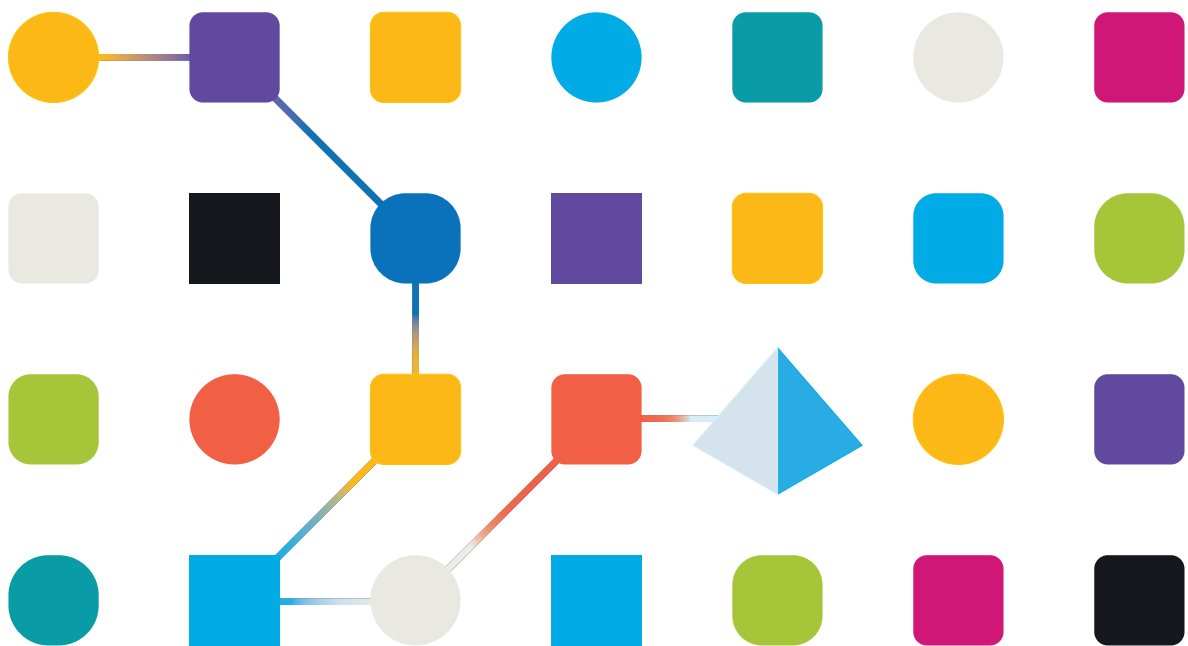




Decision 4.5

Install Guide

Document Revision: 5.0



Trademarks and Copyright

The information contained in this document is the proprietary and confidential information of Blue Prism Limited and should not be disclosed to a third-party without the written consent of an authorized Blue Prism representative. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying without the written permission of Blue Prism Limited.

© 2023 Blue Prism Limited

“Blue Prism”, the “Blue Prism” logo and Prism device are either trademarks or registered trademarks of Blue Prism Limited and its affiliates. All Rights Reserved.

All trademarks are hereby acknowledged and are used to the benefit of their respective owners. Blue Prism is not responsible for the content of external websites referenced by this document.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

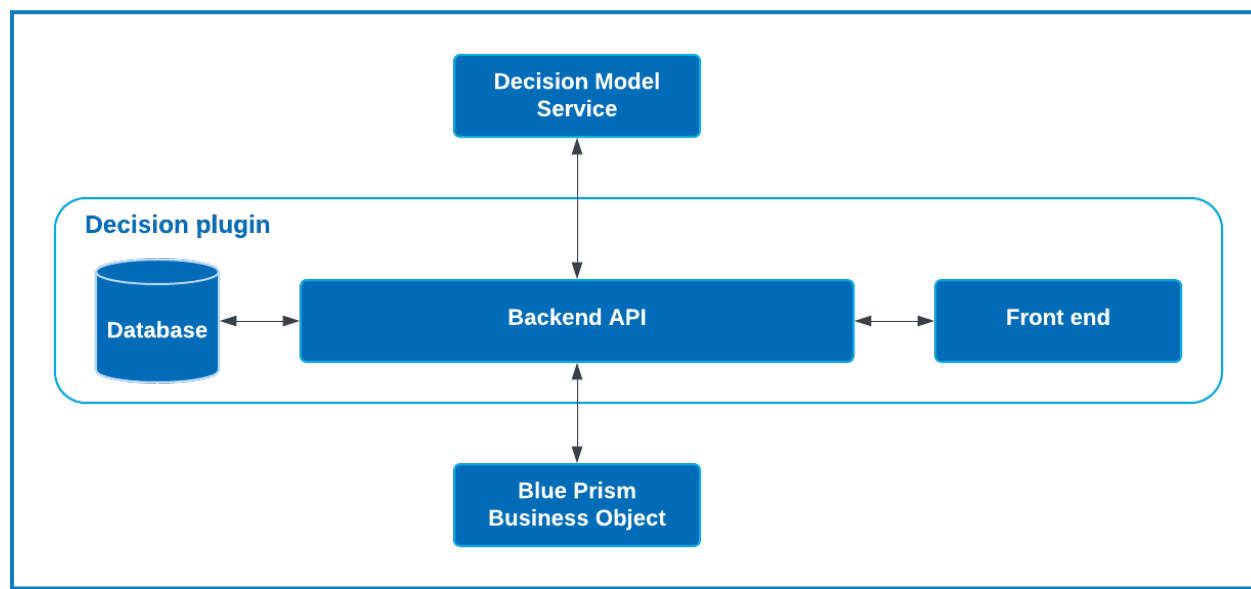
Contents

Install Blue Prism Decision	4
Intended audience	4
Installation overview	5
Decision environment setup	6
Single machine – Proof of Concept or Trial environments	6
Multiple machines – Production environments	6
Generate an SSL Certificate	7
Self-signed certificate	7
Install the Blue Prism Decision Model Service container	11
Prerequisites	11
Installation steps	11
Install Blue Prism Hub	12
Mandatory configuration	12
Install the Decision plugin	13
Configure access to the Decision plugin	14
Configure Blue Prism to use Decision	15
Set up a service account	15
Set up credentials in Blue Prism	16
Import the Blue Prism Decision API Release VBO	17
Troubleshooting	19
Install Decision in an existing Hub environment	19
OpenSSL script fails	21

Install Blue Prism Decision

Blue Prism® Decision is a license controlled plugin that is installed with SS&C | Blue Prism® Hub, using the Blue Prism Hub installer. Decision has a prerequisite and a dependency on an additional component – the Blue Prism Decision Model Service, which is distributed as a container image.

The diagram below illustrates the logical architecture of Decision, showing the interaction between the plugin front end, the Decision Model Service, and the Blue Prism interactive client (Blue Prism Business Object in the diagram).



Intended audience

This guide is aimed at IT professionals with experience in configuring and managing networks, servers, and databases. The installation process requires familiarity with installing and configuring web servers and databases.

Blue Prism recommends that Decision is only installed if you have a mature understanding of IT policies around Docker Container infrastructure, as this release is dependent on installing both Hub and a Docker Container. The next release in 2022 will also be made available via an MSI.

Installation overview

To install Blue Prism Decision, you must:

1. [Generate an SSL Certificate](#) for Decision.

Step prerequisites:

- This section includes information for using self-signed certificates for Proof of Concept (POC), Proof of Value (POV) and Development environments. The scripts supplied require [OpenSSL](#).

 Self-signed certificates should not be used for Production environments.

2. [Install the Blue Prism Decision Model Service container](#) – This contains the Model Learning API used by Decision.

Step prerequisites:


- A Docker host that is capable of running Linux containers.
- 500 MB of disk space for the container.

For more information, see [Prerequisites on page 11](#).

3. [Install Blue Prism Hub](#) – You must provide the Model Learning API URL and SSL certificate details in the Blue Prism Hub Install wizard.

Step prerequisites:

- For the Hub prerequisites, see the [Blue Prism Hub Install Guide](#).
- The Decision SSL Certificate.
- The Model Learning API URL and port number.

 If you have already installed Hub 4.5, see [Troubleshooting on page 19](#) for information on updating your installation.

4. [Install the Decision plugin](#) in Hub

Step prerequisites:

- Administrator access to Hub.
- Decision license file.

5. [Configure access to the Decision plugin](#) – Assign users to a role that provides access to Decision.

Step prerequisites:

- Administrator access to Hub.
- List of users who require access to Decision.

6. [Configure Blue Prism to use Decision](#)

Step prerequisites:

- Administrator access to Hub.
- Blue Prism 6.4.0 or later, with sufficient privileges to configure credentials and objects on the System tab.
- Blue Prism Decision API.brelease file.

Decision environment setup

The information below provides a simple overview of the environment configurations for Blue Prism® Decision.

 Blue Prism® Hub requires Windows Server 2016 or 2019.

Single machine – Proof of Concept or Trial environments

Small Proof of Concept (POC) or Trial environments can be configured on a single machine. Single machine installations are not suitable for Production environments.

Component	Windows Server (Windows Server 2016 or 2019)	Linux machine
Hub	✓	N/A
Docker Desktop	✓	N/A
Docker Engine	✗	N/A

Multiple machines – Production environments

Production environments are usually configured on multiple machines, with the web server being on a different machine than the other back-end systems. Multiple machine setups can also be used for POC environments, if required. The configurations that can be used for Decision are:

Microsoft infrastructure

If you only use Windows Servers, the configuration will be:

Component	Windows Server (Windows Server 2016 or 2019)	Linux machine
Hub	✓	N/A
Docker Desktop	✓	✗
Docker Engine	✗	✗

Combined infrastructure

If your organization is running a combined infrastructure, with both Windows Servers and Linux machines, your organization can use:

Component	Windows Server (Windows Server 2016 or 2019)	Linux machine
Hub	✓	N/A
Docker Desktop	✗	✗
Docker Engine	✗	✓

Generate an SSL Certificate

You need an SSL certificate for the Blue Prism Decision container. Depending on your infrastructure and IT organization security requirements, this could be an internally created SSL certificate or a purchased certificate.



The Blue Prism Decision container requires a client key and a server key to ensure the communication between the Decision plugin in Hub and the Decision container is secure.

Self-signed certificates can be used but are only recommended for POC \ POV \ Dev environments. For production environments, use certificates from your organization's approved certificate authority. It is recommended that you contact your IT Security team to check their requirements. You will need to ensure that your certificate authority provides you with the following files:

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

Self-signed certificate

For POC \ POV \ Dev environments, you can create a certificate using the following process. This process requires OpenSSL to be installed. These instructions are for a Windows Server. If you are using Linux, please make the necessary adjustments.



See the [online version of this guide](#) to check the formatting and line breaks in the scripts used in the steps below.

1. If you do not already have it, install [OpenSSL](#).
2. Create a folder where you will run the script (in the next step) so that the output is generated in a single place.
3. In the folder you created, use one of the following scripts depending on the host operating system ([Windows](#) or [Linux](#)), entering the indicated appropriate values in the variables at the top of the script:

`Enter certificate password` – Replace with a password that will be used to create the certificate.

`Enter CN for client certificate` – Replace with a common name for the client certificate, for example, client.decision.blueprism.com.

`Enter CA` – Replace with the Certificate Authority common name, for example, decisionCA.

`Enter CN for server certificate` – Replace with a common name for the server certificate. This must match with the Decision container fully-qualified domain name (FQDN), for example, decision.blueprism.com. Or, if the container is on the same server as Hub, use, for example, decision.local.

Script for creating certificates in Windows

Run PowerShell as an administrator and use the following script:

```
$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
```

The certificates are generated in the folder you created.

Script for creating certificates in Linux

Run the following Bash script:

```
#!/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 -req -passin pass:$CER_PWD -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
```

The certificates are generated in the folder you created.

4. Add the certificate as a trusted certificate on the local machine by running the following scripts:

```
$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. Give access to the client certificate for IIS users:
 - a. Open Manage Computer Certificates, and locate the client certificate.
 - b. Right-click the certificate, select **All Tasks**, and then **Manage Private Keys....**
 - c. Add **IIS_IUSRS** with the **Read** permission.
 - d. Click **Apply**.



If you are using different machines to host the Blue Prism Decision Model Service container and Blue Prism Hub, you will need to ensure that:

- The Decision Model Service container host has the following files:
 - server.crt
 - server.key
 - ca.crt
- The server running Blue Prism Hub has the following files:
 - client.crt
 - ca.crt

Install the Blue Prism Decision Model Service container

The Blue Prism Decision Model Service container includes the Model Learning API that is used by the Decision plugin. This container must be deployed and running before the Hub installation is carried out as you will need to enter the details into the install wizard.

▶ To watch the Decision Model Service installation process using the container, see our [Blue Prism Decision Model Service installation video](#).

Prerequisites

- A Docker host is required that is capable of running Linux containers.
 - Blue Prism recommends that your production environment uses a Linux server as the host. [Docker Engine](#) is required to run the Decision Model Service container, for more information see the Docker help: [Install Docker Engine](#).
 - For POC or Dev environments, a Windows server can be used. [Docker Desktop](#) is required to run the Decision Model Service container, for more information see the Docker help: [Install Docker Desktop on Windows](#).
- 500 MB of disk space for the container.


Installation steps

1. Open the Decision Model Service container page on [DockerHub](#).
2. Copy the pull command from the container page and run it in the command line. For example:

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

Where **<version>** matches the version number shown on the Tags tab on DockerHub.

3. Set the container running using the following command:

 The command must be on a single line – see the [online version of this 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>
```

Where:

<Absolute path of certificate location> is replaced with the full path of the certificate created in [Generate an SSL Certificate on page 7](#).

<version> is replaced with the version number of the Decision Model Service container.

4. Check the container is running using the following command:


```
docker ps -a
```

Install Blue Prism Hub

You can now run the Hub installer, see [Install Blue Prism Hub](#). On the Blue Prism Decision Setup (Optional) screen, enter the URL of where the Decision container is running followed by the port number. The URL must match the FQDN that was specified in the certificate and point to the Model Service container. The port number must match that was specified when the container was set to run.

The URL should be in the format `https://<FQDN>:<port number>`.

For example, `https://decision.blueprism.com:50051`, or `http://decision.local:50051`.

 If you have already installed Hub 4.5 without Decision, see [Troubleshooting on page 19](#) for information on updating your installation.

Mandatory configuration

Once Hub is installed, you also need to carry out the following configuration on the server.


Decision DNS resolution

Blue Prism applications communicate with each other using their respective machine names. It is therefore necessary to ensure that these can be resolved successfully, and that firewall rules allow appropriate communication on the defined ports.

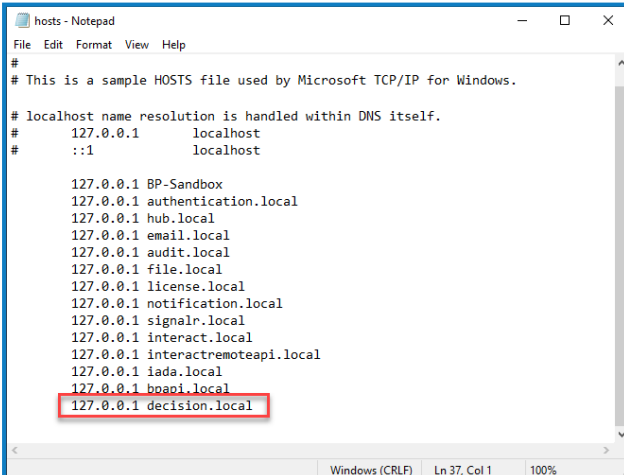
It may be necessary to set up DNS servers, Windows DNS search suffixes or local hosts file to support this.

Enterprise organizations often use formal DNS management utilities, however for tactical or experimental configurations it may be appropriate to use local host files to manipulate DNS.

1. On the Hub web server, open the hosts file using a text editor. The hosts file is typically located in `C:\Windows\System32\drivers\etc`.

 You must be logged in with administrator level access to change this file.

2. Enter the IP address and host name for Decision at the end of the list, for example:



The screenshot shows a Notepad window titled 'hosts - Notepad' with the following content:

```
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# localhost name resolution is handled within DNS itself.
#   127.0.0.1      localhost
#   ::1           localhost

127.0.0.1 BP-Sandbox
127.0.0.1 authentication.local
127.0.0.1 hub.local
127.0.0.1 email.local
127.0.0.1 audit.local
127.0.0.1 file.local
127.0.0.1 license.local
127.0.0.1 notification.local
127.0.0.1 signalr.local
127.0.0.1 interact.local
127.0.0.1 interactremotepi.local
127.0.0.1 iada.local
127.0.0.1 bpapi.local
127.0.0.1 decision.local
```

The last two lines, `127.0.0.1 bpapi.local` and `127.0.0.1 decision.local`, are highlighted with a red box.

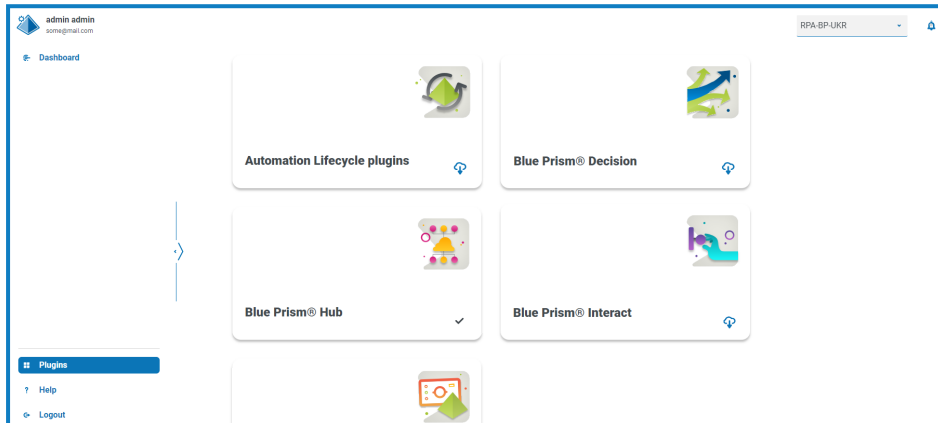
3. Save and exit the text editor.


Install the Decision plugin

The Decision plugin must be installed from the Plugin Repository by a Hub administrator.


▶ To watch the Decision plugin installation and configuration process, see our [Blue Prism Decision plugin video](#).

1. If you are a Hub administrator, log into Hub and click **Plugins** to open the plugin repository.



2. On the **Blue Prism Decision** tile, click the download icon  to initiate the install.
3. When prompted, upload the license file for Decision.

The plugin installs and a message displays informing you that the site is restarting. Once complete, the plugin repository displays and the download icon on the **Blue Prism Decision** tile is replaced with a tick.

 The site restart will affect all users who are logged into Hub. Although this does not take long, it is recommended that this is performed outside normal working hours to minimize disruption.

Configure access to the Decision plugin

The Decision plugin is automatically available to Hub administrators. Users need to be added to a role that provides access to Decision. This access can be given via a new role or added to an existing user role. If a role does not already exist, a new role can be created to grant access to the plugin:

Create role

✕ Save Delete

Role information

Role name *

Decision

Select role type

☒ Hub

☐ Interact

Role description

Role with access to the Decision plugin


Add plugin

Blue Prism Decision ✕

Add user

(test-user) Test User ✕

1. On the Roles and permissions page, click **Create role**.
The Create role section displays.
2. Enter a role name and select **Hub**.
3. If required, enter a description.
4. Select **Blue Prism Decision** from the **Add plugin** drop-down list.
5. Select the users that will be assigned this role from the **Add user** drop-down list. The list only displays Hub users and not Interact users.
6. Click **Save** to create the role and allow access to the specified users.

 Users can be added to and removed from existing roles by selecting the required role on the Roles and permissions page and clicking **Edit**. For more information, see the [Hub user guide](#).

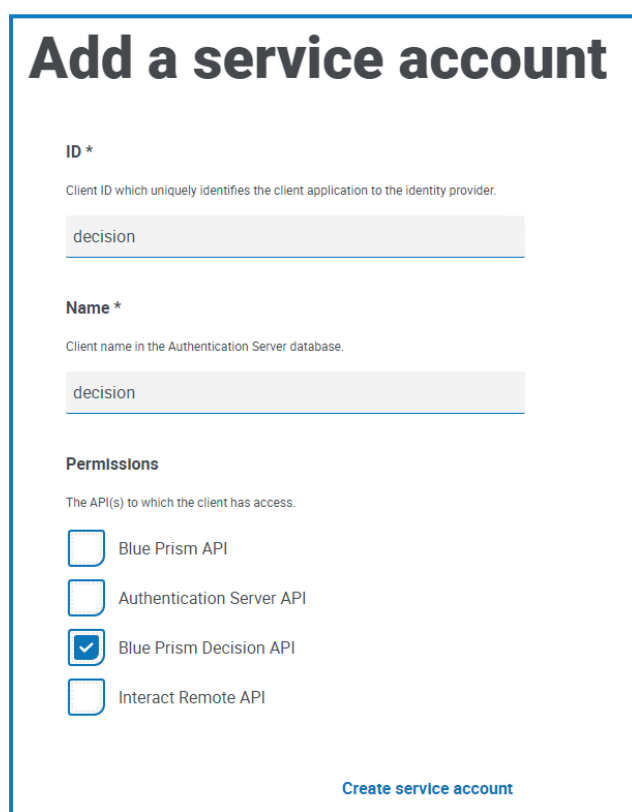
Configure Blue Prism to use Decision

To configure Blue Prism to use your Decision models, you need to:

1. [Set up a service account](#) in Hub and generate a secret key.
2. [Set up the credentials](#) for the Decision service account in Blue Prism.
3. [Import the Blue Prism Decision API Release VBO](#) to communicate with Decision.

Set up a service account

1. In Blue Prism Hub, on the Service accounts page, click **Add account**.
2. Enter a unique ID and a friendly name, for example, *Decision*.
3. Under **Permissions**, select **Blue Prism Decision API**.



The screenshot shows the 'Add a service account' dialog box. It has a title bar at the top. Below the title, there are three sections: 'ID *', 'Name *', and 'Permissions'. Each section has a text input field and a description. The 'ID' field contains 'decision'. The 'Name' field contains 'decision'. The 'Permissions' section has four checkboxes: 'Blue Prism API', 'Authentication Server API', 'Blue Prism Decision API' (which is checked), and 'Interact Remote API'. At the bottom right of the dialog is a button labeled 'Create service account'.

Add a service account

ID *
Client ID which uniquely identifies the client application to the identity provider.
decision

Name *
Client name in the Authentication Server database.
decision

Permissions
The API(s) to which the client has access.

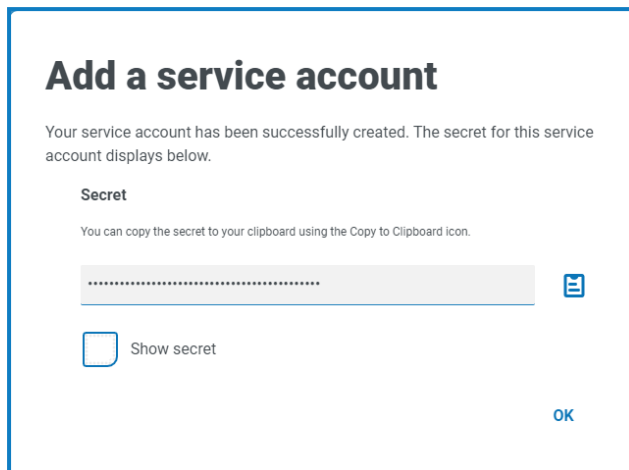
☐ Blue Prism API
☐ Authentication Server API
☒ Blue Prism Decision API
☐ Interact Remote API

Create service account

4. Click **Create service account**.

The Add a service account dialog displays with a generated secret key. You will need to enter this key into the Blue Prism interactive client when configuring the associated credential.

- Copy the generated secret to your clipboard ready to paste into the Blue Prism interactive client.



- Click **OK** to close the dialog.

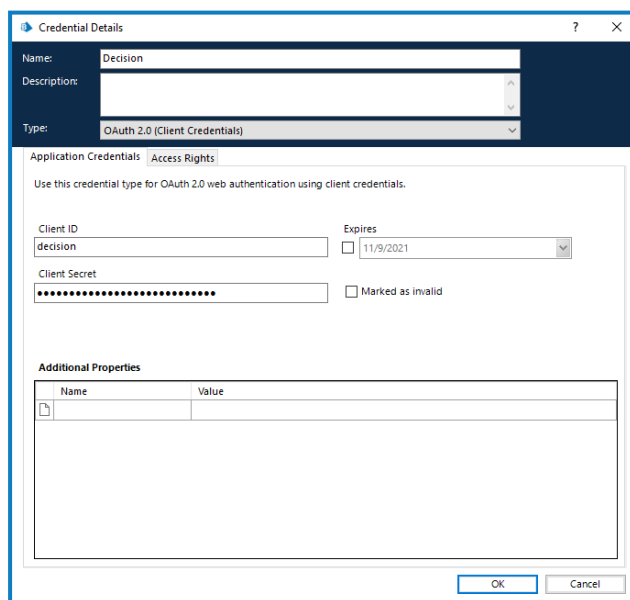
The Service accounts page displays with the newly created account shown.

Set up credentials in Blue Prism

- Log into the Blue Prism interactive client, select **System** and then click **Security > Credentials**. See [Security > Credentials](#) for additional information.
- Click **New**.

The Credential Details dialog displays.

- On the Application Credentials tab of the Credential Details dialog:
 - Enter a name.
 - Change the **Type** to **OAuth 2.0 (Client Credentials)**.
 - In **Client ID**, enter the ID that you used to create the service account above in [Set up a service account on the previous page](#).
 - In **Client Secret**, enter the secret key that was generated for the service account.



4. On the Access Rights tab of the Credential Details dialog, set up the required access permissions.
5. Click **OK**.

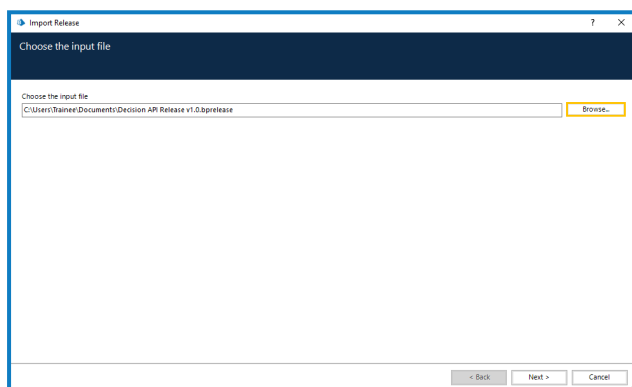
Import the Blue Prism Decision API Release VBO

1. If you haven't already, download the Decision API.bprelease file from the [Blue Prism Portal](#).
2. In Blue Prism, select **File** and click **Import > Release / Skill**.

The Import Release dialog displays.

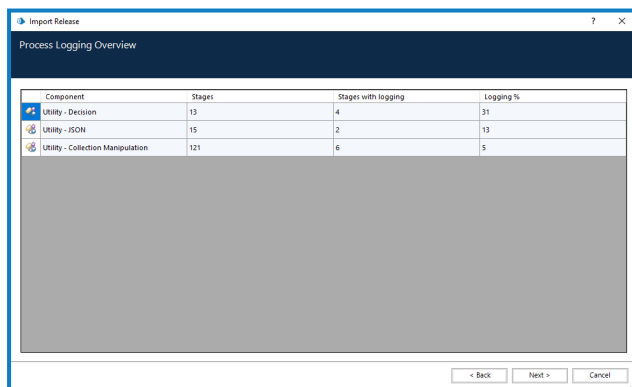
3. Click **Browse**.
4. Locate and select the Decision API.bprelease file.

For example:



5. Click **Next**.

The Process Logging Overview screen displays with a summary of the components that will be imported.



6. Click **Next**.
A progress screen displays.
7. When the import has completed, click **Finish**.
8. In Blue Prism, select **System** and then click **Objects > Web API Services**.
9. Select **DecisionAPI** and click **Edit Service**.

10. On the Web API: DecisionAPI opening screen, in **Base URL**, enter the URL of the Decision API service in the format:

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

For example, `https://hub.blueprism.com:5002/api/blueprism-decision`

Or, if the default port was used, `https://hub.blueprism.com/api/blueprism-decision`.

11. Select **Common Authentication** in the navigation tree, then complete the following:

- a. Ensure that **Authentication Type** is set to **OAuth 2.0 (Client Credentials)**

- b. In **Authorization URI**, enter the Authentication Server URL in the format:

`<Authentication Server URL>:<port if specified during install>/connect/token`

For example, `https://authentication.blueprism.com:5000/connect/token`

Or, if the default port was used,

`https://authentication.blueprism.com/connect/token`.



If you have upgraded from a version earlier than 4.3, your system will still be using IMS. In this case, you should enter the information in the format:

`<IMS URL>:<port if specified>/connect/token`

For example, `https://ims.blueprism.com:5000/connect/token`.

- c. In **Credential**, select the credential you created in [Set up credentials in Blue Prism on page 16](#).


12. Click **OK** to save and complete the setup of the Web API Service.

Troubleshooting

Install Decision in an existing Hub environment


We didn't add Decision when we installed/upgraded Hub to 4.5, but we now want to use it. How do we install it?

You will need to carry out the steps in [Generate an SSL Certificate on page 7](#) and [Install the Blue Prism Decision Model Service container on page 11](#). Then you need to update the Hub appsetting.json file with the Decision connection strings.

 The information below describes updating the Hub appsettings.json file. Caution must be taken to only amend the information provided, any other changes may break your existing system. Changes to the appsettings.json file should be made in conjunction with Blue Prism to ensure your system is supported.


To update the appsetting.json file to include Decision:

1. Open Windows Explorer and navigate to `C:\Program Files (x86)\Blue Prism\Hub\appsettings.json`.


 This is the default install location – adjust this if you have used a custom location.

2. Open the appsettings.json file in a text editor.
3. Locate the following section of the file:

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

 This is not the only setting you will see under `BluePrismDecision`. However, it is the only one that needs to be changed.

- Using the [Blue Prism Data Protector Tool](#) in PowerShell, create and encrypt the connection string for the Decision database, for example:

 The command should be on a single line – see the [online version of this guide](#).

If you want to use SQL Authentication:

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

If you want to use Windows Authentication:

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


Where you replace:

[SQL Server] = The SQL Server that will host the database.

[user name, for example, sqladmin] = The SQL user name (SQL Authentication only)

[password] = The password for the SQL user (SQL Authentication only)

If required, you can enter a different database name for the `Initial Catalog` parameter.
`BluePrismDecisionDB` is the default name.

 The settings above are equivalent to the values you would enter on the Configure Blue Prism Decision SQL connection screen in the Hub Install Wizard.
The Decision database will be created when you install the Decision plugin in Hub.

- Copy the encrypted string between the `""` next to the `ConnectionString` setting in the Hub `appsettings.json` file, shown in [step 3](#).
- Save the file.
- Locate the following section in the same `appsettings.json` file:


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

- Between the `""` next to the `CertificateThumbprint` setting, enter the thumbprint for the SSL certificate.

If you are using Windows, you can find this using Manage Computer Certificates, double-click the Certificate and **Thumbprint** is on the Details tab.

- Between the `""` next to the `v1` setting, enter the URL for the Blue Prism Decision Model Service container.
- Save and close the file.

11. Restart Hub:
 - a. Open Internet Information Services (IIS) Manager.
 - b. In the list of connections, select **Blue Prism - Hub**.

 This is the default site name – if you have used a custom site name, select the appropriate connection.

- c. Click **Restart** from the Manage Website controls.

12. Add Decision to the hosts file. For more information, see [Decision DNS resolution on page 12](#).

The next steps are to complete [Install the Decision plugin on page 13](#) and [Configure access to the Decision plugin on page 14](#). However, before you install the plugin, you will need to temporarily provide dbcreator or sysadmin SQL Server permissions to the login used for the Application Pool Blue Prism – Hub, this login will depend on the option selected when you installed Hub:

- SQL Server Authentication – The SQL user who was specified during the install.
- Windows Authentication – The Windows service account associated with the Application Pool Blue Prism – Hub.

The Decision database is created when the Decision plugin is installed in Hub. After this, the dbcreator or sysadmin permissions can be removed.

OpenSSL script fails

If the OpenSSL script fails, add OpenSSL to Path environment variable and then try running the script again.

1. From the Windows taskbar, open Control Panel.
2. Select **System and Security**, then select **System**, and then click **Advanced system settings**.
The System Properties dialog displays.
3. Click **Environmental variables**.
The Environment Variables dialog displays.
4. In the **System variables** group, select **Path**, and then click **Edit**.
The Edit environment variable dialog displays.
5. Click **New** and on the new line, enter the path to OpenSSL. The default location is C:\Program Files\OpenSSL-Win64\bin.
6. Click **OK** to save the changes.