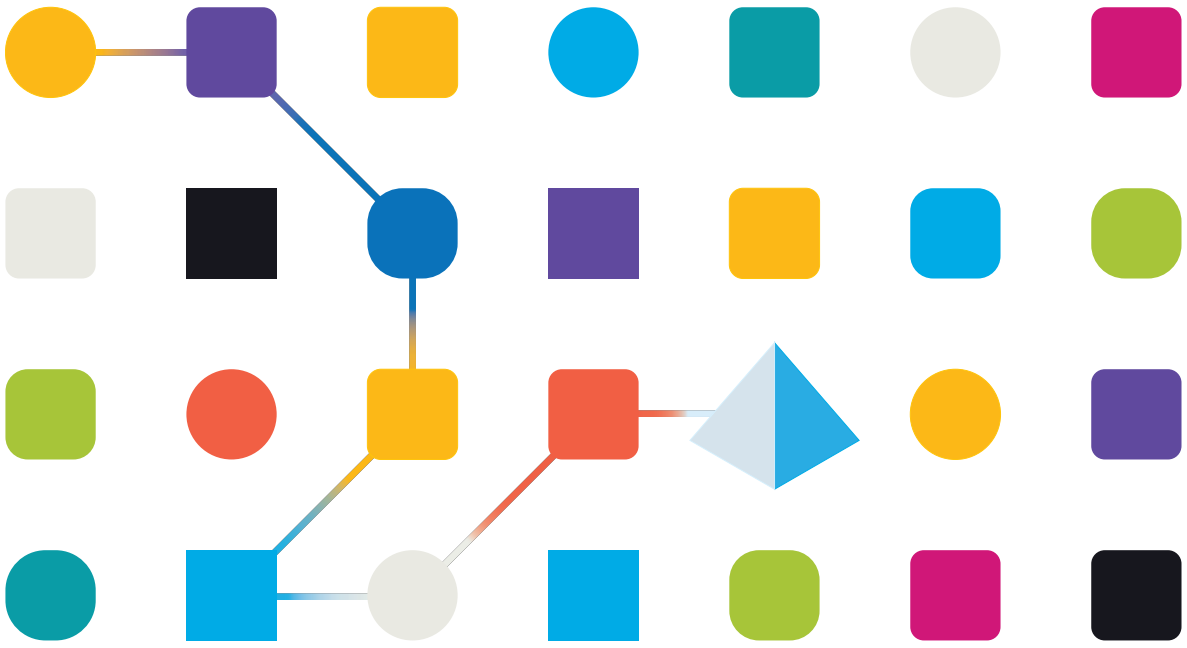
Blue Prism 7.0

Blue Prism API Install Guide

Document Revision: 2.0



Trademarks and Copyright

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

Introduction

The Blue Prism API provides a common interface for components such as Blue Prism Hub to connect with the Blue Prism database. It also provides a series of predefined capabilities that can be used by custom solutions to interact with Blue Prism programmatically using a RESTful API, such as:

- Access to monitoring data such as sessions, work queues, and schedule information.
- Schedule management control.
- Adding items to Blue Prism work queues ready for processing by your digital workforce.

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.

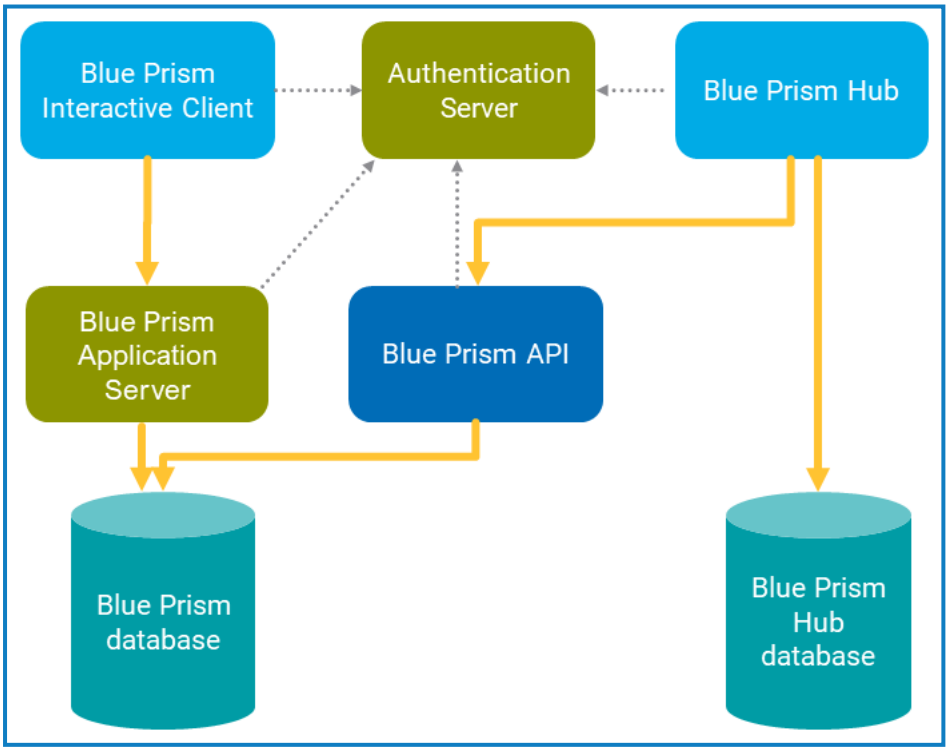
Typical deployment

The Blue Prism API must be installed to use the browser-based Control Room plugin, available in Blue Prism Hub 4.3 and later.

The API must be installed on an IIS enabled server which should have a low latency connection to the Blue Prism database.

Only one instance of the Blue Prism API can be installed and hosted on the same server.

> It is recommended that the Blue Prism API is installed on its own server. Whilst is is possible for it co-exist with other Blue Prism server components where IIS is enabled, this will increase the surface area of the device, and is therefore not recommended in production environments.



Blue Prism API prerequisites

Minimum hardware requirements

See Blue Prism software and hardware requirements for details of the minimum requirements for the web server onto which the Blue Prism API will be installed.

Web server IIS configuration

The following configuration must be applied to the web server that will host the API. This can be configured using the provided PowerShell script.

> It is recommended that the Blue Prism API is installed on its own server. Whilst is is possible for it co-exist with other Blue Prism server components where IIS is enabled, this will increase the surface area of the device, and is therefore not recommended in production environments.

Scripted configuration

To configure the web server via a script, run the following command using the PowerShell command prompt:

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

Configure SSL certificates

An SSL certificate will be required on the device(s) where the Blue Prism API will be installed. It will be used to secure the site that is created. The certificate must be present on the machine that hosts the API. Depending on your infrastructure and IT organization security requirements this could be an internally created SSL certificate or a purchased certificate to protect the website. See Generate a self-signed SSL certificate for information on generating a self-signed certificate.

Enable Authentication Server

To enable authentication against the API, your Blue Prism environment must be configured to use Authentication Server, and Authentication Server must be enabled in the Blue Prism interactive client.

- Authentication Server must be installed using the Blue Prism Hub installer (version 4.6 and later), see the Hub installation guide.
- For information on how to configure your Blue Prism environment to use Authentication Server, see the Authentication Server configuration guide.
- The authentication configuration described in this guide is only required when interacting with the Blue Prism API outside of Blue Prism Hub. When using the API to interact with the data that is used in the browser-based Control Room in Hub via the API directly, user authentication is handled by the service account that has access to the Authentication Server API.

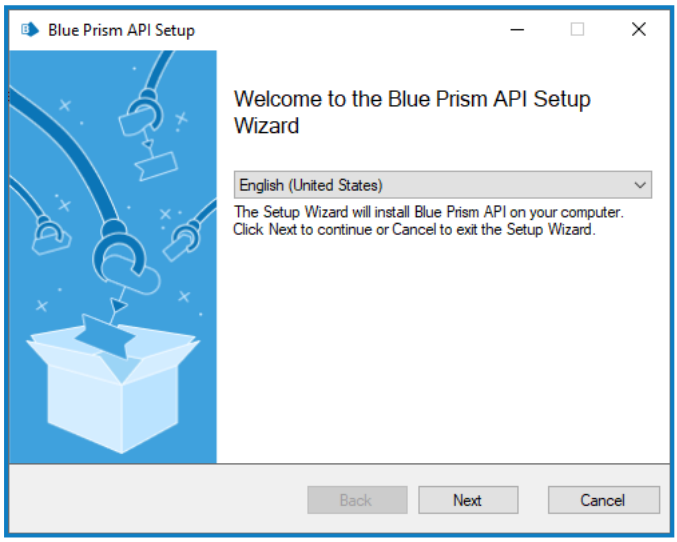
Blue Prism API installation

1. Download the Blue Prism API from the Blue Prism Portal.

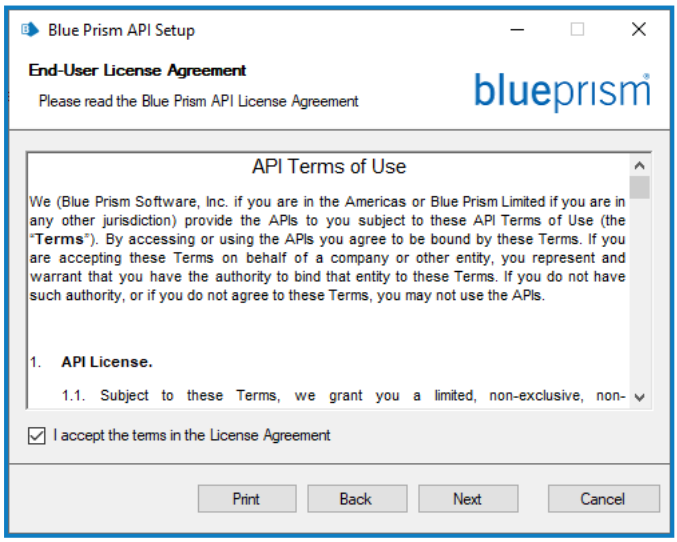
   > The API version must be the same version as the Blue Prism deployment you have installed.

2. Double-click the MSI to start installation.
3. On the Welcome screen, select the language from the drop-down and click **Next** to continue.

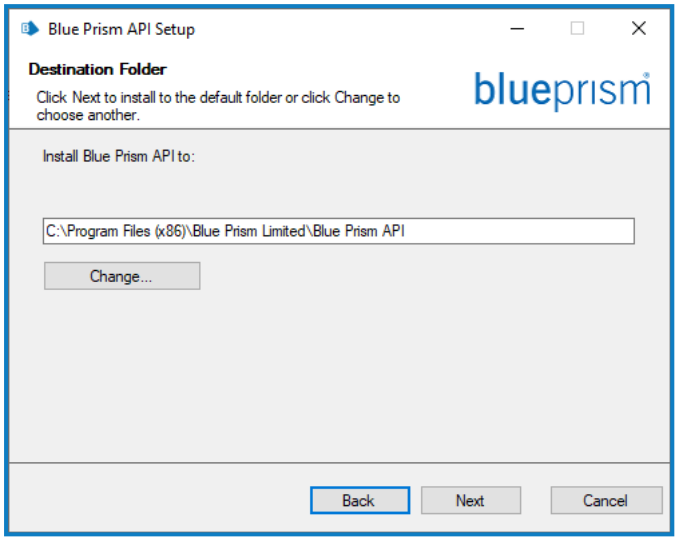
   The installer is available in English (United States), German, French, Spanish (Latin America), Simplified Chinese, and Japanese.



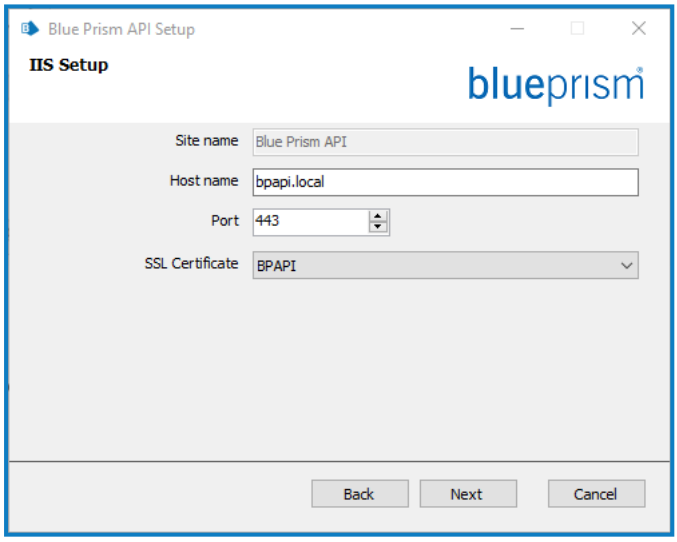
4. Read the End-User License Agreement and if you agree to the terms, select the check box and click **Next** to continue.



5. Specify the destination folder for the installation. The default location is C:\Program Files(x86)\Blue Prism Limited\Blue Prism API, but you can choose another location using the **Change** button. Click **Next** to continue.



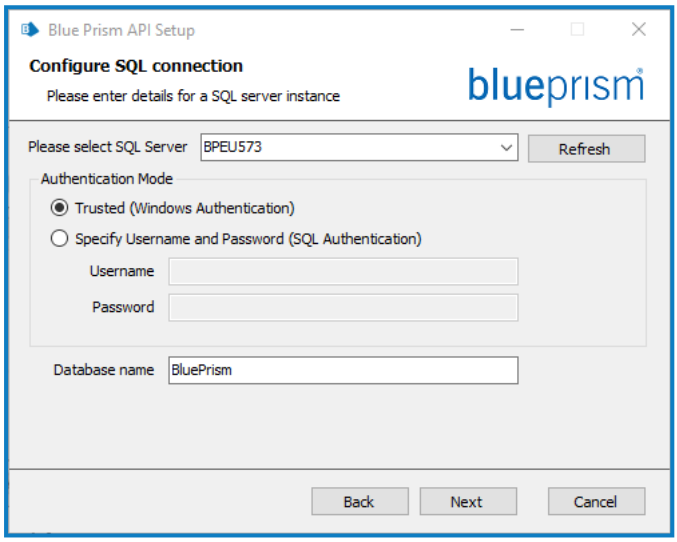
6. On the IIS Setup screen, enter the name under which you would like the API to be hosted, update the port number if required (default port number is 443), and select the certificate from the **SSL Certificate** drop-down list. Click **Next** to continue.



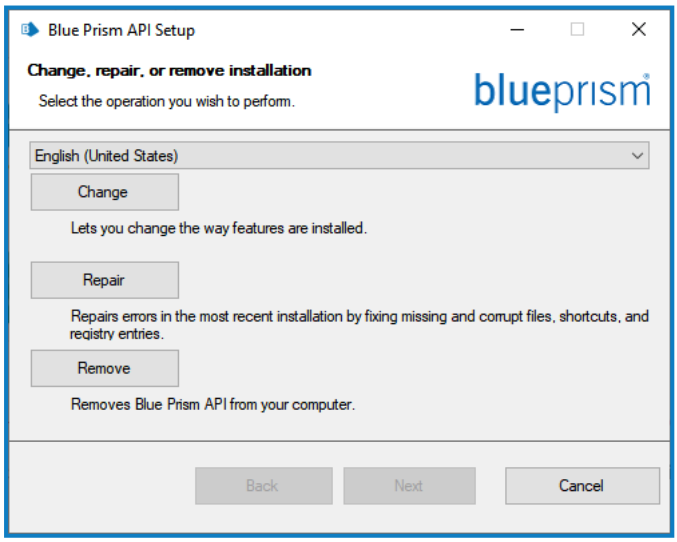
7. On the Configure SQL connection screen, select your authentication mode for the account that the API will use to connect to the Blue Prism database:
   - For Windows Authentication (default), this is the account of the IIS application pool associated with the site.
   - For SQL Authentication, enter the username and password.

   Enter the name of your Blue Prism database and click **Next** to continue.

   > The minimum SQL permissions must be granted to the user that will connect to the Blue Prism database in order for the API to function correctly.

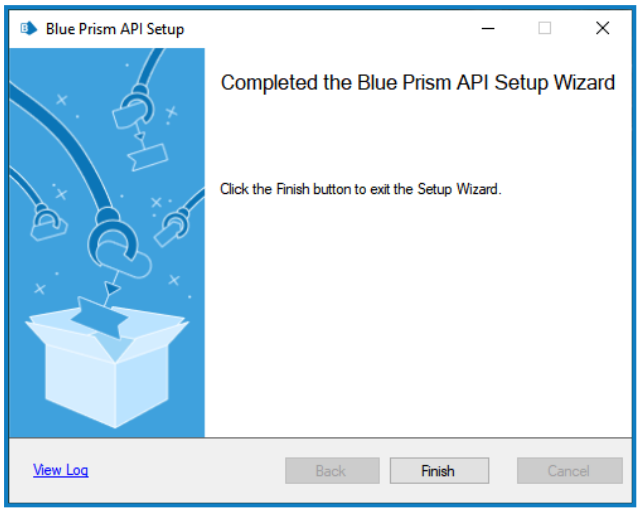


If required, you can amend these details by rerunning the API installer and clicking **Change** in the installation wizard.



8. Once the wizard has completed the installation, click **Finish** to exit the installer.

   If the installation has failed, you need to exit the installer and run the installation wizard again. You can also click **View Log** to check the installation errors.



API configuration

Mandatory configuration

Configure DNS record

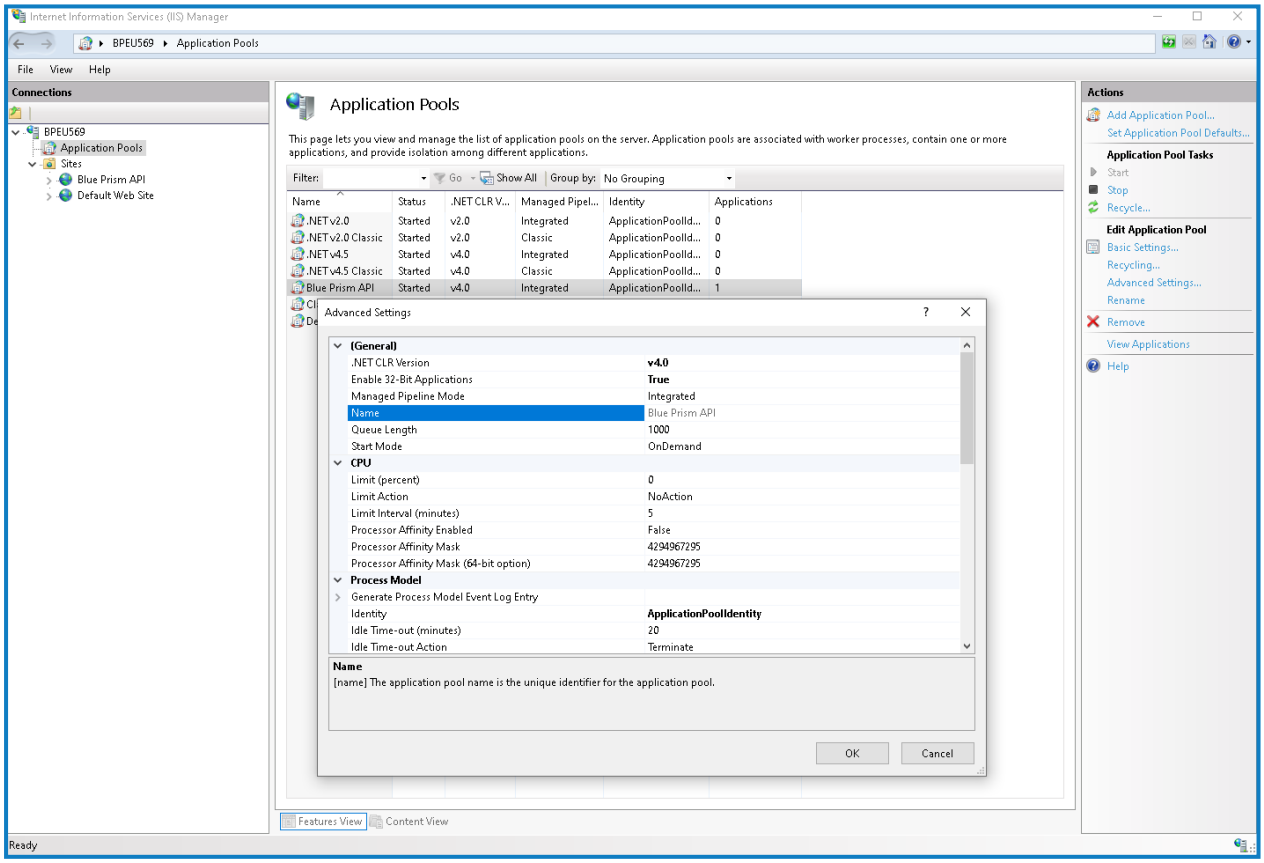
Once the Blue Prism API has been installed, a DNS record needs to be configured to map the API URL to the relevant IP address.

For more details on how to do this, see DNS resolution and Blue Prism network connectivity.

Configure IIS application pool for Windows Authentication access to database

If the account used by the API to communicate with the Blue Prism database uses Windows Authentication, the Blue Prism API application pool in IIS will need to be updated to run as a user with appropriate access to the Blue Prism database. Follow the steps below when using Windows Authentication for the database connection:

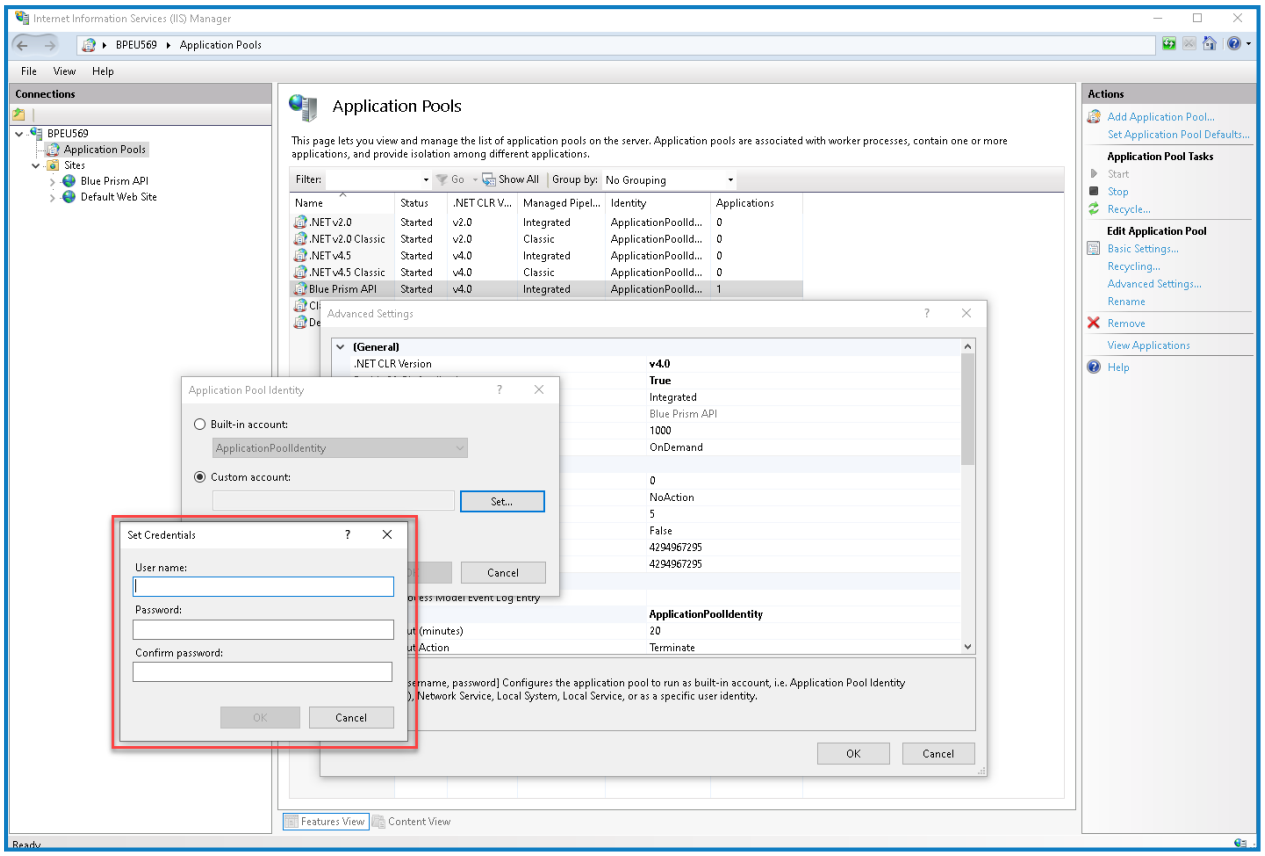
1. Launch the Internet Information Services Manager from the Windows Start menu.
2. In the Connections panel, expand the Application Pools node and select **Blue Prism API**.
3. On the Application Pools page, select **Advanced Settings**.
4. In the Advanced Settings dialog, expand **Process Model** and click the ellipsis (**...**) next to **Application Pool Identity**.



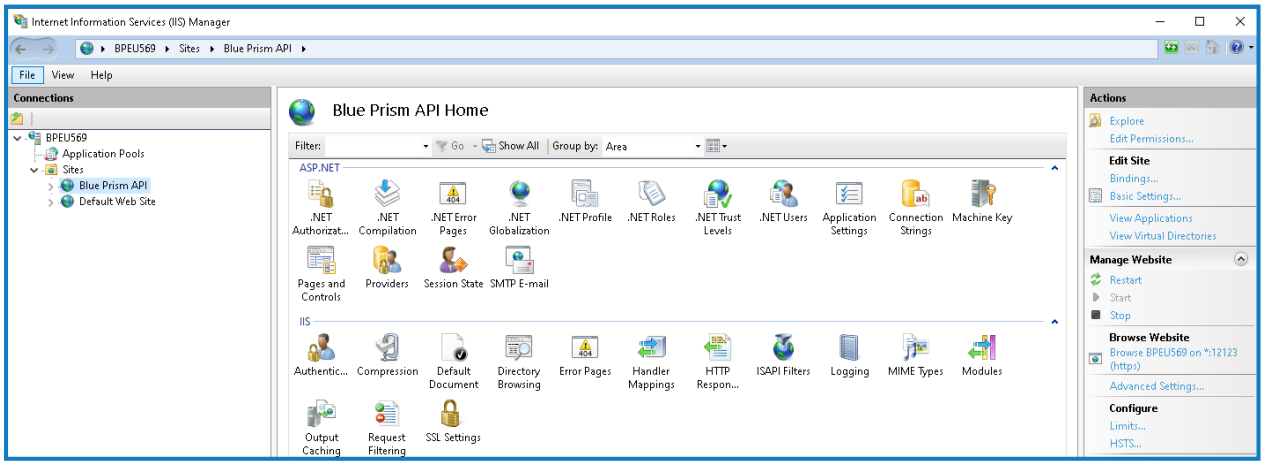
5. In the Application Pool Identity dialog, select the **Custom account** option and click **Set...**.

6. In the Set Credentials dialog, enter the Windows login credentials of a user who has access to the Blue Prism database and click **OK**.

> The database user required to connect to the Blue Prism database must have db_datareader and db_datawriter permissions.



7. In the Connections panel, expand the Sites node and select **Blue Prism API**.
8. In the Actions panel under Manage Website, click **Restart**.

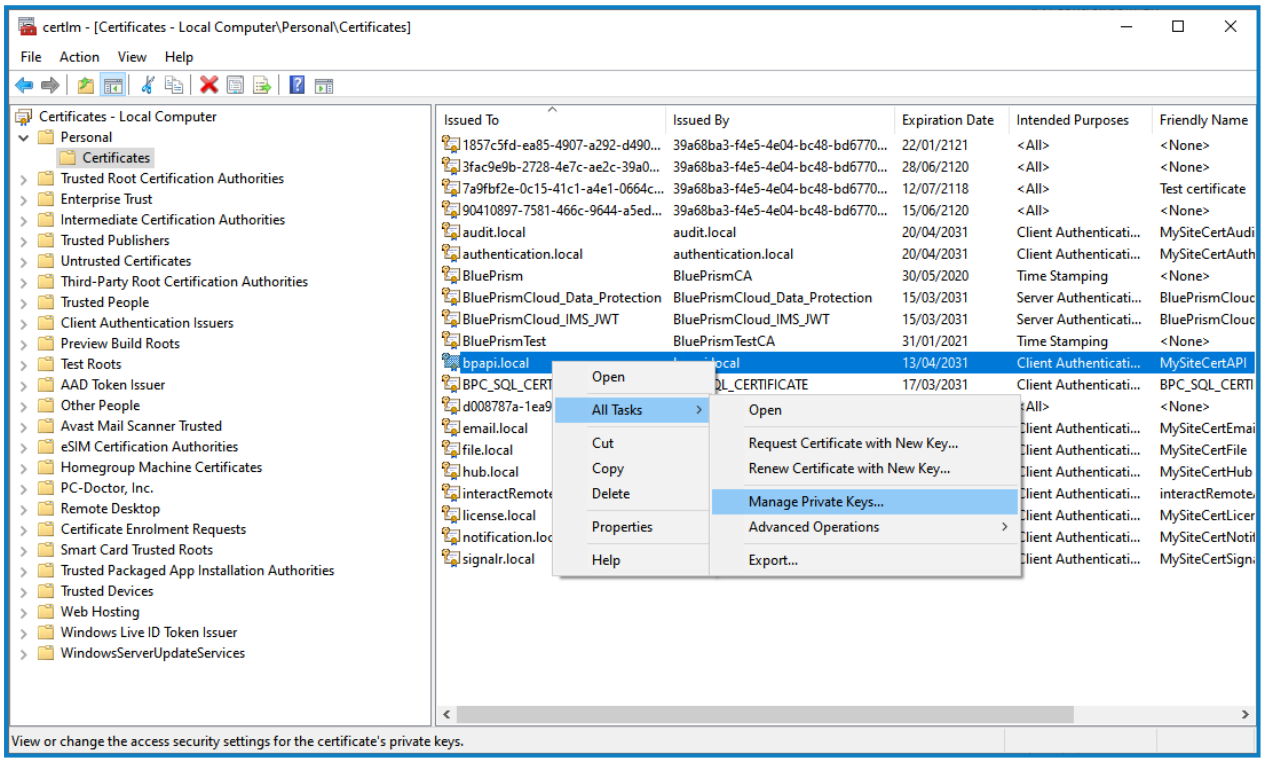


Configure SSL certificate to read private keys

Once an SSL certificate has been generated and associated with the Blue Prism API, the API needs to be able to read the private keys.

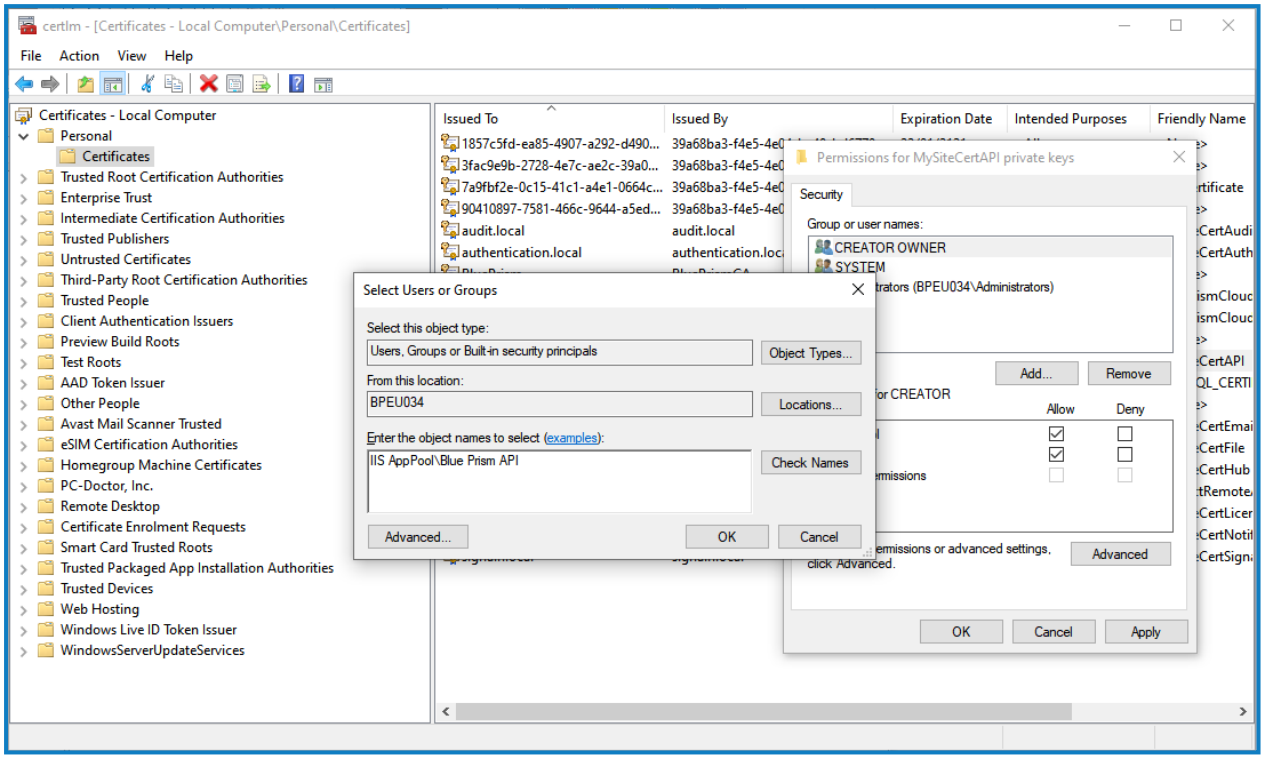
To do this:

1. From the Windows Start menu on your web server, launch Manage computer certificates.
2. Navigate to **Personal** > **Certificates** and locate the Blue Prism API certificate.
3. Right-click the certificate and select **All Tasks** > **Manage Private Keys**.

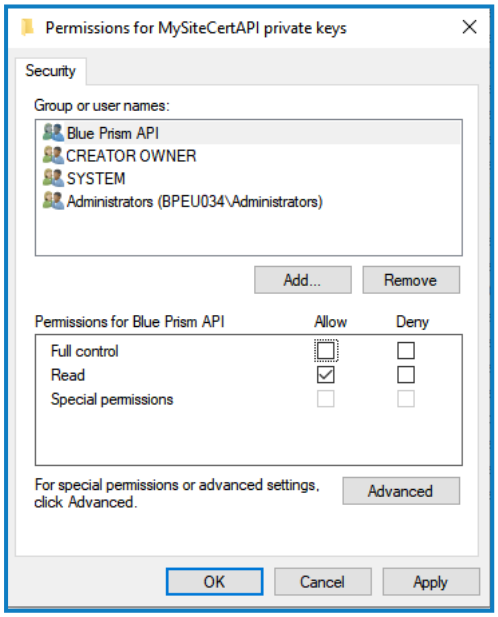


4. In the Permissions dialog, click **Add**.

5. In the Select Users or Groups dialog, enter **IIS AppPool\AppPoolName** where AppPoolName is the name of your Blue Prism API application pool, for example *IIS AppPool\Blue Prism API* (unless changed after the initial install of the API). Click **Check Names**, and then **OK**.



6. In the Permissions dialog, select the **Allow** option for **Read**, and click **Apply**.

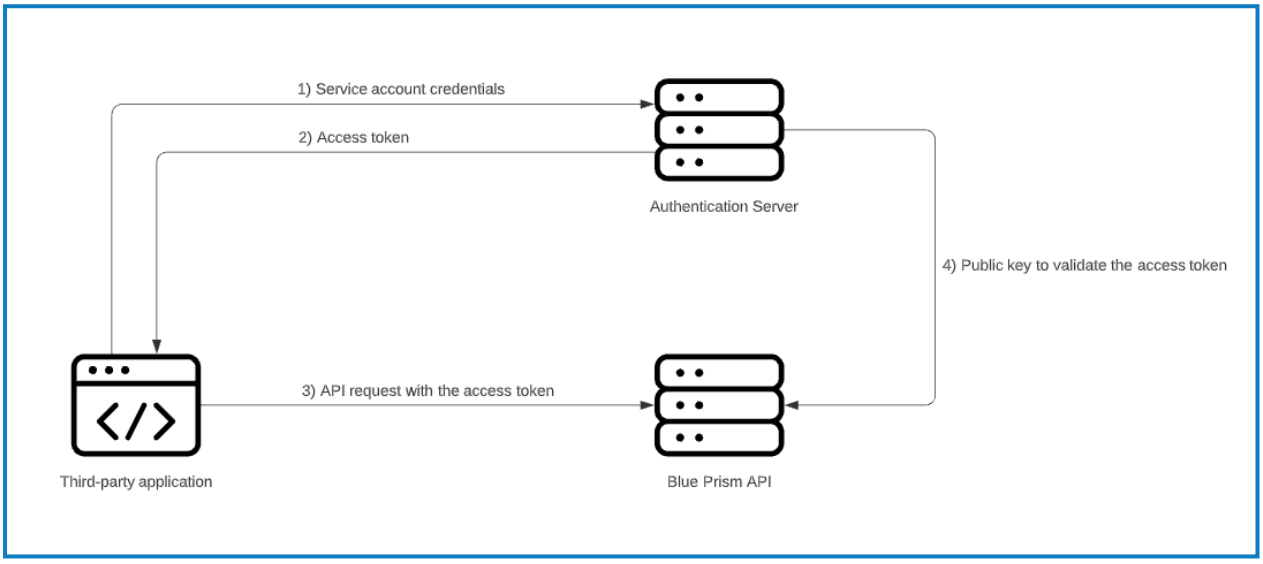


The API is now configured to read the private keys.

Enable authentication against the API

To interact with the Blue Prism API directly, at least one service account with permission to the Blue Prism API must be created in Blue Prism Hub to store the client ID and secret that users must provide to Authentication Server in order to authenticate their requests. Should users require different levels of permissions for interactions with the API, separate service accounts should be created to which the appropriate level of permission can be assigned.

The diagram below illustrates the authentication flow between Authentication Server and the Blue Prism API:

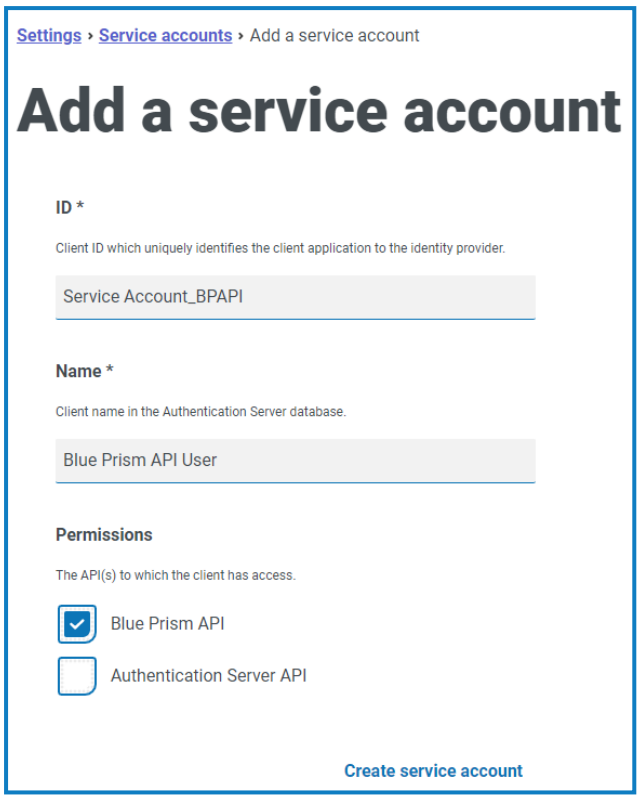


To enable authentication against the Blue Prism API, Authentication Server must be installed via the Blue Prism Hub installer (version 4.6 and later), as well as configured and enabled in your Blue Prism environment. The configuration below is only required when interacting with the Blue Prism API outside of the Control Room plugin in Hub. When using the API to interact with the data that is used in the browser-based Control Room in Hub via the API directly, user authentication is handled by the service account that has access to the Authentication Server API. For more details, see Authentication Server.

The steps below must be completed for each service account that you want to create:

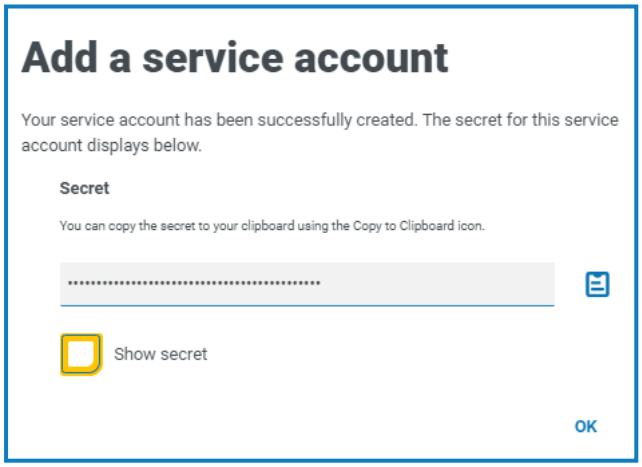
1. In Blue Prism Hub, click your profile icon to open the Settings screen, and under User Management click **Service accounts**.
2. On the Service Accounts screen, click **Add account**.
3. Enter an ID for the client application and a name for the client in the Authentication Server database. Make a note of the client ID for later.

4. Under Permissions, select **Blue Prism API**.



5. Click **Create service account**.

   The Add a service account screen displays with a generated secret.



6. Click the Copy to Clipboard icon to copy the generated secret to your clipboard. This, together with the client ID, will be used by the system used to interact with the API (for example, Swagger or Postman) to make authentication requests to the Authentication Server API.

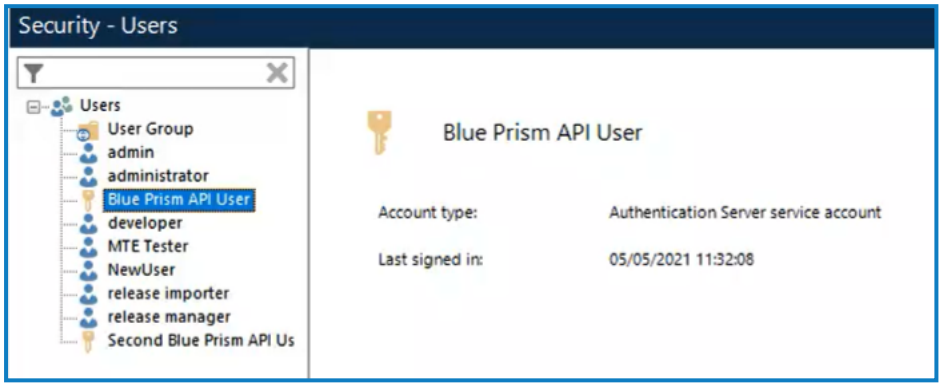
   The Authentication Server API URL that issues authentication tokens for use with the API is:

   https://<authenticationserverhostname>/connect/token, for example https://authentication.local/connect/token

7. In the Blue Prism interactive client, navigate to **System** > **Security - Users**.

   The service account displays under Users.

   > In order for users created in Hub to be synchronized and displayed in your Blue Prism environment, at least one application server in the environment needs to be configured to connect to Authentication Server and be running. For more details, see Authentication Server.



8. Double-click the service account to assign it the roles and permissions required for the actions the connecting user should be able to achieve via the available API.

   A service account's role and permissions can be set up and applied as with any other Blue Prism user account.

9. Navigate to the Authentication Server install directory on the web server that is hosting Authentication Server (for example, C:\Program Files (x86)\Blue Prism\Authentication Server) and open the appsettings.json file.

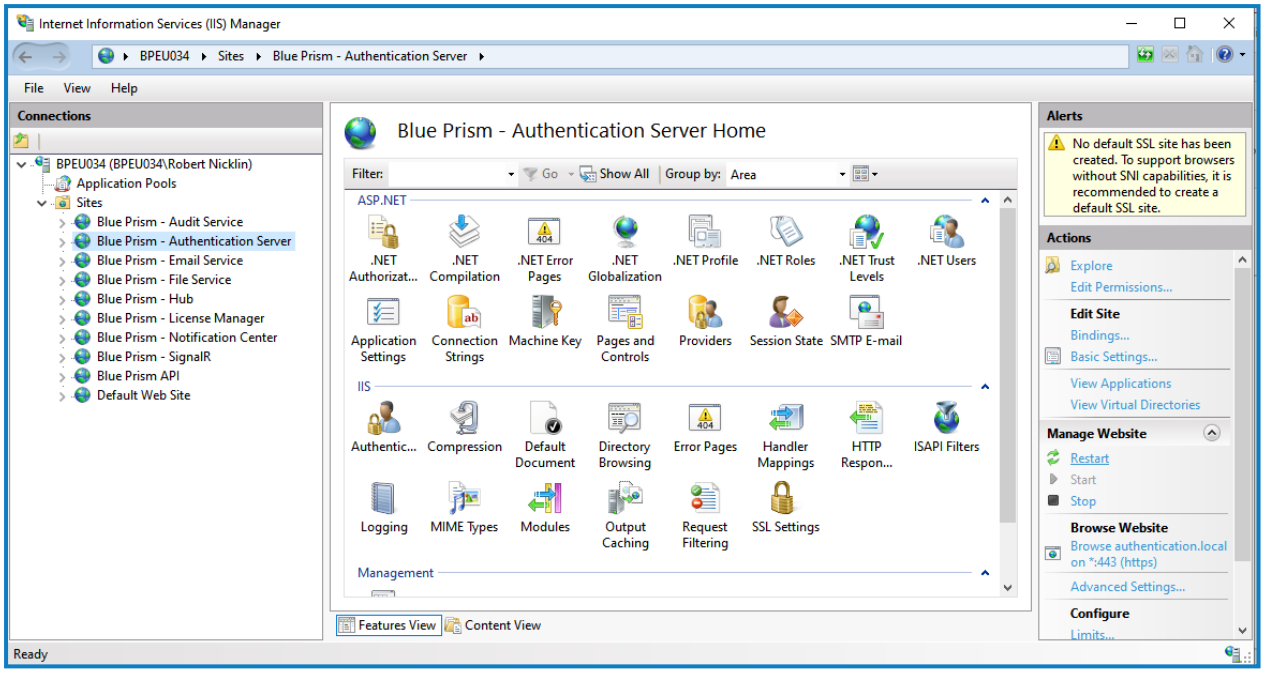
10. In the *AllowedOrigins* section of the file, add the URL of your Blue Prism API install, for example https://BluePrismAPI.local, and save your changes.

    > This step is only required if you are exposing the Blue Prism API externally, either to test in Swagger, or for any other external interface, such as a custom third-party application.

11. Launch the Internet Information Services Manager (IIS) from the Windows Start menu.

12. In the Connections panel, expand the Sites node and select **Blue Prism - Authentication Server**.

13. In the Actions panel under Manage Website, click **Restart**.



> If you have changed the user role associated with the service account as part of this process, it is recommended that you recycle the Blue Prism API application pool to ensure the change is applied immediately.

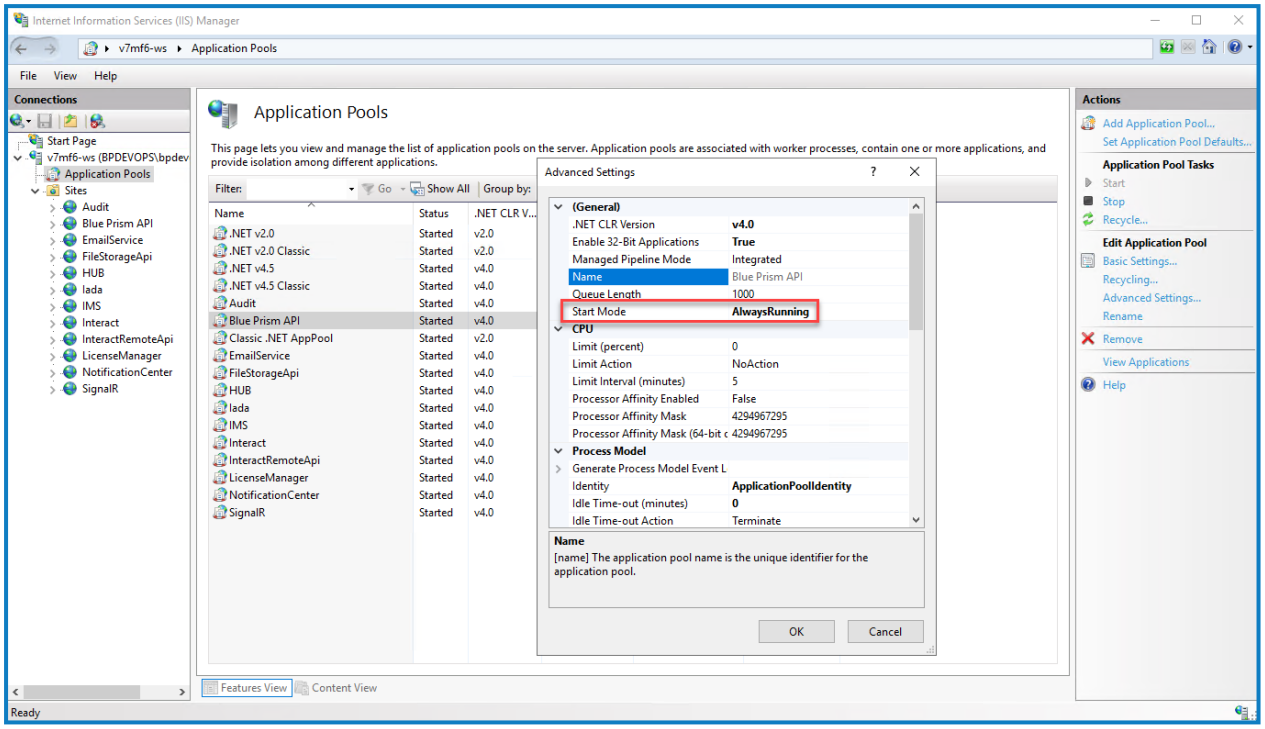
Configure the API to allow automatic cache population for Active Directory domains

Population of the cache that stores the discovered Active Directory domains only occurs when a user makes a request after the Blue Prism API website has started on the server. This could prevent Active Directory users from viewing data as expected in the Hub Control Room. This is due to their account not being authorized in the Blue Prism API, while the Active Directory cache is still being populated in the background.

To prevent this scenario, the Start Mode of the Blue Prism API application pool should be set to **AlwaysRunning** as follows:

1. Launch the Internet Information Services Manager from the Windows Start menu.
2. In the Connections panel, expand the Application Pools node and select **Blue Prism API**.
3. On the Application Pools page, select **Advanced Settings**.

4. In the Advanced Settings dialog, expand **General** and in the Start Mode field select **AlwaysRunning**.



Optional configuration

Make server-based encryption keys available to the Blue Prism API

This configuration is required if you are storing your encryption schemes on the Blue Prism application server and they need to be used by the Blue Prism API.

Add the Blue Prism application server configuration name to the config file for the Blue Prism API

1. Open Windows PowerShell as an administrator and run the following command to decrypt the API web.config file (by default, this is located in C:\Program Files (x86)\Blue Prism Limited\Blue Prism API):

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf "appSettings"
"C:\Program Files (x86)\Blue Prism Limited\Blue Prism API"
```

2. Once decrypted, open the API web.config file in a text editor and in the `<appSettings>` section, find the "BPServerConfigName" key and enter the name of your Blue Prism application server configuration in the value parameter.

> This is the name that is set when configuring the application server. The first time the application server is configured, the configuration name is Default, but this can be changed if required.

```
<configuration>
  <appSettings>
    <clear />
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="DocumentProcessing.ResultQueue.Password" value="" />
    <add key="MaxItemsPerPage" value="1000" />
    <add key="SessionLogs.MaxResultTextLength" value="100" />
    <add key="Authorization.Audience" value="bp-api"/>
    <add key="Swagger.Enable" value="false" />
    <add key="CreateWorkQueueItems.MaxRequestsInBatch" value="100" />
    <add key="CreateWorkQueueItems.MaxStatusLength" value="255" />
    <add key="CreateWorkQueueItems.MaxTagLength" value="255" />
    <add key="ConnectionName" value="CONNECTION_NAME" />
    <add key="ServerName" value="SERVER_NAME" />
    <add key="DatabaseName" value="DATABASE_NAME" />
    <add key="DatabaseUsername" value="DATABASE_USERNAME" />
    <add key="DatabasePassword" value="DATABASE_PASSWORD" />
    <add key="UsesWindowAuth" value="USE_WINDOWS_AUTH" />
    <add key="BPusername" value="BP_USERNAME" />
    <add key="BPpassword" value="BP_PASSWORD" />
    <add key="BPServerConfigName" value="Default"/>
  </appSettings>
```

3. Open Windows PowerShell as an administrator and run the following command to re-encrypt the API web.config file:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef "appSettings"
"C:\Program Files (x86)\Blue Prism Limited\Blue Prism API"
```

The next steps depend on whether the Blue Prism API and Blue Prism application server are running on the same machine or not:

- The Blue Prism API and Blue Prism application server are running on the same machine
- The Blue Prism API and Blue Prism application server are running on different machines

The Blue Prism API and Blue Prism application server are running on the same machine

1. Grant read permission on the Automate.config file to the user that the Blue Prism API application pool is running under:
    a. Locate the Automate.config file (C:\ProgramData\Blue Prism Limited\Automate V3), right-click the file and select **Properties**.
    b. On the Security tab, click **Edit**.
    c. In the Permissions dialog, click **Add**.
    d. In the Select Users or Groups dialog, enter the identity the application pool is running under, for example, if running the application pool under the application pool identity enter *IIS AppPool\AppPoolName*. The *AppPoolName* is the name of your Blue Prism API application pool, for example *IIS AppPool\Blue Prism API* (unless changed after the initial install of the API).
    e. Click **Check Names** and then **OK**.
    f. In the Permissions dialog, select the **Read** option and click **Apply**.
2. If storing encryption keys in external BPK files, grant read permission to these files to the user that the Blue Prism API application pool is running under:
    a. Browse to the location of the encryption keys, right-click the BPK file and select **Properties**.
    b. On the Security tab, click **Edit**.
    c. In the Select Users or Groups dialog, enter the identity the application pool is running under, for example, if running the application pool under the application pool identity enter *IIS AppPool\AppPoolName*. The *AppPoolName* is the name of your Blue Prism API application pool, for example *IIS AppPool\Blue Prism API* (unless changed after the initial install of the API).
    d. Click **Check Names** and then **OK**.
    e. In the Permissions dialog, select the **Read** option and click **Apply**.

3. If the Automate.config file is certificate encrypted, grant read access to the private keys of the encrypting certificate to the user that the Blue Prism API application pool is running under:
    a. From the Windows Start menu on your web server, launch Manage computer certificates.
    b. Navigate to **Personal** > **Certificates** and locate the Blue Prism API certificate.
    c. Right-click the certificate and select **All Tasks** > **Manage Private Keys**.
    d. In the Permissions dialog, click **Add**.
    e. In the Select Users or Groups dialog, enter the identity the application pool is running under, for example, if running the application pool under the application pool identity enter *IIS AppPool\AppPoolName*. The *AppPoolName* is the name of your Blue Prism API application pool, for example *IIS AppPool\Blue Prism API* (unless changed after the initial install of the API).
    f. Click **Check Names** and then **OK**.
    g. In the Permissions dialog, select the **Read** option and click **Apply**.
    h. In the Internet Information Services (IIS) Manager, right-click the Blue Prism API application pool and select **Recycle**.

    The API is now configured to read the private keys.

    Alternatively, you can apply the permission to the folder which contains the files.

The Blue Prism API and Blue Prism application server are running on different machines

1. Copy the Automate.config file from the machine on which the Blue Prism application server is installed and configured to the following location %PROGRAMDATA%\Blue Prism Limited\Automate V3 on the machine on which the API is running.
2. Grant read permission on this copy of the Automate.config file to the user that the Blue Prism API application pool is running under, as outlined above.
3. If storing encryption keys in external BPK files, copy the BPK files from the Blue Prism Server machine to the same location on the machine on which the API is running.
4. Grant read permission on these copied BPK files to the user that the Blue Prism API application pool is running under, as outlined above.
5. If your Automate.config file is certificate encrypted, export the encryption certificate from the machine on which the Blue Prism application server is running, and import it onto the machine on which the API is running.

    To export the encrypted certificate from the Blue Prism application server machine:
    a. Log in as an Administrator.
    b. From a command prompt or the run menu enter "mmc".
    c. Open your Local Computer certificates (click **File** > **Add/Remove Snap-in...** > **Certificates** > **Computer account** > **Next** > **Local computer** > **Finish** > **OK**).
    d. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates.**
    e. Right-click the certificate you want to export and select **All Tasks** > **Export** > **Next**.
    f. Select **Yes, export the private key** then **Next**.
    g. Select the **PKCS#12** option.
    h. Select **Include all certificates in the certification path if possible**.

i. Select **Export all extended properties**.
j. Click **Next**.
k. Provide a password for the private key if you are prompted.
l. Give the file a meaningful name, for example as certname.pfx, and save it somewhere safe.

To import the encrypted certificate onto the machine on which the Blue Prism API is running:

a. Copy the file you exported to the machine on which the API is running. The *.pfx file is in PKCS#12 format and includes both the certificate and the private key.
b. From a command prompt or the run menu enter "mmc".
c. Open your Local Computer certificates (click **File** > **Add/Remove Snap-in...** > **Certificates** > **Computer account** > **Next** > **Local computer** > **Finish** > **OK**).
d. Navigate to **Certificates (Local Computer)** > **Personal** > **Certificates.**
e. Right-click the certificate you want to export and select **All Tasks** > **Import** > **Next**.
f. Click **Browse** to select the certificate from the saved location.
g. Click **Next**.
h. Specify the certificate store where you want to place the certificate, and click **Next**.
i. Click **Finish**.

6. Grant read access to the private keys of this imported certificate to the user that the Blue Prism API application pool is running under, as outlined above.

> If any changes are made to the encryption keys on the machine on which the Blue Prism application server is running, you will need to make sure these are copied across to the machine on which the Blue Prism API is running.

7. In the Internet Information Services (IIS) Manager, right-click the Blue Prism API application pool and select **Recycle**.

   The API is now configured to read the private keys.

> If any changes are made to the server encryption schemes that the application server uses, or to the certificate used to encrypt the config file, then you will need to carry out all these steps again.

Enable Swagger UI

To enable interaction with the Blue Prism API, Swagger UI has been included alongside the Blue Prism API install. Swagger UI is disabled by default, and must be enabled should an administrator want users to interact with the Blue Prism API using this tool.

To enable the Swagger UI:

1. Decrypt the API web.config file (located in C:\Program Files (x86)\Blue Prism Limited\Blue Prism API) by running run Windows PowerShell as an administrator and using the following command:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf
"appSettings" "C:\Program Files (x86)\Blue Prism Limited\Blue Prism API"
```

2. Once decrypted, open the API web.config file and change the Swagger.Enable property to `true`. This property is set to `false` by default.

3. Re-encrypt the API web.config file by running Windows Powershell as an administrator and using the following command:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef
"appSettings" "C:\Program Files (x86)\Blue Prism Limited\Blue Prism API"
```

4. Launch the Swagger UI using a link in the format:

   https://[hostname]:[portnumber]/swagger/ui/index, for example https://bpapi.local:443/swagger/ui/index.

Generate a self-signed SSL certificate for non-production environments

> Self-signed certificates can be used but are only recommended for POC \ POV \ Dev environments, and not production environments. It is recommended that you contact your IT Security team for guidance on obtaining an appropriate certificate.

To generate a self-signed certificate:

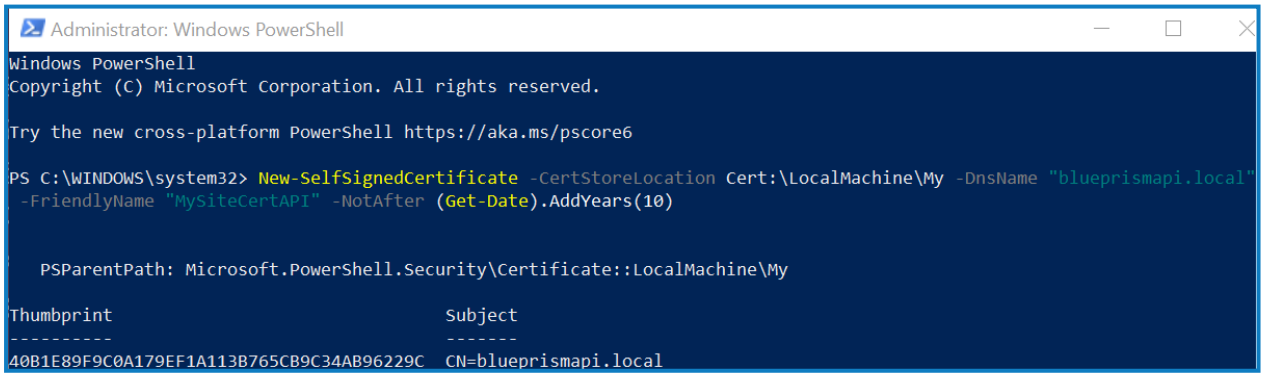
1. Run PowerShell as an administrator on your web server and use the following command, replacing `[Website]` and `[ExpiryYears]` with appropriate values:

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

   For example:

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

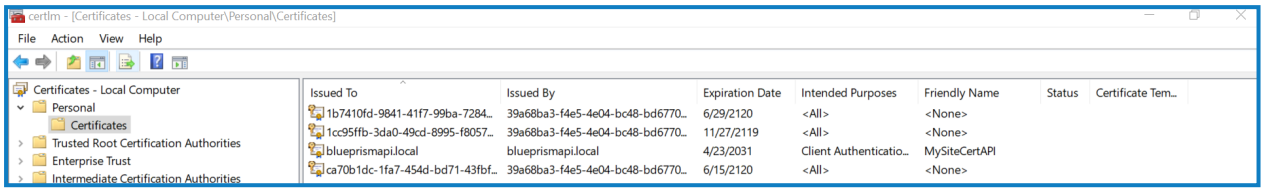
   This example creates a self-signed certificate called *MySiteCertAPI* in the Personal Certificates store, with *blueprismapi.local* as the subject and is valid for 10 years from the point of creation.



2. Open the Manage Computer Certificates application on your web server (type **manage computer** into the search bar).

3. Copy and paste the certificate from Personal > Certificates to Trusted Root Certification > Certificates.

   This is to comply with the requirement for SSL certificates to be trusted when used with a website.



Add the API URL to the Hub database connection

If you want to use the browser-based Control Room plugin in Hub, you must add the API URL to the Hub database connection.

The Blue Prism API powers the browser-based Control Room within Blue Prism Hub. To ensure the Control Room can retrieve information from the environment, the API location needs to be defined within Hub's Environment management. Blue Prism Hub Control Room will then utilize the API to retrieve data and trigger actions initiated through the Control Room. When logged into Hub, you will have the same permission within Control Room as you do in Blue Prism Enterprise.

1. In Blue Prism Hub, click your profile icon to open the Settings page, and under Platform Management click **Environment management**.

   > Only administrator users will have access to this option.

2. On the Environment management page, click the **Edit** icon on the database connection that you would like to update.

   The Edit connection page displays.

3. Enter the **URL** under the **API configuration** section.

   > You must enter the full URL including the protocol, such as, http:// or https://. For example: *https://bpapi.yourdomain.com*

4. Click **Save**.
5. On the Environment management page, click the refresh icon on your updated connection. This updates the information in Hub with the digital workers and queues held in the database.

For more information, see the Hub Environment management guide.

Silent installation and configuration

Downloading and installing any of the Blue Prism® components, including by silent installation via command line, means that you accept the End User License Terms.

The installation and configuration of the Blue Prism API can be scripted using the commands below in PowerShell. To perform a silent installation, you must have administrator access to the web server.

When using the Blue Prism API installer wizard you can validate information that you have entered into text fields by clicking buttons in the wizard. There is no validation when performing a silent install. Entering any incorrect parameters could result in a broken web server. It is recommended that you take a snapshot of the machine as a backup before running the script.

Intended audience

This topic is for IT professionals competent in:

- Editing and running scripts
- Using PowerShell
- Debugging

Prerequisites

All of the prerequisites for a regular Blue Prism API installation are also applicable to a Blue Prism API silent installation. For information on installing the required software, see Blue Prism API prerequisites on page 5.

Blue Prism API silent installation parameters

During the silent install, the following options need to be set:

Component	Description
API_IIS_HOSTNAME	The name under which the API will be hosted.
API_IIS_PORT	The port on which the API will listen for connections.
API_SSL_CERTIFICATE_ID	The thumbprint of the SSL certificate.
API_SQL_SERVER	The hostname of the SQL server hosting the Blue Prism database.
API_SQL_DATABASE_NAME	The name of the Blue Prism database.
API_SQL_AUTH_MODE	SQL authentication mode. 0 - Windows Auth; 1 - SQL Auth. If API_SQL_AUTH_MODE is set to 1 the following details also need to be supplied:

Component	Description
API_SQL_USERNAME	Username to access the Blue Prism database.
API_SQL_PASSWORD	Password to access the Blue Prism database.

If required, you can change the destination folder for the installation using the option INSTALLDIR.

Example script

The following script will:

- Use the BluePrismAPI-7.1.0.msi
- Install the API to D:\BPAPI to listen on bpapi.example.com:4343
- Use the certificate thumbprint E3AEFC6DCB900469E1E6288202B12DA3BD1EDD4D
- Use the RPA database on sql.example.com, with SQL authentication, using the sa account and password SQLP@ssw0rd

```
msiexec /i BluePrismAPI-7.1.0.msi /qn INSTALLDIR='D:\BPAPI' API_IIS_HOSTNAME=bpapi.example.com
API_IIS_PORT=4343 API_SSL_CERTIFICATE_ID=E3AEFC6DCB900469E1E6288202B12DA3BD1EDD4D API_SQL_
SERVER=sql.example.com API_SQL_DATABASE_NAME=RPA API_SQL_AUTH_MODE=1 API_SQL_USERNAME=sa API_SQL_
PASSWORD=SQLP@ssw0rd
```

Blue Prism API configuration scripts

Following the installation of the Blue Prism API, the required configuration of the IIS application pool and the SSL certificate can be carried out with PowerShell. Before running these commands, the WebAdministration module must be loaded in the session with:

```
Import-Module -Name WebAdministration
```

Configure IIS application pool for Windows Authentication access to database

Configure IIS application pool for Windows Authentication access to database with the following command. Replace NAME and PASSWORD with the appropriate values of a user who has access to the Blue Prism database.

```
Set-ItemProperty -Path 'IIS:\AppPools\Blue Prism API\' -Name processModel -Value @
{userName='NAME'; password='PASSWORD'; identityType='SpecificUser'}
```

This command must run as a single line with no breaks.

Configure SSL certificate to read private keys

To configure the certificate, run the following script, replacing THUMBPRINT with the thumbprint of your Blue Prism API certificate:

```
$Cert = Get-Item -Path Cert:\LocalMachine\My\THUMBPRINT
$UniqueName =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey
($Cert).Key.UniqueName
$KeyPath = "$env:PROGRAMDATA\Microsoft\Crypto\Keys\$UniqueName"
$Acl = Get-Acl -Path $KeyPath
$Acl.AddAccessRule([System.Security.AccessControl.FileSystemAccessRule]::new('IIS AppPool\Blue
Prism API', 'Read', 'Allow'))
et-Acl -Path $KeyPath -AclObject $Acl
```