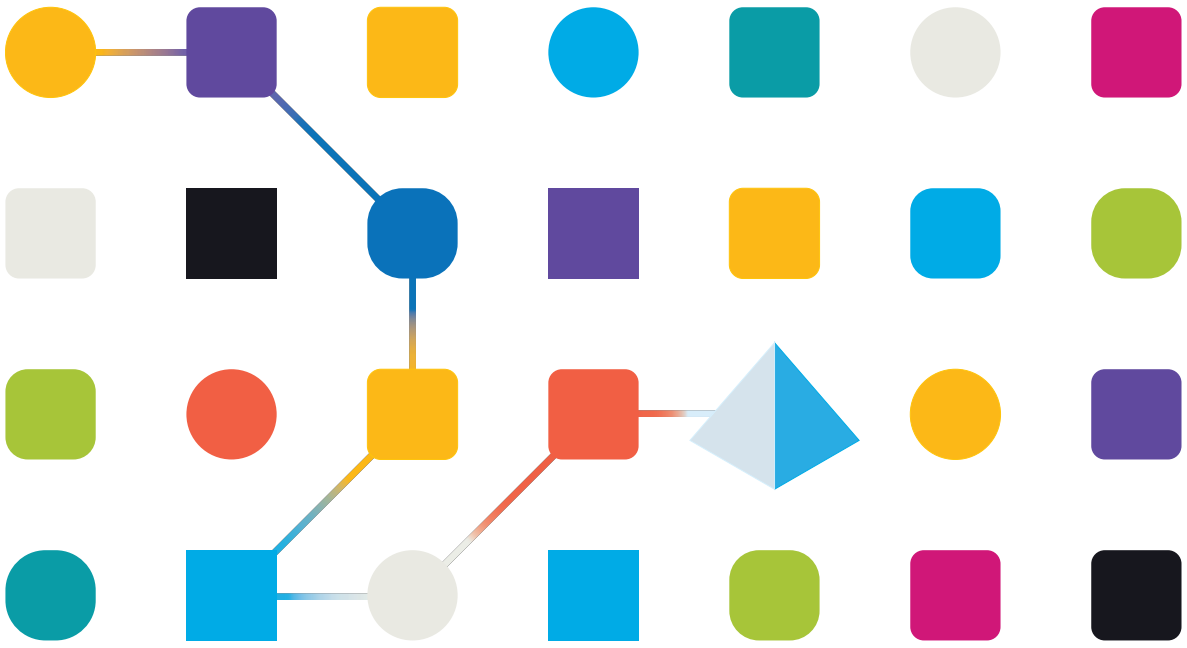
blueprism®

Decision 4.5

インストールガイド

Document Revision: 1.0



商標および著作権

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

内容

Blue Prism Decisionをインストールする

Blue Prism® DecisionはBlue Prism Hubインストーラーを使用してBlue Prism® Hubとともにインストールされる、ライセンスによって管理されるプラグインです。Decisionには前提条件があり、追加コンポーネントであるBlue Prism Decision Model Serviceに依存しています。これはコンテナイメージとして頒布されます。

このリリースはHubとDockerコンテナの両方のインストールに依存するため、Blue Prismでは、Dockerコンテナのインフラストラクチャに関するITポリシーを十分に理解している場合にのみ、Decisionをインストールすることを推奨します。また、次回2022年2月のリリースもMSI経由で利用できるようになります。

インストールの概要

Blue Prism Decisionをインストールするには、以下を実行する必要があります。

1. Decision用のSSL証明書を作成します。

   ステップの前提条件:

   - このセクションには、概念実証(POC)、価値実証(POV)、および開発環境での自己署名証明書の使用に関する情報が記載されています。提供されたスクリプトにはOpenSSLが必要です。

     ⚠ 自己署名証明書は本番環境では使用しないでください。

2. Blue Prism Decision Model Serviceコンテナをインストールします。これには、Decisionが使用するModel Learning APIが含まれています。

   ステップの前提条件:

   - Linuxコンテナを実行できるDockerホスト。
   - コンテナ用のディスク容量(500 MB)。

   詳細については、「前提条件 ページ11」を参照してください。

3. Blue Prism Hubをインストールします。Blue Prism Hubのインストールウィザードで、Model Learning APIのURLとSSL証明書の詳細を指定する必要があります。

   ステップの前提条件:

   - Hubの前提条件については、「Blue Prism Hubインストールガイド」を参照してください。
   - DecisionのSSL証明書。
   - Model Learning APIのURLとポート番号。

   すでにHub 4.5がインストール済みである場合は、「のトラブルシューティング ページ19」を参照して、インストールの更新に関する情報を確認してください。

4. HubにDecisionプラグインをインストールする

   ステップの前提条件:

   - Hubへの管理者アクセス権。
   - Decisionのライセンスファイル。

5. Decisionプラグインへのアクセスを構成します。ユーザーに、Decisionへのアクセス権を持つ役割を割り当てます。

   ステップの前提条件：

   - Hubへの管理者アクセス権。
   - Decisionへのアクセス権を必要とするユーザーのリスト。

6. DecisionをBlue Prismで使用するように構成する

   ステップの前提条件：

   - Hubへの管理者アクセス権。
   - Blue Prism 6.4.0以降と、[システム]タブで認証情報とオブジェクトを構成できる十分な権限があること。
   - Blue Prism DecisionのAPI.bpreleaseファイル。

Decision環境の設定

以下の情報は、Blue Prism® Decisionの環境構成の簡単な概要を説明しています。

Blue Prism® HubにはWindows Server 2016または2019が必要です。

1台のマシン – 概念実証環境または試験環境

小規模な概念実証(POC)環境または試験環境は、1台のマシンで構成できます。1台のマシンのインストールは、本番環境には適していません。

コンポーネント	Windows Server (Windows Server 2016または2019)	Linuxマシン
Hub	✓	該当なし
Docker Desktop	✓	該当なし
Docker Engine	✗	該当なし

複数のマシン – 本番環境

通常、本番環境は複数のマシンで構成され、Webサーバーは他のバックエンドシステムとは異なるマシン上に構成されます。Decisionに使用できる構成は次のとおりです。

Microsoftインフラストラクチャ

Windows Serverのみを使用する場合、構成は次のようになります。

コンポーネント	Windows Server (Windows Server 2016または2019)	Linuxマシン
Hub	✓	該当なし
Docker Desktop	✓	✗
Docker Engine	✗	✗

混合インフラストラクチャ

組織がWindows ServerとLinuxマシンの両方を組み合わせたインフラストラクチャを実行している場合は、以下を使用できます。

コンポーネント	Windows Server (Windows Server 2016または2019)	Linuxマシン
Hub	✓	該当なし
Docker Desktop	✗	✗
Docker Engine	✗	✓

SSL証明書の作成

Blue Prism Decisionコンテナには SSL証明書が必要です。インフラストラクチャおよび組織のITセキュリティ要件に応じて、内部で作成されたSSL証明書または購入済み証明書のいずれかにできます。

> Blue Prism Decisionコンテナでは、HubのDecisionプラグインとDecisionコンテナ間でセキュアに通信できるようにするため、クライアントキーとサーバーキーが必要です。

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

自己署名証明書

POC、POV、Dev環境では、次のプロセスを使用して証明書を作成できます。このプロセスでは、OpenSSLがインストールされている必要があります。以下はWindows Server用の手順です。Linuxをお使いの場合は、必要な調整を行ってください。

> 以下のステップで使用されたスクリプトのフォーマットと改行については、このガイドのオンライン版を参照してください。

1. まだインストールされていない場合は、OpenSSLをインストールします。
2. 次のステップでスクリプトを実行するためのフォルダーを作成し、出力が1か所に生成されるようにします。
3. 作成したフォルダーで、ホストのオペレーティングシステム(WindowsまたはLinux) に応じて次のいずれかのスクリプトを使用し、スクリプトの上部にある変数で指定された適切な値を入力します。

   `Enter certificate password` – 証明書の作成に使用するパスワードに置き換えます。

   `Enter CN for client certificate` – クライアント証明書のコモンネーム (client.decision.blueprism.comなど) に置き換えます。

   `Enter CA` – 証明局のコモンネーム(decisionCAなど) に置き換えます。

   `Enter CN for server certificate` – サーバー証明書のコモンネームに置き換えます。これは、DecisionコンテナのFQDN(decision.blueprism.comなど) と一致する必要があります。または、コンテナがHubと同じサーバー上にある場合はdecision.localなどを使用します。

Windowsで証明書を作成するためのスクリプト

管理者としてPowerShellを実行し、次のスクリプトを使用します。

```
$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
```

証明書は作成したフォルダー内で生成されます。

Linuxで証明書を作成するためのスクリプト

次のBashスクリプトを実行します。

```
#!/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
```

証明書は作成したフォルダー内で生成されます。

4. 次のスクリプトを実行して、証明書をローカルマシンの信頼できる証明書として追加します。

```
$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. IISユーザーに証明書へのアクセス権を付与します。
   a. [コンピューター証明書の管理]を開き、証明書を見つけます。
   b. 証明書を右クリックし、**[すべてのタスク]**、**[プライベートキーの管理...]**の順に選択します。
   c. **読み取り**許可を持つ**IIS_IUSRS**を追加します。
   d. **[適用]**をクリックします。

Blue Prism Decision Model ServiceコンテナとBlue Prism Hubのホストに異なるマシンを使用している場合は、次の点を確認する必要があります。

- Decision Model Serviceコンテナのホストに次のファイルがある。
  - server.crt
  - server.key
  - ca.crt
- Blue Prism Hubを実行しているサーバーに次のファイルがある。
  - client.crt
  - ca.crt

Blue Prism Decision Model Serviceコンテナをインストールする

Blue Prism Decision Model Serviceコンテナには、Decisionプラグインが使用するModel Learning APIが含まれています。インストールウィザードに詳細を入力する必要があるため、このコンテナは、Hubのインストール前にデプロイおよび実行する必要があります。

前提条件

- Linuxコンテナを実行できるDockerホストが必要です。
  - Blue Prismでは、本番環境でLinuxサーバーをホストとして使用することを推奨しています。Decision Model Serviceコンテナを実行するにはDocker Engineが必要です。詳細については、Dockerヘルプの「Docker Engineのインストール」を参照してください。
  - POCまたはDev環境では、Windows Serverを使用できます。Decision Model Serviceコンテナを実行するには、Docker Desktopが必要です。詳細については、Dockerヘルプの「Windows に Docker Desktopをインストール」を参照してください。
- コンテナ用のディスク容量(500 MB)。

インストール手順

1. DockerHubでDecision Model Serviceコンテナページを開きます。
2. コンテナページからプルコマンドをコピーし、コマンドラインで実行します。例:

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

<version>はDockerHubの[タグ]タブに表示されるバージョン番号と一致します。

3. 次のコマンドを使用して、実行中のコンテナを設定します。

> コマンドは1行で入力してください。このガイドのオンライン版を参照してください。

```
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>
```

ここでは、

<Absolute path of certificate location>はSSL証明書の作成 ページ7で作成した証明書のフルパスに置き換えます。

<version>は、Decisionのバージョン番号に置き換えます。

4. 次のコマンドを使用して、コンテナが実行中であることを確認します。

```
docker ps -a
```

Blue Prism Hubをインストールする

これで、Hubインストーラーを実行できます。の「Blue Prism Hubをインストールする」を参照してください。 [Blue Prism Decisionの設定(オプション)]画面で、Decisionコンテナが実行されている場所のURLを入力し、続いてポート番号を入力します。URLは証明書に指定されたFQDNと一致させ、Model Serviceコンテナを指定する必要があります。ポート番号は、コンテナの実行時に指定したものと一致させる必要があります。

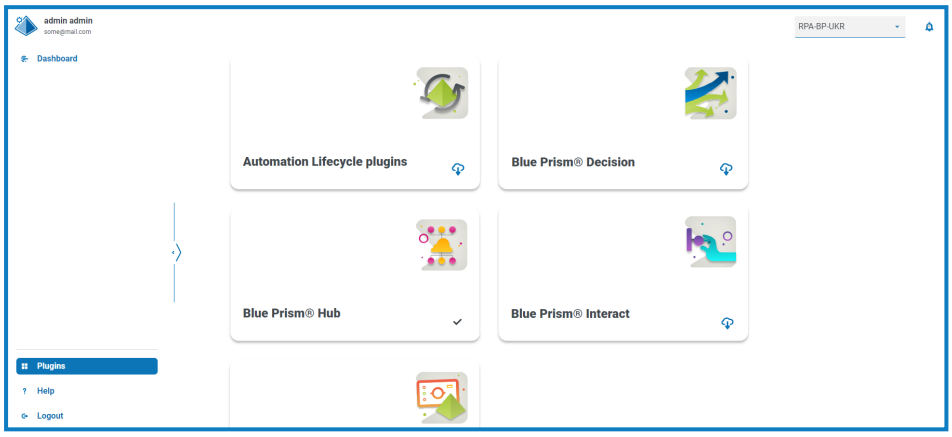
URLの形式はhttps://<FQDN>:<ポート番号>にする必要があります。
例:https://decision.blueprism.com:50051、またはhttp://decision.local:50051。

すでにHub 4.5がインストール済みである場合は、「のトラブルシューティング ページ19」を参照して、インストールの更新に関する情報を確認してください。

Decisionプラグインをインストールする

Decisionプラグインは、Hub管理者がプラグインリポジトリからインストールする必要があります。

1. Hub管理者の場合は、Hubにログインし、 [**プラグイン**] をクリックしてプラグインリポジトリを開きます。



2. [**Blue Prism Decision**] タイルで、ダウンロードアイコン をクリックしてインストールを開始します。

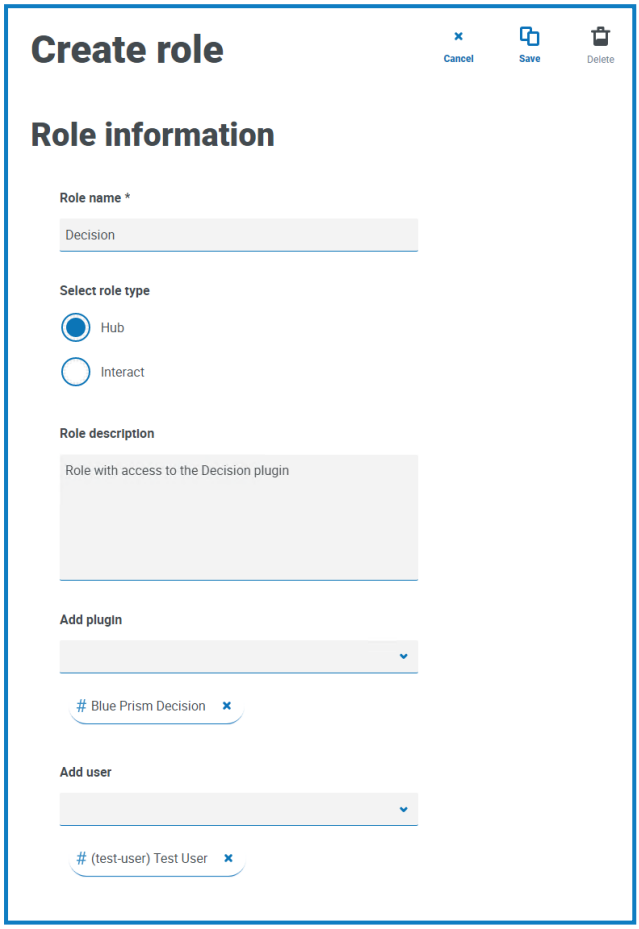
3. プロンプトが表示されたら、Decision用のライセンスファイルをアップロードします。

   プラグインがインストールされ、サイトが再起動中であることを示すメッセージが表示されます。完了すると、プラグインリポジトリが表示され、 [**Blue Prism Decision**] タイルのダウンロードアイコンがチェックマークに置き換えられます。

> サイトの再起動は、Hubにログインしているすべてのユーザーに影響します。時間はかかりませんが、中断を最小限に抑えるため、通常の勤務時間外に行うことをお勧めします。

Decisionプラグインへのアクセスを構成する

Hub管理者はDecisionプラグインを自動的に使用できるようになります。ユーザーは、Decisionへのアクセス権が付与されている役割に追加される必要があります。このアクセス権は、新しい役割を介して付与するか、既存のユーザーの役割に追加できます。役割がまだ存在しない場合は、新しい役割を作成してプラグインへのアクセスを許可できます。



1. [役割と許可]ページで、**[役割を作成]**をクリックします。

   [役割を作成]セクションが表示されます。
2. 役割名を入力し、**[Hub]**を選択します。
3. 必要に応じて、説明を入力します。
4. **[プラグインを追加]**ドロップダウンリストから**[Blue Prism Decision]**を選択します。
5. **[ユーザーを追加]**ドロップダウンリストから、この役割を割り当てるユーザーを選択します。このリストには、Hubユーザーのみが表示され、Interactユーザーは表示されません。
6. **[保存]**をクリックして役割を作成し、指定したユーザーへのアクセスを許可します。

[役割と権限]ページで必要な役割を選択し、**[編集]**をクリックすると、既存の役割にユーザーを追加したり、既存の役割からユーザーを削除したりできます。詳細については「Hubユーザーガイド」を参照してください。

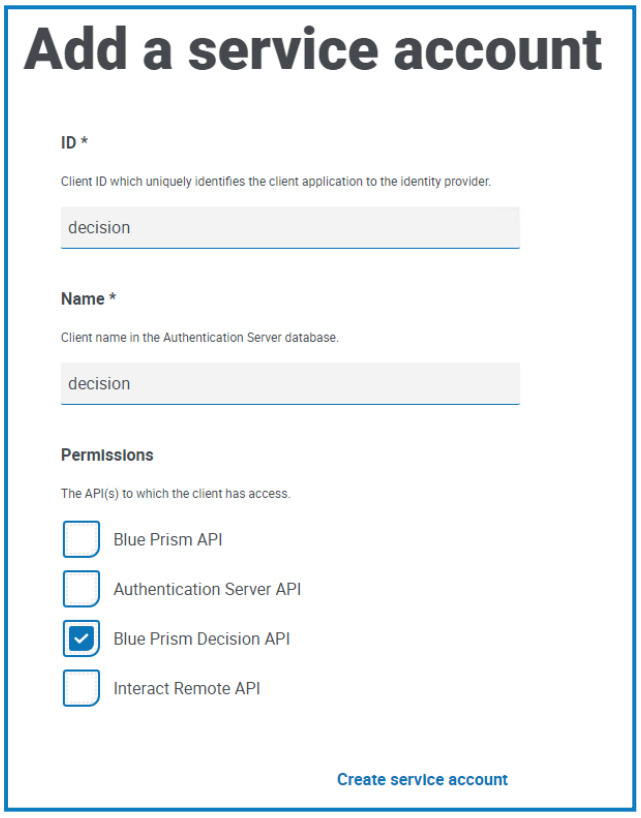
Decisionを使用するようにBlue Prismを構成する

Decisionモデルを使用するようにBlue Prismを構成するには、次を実行する必要があります。

1. Hubでサービスアカウントを設定し、シークレットキーを生成します。
2. Blue PrismのDecisionサービスアカウントの認証情報を設定します。
3. Blue Prism Decision APIリリースVBOをインポートして、Decisionと通信します。

サービスアカウントを設定する

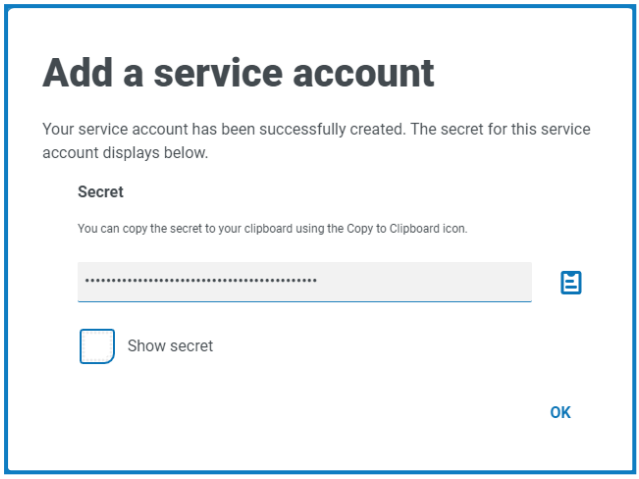
1. Blue Prism Hubの [サービスアカウント] ページで、 **[アカウントを追加]** をクリックします。
2. 一意のIDとフレンドリ名 (*Decision*など) を入力します。
3. **[アクセス許可]** で **[Blue Prism Decision API]** を選択します。



4. **[サービスアカウントを作成]** をクリックします。

   [サービスアカウントを追加] ダイアログに、生成されたシークレットキーが表示されます。関連する認証情報を構成する際は、このキーをBlue Prismのインタラクティブクライアントに入力する必要があります。

5. 生成されたシークレットをクリップボードにコピーし、Blue Prismインタラクティブクライアントに貼り付ける準備ができます。



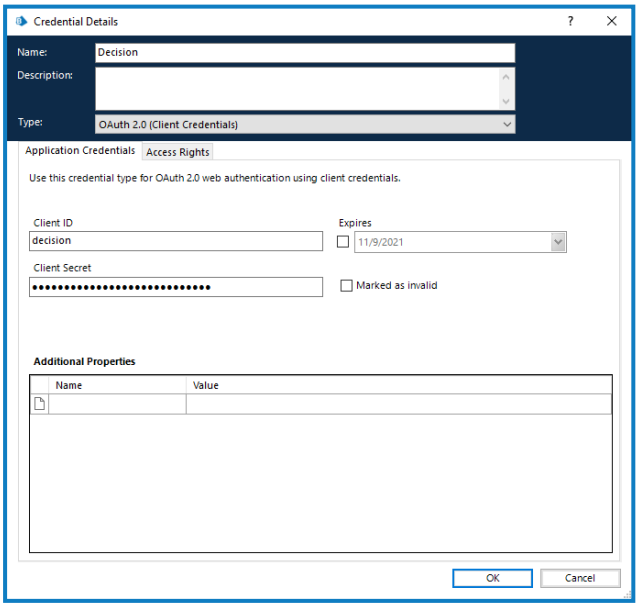
6. [OK]をクリックしてダイアログを閉じます。

   [サービスアカウント]ページに、新しく作成されたアカウントが表示されます。

Blue Prismで認証情報を設定する

1. Blue Prismにログインし、[**システム**]を選択して[**セキュリティ**] > [**認証情報**]をクリックします。詳細については、[セキュリティ] > [認証情報]を参照してください。
2. [**新規**]をクリックします。

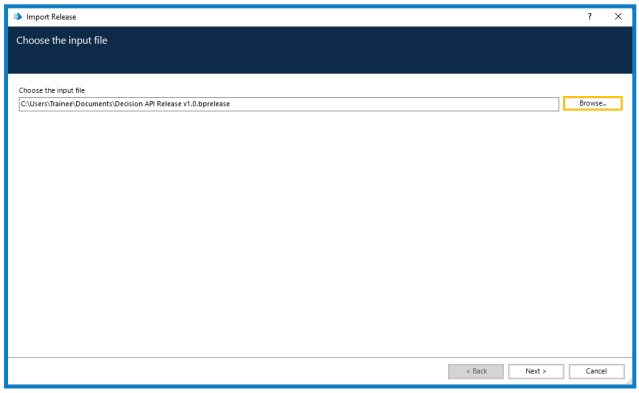
   [認証情報の詳細]ダイアログが表示されます。
3. [認証情報の詳細]ダイアログの[アプリケーション認証情報]タブで、次の手順を実行します。
   a. 名前を入力します。
   b. [**タイプ**]を[**OAuth 2.0(クライアント認証情報)**]に変更します。
   c. [**クライアントID**]に、サービスアカウントを設定する前のページでサービスアカウントの作成に使用したIDを入力します。
   d. [**クライアントシークレット**]に、サービスアカウント用に生成したシークレットキーを入力します。



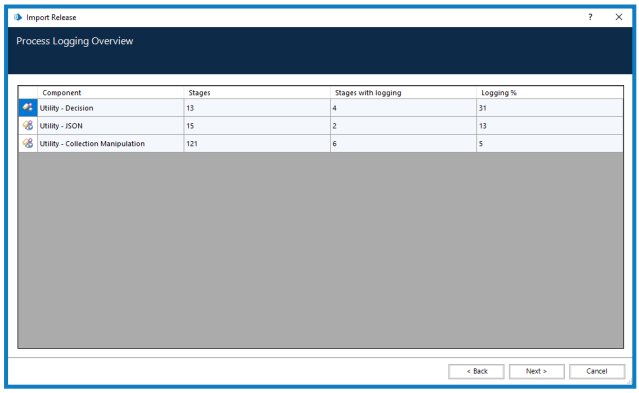
4. [認証情報の詳細]ダイアログの[アクセス権]タブで、必要なアクセス許可を設定します。
5. [OK]をクリックします。

Blue Prism Decision APIリリースVBOをインポートする

1. Blue PrismポータルからDecision API.bpreleaseファイルをまだダウンロードしていない場合は、ダウンロードします。
2. Blue Prismで[ファイル]を選択して、[インポート] > [リリース/スキル]の順にクリックします。
   [リリースをインポート]ダイアログが表示されます。
3. [参照]をクリックします。
4. Decision API.bpreleaseファイルを見つけて選択します。
   例：



5. [次へ]をクリックします。
   [プロセスログの概要]画面に、インポートするコンポーネントの概要が表示されます。



6. [次へ]をクリックします。
   処理中画面が表示されます。
7. インポートが完了したら、[終了]をクリックします。
8. Blue Prismで[システム]を選択して、[オブジェクト] > [Web APIサービス]の順にクリックします。
9. [DecisionAPI]を選択し、[サービスを編集]をクリックします。

10. Web API:DecisionAPIの開始画面の [**ベースURL**] に、Decision APIサービスのURLを次の形式で入力します。

    <HubホストのURL>:<ポート（インストール中に指定した場合）>/api/blueprism-decision

    例：https://hub.blueprism.com:5002/api/blueprism-decision

    デフォルトのポートを使用する場合：https://hub.blueprism.com/api/blueprism-decision。

11. [**共通認証**] を選択し、次の手順を実行します。
    a. [**認証タイプ**] が [**OAuth 2.0（クライアント認証情報）**] に設定されていることを確認します
    b. [**承認URI**] で、Authentication ServerのURLを

    <Authentication ServerのURL>:<ポート（インストール中に指定した場合）>/connect/token

    の形式で入力します
    （例：https://authentication.blueprism.com:5000/connect/token）。

    デフォルトのポートを使用する場合は、
    https://authentication.blueprism.com/connect/tokenのようになります。

    > 4.3より前のバージョンからアップグレードした場合、お使いのシステムは引き続きIMSを使用します。この場合、次の形式で情報を入力します。
    >
    > <IMSのURL>/<ポート（指定した場合）>connect/token
    >
    > 例：https://ims.blueprism.com:5000/connect/token。

    c. [**認証情報**] で、Blue Prismで認証情報を設定する ページ16で作成した認証情報を選択します。

12. [**OK**] をクリックして保存し、Web APIサービスの設定を完了します。

のトラブルシューティング

4.5にHubをインストール/アップグレードしたときにDecisionを追加しませんでしたが、今は使用したいと考えています。どのようにインストールすればよいですか?

「SSL証明書の作成 ページ7」と「Blue Prism Decision Model Serviceコンテナをインストールする ページ11」にあるステップを実行する必要があります。その後、次の2つの方法のいずれかでHubを更新します。

- Hubをアンインストールし、4.5インストーラーを使用して再インストールします。既存のデータベース情報を画面に入力し、Decisionの画面にも必要な設定を入力できます。
- Hubのappsetting.jsonファイルをDecision接続文字列で更新します。

> ⚠ 以下で、Hubのappsettings.jsonファイルの更新方法を詳細に説明します。提供された情報のみを修正するよう注意する必要があります。その他の変更を行うと、既存のシステムが壊れるおそれがあります。appsettings.jsonファイルへの変更は、Blue Prismと連携して行い、システムが確実にサポートされるようにする必要があります。

appsetting.jsonファイルを更新してDecisionを含めるには、以下を実行します。

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

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

2. appsettings.jsonファイルをテキストエディターで開きます。
3. ファイルで次のセクションを見つけます。

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

   > これは、`BluePrismDecision`で表示できる唯一の設定ではありません。ただし、変更が必要なのはこれだけです。

4. PowerShellのBlue Prism Data Protectorツールを使用してDecisionデータベースの接続文字列を作成し、暗号化します。たとえば、次のようになります。

   コマンドは1行で入力してください。このガイドのオンライン版を参照してください。

   SQL認証を使用する場合：

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

   Windows認証を使用する場合：

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

   置換する部分：

   [SQL Server] = データベースをホストするSQL Server。

   [sqladminのようなユーザー名] = SQLユーザー名 (SQL認証のみ)

   [password] = SQLユーザーのパスワード (SQL認証のみ)

   必要に応じて、 [Initial Catalog] パラメーターに別のデータベース名を入力できます。デフォルトの名前は「BluePrismDecisionDB」です。

   上記の設定で入力する値は、Hubのインストールウィザードの [Blue Prism Decision SQL接続を構成] 画面のものと同じです。

   HubにDecisionプラグインをインストールすると、Decisionデータベースが作成されます。

5. Hubのappsettings.jsonファイルのConnectionString設定の横にある""の間に暗号化した文字列をコピーします(ステップ3を参照) 。
6. ファイルを保存します。
7. 同じappsettings.jsonファイルで次のセクションを見つけます。

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

8. CertificateThumbprint設定の横にある""の間に、SSL証明書のサムプリントを入力します。

   Windowsを使用している場合は、 [コンピューター証明書の管理] を使用して、 [詳細] タブで証明書と**サムプリント**をダブルクリックすると、サムプリントを見つけることができます。

9. v1設定の横にある""の間に、Blue Prism Decision Model Serviceコンテナのurlを入力します。
10. ファイルを保存して閉じます。

11. Hubを再起動します。
    a. Internet Information Services(IIS) マネージャーを開きます。
    b. 接続のリストで、**Blue Prism - Hub**を選択します。

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

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

次のステップでは、「Decisionプラグインをインストールする ページ13」と「Decisionプラグインへのアクセスを構成する ページ14」を完了します。ただし、プラグインをインストールする前にアプリケーションプールBlue Prism – Hubのログインに SQL Serverの許可「dbcreator」または「sysadmin」を一時的に提供する必要があります。このログインは、Hubのインストール時に選択したオプションによって異なります。

- SQL Server認証 : インストール時に指定されたSQLユーザー。
- Windows認証:アプリケーションプールBlue Prism – Hubに関連付けられたWindowsのサービスアカウント。

HubにDecisionプラグインをインストールすると、Decisionデータベースが作成されます。その後、許可「dbcreator」または「sysadmin」を削除します。