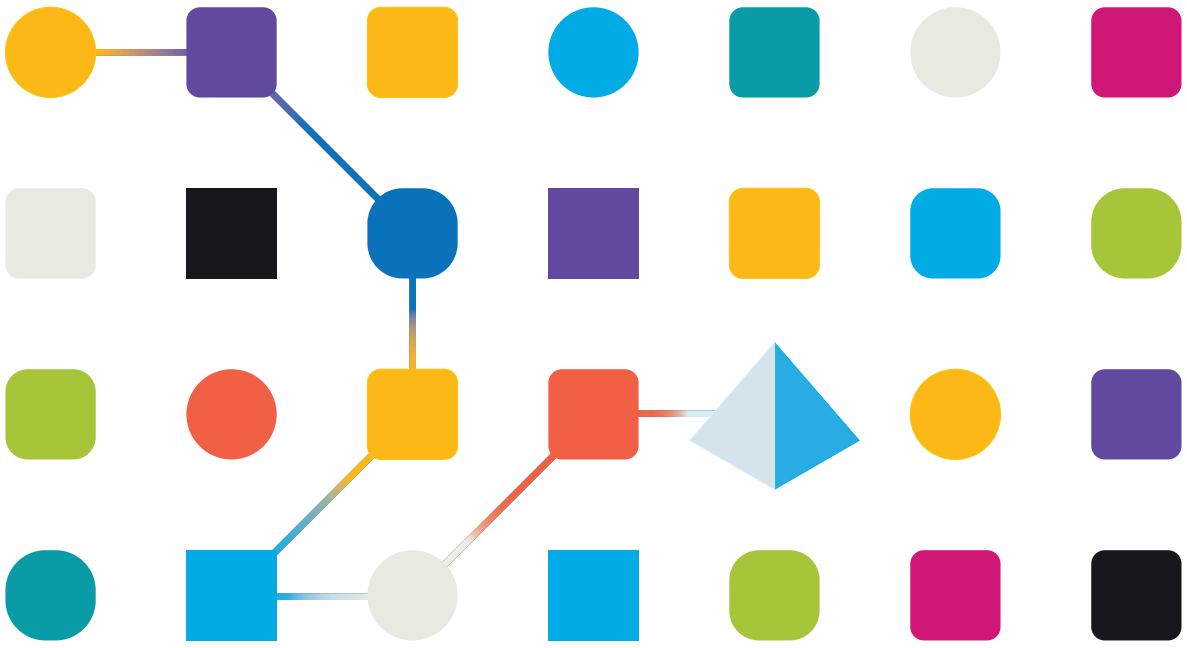
blueprism®

Decision 4.5

Installationshandbuch

Dokumentrevision: 1.0



Marken- und Urheberrechtshinweise

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

Inhalt

Blue Prism Decision installieren

Blue Prism® Decision ist ein lizenzbasiertes Plug-in, das unter Verwendung des Blue Prism Hub Installationsprogramms mit Blue Prism® Hub installiert wird. Für Decision gibt es eine Voraussetzung und eine Abhängigkeit – nämlich von einer zusätzlichen Komponente, dem Blue Prism Decision Model Service, der als Container-Image bereitgestellt wird.

Zielgruppe

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

Blue Prism empfiehlt, Decision nur dann zu installieren, wenn Sie umfassende Kenntnisse zu IT-Richtlinien bezüglich der Docker Container Infrastruktur haben, da für diesen Release sowohl Hub als auch ein Docker Container installiert werden müssen. Der nächste Release im Jahr 2022 wird auch über ein MSI verfügbar gemacht.

Überblick über die Installation

Um Blue Prism Decision zu installieren, müssen Sie:

1. Ein SSL-Zertifikat für Decision generieren.

   Voraussetzungen für den Schritt:

   - Dieser Abschnitt enthält Informationen zur Verwendung selbstsignierter Zertifikate für POC- (Proof Of Concept), POV- (Proof Of Value) und Entwicklungsumgebungen. Die bereitgestellten Skripts erfordern OpenSSL.

     ⚠ Selbstsignierte Zertifikate sollten nicht für Produktionsumgebungen verwendet werden.

2. Blue Prism Decision Model Service Container installieren – Darin ist die von Decision verwendete Model Learning API enthalten.

   Schrittvoraussetzungen:

   - Ein Docker-Host, der Linux-Container ausführen kann.
   - 500 MB Speicherplatz für den Container.

   Mehr erfahren Sie unter Voraussetzungen auf Seite12.

3. Blue Prism Hub installieren – Sie müssen die Details zur Model Learning API URL und zum SSL-Zertifikat im Blue Prism Hub Installationsassistenten angeben.

   Voraussetzungen für den Schritt:

   - Die Voraussetzungen für Hub finden Sie im Blue Prism Hub Installationshandbuch.
   - Das SSL-Zertifikat für Decision.
   - Die Model Learning API URL und Portnummer.

   Wenn Sie Hub 4.5 bereits installiert haben, finden Sie unter Fehlerbehebung bei der auf Seite20 Informationen zur Aktualisierung Ihrer Installation.

4. Decision Plug-in in Hub installieren

   Voraussetzungen für den Schritt:

   - Administrator-Zugriff auf Hub.
   - Decision Lizenzdatei.

5. Zugriff auf das Decision Plug-in konfigurieren – Weisen Sie Benutzer einer Rolle zu, die Zugriff auf Decision bietet.

   Voraussetzungen für den Schritt:

   - Administrator-Zugriff auf Hub.
   - Liste der Benutzer, die Zugriff auf Decision benötigen.

6. Blue Prism zur Verwendung von Decision konfigurieren

   Voraussetzungen für den Schritt:

   - Administrator-Zugriff auf Hub.
   - Blue Prism 6.4.0 und höher, mit ausreichenden Berechtigungen zum Konfigurieren von Anmeldedaten und Objekten auf der Registerkarte „System“.
   - Blue Prism Decision API.bprelease-Datei.

Einrichtung der Decision Umgebung

Die folgenden Informationen bieten einen einfachen Überblick über die Umgebungskonfigurationen für Blue Prism® Decision.

Blue Prism® Hub erfordert Windows Server 2016 oder 2019.

Einzelner Computer – Proof-of-Concept- oder Testumgebungen

Kleine Proof-of-Concept- (POC) oder Testumgebungen können auf einem einzigen Computer konfiguriert werden. Installationen mit einem einzigen Computer sind nicht für Produktionsumgebungen geeignet.

Komponente	Windows Server (Windows Server 2016 oder 2019)	Linux-Computer
Hub	✓	n. z.
Docker Desktop	✓	n. z.
Docker Engine	✗	n. z.

Mehrere Computer – Produktionsumgebungen

Produktionsumgebungen werden normalerweise auf mehreren Computern konfiguriert, wobei sich der Webserver auf einem anderen Computer als die anderen Back-End-Systeme befindet. Bei Bedarf können auch mehrere Maschinenkonfigurationen für POC-Umgebungen verwendet werden. Die Konfigurationen, die für Decision verwendet werden können, sind:

Microsoft-Infrastruktur

Wenn Sie nur Windows-Server verwenden, gilt die folgende Konfiguration:

Komponente	Windows Server (Windows Server 2016 oder 2019)	Linux-Computer
Hub	✓	n. z.
Docker Desktop	✓	✗
Docker Engine	✗	✗

Kombinierte Infrastruktur

Wenn Ihr Unternehmen eine kombinierte Infrastruktur mit Windows-Servern und Linux-Computern einsetzt, kann Ihr Unternehmen Folgendes verwenden:

Komponente	Windows Server (Windows Server 2016 oder 2019)	Linux-Computer
Hub	✓	n. z.
Docker Desktop	✗	✗
Docker Engine	✗	✓

SSL-Zertifikat generieren

Sie benötigen ein SSL-Zertifikat für den Blue Prism Decision Container. Je nach den Sicherheitsanforderungen Ihrer Infrastruktur und IT-Organisation kann dies ein intern erstelltes SSL-Zertifikat oder ein erworbenes Zertifikat sein.

> Der Blue Prism Decision Container erfordert einen Clientschlüssel und einen Serverschlüssel, um sicherzustellen, dass die Kommunikation zwischen dem Decision Plug-in von Hub und dem Decision Container sicher ist.

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

Selbstsigniertes Zertifikat

Für POC-/POV-/Dev-Umgebungen können Sie ein Zertifikat mit dem folgenden Prozess erstellen. Für diesen Prozess muss OpenSSL installiert sein. Diese Anweisungen gelten für einen Windows-Server. Wenn Sie Linux verwenden, nehmen Sie bitte die notwendigen Anpassungen vor.

> Lesen Sie die Onlineversion dieses Handbuchs, um die Formatierung und Zeilenumbrüche in den Skripts zu überprüfen, die in den folgenden Schritten verwendet werden.

1. Wenn es noch nicht vorhanden ist, installieren Sie OpenSSL.
2. Erstellen Sie einen Ordner, in dem Sie das Skript ausführen (im nächsten Schritt), damit der Output an einem einzigen Ort generiert wird.
3. Verwenden Sie in dem erstellten Ordner eines der folgenden Skripts, abhängig vom Host-Betriebssystem (Windows oder Linux), und geben Sie die jeweils angegebenen Werte in die Variablen oben im Skript ein:

   `Enter certificate password` – Ersetzen Sie dies durch ein Passwort, das zur Erstellung des Zertifikats verwendet wird.

   `Enter CN for client certificate` – Ersetzen Sie dies durch einen gemeinsamen Namen für das Client-Zertifikat, zum Beispiel client.decision.blueprism.com.

   `Enter CA` – Ersetzen Sie dies durch den gemeinsamen Namen der Zertifizierungsstelle, zum Beispiel decisionCA.

   `Enter CN for server certificate` – Ersetzen Sie dies durch einen gemeinsamen Namen für das Serverzertifikat. Dieser muss mit dem vollqualifizierten Domain-Namen (FQDN) des Decision Container übereinstimmen, zum Beispiel „decision.blueprism.com“. Wenn sich der Container auf demselben Server wie Hub befindet, können Sie beispielsweise auch „decision.local“ verwenden.

Skript zum Erstellen von Zertifikaten in Windows

Führen Sie PowerShell als Administrator aus und verwenden Sie das folgende Skript:

```
$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
```

Die Zertifikate werden in dem von Ihnen erstellten Ordner generiert.

Skript zum Erstellen von Zertifikaten in Linux

Führen Sie das folgende Bash-Skript aus:

```
#!/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
```

Die Zertifikate werden in dem von Ihnen erstellten Ordner generiert.

4. Fügen Sie das Zertifikat als vertrauenswürdiges Zertifikat auf dem lokalen Computer hinzu, indem Sie die folgenden Skripts ausführen:

```
$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. Geben Sie IIS-Benutzern Zugriff auf das Zertifikat:
   a. Öffnen Sie „Computerzertifikate verwalten“ und suchen Sie das Zertifikat.
   b. Klicken Sie mit der rechten Maustaste auf das Zertifikat, wählen Sie **Alle Aufgaben** und dann **Private Schlüssel verwalten...** aus.
   c. Fügen Sie **IIS_IUSRS** mit der Berechtigung **Lesen** hinzu.
   d. Klicken Sie auf **Anwenden**.

Wenn Sie verschiedene Computer zum Hosten des Blue Prism Decision Model Service Containers und Blue Prism Hub verwenden, müssen Sie Folgendes sicherstellen:

- Der Decision Model Service Container-Host verfügt über die folgenden Dateien:
  - server.crt
  - server.key
  - ca.crt
- Der Server, auf dem Blue Prism Hub ausgeführt wird, verfügt über die folgenden Dateien:
  - client.crt
  - ca.crt

Blue Prism Decision Model Service Container installieren

Der Blue Prism Decision Model Service Container enthält die vom Decision Plug-in verwendete Model Learning API. Dieser Container muss bereitgestellt und ausgeführt werden, bevor die Hub Installation durchgeführt wird, da Sie die Details im Installationsassistenten eingeben müssen.

Informationen zum Ansehen des Installationsvorgangs des Decision Model Service mithilfe des Containers finden Sie in unserem Blue Prism Installationsvideo zum Decision Model Service.

Voraussetzungen

- Ein Docker-Host ist erforderlich, der Linux-Container ausführen kann.
  - Blue Prism empfiehlt, dass Ihre Produktionsumgebung einen Linux-Server als Host verwendet. Docker Engine ist erforderlich, um den Decision Model Service Container auszuführen. Weitere Informationen finden Sie in der Docker-Hilfe: Docker Engine installieren.
  - Für POC- oder Dev-Umgebungen kann ein Windows-Server verwendet werden. Docker Desktop ist erforderlich, um den Decision Model Service Container auszuführen. Weitere Informationen finden Sie in der Docker-Hilfe: Docker Desktop unter Windows installieren.
- 500 MB Speicherplatz für den Container.

Installationsschritte

1. Öffnen Sie die Decision Model Service Containerseite auf DockerHub.
2. Kopieren Sie den Pull-Befehl von der Containerseite und führen Sie ihn in der Befehlszeile aus. Zum Beispiel:

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

   Dabei entspricht `<version>` der Versionsnummer, die auf der Registerkarte „Tags“ auf DockerHub zu sehen ist.
3. Konfigurieren Sie die Ausführung des Containers mit dem folgenden Befehl:

   Der Befehl muss sich in einer einzigen Zeile befinden – siehe die Onlineversion dieses Handbuchs.

   ```
   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>
   ```

   Dabei gilt:

   `<Absolute path of certificate location>` wird durch den vollständigen Pfad des Zertifikats ersetzt, das in SSL-Zertifikat generieren auf Seite8 erstellt wurde.

   `<version>` wird durch die Versionsnummer des Decision Model Service Containers ersetzt.
4. Überprüfen Sie die Ausführung des Containers mit dem folgenden Befehl:

   ```
   docker ps -a
   ```

Blue Prism Hub installieren

Sie können jetzt das Hub Installationsprogramm ausführen, siehe Blue Prism Hub installieren. Geben Sie im Bildschirm „Setup von Blue Prism Decision (optional)“ die URL ein, unter der der Decision Container ausgeführt wird, gefolgt von der Portnummer. Die URL muss mit dem FQDN übereinstimmen, der im Zertifikat angegeben wurde, und auf den Model Service Container verweisen. Die Portnummer muss mit derjenigen übereinstimmen, die bei der Einrichtung des Container zur Ausführung angegeben wurde.

Die URL sollte das Format https://<FQDN>:<Portnummer> haben.
Zum Beispiel https://decision.blueprism.com:50051 oder http://decision.local:50051.

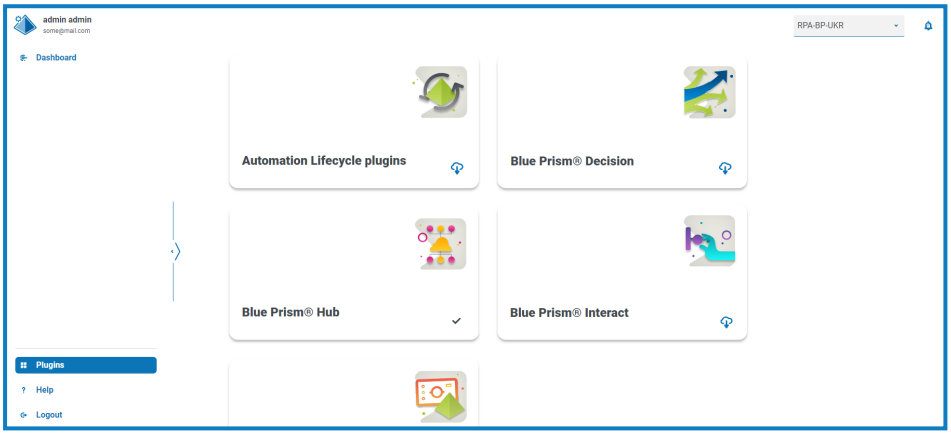
Wenn Sie Hub 4.5 bereits ohne Decision installiert haben, finden Sie unter Fehlerbehebung bei der auf Seite20 Informationen zur Aktualisierung Ihrer Installation.

Decision Plug-in installieren

Das Decision Plug-in muss von einem Hub Administrator aus dem Plug-in-Repository installiert werden.

Informationen zur Installation und Konfiguration des Decision Plug-ins finden Sie in unserem Video zum Blue Prism Decision Plug-in.

1. Wenn Sie ein Hub Administrator sind, melden Sie sich bei Hub an und klicken Sie auf **Plug-ins**, um das Plug-in-Repository zu öffnen.



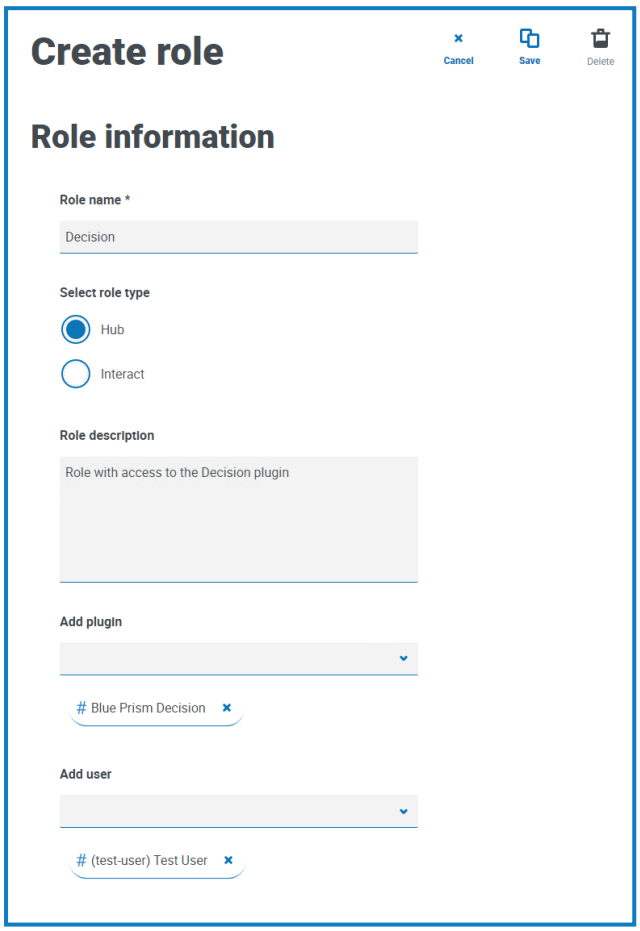
2. Klicken Sie auf der Kachel **Blue Prism Decision** auf das Download-Symbol , um die Installation zu starten.
3. Wenn Sie dazu aufgefordert werden, laden Sie die Lizenzdatei für Decision hoch.

   Das Plug-in wird installiert und eine Nachricht informiert Sie darüber, dass die Site neu gestartet wird. Nachdem der Vorgang abgeschlossen ist, wird das Plug-in-Repository angezeigt und das Download-Symbol auf der Kachel **Blue Prism Decision** wird durch ein Häkchen ersetzt.

   Der Site-Neustart wirkt sich auf alle Benutzer aus, die in Hub angemeldet sind. Obwohl er nicht lange dauert, wird empfohlen, ihn außerhalb der normalen Arbeitszeiten durchzuführen, um Störungen zu minimieren.

Zugriff auf das Decision Plug-in konfigurieren

Das Decision Plug-in steht Hub Administratoren automatisch zur Verfügung. Benutzer müssen zu einer Rolle hinzugefügt werden, die Zugriff auf Decision bietet. Dieser Zugriff kann über eine neue Rolle gewährt oder einer vorhandenen Benutzerrolle hinzugefügt werden. Wenn eine Rolle nicht bereits vorhanden ist, kann eine neue Rolle erstellt werden, um Zugriff auf das Plug-in zu gewähren:



1. Klicken Sie auf der Seite „Rollen und Berechtigungen“ auf **Rolle erstellen**.

   Der Abschnitt „Rolle erstellen“ wird angezeigt.
2. Geben Sie einen Rollennamen ein und wählen Sie **Hub** aus.
3. Falls erforderlich, geben Sie eine Beschreibung ein.
4. Wählen Sie **Blue Prism Decision** in der Dropdown-Liste **Plug-in hinzufügen** aus.
5. Wählen Sie aus der Dropdown-Liste **Benutzer hinzufügen** die Benutzer aus, denen diese Rolle zugewiesen wird. Die Liste zeigt nur Hub Benutzer und keine Interact Benutzer an.
6. Klicken Sie auf **Speichern**, um die Rolle zu erstellen und den Zugriff auf die angegebenen Benutzer zu ermöglichen.

Benutzer können zu vorhandenen Rollen hinzugefügt und davon entfernt werden, indem die gewünschte Rolle auf der Seite „Rollen und Berechtigungen“ ausgewählt und auf **Bearbeiten** geklickt wird. Weitere Informationen erhalten Sie im Hub Benutzerhandbuch.

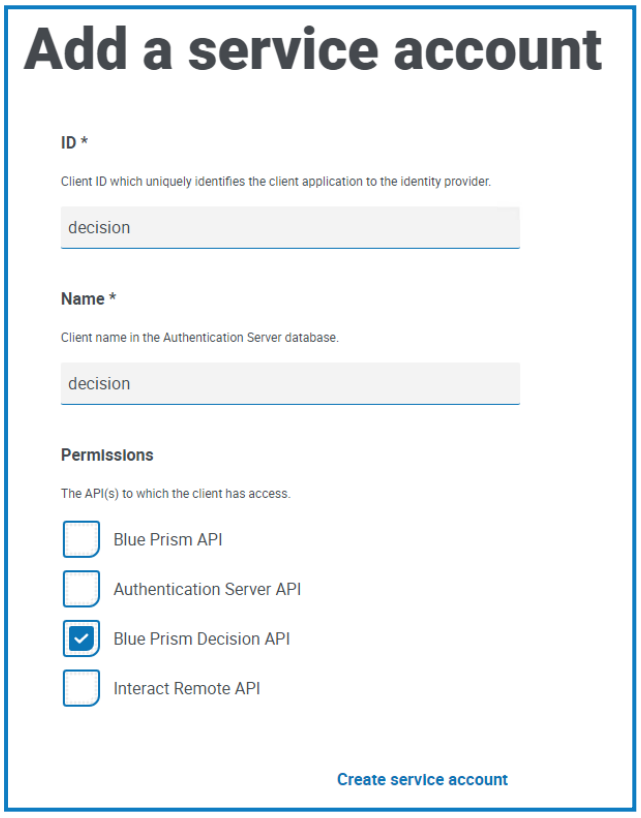
Blue Prism zur Verwendung von Decision konfigurieren

Um Blue Prism zur Verwendung Ihrer Decision Modelle zu konfigurieren, ist Folgendes erforderlich:

1. Dienstkonto einrichten in Hub und geheimen Schlüssel generieren.
2. Anmeldedaten einrichten für das Decision Dienstkonto in Blue Prism.
3. Blue Prism Decision API Release VBO importieren, um mit Decision zu kommunizieren.

Dienstkonto einrichten

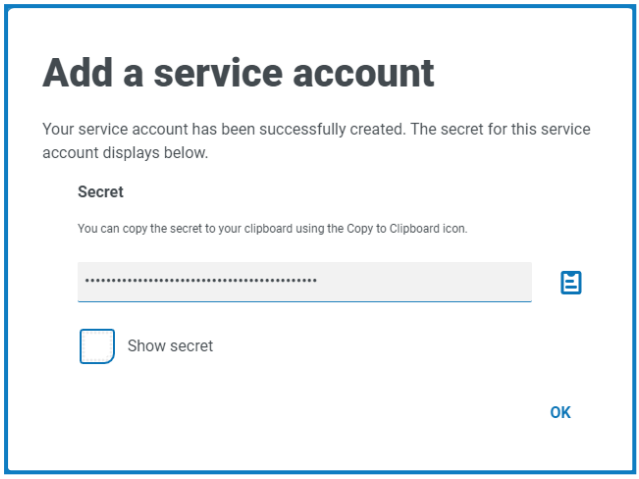
1. Klicken Sie in Blue Prism Hub auf der Dienstkonten-Seite auf **Konto hinzufügen**.
2. Geben Sie eine eindeutige ID und einen Anzeigenamen ein, zum Beispiel *Decision*.
3. Wählen Sie unter **Berechtigungen** die **Blue Prism Decision API** aus.



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

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

5. Kopieren Sie das generierte Geheimnis in Ihre Zwischenablage, um es im interaktiven Blue Prism Client einfügen zu können.



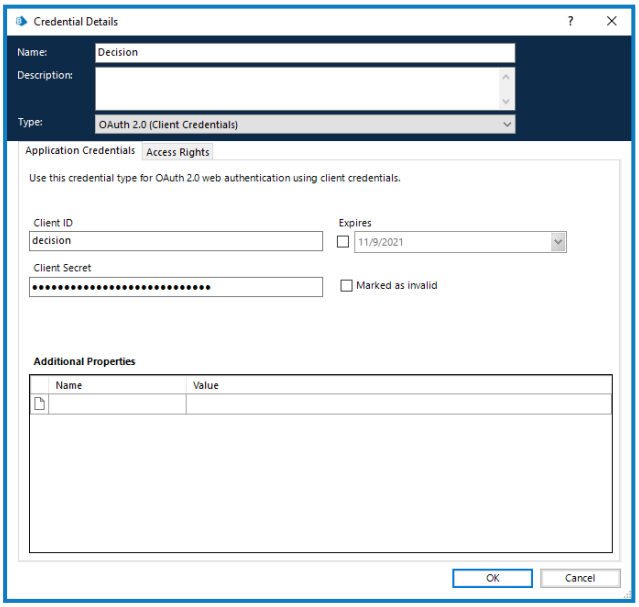
6. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

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

Anmeldedaten in Blue Prism einrichten

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

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



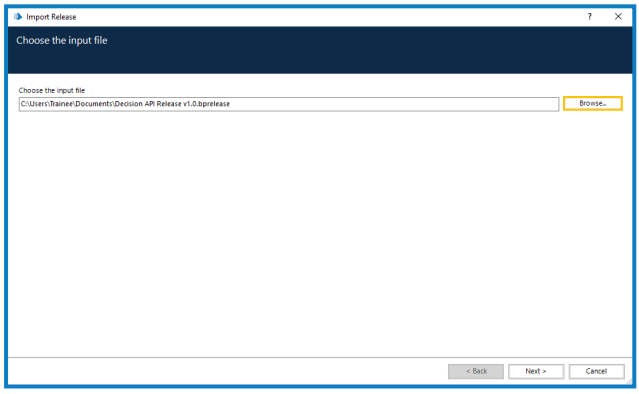
4. Richten Sie auf der Registerkarte „Zugriffsrechte“ im Dialogfeld „Anmeldedaten-Details“ die erforderlichen Zugriffsberechtigungen ein.
5. Klicken Sie auf **OK**.

Blue Prism Decision API Release VBO importieren

1. Wenn Sie die Datei „Decision API.bprelease“ noch nicht haben, laden Sie sie im Blue Prism Portal herunter.
2. Wählen Sie in Blue Prism **Datei** aus und klicken Sie auf **Importieren** > **Release/Fertigkeit**.

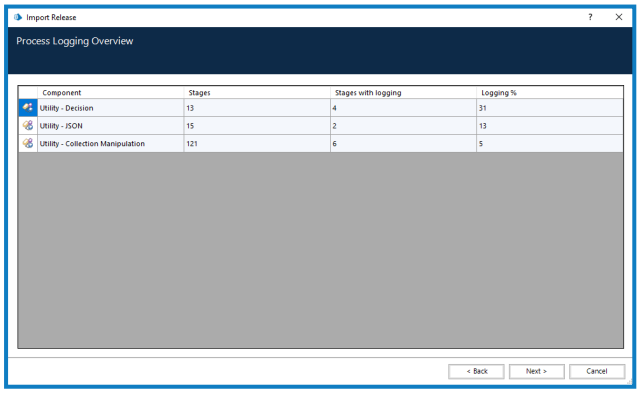
   Das Dialogfeld „Release importieren“ wird angezeigt.
3. Klicken Sie auf **Durchsuchen**.
4. Suchen Sie die Datei „Decision API.bprelease“ und wählen Sie diese aus.

   Zum Beispiel:



5. Klicken Sie auf **Weiter**.

   Der Bildschirm „Übersicht der Prozessprotokollierung“ wird mit einer Zusammenfassung der Komponenten angezeigt, die importiert werden.



6. Klicken Sie auf **Weiter**.

   Ein Bildschirm mit dem Fortschritt wird angezeigt.
7. Wenn das Importieren abgeschlossen ist, klicken Sie auf **Fertig stellen**.
8. Wählen Sie in Blue Prism **System** aus und klicken Sie dann auf **Objekte** > **Web-API-Dienste**.
9. Wählen Sie **DecisionAPI** aus und klicken Sie auf **Dienst bearbeiten**.

10. Geben Sie auf dem Startfenster von Web-API: DecisionAPI unter **Basis-URL** die URL des Decision API-Dienstes im folgenden Format ein:

    `<Hub-Host-URL>:<Port, falls während Installation angegeben>/api/blueprism-decision`

    Zum Beispiel: `https://hub.blueprism.com:5002/api/blueprism-decision`

    Oder bei Verwendung des Standard-Ports: `https://hub.blueprism.com/api/blueprism-decision`.

11. Wählen Sie **Allgemeine Authentifizierung** in der Navigationsstruktur aus und führen Sie dann Folgendes aus:
    a. Stellen Sie sicher, dass der **Authentifizierungstyp** auf **OAuth 2.0 (Client-Anmeldedaten)** festgelegt ist.
    b. Geben Sie in **Autorisierungs-URI** die Authentication Server URL im folgenden Format ein:

       `<Authentication Server URL>:<Port, falls während Installation angegeben>/connect/token`

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

       Oder bei Verwendung des Standard-Ports: `https://authentication.blueprism.com/connect/token`.

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

    c. Wählen Sie unter **Anmeldedaten** die Anmeldedaten aus, die Sie in Anmeldedaten in Blue Prism einrichten auf Seite17 erstellt haben.

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

Fehlerbehebung bei der

Installieren von Decision in einer vorhandenen Hub Umgebung

Wir haben beim Installieren/Aktualisieren von Hub auf 4.5 Decision nicht hinzugefügt, aber wir möchten es jetzt verwenden. Wie installieren wir es?

Sie müssen die Schritte in SSL-Zertifikat generieren auf Seite8 und Blue Prism Decision Model Service Container installieren auf Seite12 ausführen. Es gibt dann zwei Methoden, wie Sie Hub aktualisieren können:

- Deinstallieren Sie Hub und installieren Sie es mit dem 4.5 Installationsprogramm neu – Sie können die Bildschirme mit Ihren vorhandenen Datenbankinformationen füllen und dann die erforderlichen Einstellungen in den Decision Bildschirmen eingeben.
- Aktualisieren Sie die Hub Datei appsetting.json mit den Decision Verbindungszeichenfolgen.

> ⚠ Nachfolgend finden Sie Details zur Aktualisierung der Hub Datei appsettings.json. Achten Sie darauf, nur die bereitgestellten Informationen abzuändern. Andere Änderungen können dazu führen, dass Ihr bestehendes System nicht mehr funktioniert. Änderungen an der Datei appsettings.json sollten in Zusammenarbeit mit Blue Prism vorgenommen werden, um sicherzustellen, dass Ihr System unterstützt wird.

So aktualisieren Sie die Datei appsetting.json, damit Decision inbegriffen ist:

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

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

2. Öffnen Sie die Datei „appsettings.json“ in einem Texteditor.
3. Suchen Sie den folgenden Abschnitt der Datei:

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

> Dies ist nicht die einzige Einstellung, die Sie unter `BluePrismDecision` sehen. Es ist aber die einzige, die geändert werden muss.

4. Erstellen und verschlüsseln Sie mithilfe des Blue Prism Data Protector Tool in PowerShell die Verbindungszeichenfolge für die Decision Datenbank, zum Beispiel:

   > Der Befehl sollte sich in einer einzigen Zeile befinden – siehe die Onlineversion dieses Handbuchs.

   Wenn Sie SQL-Authentifizierung verwenden möchten:

   ```
   .\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 ".\"
   ```

   Wenn Sie Windows-Authentifizierung verwenden möchten:

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

   Dabei ersetzen Sie:

   `[SQL Server]` = Der SQL Server, der die Datenbank hosten wird.

   `[user name, for example, sqladmin]` = Der SQL-Benutzername (nur SQL-Authentifizierung)

   `[password]` = Das Passwort für den SQL-Benutzer (nur SQL-Authentifizierung)

   Falls erforderlich, können Sie einen anderen Datenbanknamen für den Parameter `Initial Catalog` eingeben. `BluePrismDecisionDB` ist der Standardname.

   > Die obigen Einstellungen entsprechen den Werten, die Sie im Bildschirm „Blue Prism Decision SQL-Verbindung konfigurieren“ im Hub Installationsassistenten eingeben würden.
   >
   > Die Decision Datenbank wird erstellt, wenn Sie das Decision Plug-in in Hub installieren.

5. Kopieren Sie die verschlüsselte Zeichenfolge zwischen den `""` neben der Einstellung `ConnectionString` in der Hub Datei appsettings.json, wie in Schritt 3 gezeigt.
6. Speichern Sie die Datei.
7. Suchen Sie in derselben appsettings.json-Datei den folgenden Abschnitt:

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

8. Geben Sie zwischen den `""` neben der Einstellung `CertificateThumbprint` den Fingerabdruck für das SSL-Zertifikat ein.

   Wenn Sie Windows verwenden, finden Sie dies über „Computerzertifikate verwalten“. Doppelklicken Sie auf das Zertifikat und der **Fingerabdruck** befindet sich auf der Registerkarte „Details“.

9. Geben Sie zwischen den `""` neben der Einstellung `v1` die URL für den Blue Prism Decision Model Service Container ein.
10. Speichern und schließen Sie die Datei.

11. Hub neu starten:
    a. Öffnen Sie Internet Information Services (IIS) Manager.
    b. Wählen Sie in der Liste der Verbindungen **Blue Prism - Hub** aus.

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

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

Die nächsten Schritte sind, Decision Plug-in installieren auf Seite14 und Zugriff auf das Decision Plug-in konfigurieren auf Seite15 abzuschließen. Bevor Sie das Plug-in installieren, müssen Sie jedoch vorübergehend die SQL Server-Berechtigungen dbcreator oder sysadmin für die Anmeldung bereitstellen, die für den Anwendungspool Blue Prism – Hub verwendet wird. Diese Anmeldung hängt von der Option ab, die Sie beim Installieren von Hub ausgewählt haben:

- SQL Server-Authentifizierung – Der SQL-Benutzer, der bei der Installation angegeben wurde.
- Windows-Authentifizierung – Das Windows-Dienstkonto, das mit dem Anwendungspool Blue Prism – Hub verknüpft ist.

Die Decision Datenbank wird erstellt, wenn das Decision Plug-in in Hub installiert wird. Danach können die Berechtigungen dbcreator oder sysadmin entfernt werden.

OpenSSL-Skript schlägt fehl

Wenn das OpenSSL-Skript fehlschlägt, fügen Sie OpenSSL zur Pfadumgebungsvariablen hinzu und versuchen Sie dann, das Skript erneut auszuführen.

1. Öffnen Sie in der Windows-Taskleiste die Systemsteuerung.
2. Wählen Sie **System und Sicherheit** und dann **System** und klicken Sie dann auf **Erweiterte Systemeinstellungen**.

   Das Dialogfeld „Systemeigenschaften“ wird angezeigt.
3. Klicken Sie auf **Umgebungsvariablen**.

   Das Dialogfeld „Umgebungsvariablen“ wird angezeigt.
4. Wählen Sie in der Gruppe **Systemvariablen Pfad** und klicken Sie dann auf **Bearbeiten**.

   Das Dialogfeld „Umgebungsvariable bearbeiten“ wird angezeigt.
5. Klicken Sie auf **Neu** und geben Sie in der neuen Zeile den Pfad zu OpenSSL ein. Der Standardspeicherort ist C:\Programmdateien\OpenSSL-Win64\bin.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.