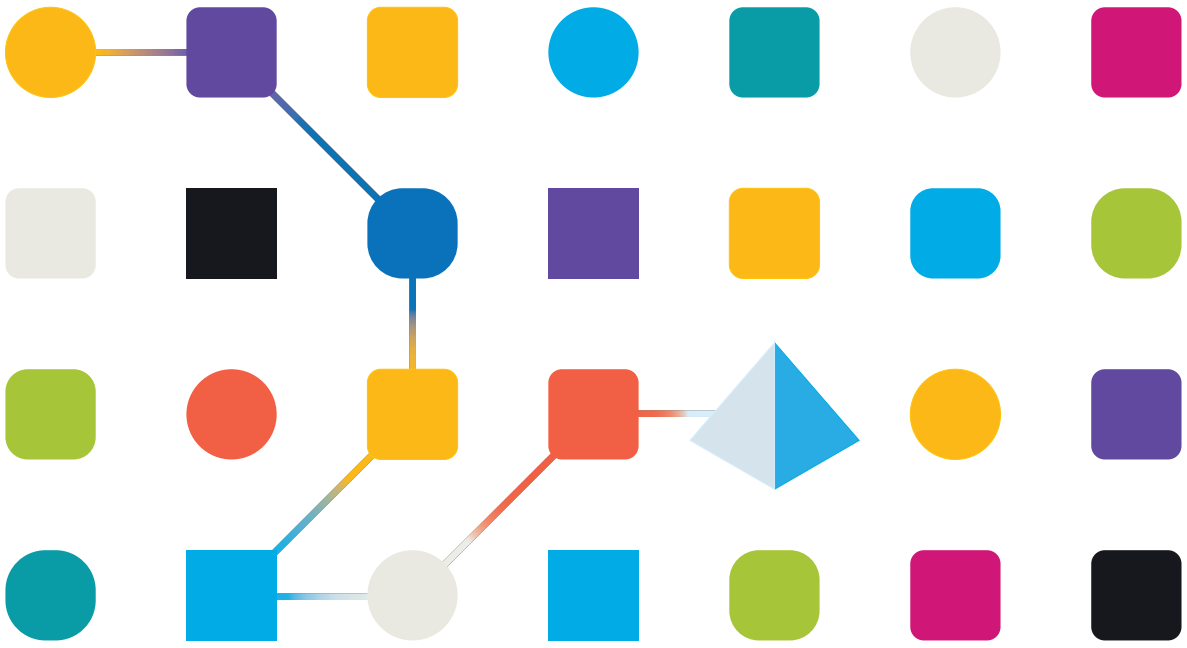
blueprism®

Decision 4.5

Guide d'installation

Révision des documents : 4.0



Marques déposées et droits d'auteur

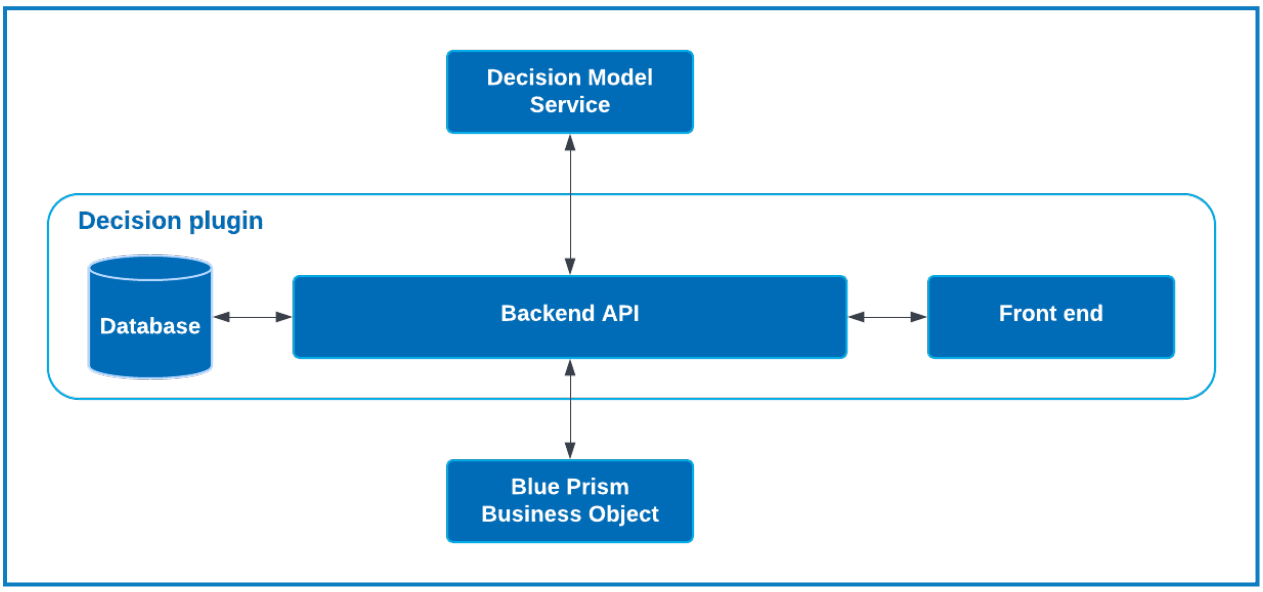
Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Enregistré en Angleterre : numéro d'enregistrement 4260035. Tél. : +44 370 879 3000. Web : www.blueprism.com

Contenu

Installer Blue Prism Decision

Blue Prism® Decision est un plug-in contrôlé par licence qui est installé avec Blue Prism® Hub, à l'aide de l'assistant d'installation de Blue Prism Hub. Decision a un prérequis et une dépendance sur un composant supplémentaire, Blue Prism Decision Model Service, qui est distribué sous la forme d'une image de conteneur.

Le diagramme ci-dessous illustre l'architecture logique de Decision, montrant l'interaction entre le plug-in frontend, Decision Model Service et le client interactif Blue Prism (l'objet métier Blue Prism dans le diagramme).



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.

Blue Prism recommande que Decision soit installé uniquement si vous avez une compréhension mature des stratégies informatiques à propos de l'infrastructure de conteneur Docker, car cette version dépend de l'installation de Hub et d'un conteneur Docker. La prochaine version en 2022 sera également disponible via un MSI.

Vue d'ensemble de l'installation

Pour installer Blue Prism Decision, vous devez :

1. Générer un certificat SSL pour Decision.

   Prérequis de l'étape :

   - Cette section comprend des informations sur l'utilisation des certificats autosignés pour les environnements de preuve de concept (POC), de preuve de valeur (POV) et de développement (Dev). Les scripts fournis nécessitent OpenSSL.

     ⚠ Les certificats autosignés ne doivent pas être utilisés pour les environnements de production.

2. Installer le conteneur de Blue Prism Decision Model Service : il contient l'API d'apprentissage pour modèle utilisée par Decision.

   Conditions préalables à l'étape :

   - Hôte Docker capable d'exécuter des conteneurs Linux.
   - 500 Mo d'espace disque pour le conteneur.

   Voir Prérequis sur la page 11 pour en savoir plus.

3. Installer Blue Prism Hub : vous devez fournir l'URL de l'API d'apprentissage pour modèle et les détails du certificat SSL dans l'assistant d'installation de Blue Prism Hub.

   Prérequis de l'étape :

   - Pour les prérequis de Hub, consultez le guide d'installation de Blue Prism Hub.
   - Certificat SSL de Decision.
   - URL et numéro de port de l'API d'apprentissage pour modèle.

   Si vous avez déjà installé Hub 4.5, consultez Dépannage sur la page 19 pour plus d'informations sur la mise à jour de votre installation.

4. Installer le plug-in Decision dans Hub

   Prérequis de l'étape :

   - Accès administrateur à Hub.
   - Fichier de licence de Decision.

5. Configurer l'accès au plug-in Decision : affectez des utilisateurs à un rôle donnant accès à Decision.

   Prérequis de l'étape :

   - Accès administrateur à Hub.
   - Liste des utilisateurs qui ont besoin d'accéder à Decision.

6. Configurer Blue Prism pour utiliser Decision

   Prérequis de l'étape :

   - Accès administrateur à Hub.
   - Blue Prism 6.4.0 ou versions ultérieures, avec des privilèges suffisants pour configurer les identifiants et les objets dans l'onglet Système.
   - Fichier API.bprelease de Blue Prism Decision.

Configuration de l'environnement de Decision

Les informations ci-dessous fournissent un aperçu simple des configurations d'environnement pour Blue Prism® Decision.

Blue Prism® Hub requiert Windows Server 2016 ou 2019.

Machine unique – Environnements de preuve de concept ou d'essai

Les petits environnements de preuve de concept (POC) ou d'essai peuvent être configurés sur une machine unique. Les installations à machine unique ne sont pas adaptées aux environnements de production.

Composant	Windows Server (Windows Server 2016 ou 2019)	Machine Linux
Hub	✓	Indisponible
Docker Desktop	✓	Indisponible
Docker Engine	✗	Indisponible

Machines multiples – Environnements de production

Les environnements de production sont généralement configurés sur plusieurs machines, le serveur Web étant sur une machine différente de celle des autres systèmes dorsaux. Plusieurs configurations de machine peuvent également être utilisées pour les environnements POC, si nécessaire. Les configurations pouvant être utilisées pour Decision sont les suivantes :

Infrastructure Microsoft

Si vous utilisez uniquement des serveurs Windows Server, la configuration sera :

Composant	Windows Server (Windows Server 2016 ou 2019)	Machine Linux
Hub	✓	Indisponible
Docker Desktop	✓	✗
Docker Engine	✗	✗

Infrastructure combinée

Si votre organisation exécute une infrastructure combinée, avec des serveurs Windows Server et des machines Linux, votre organisation peut utiliser :

Composant	Windows Server (Windows Server 2016 ou 2019)	Machine Linux
Hub	✓	Indisponible
Docker Desktop	✗	✗
Docker Engine	✗	✓

Générer un certificat SSL

Vous avez besoin d'un certificat SSL pour le conteneur de Blue Prism Decision. 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.

> Le conteneur de Blue Prism Decision nécessite une clé client et une clé serveur pour s'assurer que la communication entre le plug-in Decision dans Hub et le conteneur Decision est sécurisée.

Les certificats autosignés peuvent être utilisés, mais ne sont recommandés que pour les environnements POC\POV\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. Vous devrez vous assurer que votre autorité du certificat fournit les fichiers suivants :

- server.crt
- server.key
- ca.crt
- client.crt

Certificat autosigné

Pour les environnements POC\POV\Dev, vous pouvez créer un certificat à l'aide du processus suivant. Ce processus nécessite l'installation d'OpenSSL. Ces instructions concernent un serveur Windows Server. Si vous utilisez Linux, veuillez faire les ajustements nécessaires.

> Consultez la version en ligne de ce guide pour vérifier le formatage et les sauts de ligne dans les scripts utilisés dans les étapes ci-dessous.

1. Si vous ne l'avez pas déjà, installez OpenSSL.
2. Créez un dossier dans lequel vous exécuterez le script (à l'étape suivante) afin que la sortie soit générée à un seul endroit.
3. Dans le dossier que vous avez créé, utilisez l'un des scripts suivants en fonction du système d'exploitation hôte (Windows ou Linux), en saisissant les valeurs appropriées indiquées dans les variables en haut du script :

   `Saisir le mot de passe du certificat` : remplacer par un mot de passe qui sera utilisé pour créer le certificat.

   `Saisir CN pour le certificat client` : remplacer par un nom commun pour le certificat client, par exemple, client.decision.blueprism.com.

   `Saisir CA` : remplacer par le nom commun de l'autorité du certificat, par exemple, decisionCA.

   `Saisir CN pour le certificat de serveur` : remplacer par un nom commun pour le certificat de serveur. Il doit correspondre au nom de domaine explicite (FQDN) du conteneur Decision, par exemple, decision.blueprism.com. Ou, si le conteneur se trouve sur le même serveur que Hub, utilisez, par exemple, decision.local.

Script pour la création de certificats dans Windows

Exécutez PowerShell en tant qu'administrateur et utilisez le script suivant :

```
$cred = Get-Credential -UserName 'Enter certificate password' -Message 'Enter certificate password'
$mypwd = $cred.GetNetworkCredential().password
$clientCN = Read-Host "Enter CN for client certificate"
$CA = Read-Host "Enter CA"
$serverCN = Read-Host "Enter CN for server certificate"

echo Generate CA key:
openssl genrsa -passout pass:$mypwd -des3 -out ca.key 4096

echo Generate CA certificate:
$CASubject = "/CN=" + $CA
openssl req -passin pass:$mypwd -new -x509 -days 365 -key ca.key -out ca.crt -subj $CASubject

echo Generate server key:
openssl genrsa -passout pass:$mypwd -des3 -out server.key 4096

echo Generate server signing request:
$serverSubject = "/CN=" + $serverCN
openssl req -passin pass:$mypwd -new -key server.key -out server.csr -subj $serverSubject

echo Self-sign server certificate:
openssl x509 -req -passin pass:$mypwd -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt

echo Remove passphrase from server key:
openssl rsa -passin pass:$mypwd -in server.key -out server.key

echo Generate client key
openssl genrsa -passout pass:$mypwd -des3 -out client.key 4096

echo Generate client signing request:
$clientSubject = "/CN=" + $clientCN
openssl req -passin pass:$mypwd -new -key client.key -out client.csr -subj $clientSubject

echo Self-sign client certificate:
openssl x509 -passin pass:$mypwd -req -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out client.crt

echo Remove passphrase from client key:
openssl rsa -passin pass:$mypwd -in client.key -out client.key

echo Generate pfx from client key:
openssl pkcs12 -export -password pass:$mypwd -out client.pfx -inkey client.key -in client.crt
```

Les certificats sont générés dans le dossier que vous avez créé.

Script pour la création de certificats dans Linux

Exécutez le script Bash suivant :

```
#!/bin/sh

read -s -p 'Enter certificate password: ';
CER_PWD=${REPLY};
echo "";

read -p 'Enter CN for client certificate: ';
CLIENT_CN=${REPLY};
#echo "";

read -p 'Enter CA: ';
CA=${REPLY};
#echo "";

read -p 'Enter CN for server certificate: ';
SERVER_CN=${REPLY};
#echo "";

unset REPLY;

echo Generate CA key:
openssl genrsa -passout pass:$CER_PWD -des3 -out ca.key 4096

echo Generate CA certificate:
CA_SUBJECT="/CN=${CA}"
openssl req -passin pass:$CER_PWD -new -x509 -days 365 -key ca.key -out ca.crt -subj $CA_SUBJECT

echo Generate server key:
openssl genrsa -passout pass:$CER_PWD -des3 -out server.key 4096

echo Generate server signing request:
SERVER_SUBJECT="/CN=${SERVER_CN}"
openssl req -passin pass:$CER_PWD -new -key server.key -out server.csr -subj $SERVER_SUBJECT

echo Self-sign server certificate:
openssl x509 -req -passin pass:$CER_PWD -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out
server.crt

echo Remove passphrase from server key:
openssl rsa -passin pass:$CER_PWD -in server.key -out server.key

echo Generate client key
openssl genrsa -passout pass:$CER_PWD -des3 -out client.key 4096

echo Generate client signing request:
CLIENT_SUBJECT="/CN=${CLIENT_CN}"
openssl req -passin pass:$CER_PWD -new -key client.key -out client.csr -subj $CLIENT_SUBJECT

echo Self-sign client certificate:
openssl x509 -passin pass:$CER_PWD -req -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out
client.crt

echo Remove passphrase from client key:
openssl rsa -passin pass:$CER_PWD -in client.key -out client.key

echo Generate pfx from client key:
openssl pkcs12 -export -password pass:$CER_PWD -out client.pfx -inkey client.key -in client.crt
```

Les certificats sont générés dans le dossier que vous avez créé.

4. Ajoutez le certificat en tant que certificat de confiance sur la machine locale en exécutant les scripts suivants :

```
$scriptPath = (Get-Item .).FullName
$crt = "$($scriptPath)\client.pfx"
$mypwd = Get-Credential -UserName 'Enter password' -Message 'Enter password'
Import-PfxCertificate -FilePath $crt -CertStoreLocation Cert:\LocalMachine\My -Password $mypwd.Password
```

```
$scriptPath = (Get-Item .).FullName
$crt = "$($scriptPath)\ca.crt"
Import-Certificate -FilePath $crt -CertStoreLocation Cert:\LocalMachine\Root
```

5. Accorder aux utilisateurs IIS l'accès au certificat client :
   a. Ouvrez Gérer les certificats informatiques et localisez le certificat client.
   b. Cliquez avec le bouton droit de la souris sur le certificat, sélectionnez **Toutes les tâches**, puis **Gérer les clés privées...**.
   c. Ajoutez **IIS_IUSRS** avec la permission **Lecture**.
   d. Cliquez sur **Appliquer**.

Si vous utilisez différentes machines pour héberger le conteneur de Blue Prism Decision Model Service et Blue Prism Hub, vous devrez vous assurer que :

- L'hôte du conteneur de Decision Model Service comporte les fichiers suivants :
  - server.crt
  - server.key
  - ca.crt
- Le serveur exécutant Blue Prism Hub possède les fichiers suivants :
  - client.crt
  - ca.crt

Installer le conteneur de Blue Prism Decision Model Service

Le conteneur de Blue Prism Decision Model Service inclut l'API d'apprentissage du modèle qui est utilisée par le plug-in Decision. Ce conteneur doit être déployé et en cours d'exécution avant l'installation de Hub, car vous devrez saisir les détails dans l'assistant d'installation.

Pour voir le processus d'installation de Decision Model Service à l'aide du conteneur, regardez notre vidéo d'installation de Blue Prism Decision Model Service.

Prérequis

- Un hôte Docker est requis, capable d'exécuter des conteneurs Linux.
  - Blue Prism recommande que votre environnement de production utilise un serveur Linux comme hôte. Docker Engine est requis pour exécuter le conteneur de Decision Model Service. Pour plus d'informations, consultez l'aide de Docker : Installer Docker Engine.
  - Pour les environnements POC ou Dev, un serveur Windows peut être utilisé. Docker Desktop est requis pour exécuter le conteneur de Decision Model Service. Pour plus d'informations, consultez l'aide de Docker : Installer Docker Desktop sur Windows.
- 500 Mo d'espace disque pour le conteneur.

Étapes d'installation

1. Ouvrez la page du conteneur de Decision Model Service sur DockerHub.
2. Copiez la commande pull à partir de la page du conteneur et exécutez-la dans la ligne de commande. Par exemple :

   ```
   docker pull blueprism/decision-model-service:<version>
   ```

   Où `<version>` correspond au numéro de version affiché dans l'onglet Balises sur DockerHub.
3. Définissez le conteneur en cours d'exécution à l'aide de la commande suivante :

   La commande doit être sur une seule ligne. Voir la version en ligne de ce guide.

   ```
   docker run -d -v "<Absolute path of certificate location>:/certs" -e server_key="/certs/server.key" -e server_
   cert="/certs/server.crt" -e ca_cert="/certs/ca.crt" --restart always -p 50051:50051 blueprism/decision-model-
   service:<version>
   ```

   Où :

   `<Absolute path of certificate location>` est remplacé par le chemin d'accès complet du certificat créé dans Générer un certificat SSL sur la page 7.

   `<version>` est remplacé par le numéro de version du conteneur de Decision Model Service.
4. Vérifiez que le conteneur est en cours d'exécution à l'aide de la commande suivante :

   ```
   docker ps -a
   ```

Installer Blue Prism Hub

Vous pouvez maintenant exécuter l'assistant d'installation de Hub. Voir Installer Blue Prism Hub. Sur l'écran Configuration de Blue Prism Decision (facultatif), saisissez l'URL de l'emplacement d'exécution du conteneur de Decision, suivi du numéro de port. L'URL doit correspondre au nom de domaine explicite (FQDN) spécifié dans le certificat et pointer vers le conteneur de Model Service. Le numéro de port doit correspondre à celui spécifié lorsque le conteneur a été défini pour s'exécuter.

L'URL doit être au format https://<FQDN>:<port number>.
Par exemple, https://decision.blueprism.com:50051 ou http://decision.local:50051.

> Si vous avez déjà installé Hub 4.5 sans Decision, consultez Dépannage sur la page 19 pour plus d'informations sur la mise à jour de votre installation.

Configuration obligatoire

Une fois Hub installé, vous devez également effectuer la configuration suivante sur le serveur.

Résolution DNS de Decision

Les applications Blue Prism communiquent entre elles à l'aide de leurs noms de machine respectifs. Il faut donc s'assurer qu'elles fonctionnent et que les règles de pare-feu permettent une communication appropriée sur les ports définis.

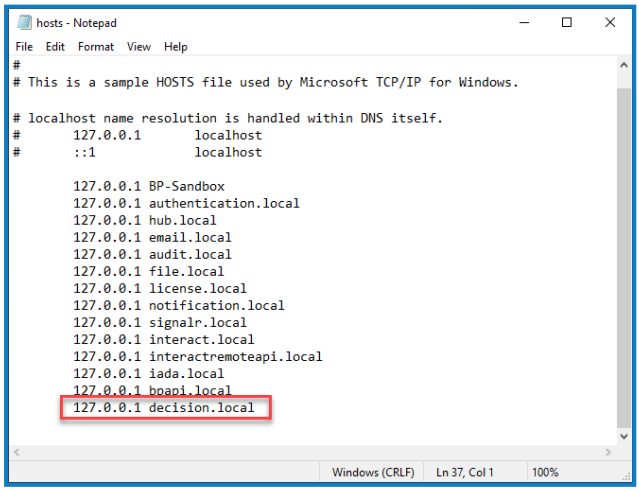
Il peut être nécessaire de configurer des serveurs DNS, des suffixes de recherche DNS Windows ou un fichier d'hôtes local pour la prise en charge.

Les organisations d'entreprise utilisent souvent des utilitaires de gestion DNS officiels, cependant pour des configurations tactiques ou expérimentales, il convient d'utiliser des fichiers d'hôtes locaux pour manipuler le DNS.

1. Sur le serveur Web Hub, ouvrez le fichier d'hôtes à l'aide d'un éditeur de texte. Le fichier d'hôtes se trouve généralement dans C:\Windows\System32\drivers\etc.

   > Vous devez être connecté avec un accès de niveau administrateur pour modifier ce fichier.

2. Saisissez l'adresse IP et le nom d'hôte de Decision à la fin de la liste, par exemple :



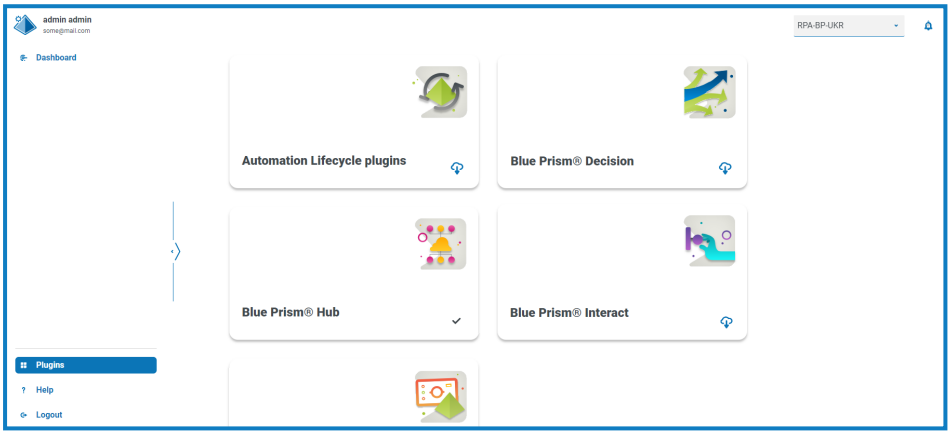
3. Enregistrez et quittez l'éditeur de texte.

Installer le plug-in Decision

Le plug-in Decision doit être installé à partir du référentiel de plug-ins par un administrateur Hub.

Pour voir le processus d'installation et de configuration du plug-in Decision, regardez notre vidéo relative au plug-in Blue Prism Decision.

1. Si vous êtes un administrateur Hub, connectez-vous à Hub et cliquez sur **Plug-ins** pour ouvrir le référentiel de plug-ins.



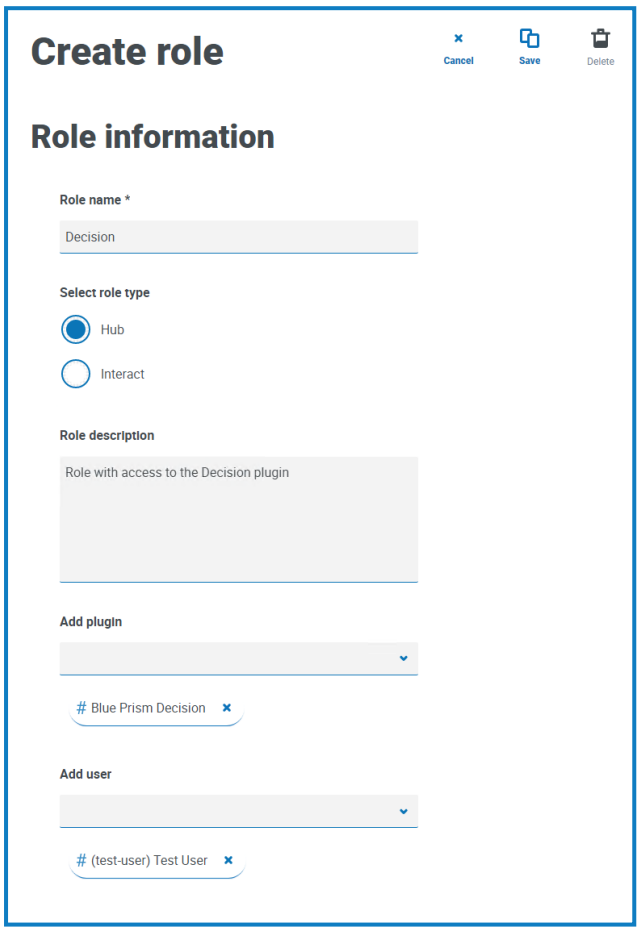
2. Sur la dalle **Blue Prism Decision**, cliquez sur l'icône de téléchargement pour lancer l'installation.
3. Lorsque vous y êtes invité, chargez le fichier de licence pour Decision.

   Le plug-in s'installe et un message s'affiche pour vous informer que le site redémarre. Une fois terminé, le référentiel de plug-ins s'affiche et l'icône de téléchargement sur la dalle de **Blue Prism Decision** est remplacée par une coche.

   Le redémarrage du site affectera tous les utilisateurs connectés à Hub. Bien que cela ne prenne pas longtemps, il est recommandé d'effectuer cette opération en dehors des heures normales de travail pour minimiser les perturbations.

Configurer l'accès au plug-in Decision

Le plug-in Decision est automatiquement disponible pour les administrateurs Hub. Les utilisateurs doivent être ajoutés à un rôle qui donne accès à Decision. Cet accès peut être donné via un nouveau rôle ou ajouté à un rôle d'utilisateur existant. Si un rôle n'existe pas déjà, un nouveau rôle peut être créé pour accorder l'accès au plug-in :



1. Sur la page Rôles et permissions, cliquez sur **Créer un rôle**.

   La section Créer un rôle s'affiche.
2. Saisissez un nom de rôle et sélectionnez **Hub**.
3. Si nécessaire, saisissez une description.
4. Sélectionnez **Blue Prism Decision** dans la liste déroulante **Ajouter un plug-in**.
5. Sélectionnez les utilisateurs auxquels ce rôle sera attribué dans la liste déroulante **Ajouter un utilisateur**. La liste affiche uniquement les utilisateurs Hub et non les utilisateurs Interact.
6. Cliquez sur **Enregistrer** pour créer le rôle et autoriser l'accès aux utilisateurs spécifiés.

Les utilisateurs peuvent être ajoutés aux rôles existants, et supprimés de ceux-ci, en sélectionnant le rôle requis sur la page Rôles et permissions et en cliquant sur **Modifier**. Pour plus d'informations, consultez le guide de l'utilisateur Hub.

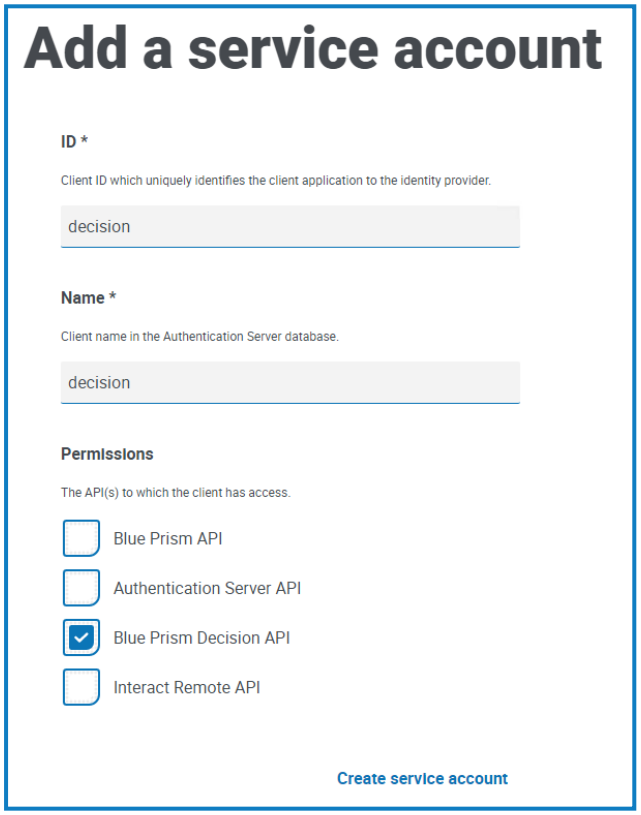
Configurer Blue Prism pour utiliser Decision

Pour configurer Blue Prism pour utiliser vos modèles Decision, vous devez :

1. Configurer un compte de service dans Hub et générer une clé secrète.
2. Configurer les identifiants pour le compte de service Decision dans Blue Prism.
3. Importer le VBO de publication de Blue Prism Decision API pour communiquer avec Decision.

Configurer un compte de service

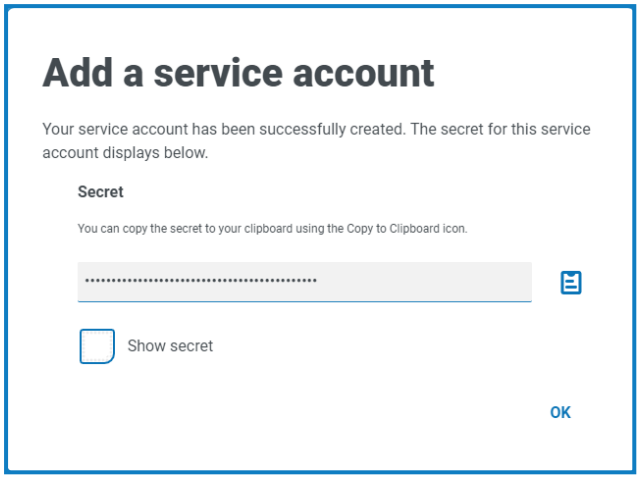
1. Dans Blue Prism Hub, sur la page Comptes de service, cliquez sur **Ajouter un compte**.
2. Saisissez un ID unique et un nom convivial, par exemple, *Decision*.
3. Sous **Permissions**, sélectionnez **Blue Prism Decision API**.



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 le secret généré dans votre presse-papiers afin de le coller dans le client interactif Blue Prism.



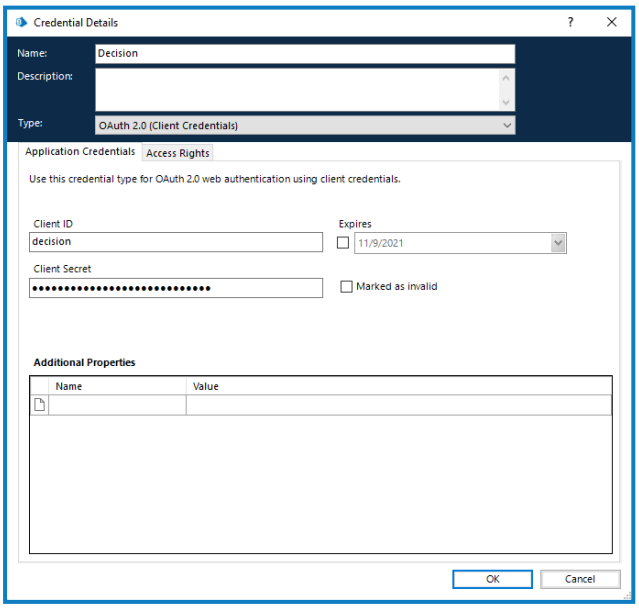
6. Cliquez sur **OK** pour fermer la boîte de dialogue.

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

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 un compte de service sur la page précédente.
   d. Dans **Secret client** : saisissez la clé secrète générée pour le compte de service.



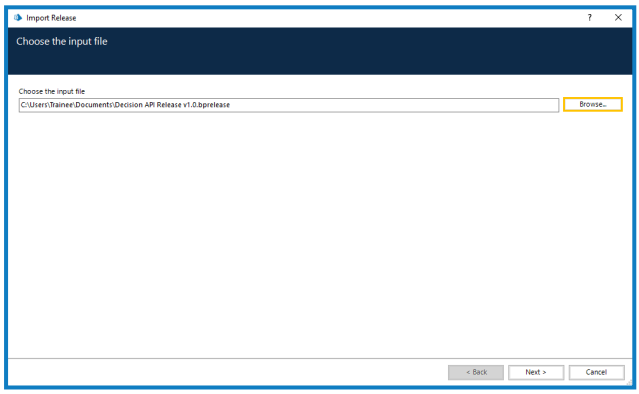
4. Dans l'onglet Droits d'accès de la boîte de dialogue Détails des identifiants, définissez les permissions d'accès requises.
5. Cliquez sur **OK**.

Importer le VBO de publication de Blue Prism Decision API

1. Si vous ne l'avez pas déjà fait, téléchargez le fichier API.bprelease de Decision à partir du portail Blue Prism.
2. Dans Blue Prism, sélectionnez **Fichier** et cliquez sur **Importer** > **Version / Compétence**.

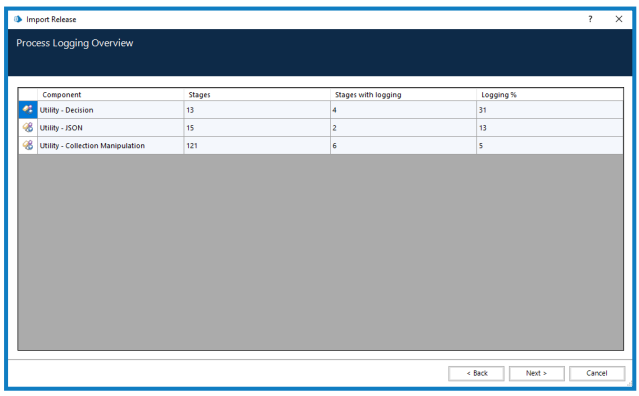
   La boîte de dialogue Importer la version s'affiche.
3. Cliquez sur **Parcourir**.
4. Recherchez et sélectionnez le fichier API.bprelease de Decision.

   Par exemple :



5. Cliquez sur **Suivant**.

   L'écran Aperçu du logging du processus s'affiche avec un résumé des composants qui seront importés.



6. Cliquez sur **Suivant**.

   Un écran de progression s'affiche.
7. Lorsque l'importation est terminée, cliquez sur **Terminer**.
8. Dans Blue Prism, sélectionnez **Système**, puis cliquez sur **Objets** > **Services API Web**.
9. Sélectionnez **DecisionAPI** et cliquez sur **Modifier le service**.

10. Sur l'API Web : Sur l'écran d'ouverture API Web, dans **URL de base**, saisissez l'URL du service API de Decision au format :

    `<Hub host URL>:<port if specified during install>/api/blueprism-decision`

    Par exemple, `https://hub.blueprism.com:5002/api/blueprism-decision`

    Ou, si le port par défaut a été utilisé, `https://hub.blueprism.com/api/blueprism-decision`.

11. 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 :

    `<Authentication Server URL>:<port if specified during install>/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 :
    >
    > `<IMS URL>:<port if specified>/connect/token`
    >
    > Par exemple, `https://ims.blueprism.com:5000/connect/token`.

    c. Dans **Identifiants**, sélectionnez les identifiants que vous avez créés dans Configurer des identifiants dans Blue Prism sur la page 16.

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

Dépannage

Installer Decision dans un environnement Hub existant

Nous n'avons pas ajouté Decision lors de l'installation de Hub/de la mise à niveau de Hub vers 4.5, mais nous voulons maintenant l'utiliser. Comment l'installer ?

Vous devrez suivre les étapes décrites dans Générer un certificat SSL sur la page 7 et Installer le conteneur de Blue Prism Decision Model Service sur la page 11. Vous devez ensuite mettre à jour le fichier appsetting.json de Hub avec les chaînes de connexion de Decision.

⚠ Les informations ci-dessous décrivent la mise à jour du fichier appsettings.json de Hub. Veillez à ne modifier que les informations fournies ; toute autre modification peut endommager votre système existant. Les modifications apportées au fichier appsettings.json doivent être effectuées conjointement avec Blue Prism pour garantir la prise en charge de votre système.

Pour mettre à jour le fichier appsetting.json afin d'inclure Decision :

1. Ouvrez l'Explorateur Windows et accédez à `C:\Program Files (x86)\Blue Prism\Hub\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 suivante du fichier :

```
"BluePrismDecision": {
    ...
    "ConnectionString": "",
    ...
}
```

   Ce n'est pas le seul réglages que vous verrez sous `BluePrismDecision`. Cependant, c'est le seul qui doit être modifié.

4. À l'aide de l'outil de protection des données Blue Prism dans PowerShell, créez et chiffrez la chaîne de connexion pour la base de données Decision, par exemple :

   La commande doit être sur une seule ligne. Voir la version en ligne de ce guide.

   Si vous souhaitez utiliser l'authentification SQL :

   ```
   .\BluePrismDataProtector.Console.exe protect -v "Data Source=[SQL Server];Initial Catalog=BluePrismDecisionDB;User Id=[user name, for example, sqladmin];Password=[password];Max Pool Size=500;MultiSubnetFailover=True;" -p ".\"
   ```

   Si vous souhaitez utiliser l'authentification Windows :

   ```
   .\BluePrismDataProtector.Console.exe protect -v "Data Source=[SQL Server];Initial Catalog=BluePrismDecisionDB;Integrated Security=True;Max Pool Size=500;MultiSubnetFailover=True;" -p ".\"
   ```

   Où vous remplacez :

   `[SQL Server]` = Le serveur SQL Server qui hébergera la base de données.

   `[nom d'utilisateur, par exemple, sqladmin]` = Le nom d'utilisateur SQL (authentification SQL uniquement)

   `[mot de passe]` = Le mot de passe de l'utilisateur SQL (authentification SQL uniquement)

   Si nécessaire, vous pouvez saisir un nom de base de données différent pour le paramètre `Catalogue initial`. `BluePrismDecisionDB` est le nom par défaut.

   Les réglages ci-dessus sont équivalents aux valeurs que vous saisiriez sur l'écran Configurer la connexion SQL de Blue Prism Decision dans l'assistant d'installation de hub.

   La base de données Decision sera créée lorsque vous installerez le plug-in Decision dans Hub.

5. Copiez la chaîne cryptée entre les `""` à côté du réglage `ConnectionString` dans le fichier appsettings.json de Hub, illustré à l'étape 3.
6. Enregistrez le fichier.
7. Recherchez la section suivante dans ce même fichier appsettings.json :

   ```
   "BluePrismDecisionSettings": {
       "Certificate": {
           "CertificateThumbprint": ""
       },
       "DruidModelServices": {
           "v1": ""
       }
   }
   ```

8. Saisissez l'empreinte du certificat SSL entre les `""` à côté du réglage `CertificateThumbprint`.

   Si vous utilisez Windows, vous pouvez la trouver à l'aide de la fonctionnalité Gérer les certificats informatiques : double-cliquez sur le certificat, l'**empreinte** se trouve dans l'onglet Détails.

9. Saisissez l'URL du conteneur de Blue Prism Decision Model Service entre les `""` à côté du réglage `v1`.
10. Enregistrez et fermez le fichier.

11. Redémarrez Hub :
    a. Ouvrez le gestionnaire d'Internet Information Services (IIS).
    b. Dans la liste des connexions, sélectionnez **Blue Prism - Hub**.

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

    c. Cliquez sur **Redémarrer** dans les commandes de la fonctionnalité Gérer le site Web.
12. Ajoutez Decision au fichier d'hôtes. Voir Résolution DNS de Decision sur la page 12 pour en savoir plus.

Les étapes suivantes consistent à terminer l'Installer le plug-in Decision sur la page 13 et la Configurer l'accès au plug-in Decision sur la page 14. Toutefois, avant d'installer le plug-in, vous devrez fournir temporairement des permissions dbcreator ou sysadmin SQL Server à la connexion utilisée pour le pool d'applications Blue Prism – Hub. Cette connexion dépendra de l'option sélectionnée lorsque vous avez installé Hub :

- Authentification SQL Server : l'utilisateur SQL spécifié pendant l'installation.
- Authentification Windows : le compte de service Windows associé au pool d'applications Blue Prism – Hub.

La base de données Decision est créée lorsque le plug-in Decision est installé dans Hub. Après cela, les permissions dbcreator ou sysadmin peuvent être supprimées.

Échec du script OpenSSL

Si le script OpenSSL échoue, ajoutez OpenSSL à la variable environnementale Path, puis réessayez d'exécuter le script.

1. Dans la barre des tâches Windows, ouvrez le Panneau de configuration.
2. Sélectionnez **Système et sécurité**, puis **Système**, puis cliquez sur **Paramètres système avancés**.

   La boîte de dialogue Propriétés système s'affiche.
3. Cliquez sur **Variables d'environnement**.

   La boîte de dialogue Variables d'environnement s'affiche.
4. Dans le groupe **Variables système,** sélectionnez **Path**, puis cliquez sur **Modifier**.

   La boîte de dialogue Modifier la variable d'environnement s'affiche.
5. Cliquez sur **Nouveau** et sur la nouvelle ligne, saisissez le chemin d'accès à OpenSSL. L'emplacement par défaut est C:\Program Files\OpenSSL-Win64\bin.
6. Cliquez sur **OK** pour enregistrer les modifications.