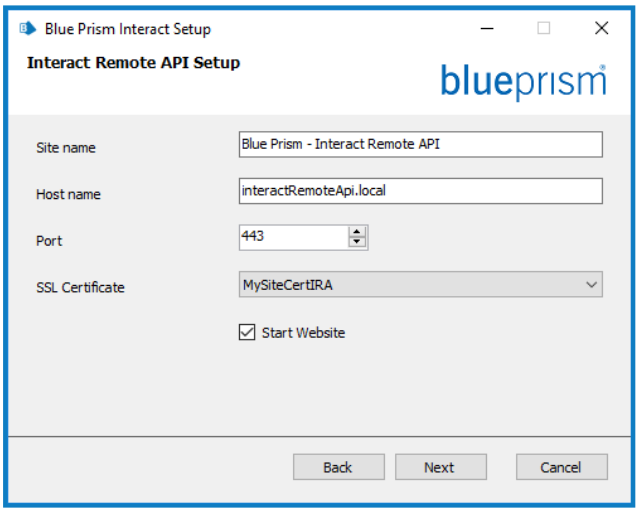
Téléchargez et exécutez le programme d'installation de Blue Prism Interact, disponible sur le portail Blue Prism, et progressez dans le programme d'installation comme indiqué ci-dessous. L'assistant d'installation doit être exécuté avec des droits d'administrateur.

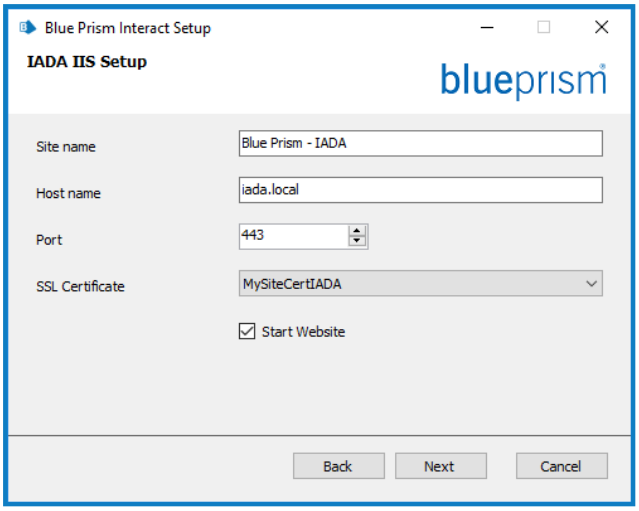
Pour voir le processus d'installation et de configuration d'Interact, regardez notre vidéo d'installation de Blue Prism Interact.

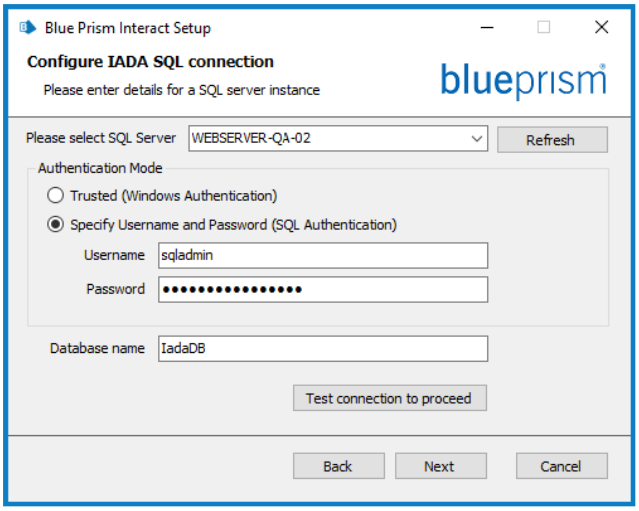
Étape	Page du programme d'installation	Détails
1		**Bienvenue** Si nécessaire, sélectionnez une autre langue pour l'assistant d'installation dans la liste déroulante. La langue par défaut est l'anglais (États-Unis). Cliquez sur **Suivant**.
2		**Contrat de licence** Lisez le contrat de licence de l'utilisateur final et, si vous acceptez les conditions, cochez la case.

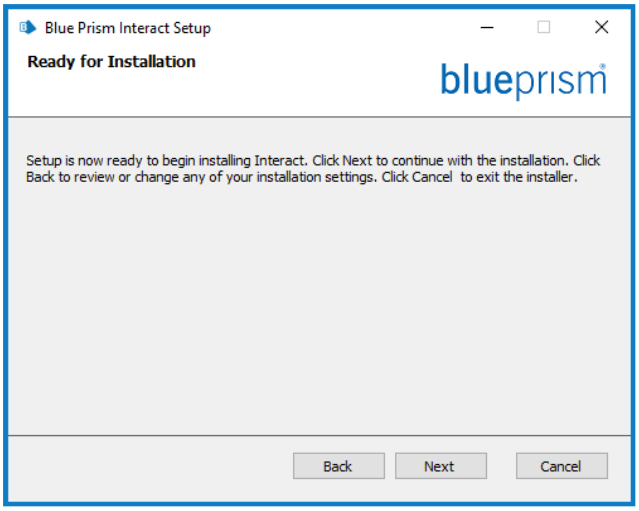
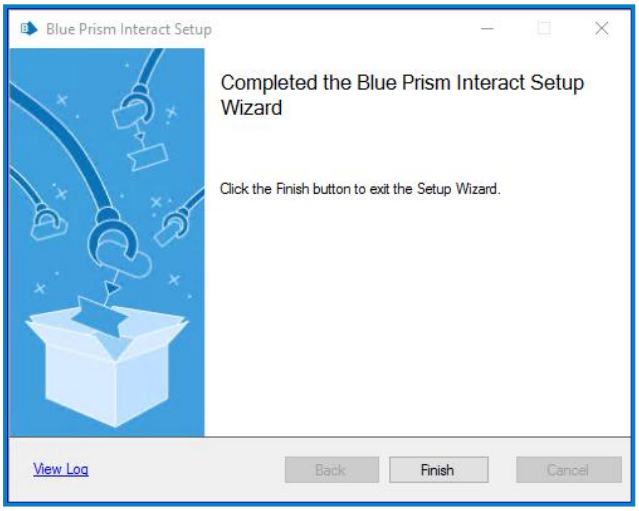
Étape	Page du programme d'installation	Détails
3		**Prérequis du produit** Le programme d'installation vérifie que les prérequis ont été installés. Si le programme d'installation trouve qu'il manque des prérequis, ceux-ci vous seront notifiés. Sinon, poursuivez l'installation. Vous ne pouvez pas continuer à moins que tous les prérequis aient été installés.
4		**Dossier de destination** Spécifiez le dossier d'installation requis. L'emplacement par défaut est C:\Program Files (x86)\Blue Prism, mais vous pouvez choisir un autre emplacement à l'aide du bouton **Modifier**.

Étape	Page du programme d'installation	Détails
5		**Définir la configuration SQL d'Interact** Configurer les réglages de la base de données Interacten fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Interact sur la page 92 pour plus de détails.

Étape	Page du programme d'installation	Détails
6		**Configuration d'Interact IIS** Configurez le site Web Interact. Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.
7		**Configuration d'Interact Remote API** Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

Étape	Page du programme d'installation	Détails
8		**Configuration d'IADA IIS** Vous devez : • Saisir un nom de site. • Saisir un nom d'hôte. Il sera utilisé comme URL pour le site. Assurez-vous de prendre en compte votre structure DNS et de domaine lorsque vous choisissez un nom d'hôte. • Saisir le numéro de port. • Sélectionner le certificat SSL approprié. • Laisser l'option **Démarrer le site Web** sélectionnée, à moins que vous ne souhaitiez pas que le site Web démarre automatiquement à la fin de l'installation.

Étape	Page du programme d'installation	Détails
9		**Définir la configuration SQL d'IADA** Configurer les réglages d'IADAen fournissant le nom d'hôte ou l'adresse IP SQL Server et les identifiants du compte pour créer la base de données : • Si l'**authentification Windows** est sélectionnée, le compte doit disposer des permissions appropriées. Voir Installation d'à l'aide de l'authentification Windows sur la page suivante pour en savoir plus. • Si l'**authentification SQL** est sélectionnée, saisissez le nom d'utilisateur et le mot de passe. ⚠ Vous devez vous assurer que votre mot de passe de base de données ne contient pas de signe égal (=) ou de point-virgule (;). Ces caractères ne sont pas pris en charge et entraîneront des problèmes lors de la tentative de connexion à la base de données. Le nom de la base de données peut être laissé comme valeur par défaut ou modifié si nécessaire. Cliquez sur **Tester la connexion pour tester** les identifiants SQL et vérifier la connectivité. Une notification affichera le résultat du test. Vous ne pourrez passer à l'étape suivante que si le test a réussi. Si le test a échoué, voir Dépanner une installation Interact sur la page 92 pour plus de détails.

Étape	Page du programme d'installation	Détails
10		**Prêt pour l'installation** Cliquez sur **Suivant** pour installer Interact.
11		**Installation terminée** Si l'installation échoue, l'option **Afficher le log** donne des détails sur l'erreur qui s'est produite. Pour plus d'informations, voir Dépanner une installation. Cliquez sur **Terminer.**

Installation d'à l'aide de l'authentification Windows

Le compte utilisé lors de l'exécution de l'installation doit disposer des permissions SQL Server appropriées pour effectuer l'installation, à savoir l'appartenance aux rôles de serveur fixes sysadmin ou dbcreator.

Si l'authentification Windows est choisie lors du processus d'installation, un compte de service Windows doit être utilisé pour les pools d'applications et les services disposant des permissions nécessaires pour exécuter les tâches et les processus pendant le fonctionnement normal. Le compte de service Windows aura besoin de ce qui suit :

- La possibilité d'exécuter les processus de base de données SQL (voir Permissions SQL minimales sur la page 15).
- Les permissions pour les certificats requis.
- La propriété sur le pool d'applications IIS.
- La propriété des services Windows installés par Hub et Interact.

⚠ Vous devez affecter les pools d'applications et les services pour utiliser les comptes Windows avant de créer un environnement dans Hub. Si vous affectez les comptes après avoir créé un environnement, vous pouvez rencontrer des problèmes de performances, par exemple, les formulaires créés à l'aide du plug-in Interact peuvent ne pas s'afficher pour les utilisateurs dans Interact.

Affectation du compte de service Windows en tant que propriétaire sur les certificats

Le compte de service Windows doit être autorisé à accéder aux certificats BluePrismCloud. Pour ce faire :

1. Sur le serveur Web, ouvrez le Gestionnaire de certificats. Pour ce faire, saisissez *Certificats* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gérer les certificats informatiques**.
2. Dans le volet de navigation, développez **Personnel** et cliquez sur **Certificats**.
3. Suivez les étapes ci-dessous pour les certificats BluePrismCloud_Data_Protection et BluePrismCloud_IMS_JWT :
    a. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches**, puis cliquez sur **Gérer les clés privées...**.

       La boîte de dialogue Permissions du certificat s'affiche.
    b. Cliquez sur **Ajouter**, puis saisissez le compte de service et cliquez sur **OK**.
    c. Lorsque le compte de service est sélectionné dans la liste **Groupe ou nom d'utilisateur**, assurez-vous que le **contrôle complet** est sélectionné dans la liste **Permissions pour {nom du compte}**.
    d. Cliquez sur **OK**.

       Le compte de service a désormais accès au certificat.

Affectation d'un compte de service Windows au pool d'applications

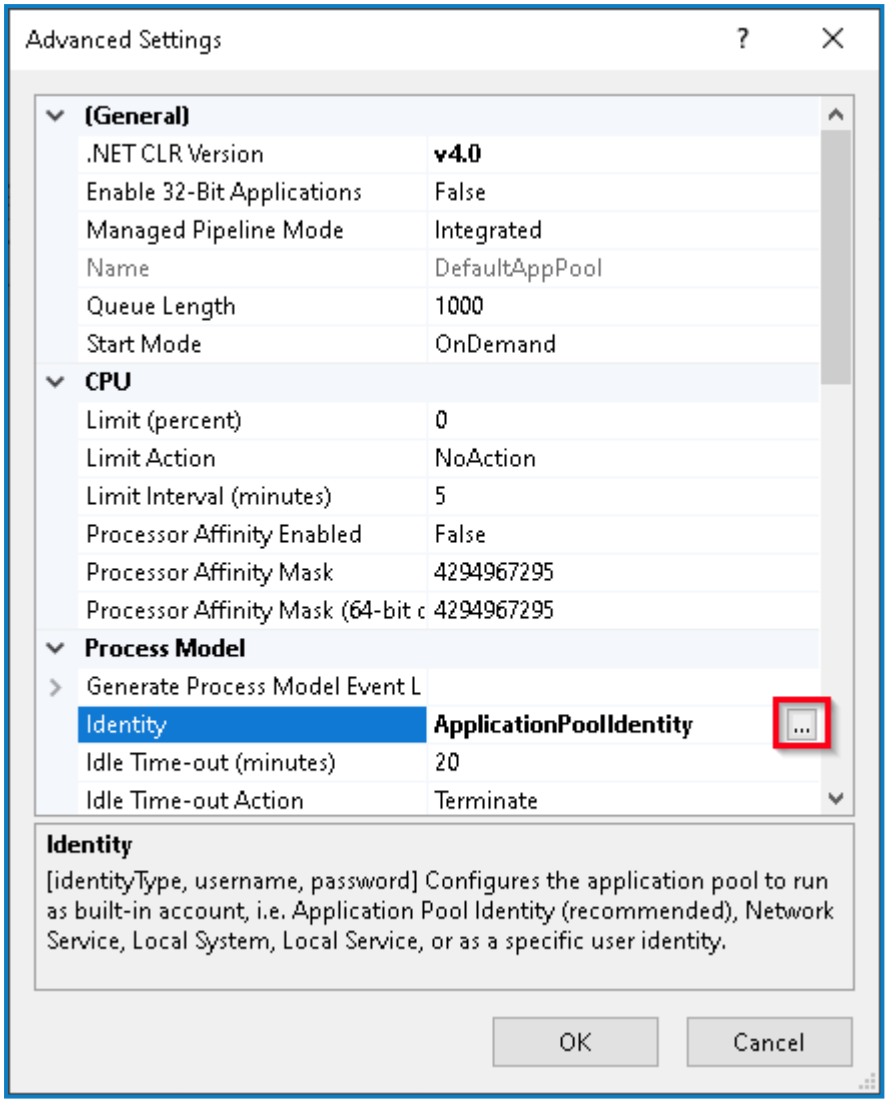
Par défaut, les pools d'applications sont créés avec l'identité « ApplicationPoolIdentity ». Une fois que l'assistant d'installation a terminé, le compte de service Windows doit être autorisé à gérer les pools d'applications. Pour ce faire :

1. Sur le serveur Web, ouvrez le gestionnaire d'Internet Information Services (IIS).
2. Dans le panneau Connexions, développez l'hôte et sélectionnez **Pools d'applications**.
3. Vérifiez les valeurs de la colonne **Identité**.

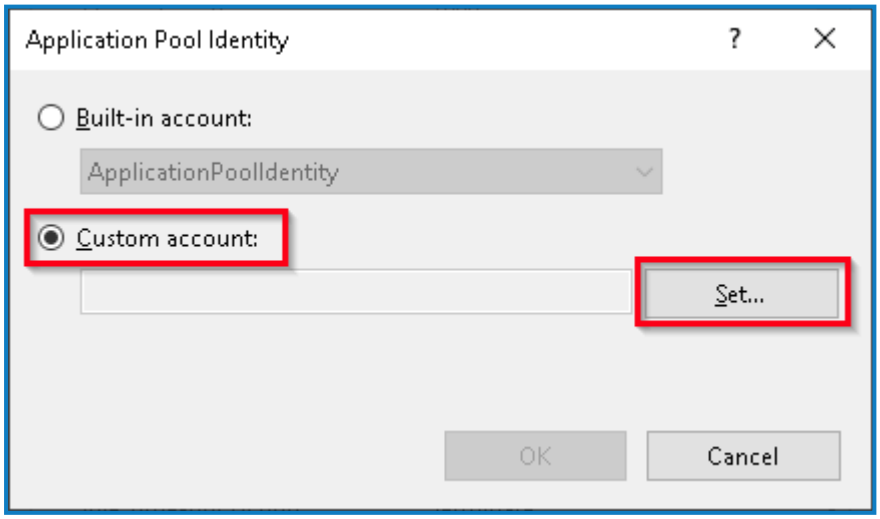
   L'identité d'un pool d'applications doit correspondre au compte de service Windows spécifique.
4. Pour tous les pools d'applications dont la colonne *Identité* contient **ApplicationPoolIdentity**, cliquez avec le bouton droit de la souris sur la ligne et sélectionnez **Réglages avancés...**.

   La boîte de dialogue Réglages avancés s'affiche.

5. Sélectionnez le réglage **Identité**, puis cliquez sur le bouton **...** (ellipse) :



6. Dans la boîte de dialogue Identité du pool d'applications, sélectionnez **Compte personnalisé**, puis cliquez sur **Définir...**.



La boîte de dialogue Définir les identifiants s'affiche.

7. Saisissez les identifiants du compte de service Windows requis et cliquez sur **OK**.

8. Répétez l'opération pour tous les pools d'applications à modifier.
9. Redémarrez le service RabbitMQ.
10. Redémarrez tous les pools d'applications.
11. Redémarrez IIS.

En cas de problèmes avec le service Audit Service, assurez-vous que le compte de service Windows a accès à l'auditeur du service d'audit ainsi qu'à la base de données Audit.

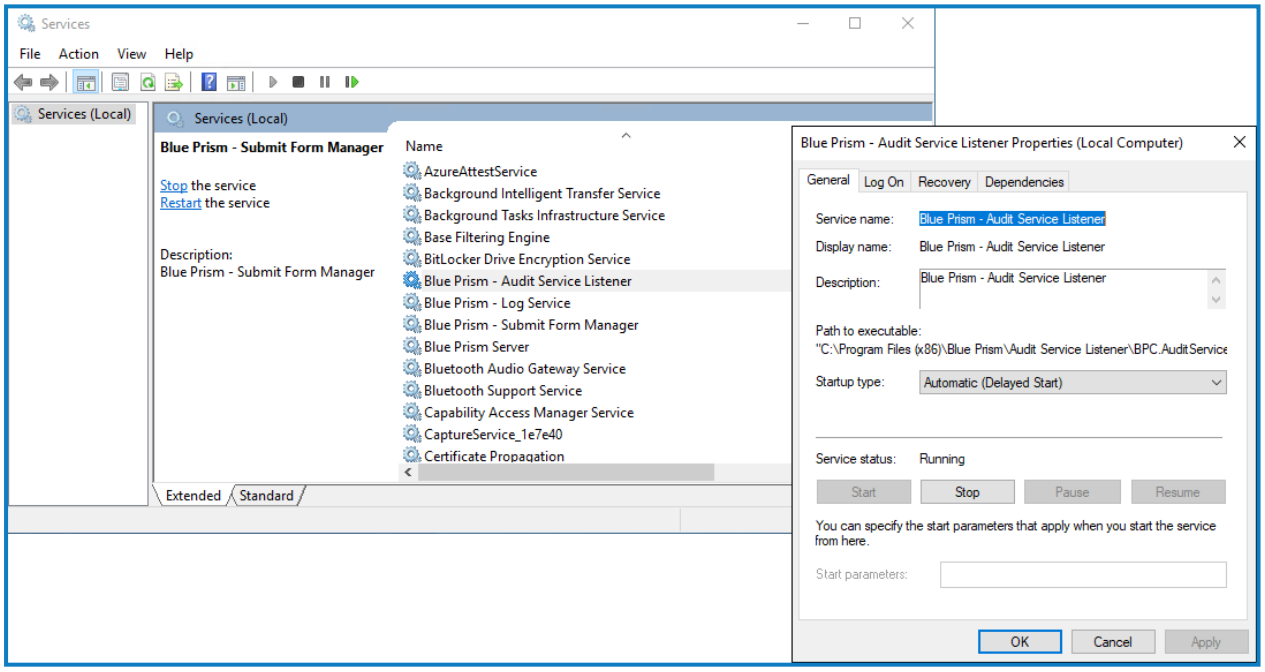
Affectation d'un compte de service Windows à un service

Le compte de service Windows doit être affecté pour gérer les services suivants :

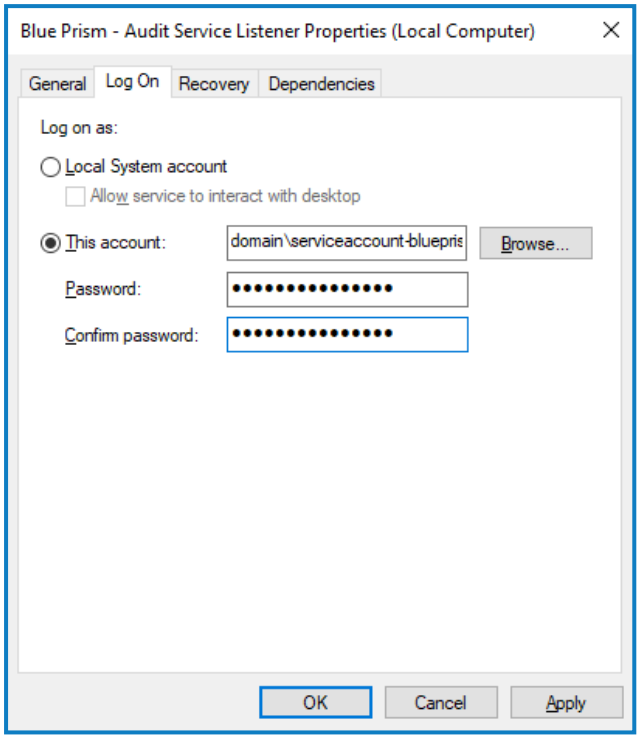
- Blue Prism - Auditeur du service d'audit
- Blue Prism - Service de log
- Blue Prism - Submit Form Manager

Pour ce faire :

1. Ouvrez Services dans le serveur Web.
2. Cliquez avec le bouton droit sur le service et sélectionnez **Propriétés**.



3. Dans l'onglet Connexion, sélectionnez **Ce compte**, puis saisissez le nom du compte ou cliquez sur **Parcourir** pour rechercher le compte que vous souhaitez utiliser.



4. Saisissez le mot de passe du compte et cliquez sur **OK**.
5. Dans la fenêtre Services, cliquez avec le bouton droit sur le service et cliquez sur **Redémarrer**.
6. Répétez l'opération pour les autres services Blue Prism.

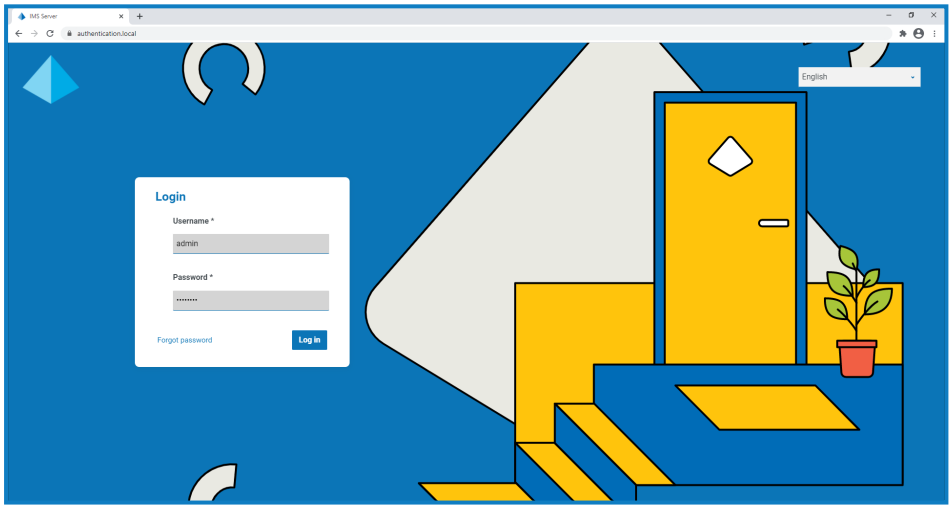
Configuration initiale de Hub

Vous pouvez désormais vous connecter pour la première fois et effectuer une configuration à l'échelle du système.

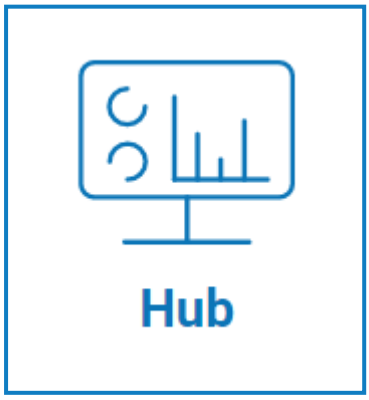
Lorsque vous ouvrez la page de connexion pour Authentication Server, les réglages de localisation sont automatiquement appliqués à partir de votre navigateur Web. La page de connexion et Hub s'affichent dans la langue la plus compatible avec les réglages linguistiques configurés dans le navigateur. Si la langue sélectionnée dans les réglages de votre navigateur n'est pas prise en charge, l'anglais est utilisé par défaut. Si nécessaire, vous pouvez modifier manuellement la langue que vous souhaitez utiliser à partir de la liste déroulante sur la page de connexion.

Pour regarder le processus d'installation et de configuration de Hub, accédez à notre vidéo d'installation de Blue Prism Hub.

1. Lancez un navigateur et accédez au site Web Authentication Server, dans notre exemple : https://authentication.local



2. Connectez-vous en utilisant les identifiants par défaut.
   - **Nom d'utilisateur** : administrateur
   - **Mot de passe** : Qq1234!!
3. Cliquez sur **Hub** pour lancer le site Web Hub.



4. Remplacez le mot de passe par défaut par un nouveau mot de passe sécurisé.
   a. Dans Hub, cliquez sur l'icône de profil pour ouvrir la page Réglages, puis sur **Profil**.
   b. Cliquez sur **Mettre à jour le mot de passe**.

      La boîte de dialogue Mettre à jour votre mot de passe s'affiche.
   c. Saisissez le mot de passe administrateur actuel, puis saisissez et répétez un nouveau mot de passe.
   d. Cliquez sur **Mettre à jour**.

      Le mot de passe administrateur est modifié.

Réglages de la base de données

⚠ Si vous avez installé votre environnement pour utiliser l'authentification Windows, vous devez affecter les pools d'applications et les services pour utiliser les comptes Windows avant de créer un environnement dans Hub. Si vous ne le faites pas, vous risquez de rencontrer des problèmes de performances. Par exemple, les formulaires créés à l'aide du plug-in Interact peuvent ne pas s'afficher pour les utilisateurs dans Interact. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 pour en savoir plus.

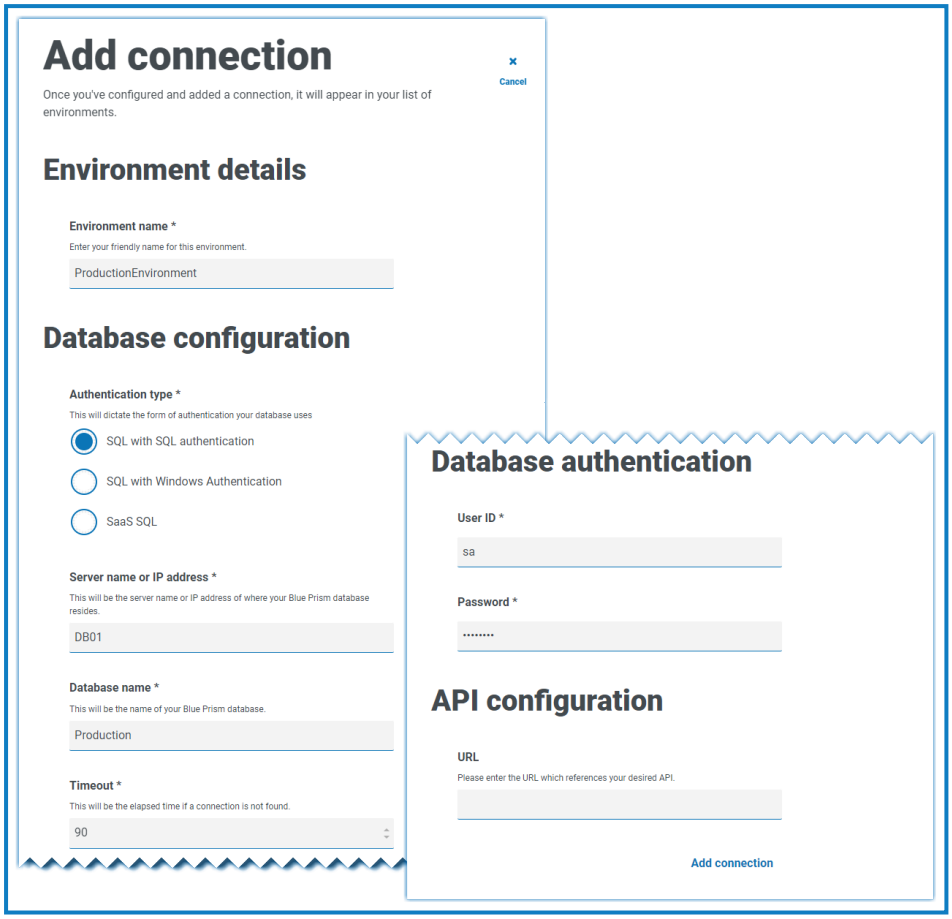
Le cryptage SSL est utilisé par toutes les bases de données installées dans le cadre du programme d'installation de Hub. Pour que Hub se connecte avec succès à la base de données Blue Prism, la base de données Blue Prism doit également être configurée pour utiliser le cryptage SSL. Pour plus d'informations, veuillez consulter Prérequis sur la page 8.

Pour configurer l'accès à la base de données Blue Prism :

1. Cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Gestionnaire d'environnements**.

   La page Gestion des environnements s'affiche.

2. Cliquez sur **Ajouter une connexion** et saisissez les détails de la base de données Blue Prism. Un exemple est illustré ci-dessous :



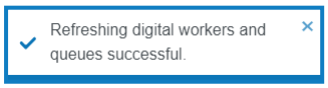
> La valeur Délai avant expiration s'exprime en secondes.

3. Cliquez sur **Ajouter une connexion** pour enregistrer les détails.

   La connexion est créée et s'affiche dans le gestionnaire d'environnements.

4. Dans le gestionnaire d'environnements, cliquez sur l'icône Actualiser sur votre nouvelle connexion. Cela met à jour les informations dans Hub avec la main-d'œuvre numérique et les files d'attente conservées dans la base de données.

   Si la connexion est établie, le message suivant s'affiche dans le coin supérieur droit de l'interface utilisateur Hub, ce qui vérifie l'installation.



   Si le message ne s'affiche pas, voir Dépanner une installation Hub sur la page 99 pour en savoir plus.

Créer un administrateur

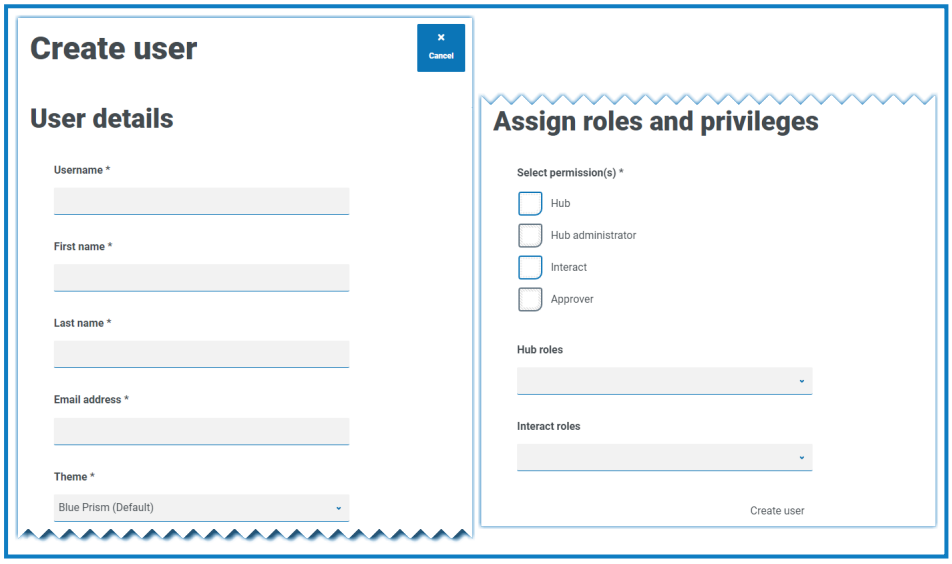
Vous devrez créer un compte administrateur avec des informations valides pour terminer la configuration de Hub. Vous ne devez pas utiliser le compte administrateur générique pour terminer la configuration, car :

- Une adresse e-mail réelle est nécessaire pour tester la configuration de la messagerie.
- Pour une piste d'audit complète, un utilisateur nommé doit être utilisé pour apporter des modifications de configuration, plutôt que le compte générique.

Pour créer un administrateur :

1. Cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Utilisateurs**.
2. Sur la page Utilisateurs, cliquez sur **Ajouter un utilisateur**.

   La section Créer un utilisateur s'affiche.



3. Saisissez les informations suivantes :
   - Nom d'utilisateur
   - Prénom
   - Nom
   - Adresse e-mail
4. Sélectionnez les permissions **Hub** et **Administrateur Hub**.
5. Cliquez sur **Créer un utilisateur**.

   La boîte de dialogue Créer un mot de passe s'affiche.
6. Sélectionnez **Mettre à jour manuellement le mot de passe de l'utilisateur**.

   Les mots de passe doivent respecter les restrictions au sein de Hub.
7. Cliquez sur **Continuer** et suivez les instructions à l'écran.
8. Enfin, cliquez sur **Créer** pour créer l'utilisateur.

   Le nouvel utilisateur apparaît dans la liste des utilisateurs.
9. Déconnectez-vous de Hub et reconnectez-vous en utilisant votre nouveau compte.

Réglages des e-mails

Il est recommandé que la configuration SMTP soit terminée. Cela permet d'envoyer des e-mails système, tels que des e-mails de mot de passe oublié.

L'adresse e-mail utilisée pour envoyer des e-mails est définie lors de la configuration de votre profil.

> Pour configurer les réglages des e-mails, vous devez vous connecter avec l'utilisateur que vous avez créé dans Créer un administrateur sur la page 69. Cela est dû au fait que le processus de configuration envoie un e-mail de test et nécessite donc un utilisateur avec une adresse e-mail active.

Vous pouvez configurer les réglages de vos e-mails à l'aide de l'une des méthodes d'authentification suivantes :

- **Nom d'utilisateur et mot de passe** : cette méthode d'authentification nécessite les informations suivantes :
  - **Hôte SMTP** : l'adresse de votre hôte SMTP.
  - **Numéro de port** : le numéro de port utilisé par le serveur de messagerie sortant.
  - **Adresse e-mail de l'expéditeur** : l'adresse e-mail utilisée lors de l'envoi d'e-mails. Les destinataires des e-mails verront cela comme l'adresse De.
  - **Chiffrement** : la méthode de chiffrement utilisée par le serveur de messagerie pour envoyer les e-mails.
  - **Nom d'utilisateur** : le nom d'utilisateur pour l'authentification SMTP.
  - **Mot de passe** : le mot de passe du compte.
  - **Destinataire de l'e-mail de test** : l'e-mail de test sera envoyé à cette adresse e-mail. Par défaut, l'adresse e-mail de l'utilisateur qui apporte les modifications est utilisée et ne peut pas être modifiée.
- **Microsoft OAuth 2.0** : cette méthode d'authentification nécessite les informations suivantes :
  - **Adresse e-mail de l'expéditeur** : l'adresse e-mail utilisée lors de l'envoi d'e-mails. Les destinataires des e-mails verront cela comme l'adresse De.
  - **ID d'application** : ces informations sont l'ID d'application (client) défini dans Azure AD et vous seront fournies par votre équipe d'assistance informatique.
  - **ID de répertoire** : ces informations sont l'ID de répertoire (locataire) défini dans Azure AD et vous seront fournies par votre équipe d'assistance informatique.
  - **Secret client** : il s'agit du secret client généré par Azure AD et qui vous sera fourni par votre équipe d'assistance informatique et qui contrôle le processus d'authentification.

    > Pour plus d'informations sur la recherche de ces détails dans Azure AD, consultez la documentation Microsoft.
  - **Destinataire de l'e-mail de test** : l'e-mail de test sera envoyé à cette adresse e-mail. Par défaut, l'adresse e-mail de l'utilisateur qui apporte les modifications est utilisée et ne peut pas être modifiée.

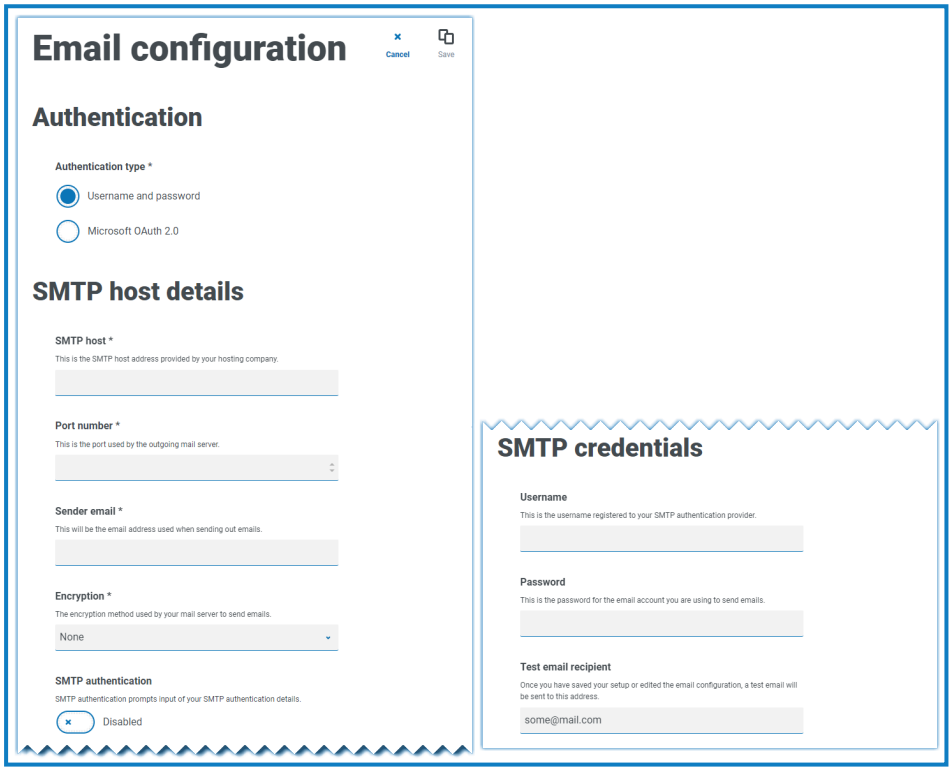
> Si vous utilisez Microsoft OAuth 2.0, la permission Mail.Send doit être activée dans Azure Active Directory. Vous le trouverez dans l'onglet Permissions de l'API sous les propriétés de l'application dans Azure Active Directory. Pour plus d'informations, voir Dépanner une installation Hub sur la page 99.

Pour configurer les réglages des e-mails :

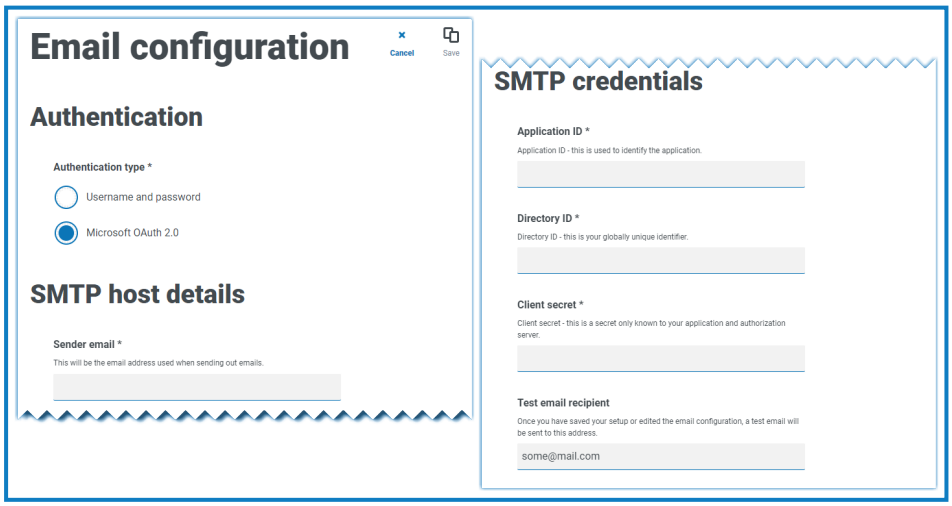
1. Cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Configuration de la messagerie**.
2. Cliquez sur **Modifier**.
3. Sélectionnez le type d'authentification que vous souhaitez utiliser.

   Les champs de la page dépendent de votre sélection, comme détaillé ci-dessus. Si vous sélectionnez :

   - **Nom d'utilisateur et mot de passe**, la page de configuration de la messagerie s'affiche comme suit :



   - **Microsoft OAuth 2.0**, la page de configuration de la messagerie s'affiche comme suit :



4. Saisissez les informations requises.
5. Cliquez sur **Enregistrer**.

Si les réglages des e-mails ne peuvent pas être configurés avec succès, cela est probablement dû au fait que le serveur de l'agent de messages n'est pas accessible. Voir Dépanner une installation Hub sur la page 99 pour plus d'informations.

Pour plus d'informations sur la configuration des réglages des e-mails, consultez le guide de l'administrateur de Hub.

Configurer Authentication Server

Authentication Server permet aux utilisateurs de se connecter à Blue Prism, Hub et Interact avec les mêmes identifiants. Authentication Server est compatible avec Blue Prism 7.0 et les versions ultérieures.

Avec Blue Prism 6

Si votre entreprise utilise Blue Prism 6 :

- Authentication Server ne peut pas être utilisé pour authentifier les utilisateurs entre Blue Prism et Hub. Les utilisateurs peuvent se connecter à Blue Prism et à Authentication Server à l'aide de comptes indépendants.
- Vous devez configurer les réglages d'authentification dans Hub. Voir Réglages d'authentification sur la page suivante.

Avec Blue Prism 7

Si votre entreprise utilise Blue Prism 7, vous devez déterminer si elle souhaite que les utilisateurs utilisent le même compte pour les applications Blue Prism.

- Si votre entreprise souhaite utiliser les mêmes comptes utilisateur :
    1. Pour configurer Authentication Server, consultez le guide de configuration d'Authentication Server.
    2. Configurez les réglages d'authentification dans Hub. Voir Réglages d'authentification sur la page suivante.
- Si votre entreprise ne souhaite pas utiliser les mêmes comptes d'utilisateurs, configurez uniquement les réglages d'authentification dans Hub. Voir Réglages d'authentification sur la page suivante.

Pour regarder les étapes de configuration, consultez notre vidéo Configurer Authentication Server.

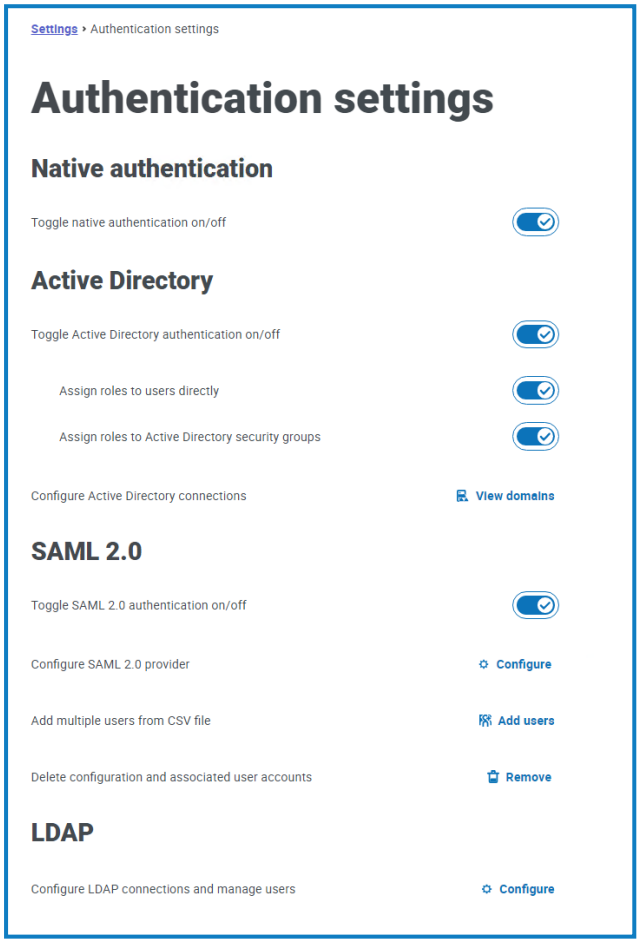
Réglages d'authentification

Les réglages d'authentification pour un environnement Hub peuvent être configurés sur la page Réglages d'authentification.

Pour configurer les réglages d'authentification :

1. Cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Réglages d'authentification**.

   La page Réglages d'authentification s'affiche.



2. Sélectionnez le(s) type(s) d'authentification que vous souhaitez utiliser et les options associées si nécessaire.
   - **Authentification native** : cette option est activée par défaut dans les nouveaux environnements ou lors de la mise à niveau de Hub.
   - **Active Directory** : cette option ne peut être activée que si le serveur hébergeant Authentication Server est membre d'un domaine Active Directory. Si cette option est activée, les domaines Active Directory et la gestion des rôles d'utilisateur peuvent également être configurés.
   - **SAML 2.0** : cette option n'est visible sur la page Réglages d'authentification que si l'extension Authentication Server SAML 2.0 a été installée sur le serveur Web hôte où Authentication Server est installé.
   - **LDAP** : pour activer l'authentification LDAP, au moins une connexion LDAP doit être créée.

En fonction des exigences de votre organisation, vous disposez des options suivantes :

- Activer tous les types d'authentification.
- Désactivez un ou plusieurs types d'authentification. Cela ne peut être fait que s'il y a au moins un utilisateur administrateur dans le système qui est configuré pour se connecter avec un type d'authentification différent du ou des types désactivé(s).

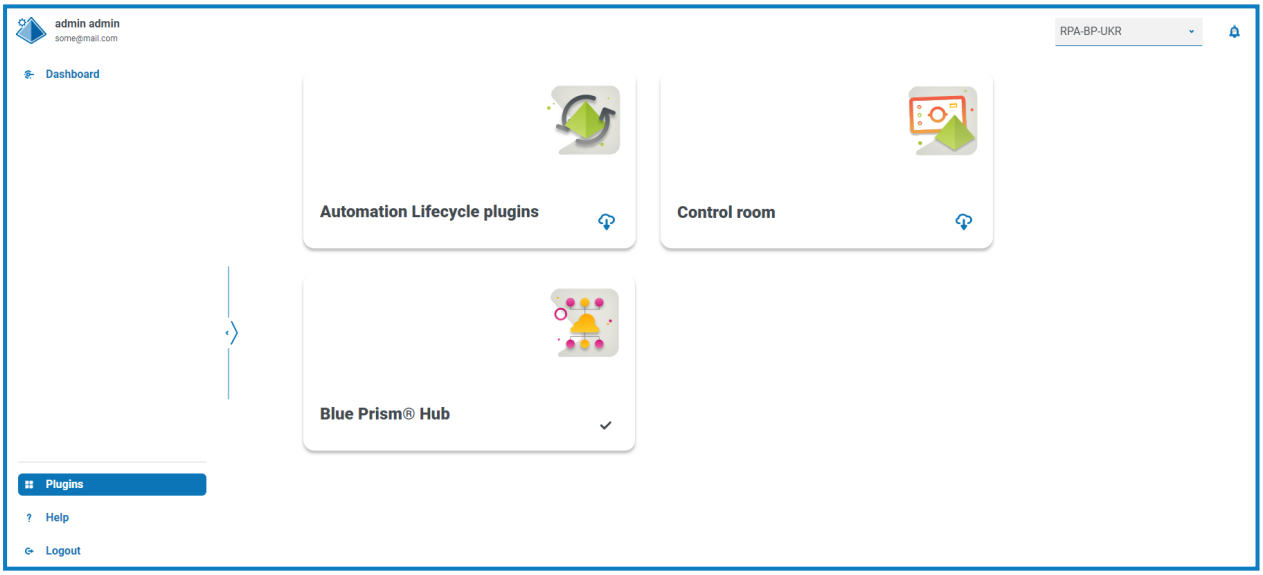
Pour plus d'informations sur la configuration des réglages d'authentification, voir dans le guide de l'administrateur de Hub.

Installer les plug-ins

Dans le cadre de l'installation, Hub installe automatiquement les plug-ins Hub. Toutefois, si vous souhaitez utiliser ALM ou Interact, vous devez d'abord installer le plug-in Processus métier disponible gratuitement.

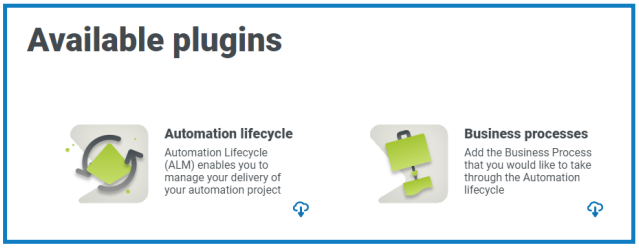
Pour regarder cette étape d'installation, accédez à notre vidéo d'installation du plug-in Processus métier.

1. Connectez-vous à Hub.
2. Cliquez sur **Plug-ins** pour ouvrir le référentiel de plug-ins.



3. Cliquez sur **Cycle de vie de l'automatisation**.

   Les composants de plug-in disponibles s'affichent.



4. Cliquez sur l'icône de téléchargement dans le coin inférieur de la dalle **Processus métier** pour lancer l'installation.

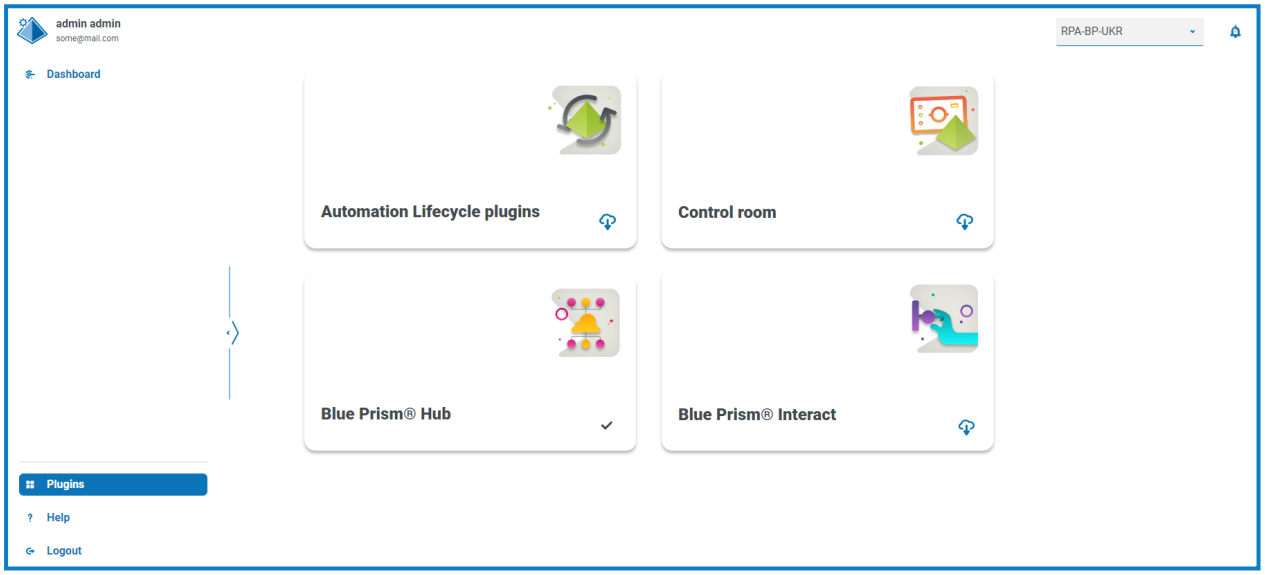
   Le site redémarre.

Installer le plug-in Interact

Le plug-in Interact dépend du plug-in Processus métier, car vous ne pouvez pas créer un formulaire sans processus métier. Le plug-in Processus métier est fourni gratuitement dans le référentiel de plug-ins et est disponible sous Automation Lifecycle Management (ALM). Assurez-vous d'avoir installé le plug-in Processus métier avant d'installer Interact. Pour plus d'informations, voir Installer les plug-ins sur la page précédente.

Le plug-in Interact doit être installé avec la licence associée.

1. Connectez-vous à Hub.
2. Cliquez sur **Plug-ins** pour ouvrir le référentiel de plug-ins.



3. Sur la dalle **Interact**, cliquez sur l'icône de téléchargement dans le coin inférieur pour lancer l'installation et appliquer la licence nécessaire.

   Le site redémarre.

Configurer les Digital Workers

Cette section fournit les étapes qui doivent être effectuées sur chaque Digital Worker pour lui permettre de se connecter à Interact.

Les étapes à suivre sont les suivantes :

- Installer les certificats SSL
- Configurer le réseau
- Installer et configurer le service API Web Interact

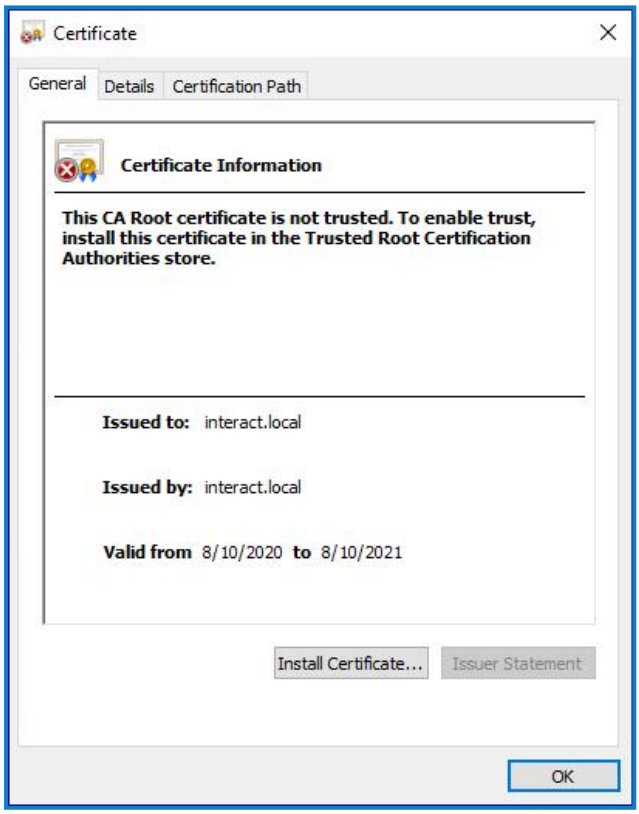
Ces instructions supposent que l'utilisateur connaît bien Blue Prism.

Installer les certificats SSL

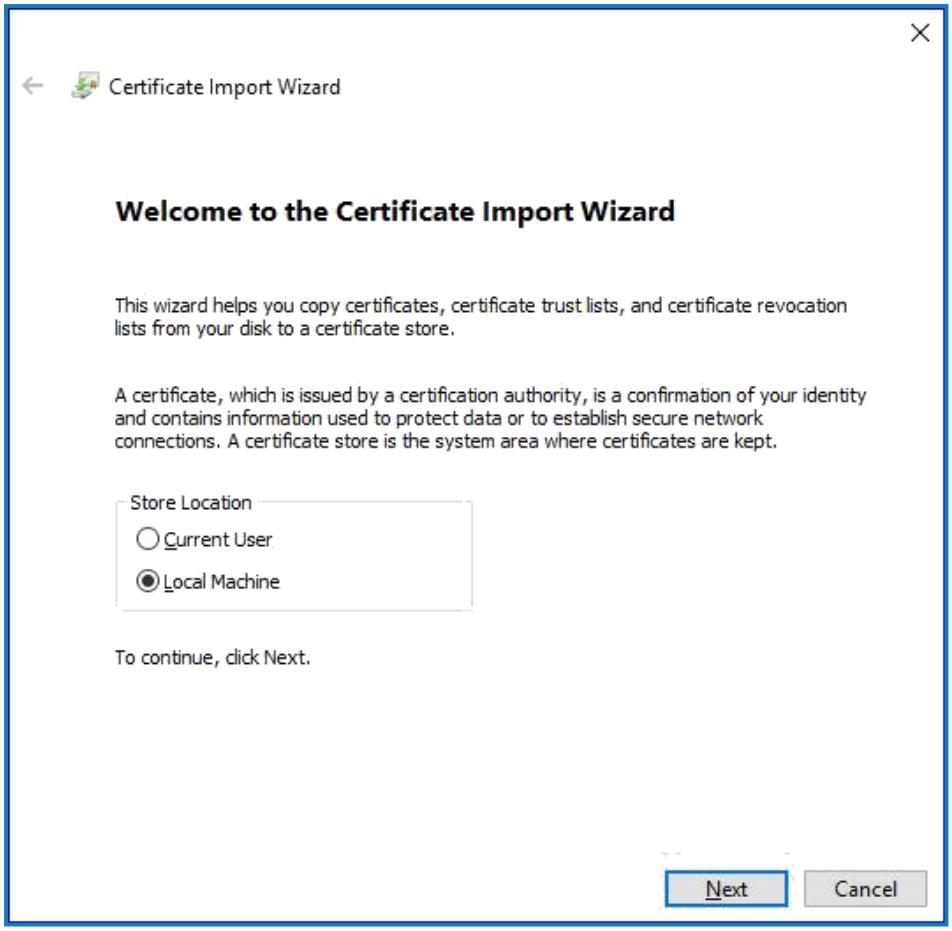
Sur chaque Digital Worker, connectez-vous et copiez les certificats SSL pour Interact, IADA, Interact Remote API, Authentication Server et SignalR.

Comme cela doit être effectué sur chaque Digital Worker, des outils tiers ou des GPO peuvent être utilisés pour effectuer cette tâche à grande échelle.

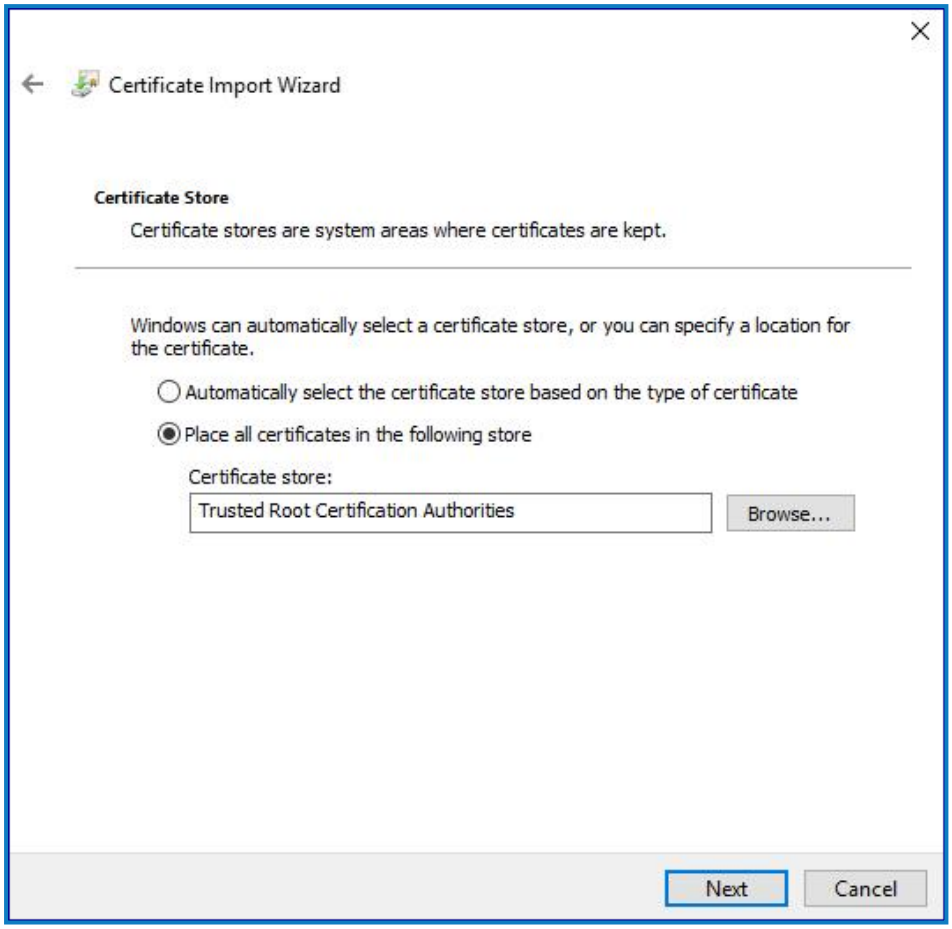
1. Double-cliquez sur chaque certificat SSL et sélectionnez **Installer le certificat**.



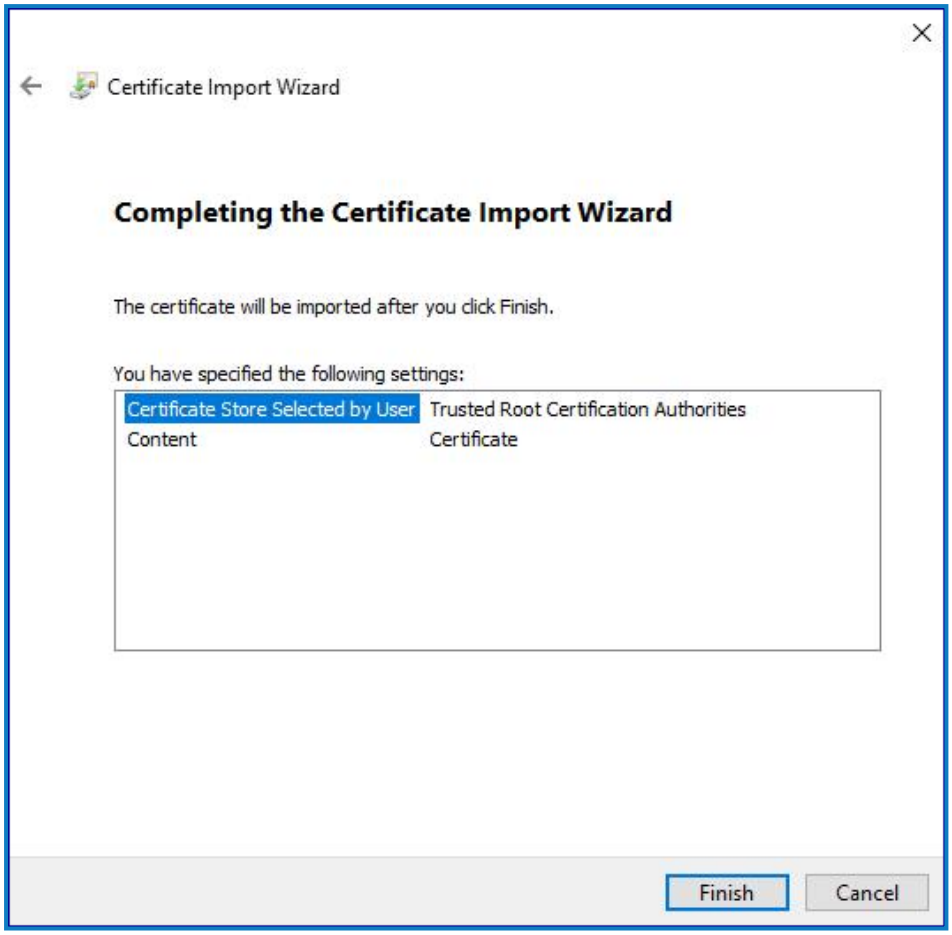
2. Définissez l'emplacement du magasin sur **Machine locale**.



3. Sélectionnez **Placer tous les certificats dans le magasin suivant**, cliquez sur **Parcourir** et sélectionnez **Magasin des autorités de certification racine de confiance**.



4. Vérifiez que le certificat SSL est attribué dans le bon magasin, puis cliquez sur **Terminer**.



5. Accusez réception du message confirmant la réussite.
6. Répétez les étapes pour tous les certificats SSL.

Configurer le réseau

Il est important que le site Web Interact et en particulier le site Interact Remote API soient accessibles.

Cela dépend de la structure de l'architecture qui a été déployée. Cela pourrait déjà être établi si les systèmes sont joints au domaine et que l'organisation informatique a configuré les serveurs. Le fichier des hôtes locaux peut également devoir être ajusté pour s'assurer que les sites sont accessibles.

Les sites qui doivent être accessibles à partir de chaque Digital Worker sont les suivants :

Site Web dans IIS	URL par défaut
Blue Prism – Interact	https://interact.local
Blue Prism – Authentication Server	https://authentication.local
Blue Prism – IADA	https://iada.local
Blue Prism – Interact Remote API	https://interactremoteapi.local
Blue Prism – SignalR	https://signalr.local

Authentication Server et SignalR sont installés dans le cadre de l'installation de Hub.

Installer et configurer le service API Web Interact

Blue Prism et Interact communiquent via l'API Blue Prism Interact Remote API. Pour utiliser cette API, le fichier de version du service API Interact doit être importé dans Blue Prism, ce qui inclut un service API Web et un VBO. Une fois le service Web importé, il doit être mis à jour avec l'URL de base et les codes d'autorisation appropriés pour permettre une communication sécurisée.

Dans le service Web, il existe un certain nombre d'actions définies. Consultez le guide de l'utilisateur du service API Web Interact pour plus d'informations.

Pour configurer Blue Prism pour utiliser Interact, vous devez :

1. Configurer un compte de service dans Hub et générer une clé secrète.
2. Importer le VBO du service API Interact dans Blue Prism.
3. Configurer les identifiants pour le compte du service API Web Interact dans Blue Prism.
4. Configurer le service API Interact pour permettre à Blue Prism de communiquer avec Interact.

Configurer un compte de service

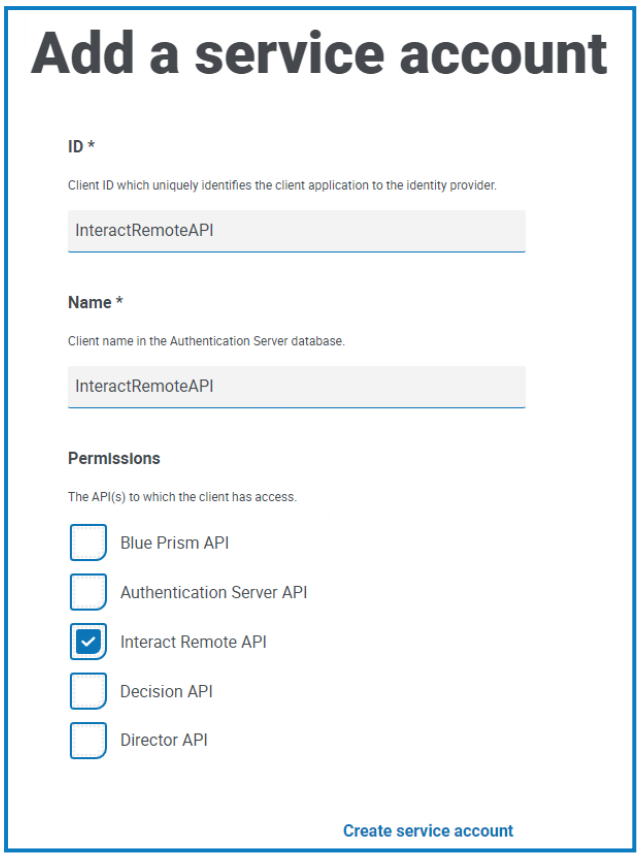
Pour configurer les identifiants de l'API Interact Remote API dans Blue Prism, une clé secrète est requise. Elle est générée à partir du compte de service associé dans Hub pour une utilisation avec l'API Interact Remote API. Si vous perdez la clé, vous pouvez en générer une autre à partir du compte de service. Pour plus d'informations, voir Comptes de service.

Pour créer un compte de service :

1. Dans Blue Prism Hub, sur la page Comptes de service, cliquez sur **Ajouter un compte**.
2. Saisissez un ID unique et un nom convivial, par exemple, *InteractRemoteAPI*.

   N'utilisez pas *InteractRemoteClient*. Ce nom est attribué en interne dans le système.

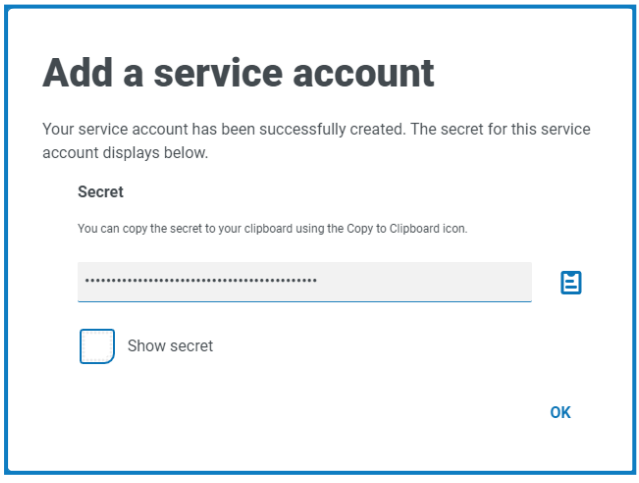
3. Sous **Permissions**, sélectionnez **Interact Remote API**.



4. Cliquez sur **Créer un compte de service**.

   La boîte de dialogue Ajouter un compte de service s'affiche avec une clé secrète générée. Vous devrez saisir cette clé dans le client interactif Blue Prism lors de la configuration de l'identifiant associé.

5. Copiez la clé secrète générée dans votre presse-papiers afin de le coller dans le client interactif Blue Prism.



6. Cliquez sur **OK** pour fermer la boîte de dialogue.

   La page Comptes de service s'affiche avec le compte nouvellement créé.

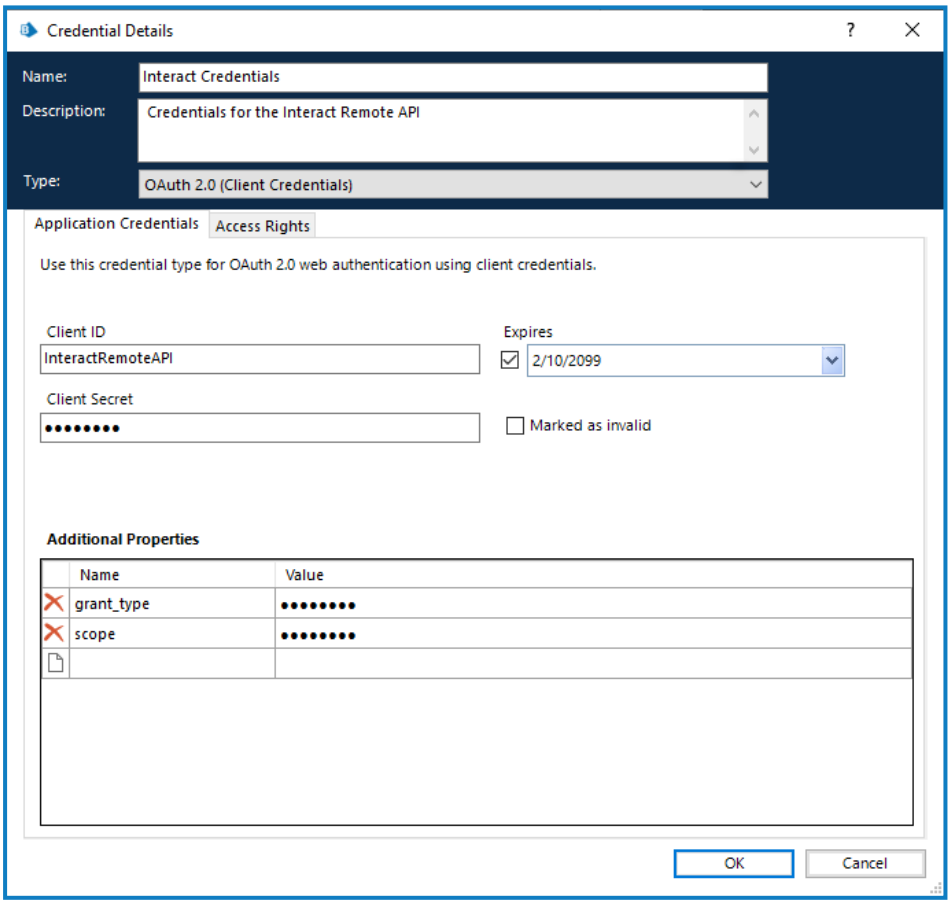
Importer le VBO

1. Téléchargez le fichier de version du service API d'Interact à partir du portail Blue Prism.
2. Dans Blue Prism, sélectionnez **Fichier** et cliquez sur **Importer** > **Version/Compétence** et suivez les invites pour importer le fichier de version dans Blue Prism. Pour plus d'informations, voir Importer un fichier.

Configurer des identifiants dans Blue Prism

1. Connectez-vous au client interactif Blue Prism, sélectionnez **Système**, puis cliquez sur **Sécurité** > **Identifiants**. Voir Sécurité > Identifiants pour en savoir plus.
2. Cliquez sur **Nouveau**.

   La boîte de dialogue des détails de l'identifiant s'affiche.
3. Dans l'onglet Identifiants de l'application de la boîte de dialogue Détails des identifiants :
   a. Saisissez un nom.
   b. Remplacez le **type** par **OAuth 2.0 (identifiants client)**.
   c. Dans **ID client**, saisissez l'ID que vous avez utilisé pour créer le compte de service ci-dessus dans Configurer les Digital Workers sur la page 77 (p. ex. *InteractRemoteAPI*).
   d. Dans **Secret client** : saisissez la clé secrète générée pour le compte de service.

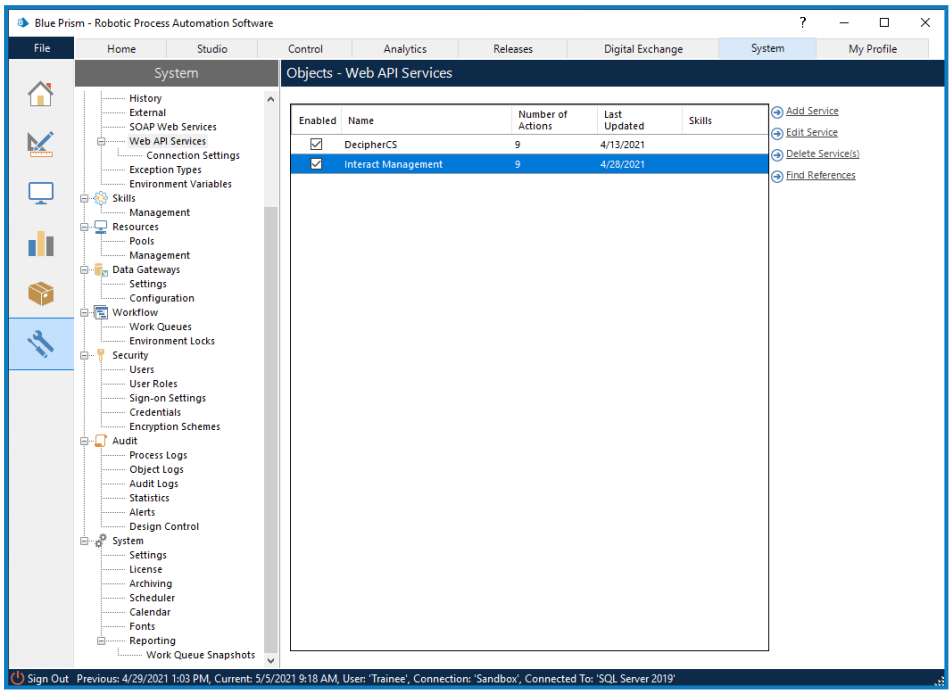


4. Dans l'onglet Droits d'accès de la boîte de dialogue Détails des identifiants, définissez les permissions d'accès requises.
5. Cliquez sur **OK**.

Configurer le service Web

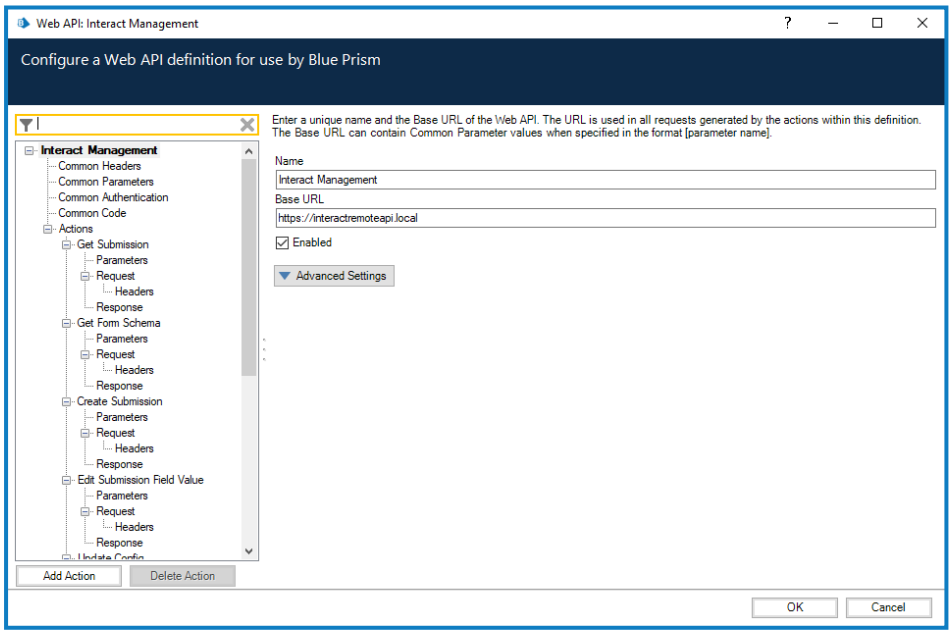
1. Dans Blue Prism, sélectionnez **Système**, puis cliquez sur **Objets** > **Services API Web**.

   L'écran Objets - Services API Web s'affiche. Par exemple :



2. Sélectionnez **Gestion d'Interact** et cliquez sur **Modifier le service**.

   L'écran API Web : Gestion d'Interact s'affiche.



3. Sur l'écran d'ouverture de l'API Web : Gestion d'Interact, dans **URL de base**, saisissez l'URL du service API Interact de votre organisation. Cela a été défini lors de l'installation d'Interact.
4. Sélectionnez **Authentification commune** dans l'arborescence de navigation, puis effectuez les opérations suivantes :

a. Assurez-vous que le **type d'authentification** est défini sur **OAuth 2.0 (identifiants client)**.

b. Dans l'**URI d'autorisation**, saisissez l'URL d'Authentication Server au format :

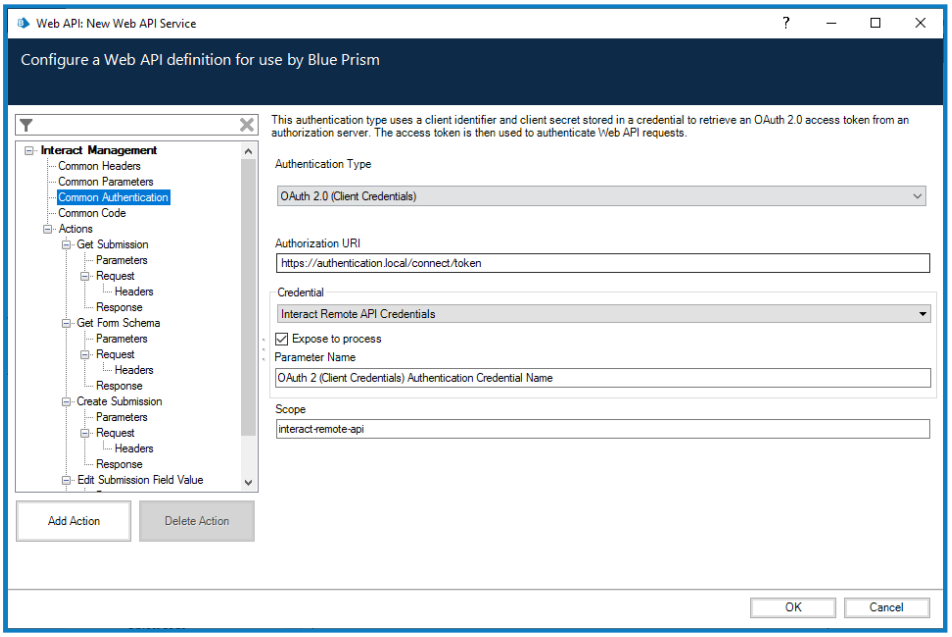
```
<URL Authentication Server>:<port si spécifié pendant l'installation>/connect/token
```

Par exemple, `https://authentication.blueprism.com:5000/connect/token`.

Ou, si le port par défaut a été utilisé, `https://authentication.blueprism.com/connect/token`.

> Si vous avez effectué une mise à niveau à partir d'une version antérieure à 4.3, votre système utilisera toujours IMS. Dans ce cas, vous devez saisir les informations au format :
>
> `<URL IMS>:<port si spécifié>/connect/token`
>
> Par exemple, `https://ims.blueprism.com:5000/connect/token`.

c. Dans **Identifiant**, sélectionnez l'identifiant que vous avez créé dans Configurer des identifiants dans Blue Prism sur la page 83.



5. Cliquez sur **OK** pour enregistrer et terminer la configuration du service API Web.

Vérifier une installation

Cette section fournit un scénario simple pour tester si les composants basiques de l'installation de Interact fonctionnent comme prévu. Ce processus de vérification nécessite :

- qu'une connexion à une base de données Blue Prism ait été configurée dans Hub (voir Réglages de la base de données sur la page 68 pour en savoir plus) ;
- qu'une file d'attente de travaux valide existe dans l'environnement Blue Prism, pouvant être utilisée pour ce test ;
- que le service API Interact soit installé et configuré dans Blue Prism (voir Configurer les Digital Workers sur la page 77 pour en savoir plus).

Voici les étapes de vérification :

- Vérifier qu'Interact peut soumettre des informations à une file d'attente de travaux dans Blue Prism :
  - Créer un processus métier dans Hub : chaque formulaire est lié à un processus métier.
  - Créer un formulaire Interact : créez un formulaire avec une page et un champ à utiliser pour le test de vérification.
  - Ajouter un formulaire à un rôle : permet à un utilisateur d'accéder au formulaire dans Interact.
  - Envoyer le formulaire et s'assurer qu'il apparaît dans une file d'attente sur Blue Prism
- Vérifier que Blue Prism peut fournir des informations à Interact :
  - Créer un processus Blue Prism simple

Ces instructions supposent que l'utilisateur connaît bien Blue Prism.

Si vous rencontrez des problèmes lors de la vérification de l'installation, voir Dépannage d'une installation.

⚠ Si vous avez installé votre environnement pour utiliser l'authentification Windows, vous devez affecter les pools d'applications et les services pour utiliser les comptes Windows, puis créer un environnement dans Hub, avant d'effectuer cette vérification. Si vous ne le faites pas, les formulaires créés dans le plug-in Interact ne s'afficheront pas pour les utilisateurs dans Interact. Voir Installation d'à l'aide de l'authentification Windows sur la page 62 et Configuration initiale de Hub sur la page 67 pour en savoir plus.

Créer un processus métier dans Hub

1. Connectez-vous à Authentication Server à l'aide d'un compte utilisateur administrateur et sélectionnez **Hub**.
2. Dans la barre de navigation de gauche, sélectionnez **Cycle de vie de l'automatisation** et cliquez sur **Processus métier**.
3. Cliquez sur **Ajouter nouveau**.
4. Saisissez un identifiant unique et un nom pour le processus métier. Vous pouvez également saisir une description.
5. Saisissez des remarques supplémentaires si nécessaire et cliquez sur **Créer un processus métier**.

Pour plus d'informations sur la création de processus métier, consultez le guide de l'utilisateur d'Automation Lifecycle Management.

Créer un formulaire Interact

Vous devez créer un formulaire comportant au moins une page avec un champ.

1. Dans la barre de navigation de gauche de Hub, sélectionnez **Interact** et cliquez sur **Formulaires**.
2. Sélectionnez **Créer un formulaire** pour créer un formulaire Interact.
3. Sélectionnez le processus métier que vous avez créé dans la liste déroulante s'il n'est pas déjà sélectionné.
4. Saisissez un nom et une description pour le formulaire Interact. Par exemple : *Formulaire de test*.
5. Sous **Méthode de livraison**, sélectionnez **File d'attente**.
6. Sélectionnez l'environnement dans la liste déroulante, puis le nom de la file d'attente requis.

   Si la file d'attente requise n'est pas affichée dans la liste, cliquez sur l'icône d'actualisation pour mettre à jour les files d'attente.
7. Laissez les champs **Priorité**, **SLA**, **E-mail** et **Rôle Interact** vides.
8. Laissez **Type d'approbation par défaut** sur **Aucun**.
9. Dans **Catégorie**, saisissez un nom pour la catégorie. Par exemple, *CatégorieTest*.
10. Sélectionnez une icône parmi celles prédéfinies pour illustrer le formulaire dans Interact.
11. Cliquez sur **Créer un formulaire**.

    La page Modifier le formulaire s'affiche.
12. Cliquez sur **Créer une page**.

    Le panneau Créer une page s'affiche.
13. Saisissez un nom et une description pour la nouvelle page et cliquez sur **Enregistrer**.

    La page Modifier le formulaire affiche la page que vous avez créée.
14. Cliquez sur les points de suspension (**...**) sur la page que vous venez de créer, puis sur **Créer un champ**.

    La boîte de dialogue Choisir le type de capture s'affiche.
15. Cliquez sur **Texte**.
16. Sur la page Créer un texte, entrez *ChampTexteTest* dans le champ **Étiquette** et laissez tout le reste par défaut.
17. Cliquez sur **Créer un champ**.
18. Sur la page Modifier le formulaire, cliquez sur **Enregistrer**.
19. Dans le panneau Augmenter la version mineure, saisissez une note de mise à jour et cliquez sur **Enregistrer**.

Pour plus d'informations sur la création de processus métier, consultez le guide de l'utilisateur du plug-in Interact.

Ajouter un rôle au formulaire

1. Dans Hub, cliquez sur l'icône de votre profil pour ouvrir la page Réglages, puis sur **Rôles et permissions**.

   La page Rôles et permissions s'affiche.
2. Cliquez sur **Créer un rôle**.

   La section Créer un rôle s'affiche.
3. Saisissez un nom de rôle tel que *Rôle test Interact*. Vous pouvez également saisir une description.
4. Changez **Type de rôle** en **Interact**.
5. Dans **Ajouter un formulaire**, sélectionnez le formulaire que vous venez de créer dans la liste déroulante. Si vous avez repris le même nom que dans l'étape Créer un formulaire Interact sur la page précédente, vous devrez saisir l'entrée suivante : **Formulaire de test**.
6. Dans **Ajouter un utilisateur**, sélectionnez les utilisateurs auxquels vous souhaitez donner accès au formulaire que vous avez créé. Ajoutez au minimum l'utilisateur administrateur que vous utilisez.
7. Cliquez sur **Enregistrer**.
8. Déconnectez-vous de Hub.

Pour plus d'informations sur le déploiement de processus métier, consultez le guide de l'utilisateur du plug-in Interact.

Envoyer le formulaire à une file d'attente de travaux dans Blue Prism

1. Connectez-vous au serveur d'authentification à l'aide des informations d'identification d'un membre dans le rôle que vous avez attribué au formulaire et sélectionnez **Interact**.

   Pour les besoins du test, vous pouvez utiliser soit l'administrateur affecté au rôle, soit un utilisateur. Seuls les membres du rôle peuvent voir le formulaire dans Interact, quels que soient leurs privilèges administratifs.
2. Cliquez sur le formulaire que vous venez de créer (**Formulaire de test**).

   Le formulaire s'affiche avec le champ de texte unique.
3. Saisissez du texte dans le champ, puis cliquez sur **Soumettre**.
4. Connectez-vous à Blue Prism et vérifiez s'il y a un élément dans la file d'attente de travaux spécifiée lors de la création du formulaire.

Pour plus d'informations sur l'utilisation d'Interact en tant qu'utilisateur final, consultez le guide de l'utilisateur d'Interact.

Cela achève la vérification de l'installation, prouvant qu'Interact peut communiquer avec Blue Prism. L'étape suivante consiste à vérifier que Blue Prism peut fournir des informations à Interact.

Créer un processus Blue Prism simple

Vous pouvez utiliser l'un des deux processus suivants. Ces deux éléments prouvent la communication entre Blue Prism et Interact. Ces processus montrent ce qui suit :

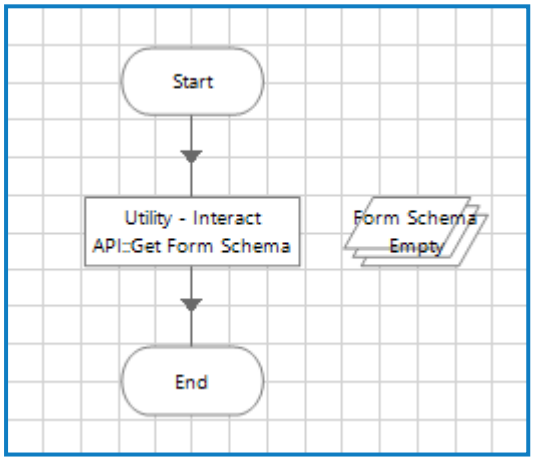
- Option 1 : Blue Prism peut interroger et recevoir une réponse d'Interact, dans ce cas, le nom du formulaire.

- Option 2 : Blue Prism peut modifier une valeur dans un formulaire, la modification étant affichée dans Interact.

Option 1 : Récupérer le nom du formulaire

1. Créez un processus dans Blue Prism.
2. Ajoutez une action à votre processus et définissez les propriétés suivantes :
   a. Réglez **Objet métier** sur **Utilitaire - API Interact**.
   b. Réglez **Action** sur **Obtenir le schéma du formulaire**.
   c. Dans l'onglet Entrée, saisissez le nom du formulaire que vous avez créé entre guillemets (p. ex. *"Formulaire de test"*) dans **Valeur du nom de formulaire**.
   d. Dans l'onglet Sortie, générez la collection Schémas de formulaire par défaut.
3. Connectez l'étape Action aux étapes Début et Fin.

   Votre processus devrait ressembler à ce qui suit :



4. Exécutez le processus.
5. Une fois terminé, ouvrez la collection Schémas de formulaire et sélectionnez l'onglet **Valeurs actuelles**. Le contenu devrait être similaire à celui du formulaire ; dans ce cas, un seul champ de texte ChampTexteTest.

Option 2 : Modifier une valeur de champ

Ce processus nécessite qu'il y ait un élément dans la file d'attente de travaux. Un élément a été envoyé dans le cadre de l'étape Envoyer le formulaire à une file d'attente de travaux dans Blue Prism sur la page précédente.

1. Créez un processus dans Blue Prism.
2. Ajoutez trois actions à votre processus et définissez les propriétés suivantes :

   Action 1 :
   a. Réglez **Objet métier** sur **Files d'attente de travaux**.
   b. Réglez **Action** sur **Obtenir l'élément suivant**.
   c. Dans l'onglet Entrée, saisissez le nom de la file d'attente à laquelle vous avez envoyé le formulaire dans **Valeur de la file d'attente**. Il a été spécifié dans Créer un formulaire Interact sur la page 87 à l'étape 6. Le nom de la file d'attente doit être saisi entre guillemets (p. ex. *"FileAttenteInteract"*).

d. Dans l'onglet Sortie, générez les champs Collecte de données et Identifiant d'élément par défaut.

Action 2 :

a. Réglez **Objet métier** sur **Utilitaire - API Interact**.

b. Réglez **Action** sur **Modifier la valeur du champ Texte**.

c. Dans l'onglet Entrée, saisissez les valeurs suivantes :

- Saisissez *[Data._requestId]* dans **ID de soumission**.
- Entrez le nom du champ entre guillemets dans **Nom du champ** (p. ex. "*ChampTexteTest*")
- Pour **Valeur de champ**, entrez entre guillemets la phase que vous souhaitez retransmettre à Interact (p. ex. "*voici un texte en guise d'exemple*").

Action 3 :

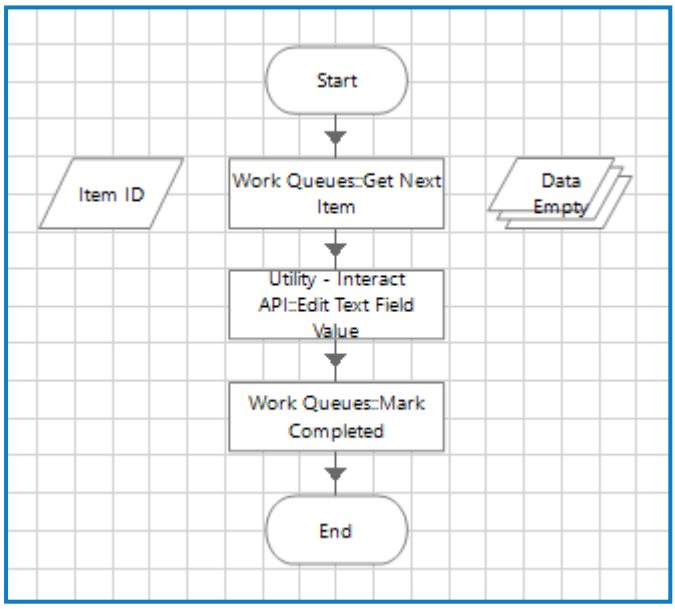
a. Réglez **Objet métier** sur **Files d'attente de travaux**.

b. Réglez **Action** sur **Marquer comme terminé**.

c. Dans l'onglet Entrée, saisissez *[Identifiant d'élément]* dans **Identifiant d'élément**. Il s'agit du type de données Texte généré par la première action.

3. Connectez les étapes d'action entre elles et aux étapes de début et de fin.

   Votre processus devrait ressembler à ce qui suit :



4. Exécutez le processus.
5. Une fois terminé :

   a. Ouvrez les files d'attente dans Blue Prism. Le formulaire précédemment envoyé doit être marqué comme complet.

   b. Ouvrez Interact, sélectionnez **Historique**, cliquez sur les points de suspension (**...**) à côté du formulaire envoyé et cliquez sur **Afficher**. Le formulaire doit afficher le texte envoyé par Blue Prism.

Vérification terminée

Cela achève la vérification de l'installation, prouvant que Blue Prism peut communiquer avec Interact et vice versa.

Vous pouvez désormais supprimer tous les éléments de test que vous avez créés, tels que :

- Suppression de la file d'attente de travaux si elle n'est plus nécessaire (voir Flux de travail – Files d'attente de travaux).
- Suppression du formulaire du plug-in Interact (voir dans le guide de l'utilisateur du plug-in Interact).
- Suppression du processus métier (voir dans le guide de l'utilisateur d'Automation Lifecycle Management).
- Suppression du rôle test (voir dans le guide de l'administrateur de Hub).

Dépanner une installation Interact

Les sections suivantes visent à fournir des instructions en cas de problèmes particuliers rencontrés pendant l'installation ou lors de la vérification de la réussite de l'installation.

Connectivité de la base de données

Le bouton **Tester la connexion pour continuer** du programme d'installation vérifie les éléments suivants :

- Si la base de données existe :
  - Qu'il est possible de s'y connecter.
  - Que le SQL Server hébergeant la base de données a un certificat valide appliqué.
  - Que le compte dispose des droits pour lire, écrire et modifier la base de données.
- Si la base de données n'existe pas :
  - Que le compte dispose du droit de créer la base de données.
  - Que le SQL Server a un certificat valide appliqué.

Si ces exigences ne peuvent pas être satisfaites, l'installation s'arrêtera.

Plusieurs vérifications peuvent être réalisées lorsqu'une connexion à un SQL Server ne peut pas se faire sur le LAN :

- Vérifier la connectivité du réseau : s'assurer que tous les appareils concernés sont connectés au même réseau et sont capables de communiquer.
- Cryptage SSL : assurez-vous que SQL Server dispose d'un certificat valide. Pour plus d'informations, veuillez consulter Prérequis sur la page 8.
- Identifiants SQL : vérifier les identifiants SQL et que l'utilisateur a les permissions appropriées sur SQL Server.
- Pare-feu : vérifiez que les pare-feux sur les serveurs eux-mêmes ou à l'intérieur du réseau n'empêchent pas la communication.
- Service SQL Browser : s'assurer que le service SQL Browser sur SQL Server est activé pour permettre de trouver une instance SQL. Pour SQL Server Express, ce service est généralement désactivé par défaut.
- Activer la connectivité TCP/IP : lorsque la connectivité à distance est requise pour SQL, vérifiez que la connectivité TCP/IP est activée pour l'instance SQL. Microsoft fournit des articles spécifiques à chaque version de SQL avec des instructions pour activer le protocole réseau TCP/IP pour SQL Server.

Une autre raison potentielle d'échec est que le compte utilisé pour créer les bases de données dans le programme d'installation ne dispose pas de privilèges suffisants pour créer les bases de données.

Serveur Web

Pendant le processus d'installation, le programme d'installation vérifiera que tous les prérequis sont installés. Il est recommandé que si les prérequis ne sont pas installés, le programme d'installation soit annulé, les prérequis installés et le processus d'installation redémarré.

Utiliser RabbitMQ avec AMQPS

Si vous utilisez RabbitMQ avec AMQPS (Advanced Message Queuing Protocol - Secure), les pools d'applications créés dans le cadre de l'installation de Interact doivent se voir accorder des permissions pour le certificat RabbitMQ. Pour ce faire :

1. Sur le serveur Web, ouvrez le Gestionnaire de certificats. Pour ce faire, saisissez *Certificats* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gérer les certificats informatiques**.
2. Naviguez jusqu'au certificat identifié à utiliser avec RabbitMQ AMQPS pendant l'installation de Hub, et cliquez avec le bouton droit dessus, puis sélectionnez **Toutes les tâches** et cliquez sur **Gérer les clés privées...**.

   La boîte de dialogue Permissions du certificat s'affiche.
3. Cliquez sur **Ajouter**, puis saisissez les pools d'applications suivants dans le champ **Saisir les noms d'objet à sélectionner** :

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

   > Il s'agit des noms de pool d'applications par défaut. Si vous avez saisi des noms différents pendant l'installation, assurez-vous que la liste reflète les noms que vous avez utilisés.
4. Si vous utilisez l'authentification Windows, ajoutez également le nom du compte de service utilisé pour les services Windows suivants :
   - Blue Prism – Auditeur du service d'audit
   - Blue Prism – Service de log
   - Blue Prism – Submit Form Manager
5. Cliquez sur **Vérifier les noms**.

   Les noms doivent être validés. Si ce n'est pas le cas, vérifiez que le nom correspond au pool d'applications ou au compte de service que vous essayez d'utiliser et corrigez-le si nécessaire.
6. Cliquez sur **OK**.
7. Sélectionnez chaque pool d'applications dans la liste **Groupe ou nom d'utilisateur** et assurez-vous que le **contrôle complet** est sélectionné dans la liste **Permissions pour {nom du compte}**.
8. Cliquez sur **OK**.

   Les pools d'applications ont désormais accès au certificat.

Authentification Windows

Le compte utilisé lors de l'exécution de l'installation doit disposer des permissions SQL Server appropriées pour effectuer l'installation, à savoir l'appartenance aux rôles de serveur fixes sysadmin ou dbcreator. Voir Préparation pour en savoir plus.

Si l'authentification Windows est choisie pendant le processus d'installation, il est recommandé d'utiliser un compte de service Windows doté des permissions nécessaires pour exécuter les tâches et les processus pendant le fonctionnement normal. Le compte de service Windows aura besoin de ce qui suit :

- La possibilité d'exécuter les processus de base de données SQL (voir Permissions SQL minimales sur la page 15).
- La propriété sur le pool d'applications IIS.
- Les permissions pour les certificats requis.

Affectation du compte de service Windows en tant que propriétaire sur les certificats

Le compte de service Windows doit être autorisé à accéder aux certificats BluePrismCloud. Pour ce faire :

1. Sur le serveur Web, ouvrez le Gestionnaire de certificats. Pour ce faire, saisissez *Certificats* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gérer les certificats informatiques**.
2. Dans le volet de navigation, développez **Personnel** et cliquez sur **Certificats**.
3. Suivez les étapes ci-dessous pour les certificats BluePrismCloud_Data_Protection et BluePrismCloud_IMS_JWT :
    a. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez **Toutes les tâches**, puis cliquez sur **Gérer les clés privées...**.

       La boîte de dialogue Permissions du certificat s'affiche.
    b. Cliquez sur **Ajouter**, puis saisissez le compte de service et cliquez sur **OK**.
    c. Lorsque le compte de service est sélectionné dans la liste **Groupe ou nom d'utilisateur**, assurez-vous que le **contrôle complet** est sélectionné dans la liste **Permissions pour {nom du compte}**.
    d. Cliquez sur **OK**.

       Le compte de service a désormais accès au certificat.

Affectation d'un compte de service Windows au pool d'applications

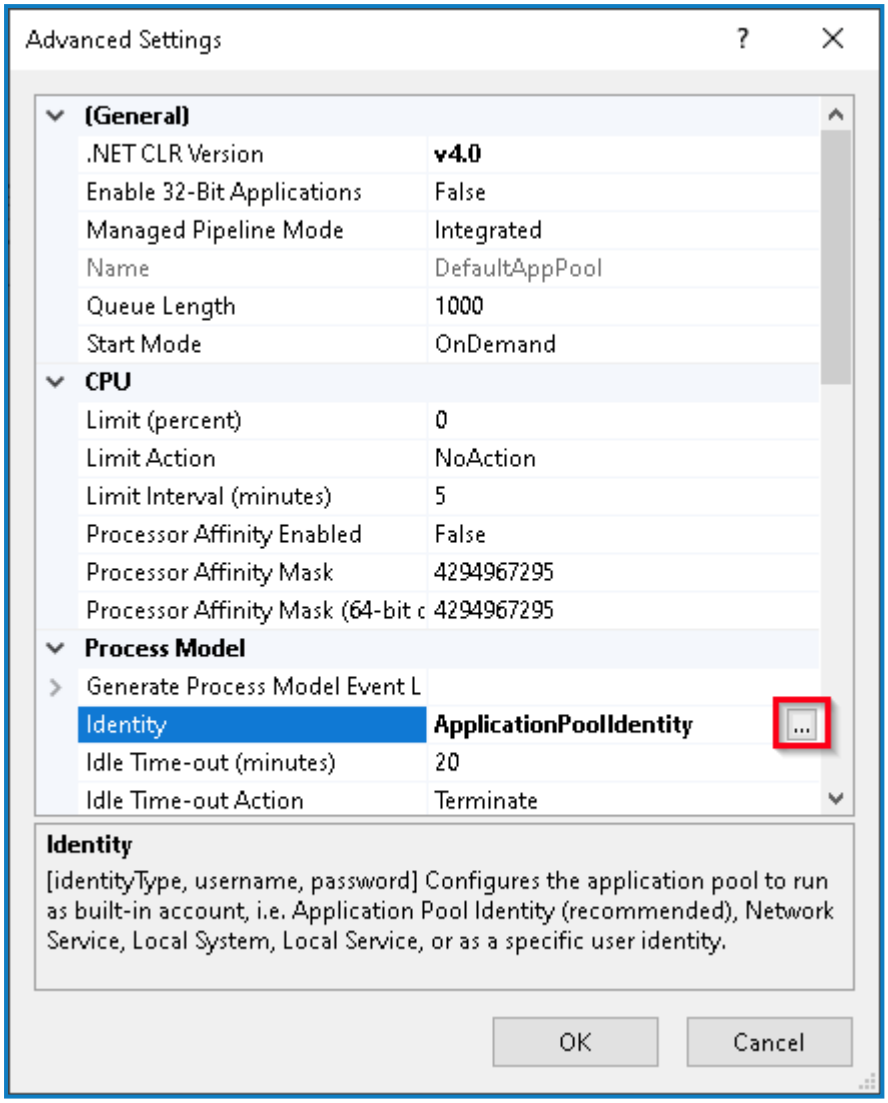
Par défaut, les pools d'applications sont créés avec l'identité « ApplicationPoolIdentity ». Une fois que l'assistant d'installation a terminé, le compte de service Windows doit être autorisé à gérer les pools d'applications. Pour ce faire :

1. Sur le serveur Web, ouvrez le gestionnaire d'Internet Information Services (IIS).
2. Dans le panneau Connexions, développez l'hôte et sélectionnez **Pools d'applications**.
3. Vérifiez les valeurs de la colonne **Identité**.

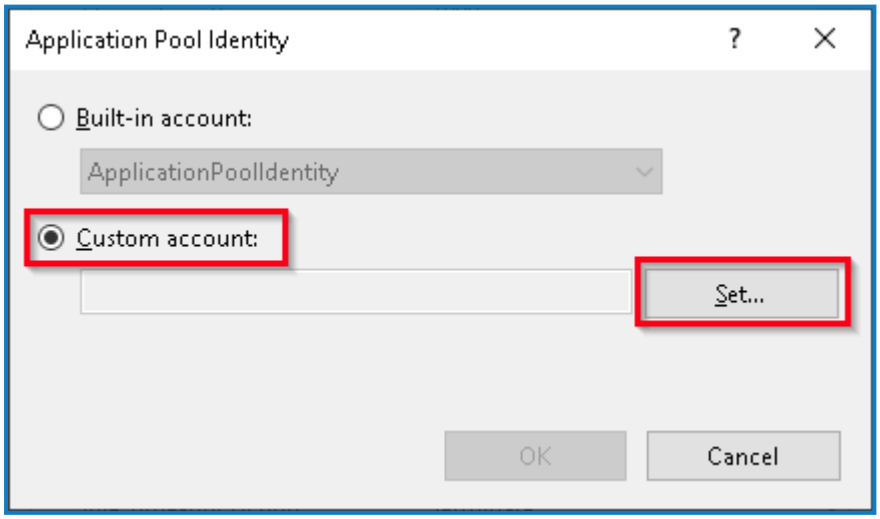
   L'identité d'un pool d'applications doit correspondre au compte de service Windows spécifique.
4. Pour tous les pools d'applications dont la colonne *Identité* contient **ApplicationPoolIdentity**, cliquez avec le bouton droit de la souris sur la ligne et sélectionnez **Réglages avancés...**.

   La boîte de dialogue Réglages avancés s'affiche.

5. Sélectionnez le réglage **Identité**, puis cliquez sur le bouton **...** (ellipse) :



6. Dans la boîte de dialogue Identité du pool d'applications, sélectionnez **Compte personnalisé**, puis cliquez sur **Définir...**.



La boîte de dialogue Définir les identifiants s'affiche.

7. Saisissez les identifiants du compte de service Windows requis et cliquez sur **OK**.

8. Répétez l'opération pour tous les pools d'applications à modifier.
9. Redémarrez le service RabbitMQ.
10. Redémarrez tous les pools d'applications.
11. Redémarrez IIS.

En cas de problèmes avec le service Audit Service, assurez-vous que le compte de service Windows a accès à l'auditeur du service d'audit ainsi qu'à la base de données Audit.

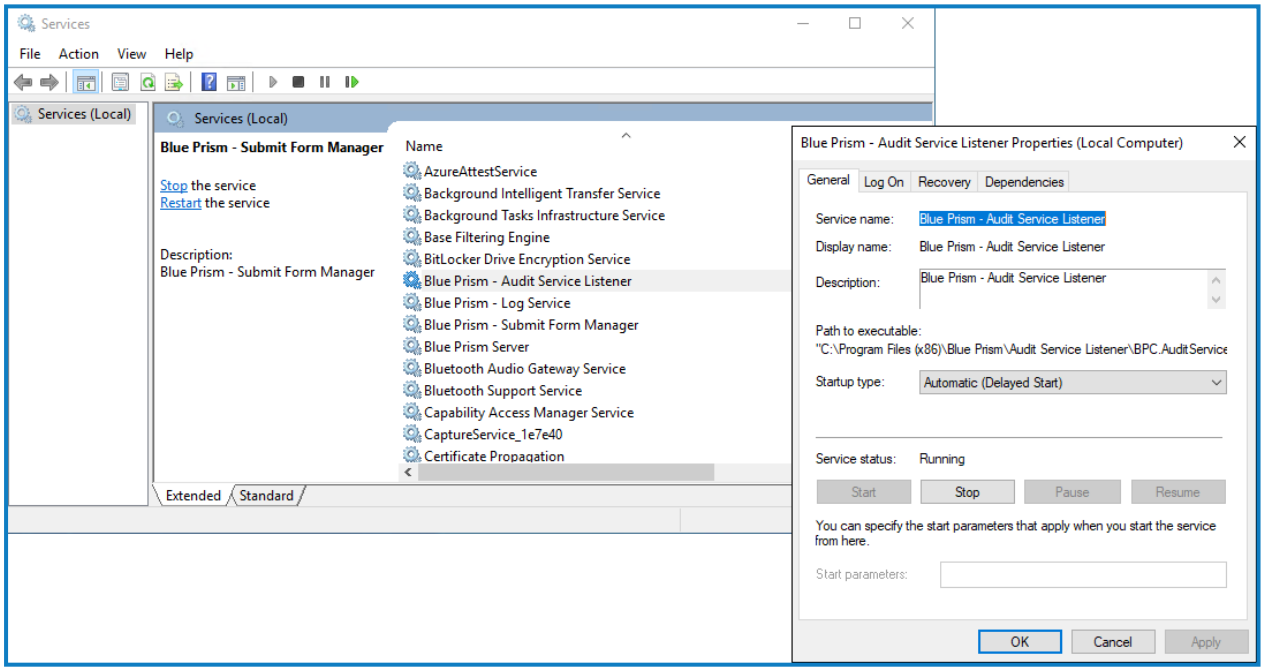
Affectation d'un compte de service Windows à un service

Le compte de service Windows doit être affecté pour gérer les services suivants :

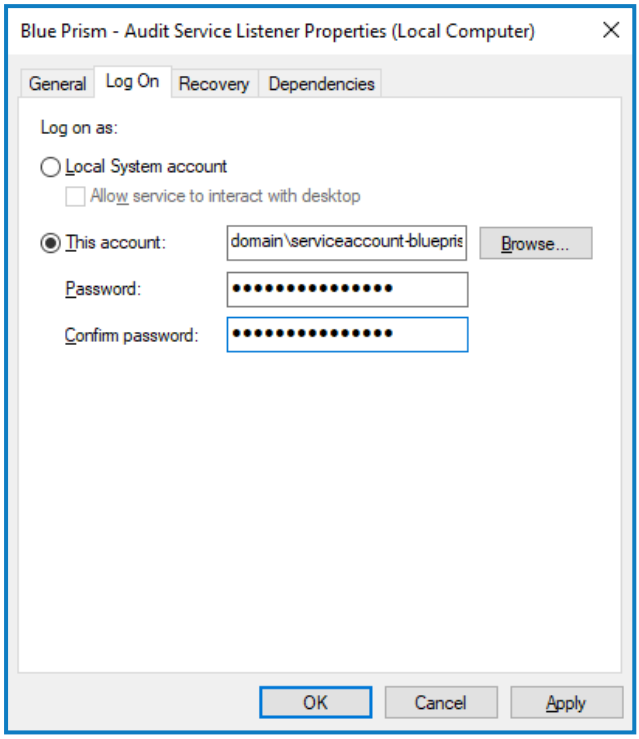
- Blue Prism - Auditeur du service d'audit
- Blue Prism - Service de log
- Blue Prism - Submit Form Manager

Pour ce faire :

1. Ouvrez Services dans le serveur Web.
2. Cliquez avec le bouton droit sur le service et sélectionnez **Propriétés**.



3. Dans l'onglet Connexion, sélectionnez **Ce compte**, puis saisissez le nom du compte ou cliquez sur **Parcourir** pour rechercher le compte que vous souhaitez utiliser.



4. Saisissez le mot de passe du compte et cliquez sur **OK**.
5. Dans la fenêtre Services, cliquez avec le bouton droit sur le service et cliquez sur **Redémarrer**.
6. Répétez l'opération pour les autres services Blue Prism.

Messages bloqués dans RabbitMQ

Si une soumission n'est pas ajoutée à la file d'attente de travaux Blue Prism Enterprise attendue, cela peut être dû au fait que la soumission n'a pas été transmise correctement par le serveur de l'agent de messages (exécution de RabbitMQ).

En cas de panne du système de Hub ou d'Interact, les soumissions de formulaire Interact peuvent être envoyées à une file d'attente d'erreurs RabbitMQ au lieu de la file d'attente de messages appropriée dans RabbitMQ (qui dirige ensuite les soumissions vers les files d'attente de travaux dans Blue Prism Enterprise). Votre administrateur système (avec accès à RabbitMQ) devra déplacer la soumission hors de la file d'attente d'erreurs.

Pour plus d'informations sur le déplacement des soumissions de formulaires Interact depuis la file d'attente d'erreurs RabbitMQ, reportez-vous à cet article de la base de connaissances : Comment déplacer les soumissions de formulaires Interact d'une file d'attente d'erreurs RabbitMQ.

Une autre cause de blocage des messages dans RabbitMQ est l'échec du traitement des messages et de la mise à jour des files d'attente par IADA. IADA dépend de la fonctionnalité d'initialisation de l'application IIS, qui aurait dû être installée par défaut pendant le processus d'installation. Cependant, si elle n'a pas été installée, vous pouvez le faire comme suit :

1. Sur le serveur Web où Interact et IADA sont installés, ouvrez le Gestionnaire de serveurs. Pour ce faire, saisissez *Serveur* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gestionnaire de serveurs**.

2. Cliquez sur **Ajouter des rôles et des fonctionnalités**.

   L'assistant Ajouter des rôles et des fonctionnalités s'affiche.
3. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez la page Rôles du serveur.
4. Développez **Serveur Web (IIS)**, développez **Serveur Web**, développez **Développement d'application**, puis sélectionnez **Initialisation d'application**.
5. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez la page Confirmer les sélections d'installation.
6. Cliquez sur **Installer**.
7. Une fois l'installation terminée, redémarrez le serveur Web.

Dépanner une installation Hub

Les sections suivantes visent à fournir des instructions en cas de problèmes particuliers rencontrés pendant l'installation ou lors de la vérification de la réussite de l'installation.

Connectivité de l'agent de messages

Pour vérifier la connectivité entre le serveur Web et l'agent de messages, vérifiez que la console de gestion RabbitMQ est accessible via un navigateur Web.

Il pourrait y avoir plusieurs raisons pour lesquelles la connectivité échoue :

- Vérifier la connectivité du réseau : s'assurer que tous les appareils concernés sont connectés au même réseau et sont capables de communiquer.
- Pare-feu : vérifiez que les pare-feux sur les serveurs eux-mêmes ou à l'intérieur du réseau n'empêchent pas la communication.

> La console de gestion RabbitMQ communique, par défaut, sur le port 15672. Les files d'attente d'agent de messages utilisent un port différent, 5672, par défaut. Le pare-feu doit être vérifié pour l'accès TCP sur tous les ports. Cela est particulièrement vrai si l'organisation informatique a spécifié des ports autres que ceux par défaut.

Connectivité de la base de données

Le bouton **Tester la connexion pour continuer** du programme d'installation vérifie les éléments suivants :

- Si la base de données existe :
  - Qu'il est possible de s'y connecter.
  - Que le SQL Server hébergeant la base de données a un certificat valide appliqué.
  - Que le compte dispose des droits pour lire, écrire et modifier la base de données.
- Si la base de données n'existe pas :
  - Que le compte dispose du droit de créer la base de données.
  - Que le SQL Server a un certificat valide appliqué.

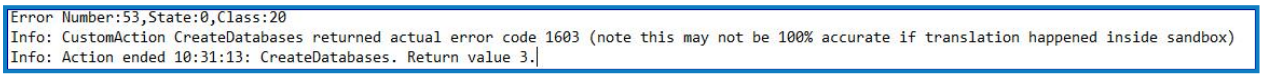
Si ces exigences ne peuvent pas être satisfaites, l'installation s'arrêtera.

Plusieurs vérifications peuvent être réalisées lorsqu'une connexion à un SQL Server ne peut pas se faire sur le LAN :

- Vérifier la connectivité du réseau : s'assurer que tous les appareils concernés sont connectés au même réseau et sont capables de communiquer.
- Cryptage SSL : assurez-vous que SQL Server dispose d'un certificat valide. Pour plus d'informations, veuillez consulter .
- Identifiants SQL : vérifier les identifiants SQL et que l'utilisateur a les permissions appropriées sur SQL Server.
- Pare-feu : vérifiez que les pare-feux sur les serveurs eux-mêmes ou à l'intérieur du réseau n'empêchent pas la communication.
- Service SQL Browser : s'assurer que le service SQL Browser sur SQL Server est activé pour permettre de trouver une instance SQL. Pour SQL Server Express, ce service est généralement désactivé par défaut.

- Activer la connectivité TCP/IP : lorsque la connectivité à distance est requise pour SQL, vérifiez que la connectivité TCP/IP est activée pour l'instance SQL. Microsoft fournit des articles spécifiques à chaque version de SQL avec des instructions pour activer le protocole réseau TCP/IP pour SQL Server.

Si, lors de l'exécution du programme d'installation, le processus d'installation échoue avec des erreurs de base de données, consultez ce qui suit, puis vérifiez que le serveur Web dispose d'une connectivité SQL à la base de données. Cela pourrait être dû à l'une des raisons potentiellement énumérées ci-dessus.



Une autre raison potentielle d'échec est que le compte utilisé pour créer les bases de données dans le programme d'installation ne dispose pas de privilèges suffisants pour créer les bases de données.

Enfin, si l'installation est une réinstallation après la suppression du logiciel. Ensuite, si les mêmes noms de base de données ont été utilisés, les bases de données d'origine doivent être sauvegardées et supprimées avant la réinstallation.

Serveur Web

Pendant le processus d'installation, le programme d'installation vérifiera que tous les prérequis sont installés. Il est recommandé que si les prérequis ne sont pas installés, le programme d'installation soit annulé, les prérequis installés et le processus d'installation redémarré.

Pour plus d'informations, voir Prérequis sur la page 8.

Utiliser RabbitMQ avec AMQPS

Si vous utilisez RabbitMQ avec AMQPS (Advanced Message Queuing Protocol - Secure), les pools d'applications créés dans le cadre de l'installation de Hub doivent se voir accorder des permissions pour le certificat RabbitMQ. Pour ce faire :

1. Sur le serveur Web, ouvrez le Gestionnaire de certificats. Pour ce faire, saisissez *Certificats* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gérer les certificats informatiques**.
2. Naviguez jusqu'au certificat identifié à utiliser avec RabbitMQ AMQPS pendant l'installation de Hub, et cliquez avec le bouton droit dessus, puis sélectionnez **Toutes les tâches** et cliquez sur **Gérer les clés privées...**.

   La boîte de dialogue Permissions du certificat s'affiche.
3. Cliquez sur **Ajouter**, puis saisissez les pools d'applications suivants dans le champ **Saisir les noms d'objet à sélectionner** :

   > Il s'agit des noms de pool d'applications par défaut. Si vous avez saisi des noms différents pendant l'installation, assurez-vous que la liste reflète les noms que vous avez utilisés.
4. Si vous utilisez l'authentification Windows, ajoutez également le nom du compte de service utilisé pour les services Windows suivants :
   - Blue Prism – Auditeur du service d'audit
   - Blue Prism – Service de log
5. Cliquez sur **Vérifier les noms**.

   Les noms doivent être validés. Si ce n'est pas le cas, vérifiez que le nom correspond au pool d'applications ou au compte de service que vous essayez d'utiliser et corrigez-le si nécessaire.

6. Cliquez sur **OK**.
7. Sélectionnez chaque pool d'applications dans la liste **Groupe ou nom d'utilisateur** et assurez-vous que le **contrôle complet** est sélectionné dans la liste **Permissions pour {nom du compte}**.
8. Cliquez sur **OK**.

   Les pools d'applications ont désormais accès au certificat.

Service de fichier

Si le service File Service ne parvient pas à localiser les images pour Authentication Server et Hub, cela est dû à une désinstallation et une réinstallation des produits Blue Prism. Ce problème ne se produira pas pour les premières installations.

Pendant le processus de suppression, les bases de données ne sont pas supprimées et, par conséquent, si la réinstallation utilise les mêmes noms de base de données, les chemins d'accès d'origine aux services de fichier et aux URL seront toujours utilisés.

Pour résoudre ce problème, après l'exécution du processus de suppression, supprimez ou nettoyez les bases de données afin que les chemins précédents aient été supprimés ou utilisez d'autres noms de base de données pendant la réinstallation.

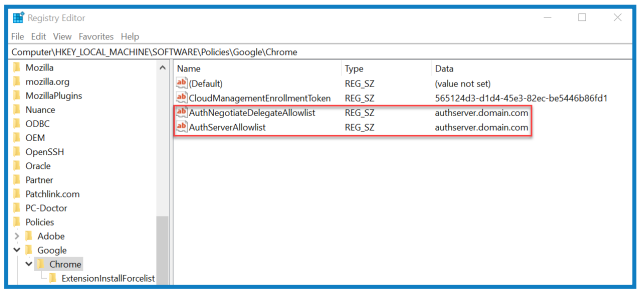
Configurer les navigateurs pour l'authentification Windows intégrée

Dans le cas où les utilisateurs Active Directory ne peuvent pas se connecter à Blue Prism Hub après l'installation, vérifiez que vous avez configuré les navigateurs Web pris en charge pour l'authentification Windows intégrée afin que les utilisateurs actuellement connectés puissent être récupérés à partir de la machine client. Les étapes de configuration sont différentes pour chaque navigateur Web pris en charge par Hub.

Configurer Google Chrome

1. Fermez toutes les instances ouvertes de Chrome.
2. Ouvrez l'éditeur de registre et saisissez ce qui suit dans la barre supérieure :

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
3. Cliquez avec le bouton droit de la souris sur le dossier Chrome et sélectionnez **Nouveau** > **Valeur de chaîne de caractères**.
4. Ajoutez les valeurs de chaîne suivantes : `AuthNegotiateDelegateAllowlist` et `AuthServerAllowlist`.
5. Cliquez avec le bouton droit de la souris sur chaque valeur de chaîne de caractères et sélectionnez **Modifier**.
6. Dans le champ **Données de valeur** pour les deux valeurs de chaîne de caractères, saisissez le nom d'hôte du site Web Authentication Server, par exemple, authserver.domaine.com, puis cliquez sur **OK**.

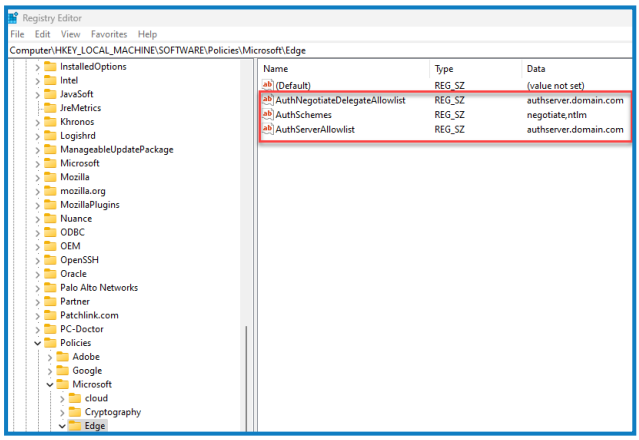


Configurer Microsoft Edge

1. Fermez toutes les instances ouvertes d'Edge.
2. Ouvrez l'éditeur de registre et saisissez ce qui suit dans la barre supérieure :

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Cliquez avec le bouton droit de la souris sur le dossier Chrome et sélectionnez **Nouveau** > **Valeur de chaîne de caractères**.
4. Ajoutez les valeurs de chaîne suivantes : `AuthNegotiateDelegateAllowlist`, `AuthServerAllowlist` et `AuthSchemes`.
5. Cliquez avec le bouton droit de la souris sur chaque valeur de chaîne de caractères et sélectionnez **Modifier**.
6. Dans le champ **Données de valeur** pour `AuthNegotiateDelegateAllowlist` et `AuthServerAllowlist`, saisissez le nom d'hôte du site Web Authentication Server, par exemple, authserver.domain.com, puis cliquez sur **OK**.
7. Dans le champ **Données de valeur** pour `AuthSchemes`, saisissez `negotiate, ntlm` et cliquez sur **OK**. Pour plus d'informations, veuillez consulter la documentation Microsoft sur les politiques Microsoft Edge.

> Cette valeur de chaîne n'est pas requise si votre organisation n'est configurée que pour l'authentification Kerberos, voir ci-dessous pour plus d'informations.

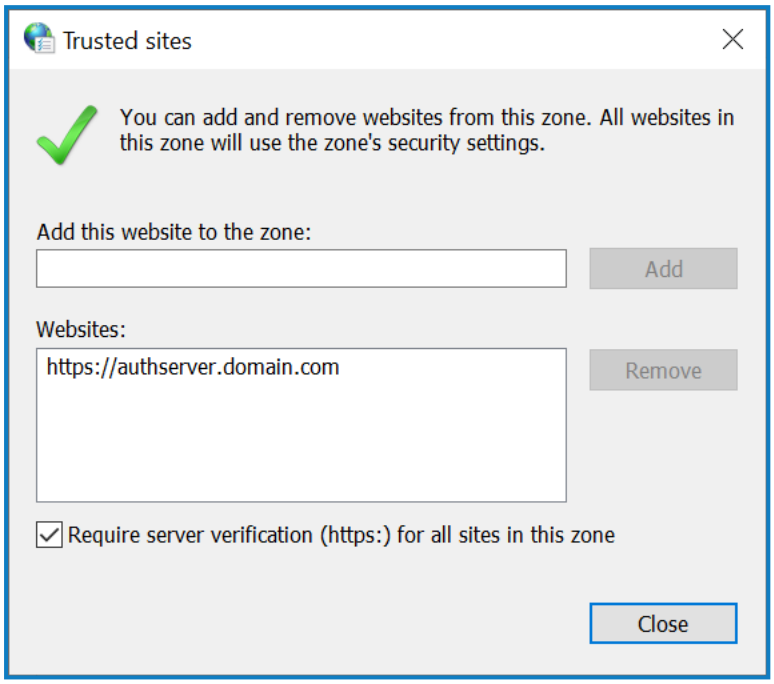


Vous pouvez également suivre ces étapes pour Microsoft Edge :

1. Fermez toutes les instances ouvertes d'Edge.
2. Allez dans **Panneau de configuration** > **Réseau et Internet** > **Options Internet**.
3. Dans l'onglet Avancé, sous Sécurité, sélectionnez **Activer l'authentification Windows intégrée**.
4. Dans l'onglet Sécurité, cliquez sur **Sites approuvés** > **Sites**.

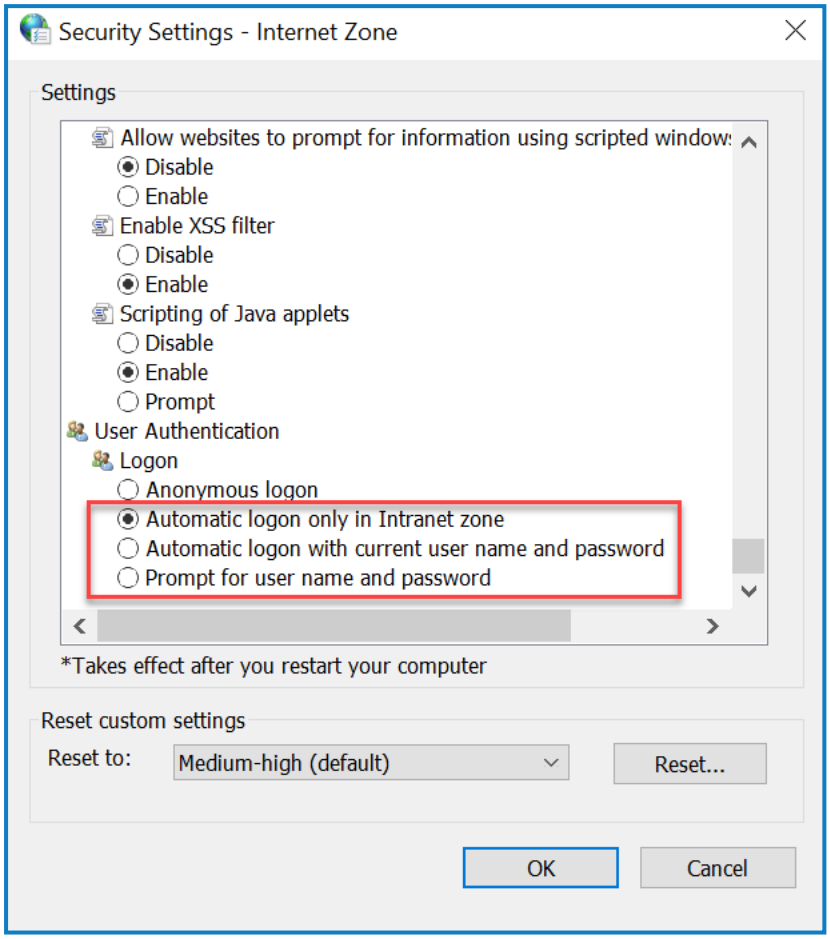
5. Dans la boîte de dialogue Sites approuvés, saisissez l'URL d'Authentication Server (par exemple, https://authserver.domaine.com) dans le champ **Ajouter ce site Web à la zone** et cliquez sur **Ajouter**.

   L'URL s'affiche dans le champ **Sites Web**.



6. Cliquez sur **Fermer**.
7. Dans l'onglet Sécurité de la boîte de dialogue Options Internet, cliquez sur **Sites approuvés** > **Niveau personnalisé**.

8. Sous **Authentification de l'utilisateur** > **Connexion**, confirmez que la **connexion anonyme** n'est pas sélectionnée. Utilisez plutôt l'un des réglages qui permet au navigateur de récupérer les identifiants de l'utilisateur, comme illustré ci-dessous.



9. Cliquez sur **OK**.

Configurer l'authentification Kerberos

Les étapes ci-dessus ne suffiront pas si l'authentification Windows New Technology LAN Manager (NTLM) a été désactivée pour votre environnement. Dans ce cas, vous devez également configurer l'authentification Kerberos et un nom de principal de service (SPN). Selon la configuration de votre organisation, vous devrez peut-être également ajouter une clé de registre Microsoft Edge WebView2. Pour plus d'informations, veuillez consulter la documentation Microsoft sur l'authentification NTLM et Kerberos.

1. Sur le serveur Web, ouvrez le gestionnaire d'Internet Information Services (IIS).
2. Depuis la liste des connexions, sélectionnez **Blue Prism - Authentication Server**.

   Il s'agit du nom de site par défaut ; si vous avez utilisé un nom de site personnalisé, sélectionnez la connexion appropriée.
3. Sous IIS, double-cliquez sur **Authentification**.

   La page Authentification s'affiche.
4. Sélectionnez **Authentification Windows** (assurez-vous qu'elle est définie sur Activé), puis cliquez sur **Fournisseurs...**.

   La boîte de dialogue Fournisseurs s'affiche.

5. Ajoutez un ou plusieurs fournisseurs à partir de la liste des fournisseurs disponibles, en fonction de la configuration de votre organisation, et cliquez sur **OK** .

Configuration du nom de principal de service (SPN)

Un nom de principal de service (SPN) doit également être configuré et enregistré pour l'URL d'Authentication Server afin de s'assurer que l'authentification Kerberos fonctionne correctement. Veuillez consulter la documentation Microsoft spécifique à cette rubrique pour en savoir plus, y compris les permissions requises. Il s'agit d'une étape essentielle à examiner avec l'équipe informatique de votre organisation pour s'assurer que la commande `Setspn` n'échoue pas à s'exécuter en raison de permissions de compte manquantes.

1. Ouvrez l'Invite de commande en tant qu'administrateur sur le serveur d'applications et exécutez la commande ci-dessous.

   Si le pool d'applications Blue Prism - Authentication Server s'exécute en tant que compte système local :

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

   Si le pool d'applications Blue Prism - Authentication Server s'exécute en tant que compte de service, utilisez :

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

   > HTTP couvre à la fois HTTP et HTTPS. Ne modifiez pas la commande pour inclure HTTPS spécifiquement, car la configuration échouera.

2. Exécutez la `Klist purge` pour actualiser les tickets Kerberos.
3. Connectez-vous à Authentication Server pour vérifier que l'authentification Kerberos fonctionne correctement.

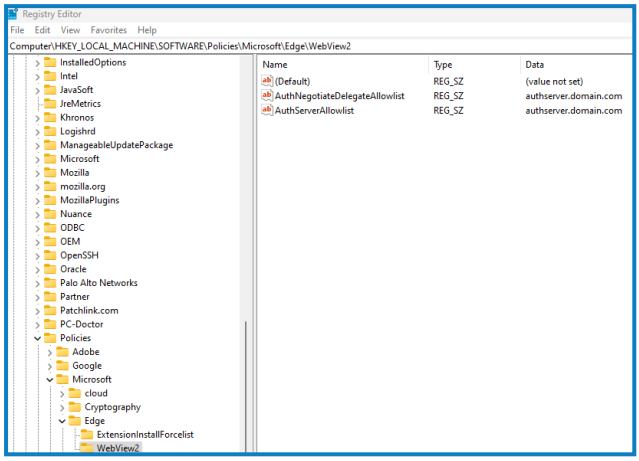
Ajouter une clé de registre Microsoft Edge WebView2

Si votre organisation n'est configurée que pour l'authentification Kerberos, et qu'Authentication Server est également utilisé pour se connecter à Blue Prism Enterprise, une clé de registre pour le navigateur Microsoft Edge WebView2 doit être ajoutée :

1. Fermez toutes les instances ouvertes d'Edge.
2. Ouvrez l'éditeur de registre et saisissez ce qui suit dans la barre supérieure :

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge
3. Cliquez avec le bouton droit de la souris sur le dossier Edge et sélectionnez **Nouveau** > **Clé**.
4. Nommez la nouvelle clé **WebView2**.
5. Cliquez avec le bouton droit de la souris sur le dossier WebView2 et ajoutez les valeurs de chaîne suivantes : `AuthNegotiateDelegateAllowlist` et `AuthServerAllowlist`.
6. Cliquez avec le bouton droit de la souris sur chaque valeur de chaîne de caractères et sélectionnez **Modifier**.

7. Dans le champ **Données de valeur** pour `AuthNegotiateDelegateAllowlist` et `AuthServerAllowlist`, saisissez le nom d'hôte du site Web Authentication Server, par exemple, authserver.domain.com, puis cliquez sur **OK**.



Hub affiche une erreur au démarrage

Si un utilisateur se connecte à Authentication Server, sélectionne Hub et que le message suivant s'affiche :

Une erreur s'est produite lors du démarrage de l'application

Cela signifie que les sites IIS doivent être redémarrés. Cette erreur affecte les systèmes qui sont installés sur un serveur unique et se produit si RabbitMQ démarre après les sites IIS. Par conséquent, il est recommandé que les sites IIS disposent d'un délai de démarrage défini pour permettre à RabbitMQ de démarrer en premier.

Si cette erreur se produit, elle peut être résolue de la manière suivante :

1. Sur le serveur, ouvrez le gestionnaire d'Internet Information Services (IIS) et arrêtez tous les sites Blue Prism. Pour une liste, voir Sites Web Hub.
2. Redémarrez le service RabbitMQ.
3. Redémarrez tous les pools d'applications Blue Prism.
4. Démarrez les sites Blue Prism qui ont été arrêtés à l'étape 1.

Pour retarder le démarrage du service des sites IIS :

1. Sur le serveur, ouvrez Services.
2. Cliquez avec le bouton droit de la souris sur **World Wide Web Publishing Service** et sélectionnez **Propriétés**.
3. Dans l'onglet Général, définissez le **type de démarrage** sur **Automatique (démarrage différé)**.
4. Cliquez sur **OK** et fermez la fenêtre Services.

Impossible de configurer les réglages SMTP dans Hub

Si vous ne parvenez pas à configurer les réglages SMTP dans Hub, cela est normalement lié à l'ordre de démarrage des services.

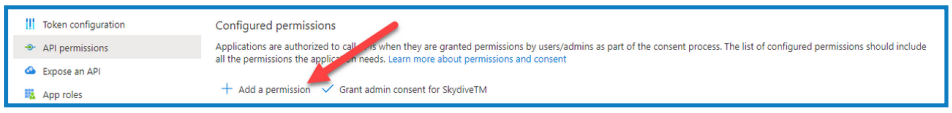
Le serveur Web doit démarrer après le démarrage des services RabbitMQ. Si les services du serveur Web démarrent avant que le service RabbitMQ ne soit prêt, alors le fait d'accéder aux réglages SMTP dans Hub entraînera un message « Une erreur s'est produite ».

L'enregistrement du réglage SMTP renvoie une erreur lors de l'utilisation d'OAuth 2.0

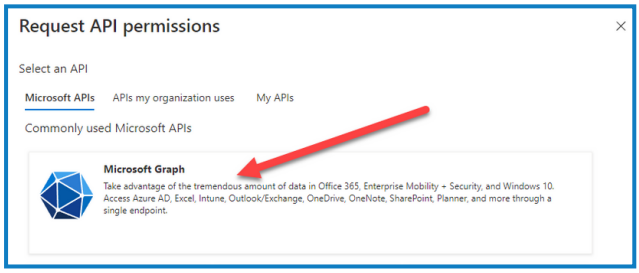
Si vous recevez une erreur lors de l'enregistrement d'une configuration de messagerie à l'aide d'OAuth 2.0, vérifiez que la permission Mail.Send est configurée pour l'application dans Azure Active Directory.

Pour ajouter la permission Mail.Send :

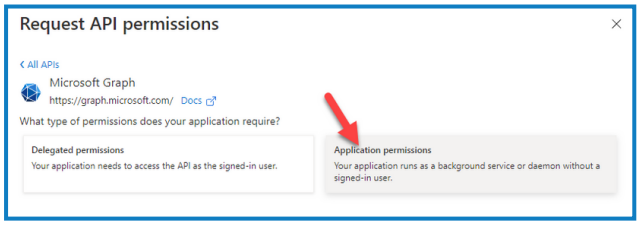
1. Dans Azure Active Directory, ouvrez les propriétés d'application pour l'application à laquelle vous associez Hub.
2. Cliquez sur **Permissions de l'API**.
3. Cliquez sur **Ajouter une permission**.



4. Dans Sélectionner une API, choisissez **Microsoft Graph** sous API Microsoft.

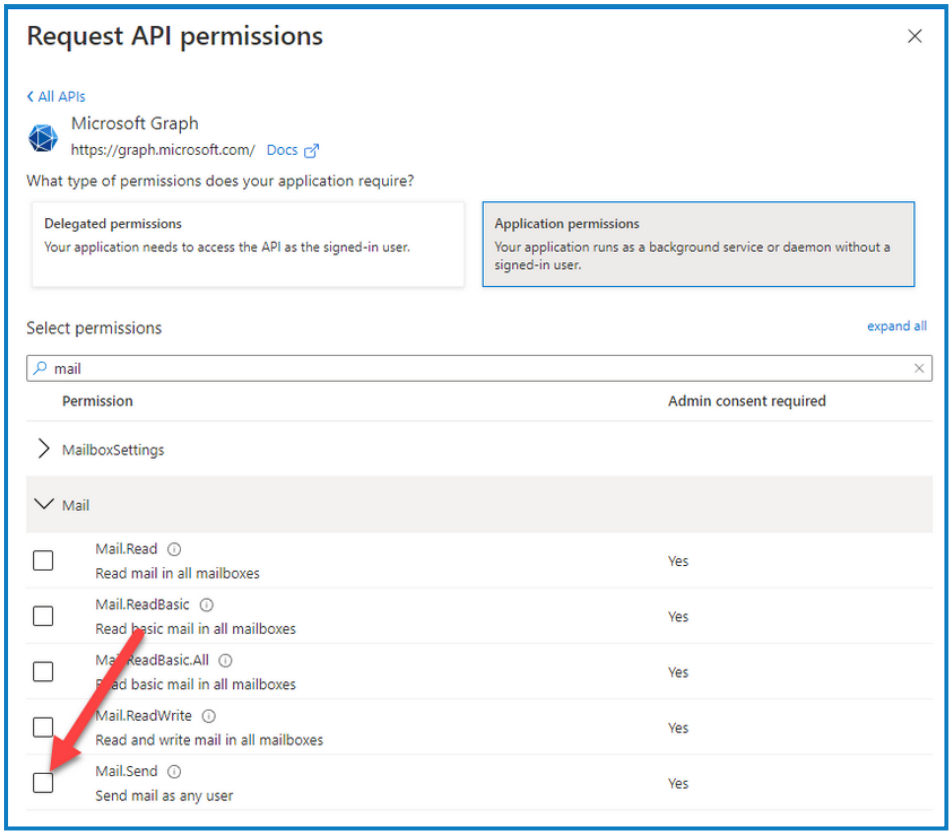


5. Sous Microsoft Graph, cliquez sur **Permissions de l'application**.

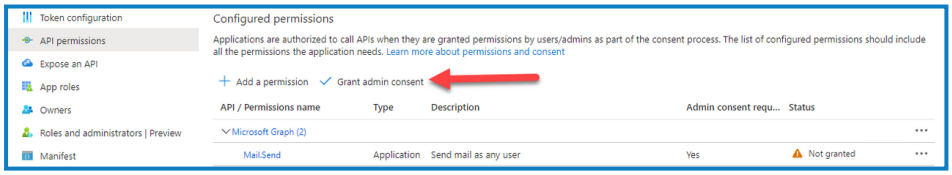


6. Saisissez *E-mail* dans le champ de recherche et appuyez sur Entrée.

7. Sous la liste de diffusion qui s'affiche, sélectionnez **Mail.Send** et cliquez sur **Ajouter des permissions**.



8. Sur la page des permissions de l'application, cliquez sur **Accorder le consentement de l'administrateur**.



Mise à jour de l'ID client après l'installation

Si vous devez saisir ou mettre à jour votre ID client après l'installation, vous devrez mettre à jour le fichier de configuration License Manager appsettings.json. Une fois que le fichier de configuration a été mis à jour, License Manager doit être redémarré dans le gestionnaire d'Internet Information Services (IIS).

Pour mettre à jour votre ID client dans le fichier appsetting.json :

1. Ouvrez l'Explorateur Windows et accédez à `C:\Program Files (x86)\Blue Prism\LicenseManager\appsettings.json`.

   Il s'agit de l'emplacement d'installation par défaut. Ajustez-le si vous avez utilisé un emplacement personnalisé.

2. Ouvrez le fichier appsettings.json dans un éditeur de texte.

3. Localisez la section `Licence:CustomerId` du fichier et saisissez votre nouvel ID client, par exemple :

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

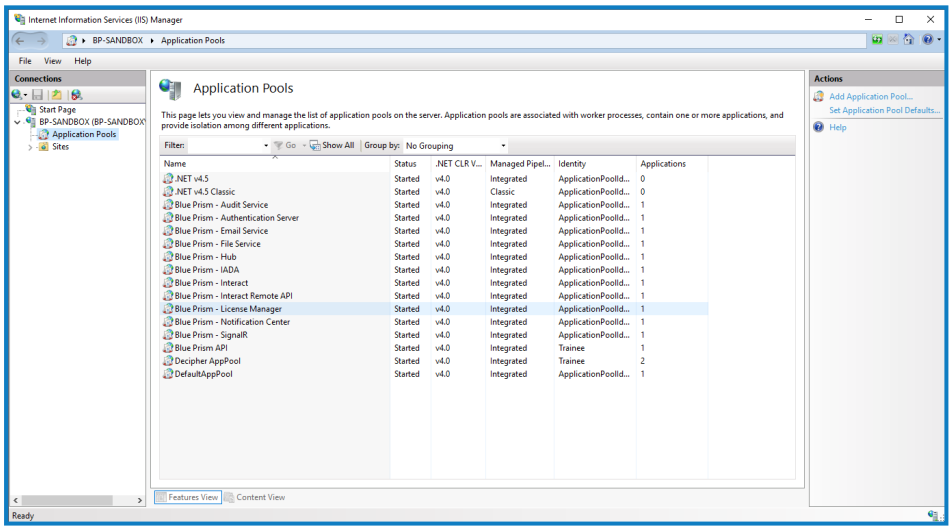
4. Enregistrez le fichier.

Pour redémarrer License Manager :

1. Ouvrez le gestionnaire d'Internet Information Services (IIS).
2. Dans la liste des connexions, sélectionnez **Blue Prism - License Manager**.

> Il s'agit du nom de site par défaut ; si vous avez utilisé un nom de site personnalisé, sélectionnez la connexion appropriée.

3. Cliquez sur **Redémarrer** dans les commandes de la fonctionnalité Gérer le site Web.



License Manager redémarre.

Désinstaller Interact

Vous devez être un administrateur système pour désinstaller Blue Prism Interact.

Pour désinstaller complètement Interact 4.7, vous devez :

1. Arrêter les pools d'applications à l'aide d'IIS.
2. Supprimer Interact à l'aide de l'application Programmes et fonctionnalités.
3. Supprimer les bases de données.
4. Supprimer les données RabbitMQ.
5. Supprimer les certificats.
6. Supprimer les fichiers restants.

Arrêter les pools d'applications à l'aide d'IIS

1. Ouvrez le gestionnaire d'Internet Information Services (IIS). Pour ce faire, tapez *IIS* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gestionnaire d'Internet Information Services (IIS)**.
2. Dans le volet **Connexions**, cliquez sur **Pools d'applications**.
3. Arrêtez tous les pools d'applications associés aux sites Blue Prism. Pour ce faire, sélectionnez chacun d'eux tour à tour et cliquez sur **Arrêter**. Pour obtenir une liste, voir Sites Web Interact sur la page 15.

Supprimer Interact à l'aide de Programmes et fonctionnalités

1. Ouvrir le Panneau de configuration. Pour ce faire, tapez *panneau de configuration* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Panneau de configuration**.
2. Cliquez sur **Programmes**, puis sur **Programmes et fonctionnalités**.
3. Sélectionnez Blue Prism Interact.
4. Cliquez sur **Désinstaller**.
5. Confirmez que vous souhaitez poursuivre la désinstallation.

Supprimer les bases de données

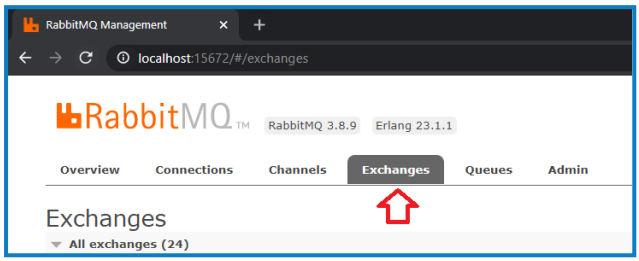
Vous devez uniquement supprimer les bases de données pour les systèmes de test. Si vous envisagez de supprimer une base de données pour un système qui était en production, vous devez déterminer si les données doivent être archivées par votre organisation ou utilisées à des fins d'audit.

> Après la désinstallation d'Interact, s'il est réinstallé ultérieurement en utilisant les mêmes bases de données, celles-ci doivent être effacées de toutes les données avant la réinstallation.

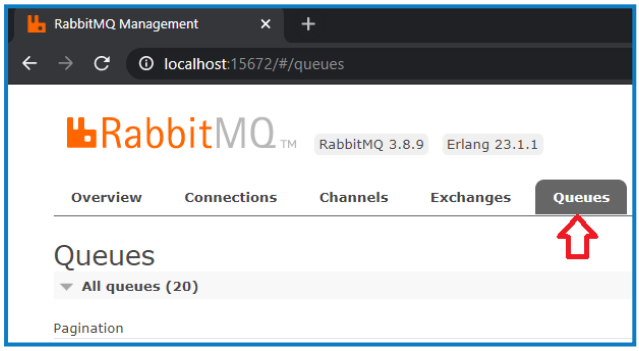
1. Supprimez, ou archivez, la base de données pour l'application Interact.

Supprimer les données RabbitMQ

1. Ouvrez la page d'administration RabbitMQ. Par défaut, l'URL est http://localhost:15672/ sur la machine locale.
2. Cliquez sur **Échanges**.



3. Trouvez et supprimez les éléments suivants :
   - bpc.interact.*
4. Cliquez sur **Files d'attente**.



5. Trouvez et supprimez les éléments suivants :
   - bpc.interact.*

Supprimer les certificats

Ces certificats sont également utilisés par Hub. Si Interact et Hub sont installés sur le même serveur, ignorez cette section et supprimez-les lorsque vous désinstallez Hub. Pour plus d'informations, consultez le guide d'installation de Hub.

1. Ouvrez le Gestionnaire de certificats. Pour ce faire, saisissez *Certificats* dans la zone de recherche de la barre des tâches Windows, puis cliquez sur **Gérer les certificats informatiques**.
2. Dans le volet de navigation, développez **Certification racine de confiance** et cliquez sur **Certificats**.
3. Sélectionnez et supprimez tous les certificats créés pour les sites Blue Prism, ainsi que :
   - BluePrismCloud_Data_Protection
   - BluePrismCloud_IMS_JWT

Supprimer les fichiers restants

1. Dans l'Explorateur Windows, ouvrez le dossier parent pour l'installation Interact. Par défaut, il s'agit du dossier `C:\Program Files (x86)\Blue Prism`, mais il a peut-être été modifié pendant l'installation d'Interact.

2. Supprimez les dossiers et fichiers suivants :
    - IADA
    - Interact
    - Interact Remote API
    - Submit Form Manager