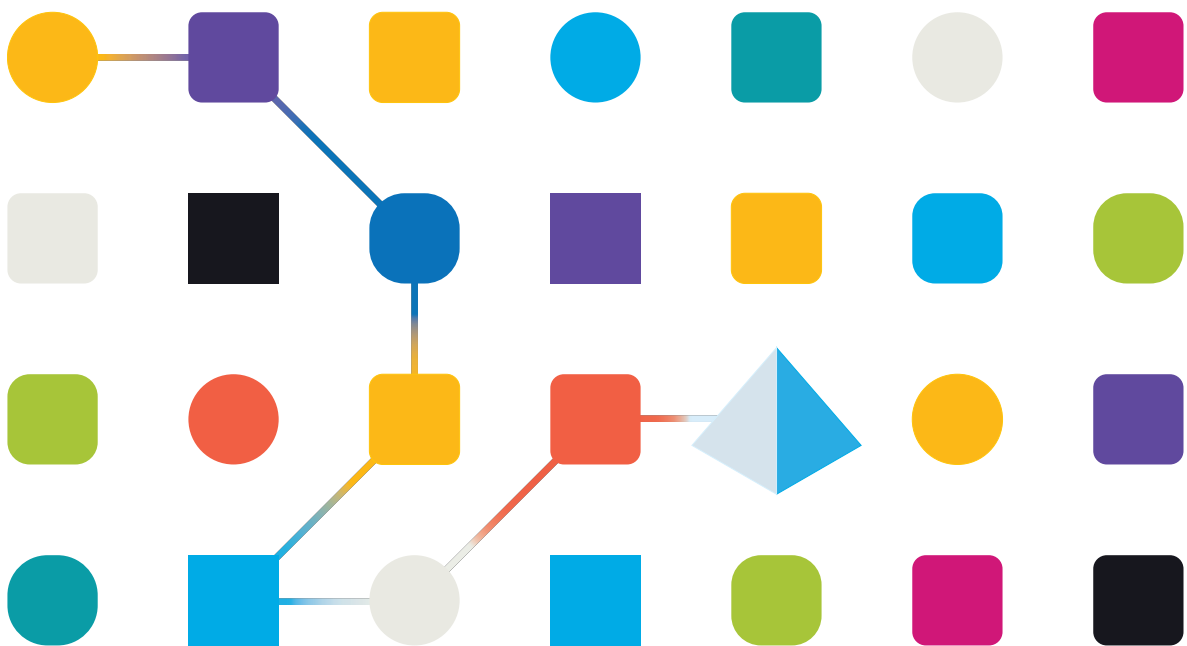




Blue Prism Desktop 1.2

Install and Configure Guide

Document Revision: 1.0



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

- Installing Desktop** 4
 - Intended audience 4
 - Desktop introduction 4
- Desktop installation overview** 5
 - Components required for Desktop 5
 - Desktop architecture 6
- Upgrade Desktop** 7
 - Upgrade a Desktop environment to 1.2 7
- Install and configure the Blue Prism Digital Worker API** 8
 - Prerequisites 8
 - Minimum hardware requirements 8
 - Web server IIS configuration 8
 - Configure SSL certificates 9
 - Enable Authentication Server 9
 - Install the Digital Worker API 10
 - Configure DNS record 14
 - Configure IIS application pool for Windows Authentication access to database 14
 - Configure IIS application pool for high usage (optional) 17
- Install and connect the Desktop client** 19
 - Prerequisites 19
 - Install the Desktop client 20
 - Configure a Desktop client connection 23
- Desktop silent installation and configuration** 30
 - Intended audience 30
 - Prerequisites 30
 - Desktop client silent installation commands 30
 - Digital Worker API silent installation parameters 30
 - Digital Worker API configuration scripts 31

Installing Desktop

This guide provides instructions on how to install and configure SS&C | Blue Prism® Desktop.

If you require further assistance while following this document please contact your Blue Prism Account Manager or Technical Support - support@blueprism.com.

Intended audience

This guide is aimed at IT professionals with experience in configuring and managing networks, servers, and databases. The environment configuration and installation process requires familiarity with installing and configuring web servers and databases. However, the installation of the Desktop client onto individual users' machines does not require specialized knowledge and can be carried out by a Desktop user, if required and depending on your organization's policy.

Desktop introduction

For processes that require human intervention, Blue Prism automations can be initiated in real time by Desktop users, from their computer, using their own credentials. Desktop enables users to run centrally-developed and validated processes with the added confidence that they are centrally managed and have been developed in full compliance with their organization's IT and security standards. As a result, organizations are assured that auditability and data governance are not compromised.

Desktop installation overview


The current version of Desktop requires the following components to be installed. This environment will be then accessed from user's computers via the Desktop client. Desktop client users only need the Desktop client to be installed on their machine locally. They then need to be given remote access to an environment that has all of the other listed components installed.

Components required for Desktop


- [SS&C | Blue Prism Desktop client 1.2](#) – The Desktop client is installed locally on each Desktop user's computer and is used to run processes in real time.

Desktop client users only need the Desktop client to be installed on their machine locally. They then need to be given remote access to an environment that has all of the following components installed:

- [SS&C | Blue Prism Enterprise Edition version 7.3](#) – Your Desktop license gives you access to the Desktop-specific functionality available in Blue Prism.

 Desktop and Enterprise licenses can be applied to the same Blue Prism database. A separate Desktop environment is not required.

- [SS&C | Blue Prism API version 7.3](#) – The API provides an interface for Desktop to connect with the Blue Prism database. It also provides a series of predefined capabilities that are used to interact with Blue Prism programmatically using a RESTful API.

 The Blue Prism API needs to be installed in your Desktop environment, however, there is no recommended order in which the APIs need to be installed.


- [SS&C | Blue Prism Hub version 4.7](#) – Hub deploys Authentication Server. Authentication Server provides a centralized, common authentication method for users across key Blue Prism components, including Desktop.
- [SS&C | Blue Prism Digital Worker API version 7.3](#) – The Blue Prism Digital Worker API provides an interface between Desktop and the Blue Prism database, allowing Desktop to obtain all the information it needs to run automated processes.

Desktop licenses

In addition to the components above, at least one Desktop license must be applied to the Blue Prism database for the system administrator to use the Blue Prism interactive client. This will enable them to use their machine with the Desktop client and its associated Desktop runtime resource.

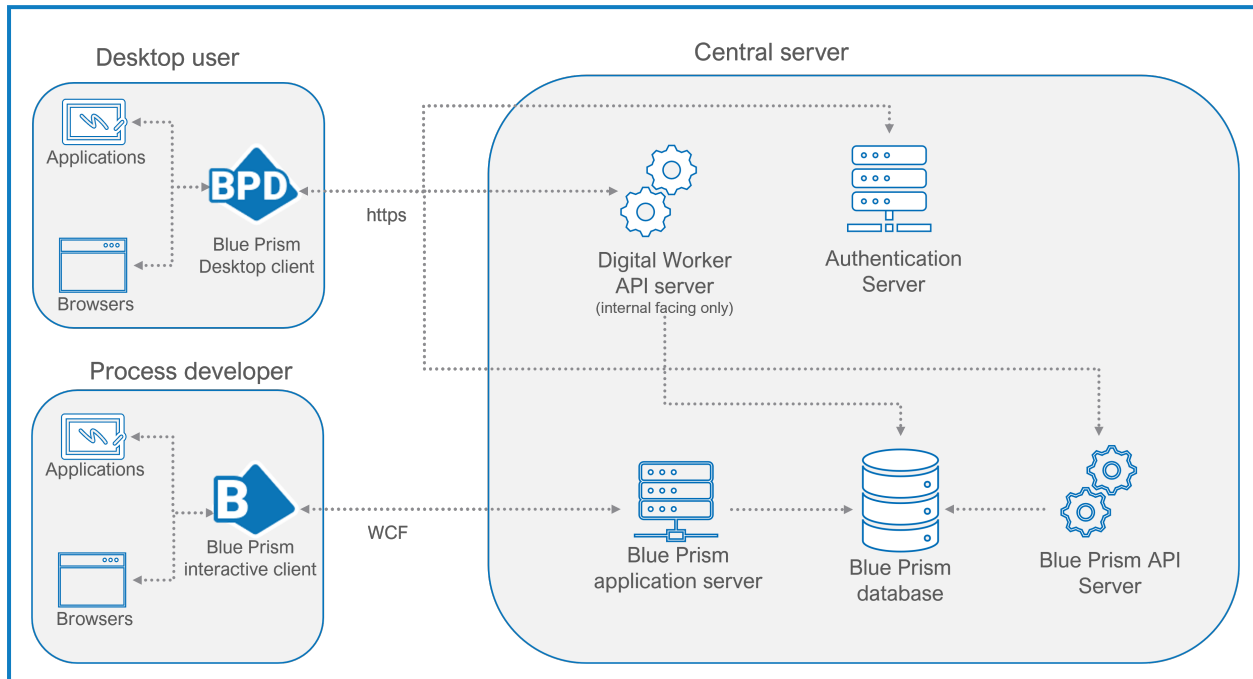
A Desktop license can be imported alongside an Enterprise, NHS, Trial, or Learning license. A separate environment is not required for this version of Desktop (separate environments were required for an earlier version). An environment with a Desktop and a Blue Prism Enterprise license applied to the same database is referred to as a *dual license Blue Prism environment*.

From version 1.2 onwards, as with Blue Prism Enterprise licenses, available Desktop licenses are determined by the number of concurrent sessions that are running. This means that available licenses are consumed on demand by any combination of users. If a user attempts to run a process and the number of available sessions has been reached, a message displays and they are returned to the Library tab.

 The licensing model for Desktop versions 1.0 and 1.1 is unchanged. Existing licenses applied to Desktop version 1.0 or 1.1 will be automatically converted to the new license model when you upgrade to version 1.2 or later, provided the Desktop license period hasn't expired.

Desktop architecture

The following diagram shows the architecture of Desktop deployment.



The *Central server* section of the diagram is intended to depict the components required to work with Desktop, and not that the components need to be installed on the same server. For the deployment requirements for Blue Prism Enterprise, see [Multi-device deployment](#), and for Hub, see [Typical Hub deployment](#).

Client architecture

- **Desktop client** – Needs to be installed on the computer of every user who will be using the Desktop client. The single installer includes:
 - The Desktop runtime resource
 - The Desktop user interface.
- **Blue Prism interactive client** – Required for process development and Control Room functionality. This is a standard installation of Blue Prism Enterprise. Any Desktop-specific functionality is controlled by the application of a Desktop license.

Server architecture

As described in [Install and configure the Digital Worker API](#), the Desktop environment requires a number of Blue Prism components to be installed. Please refer to the relevant installation instructions for the each component for details of how to install and configure them for your Desktop environment.

Digital Worker API

The following conditions apply to the Digital Worker API:

- It must be installed on an IIS-enabled server, which should have a low latency connection to the Blue Prism database.
- It can be installed on the same server as the Blue Prism API, if required.
- An SSL certificate is required on the device where the Digital Worker API will be installed to secure the site that is created (HTTPS). For more information, see [Configure SSL certificates on page 9](#).

Upgrade Desktop

It is recommended that you schedule the upgrade to take place outside of working hours.

Upgrade a Desktop environment to 1.2

Upgrade all of the components in your Desktop environment in the following order:

- Upgrade to Blue Prism Enterprise version 7.3
- Upgrade to the Blue Prism API version 7.3
- Upgrade to Hub version 4.7
- Upgrade the Digital Worker API 7.3
- Upgrade the Desktop client 1.2

Upgrade to Blue Prism Enterprise version 7.3

For upgrade steps, see [Upgrade Blue Prism](#).

Upgrade to the Blue Prism API version 7.3

Run the Blue Prism API installers, as described in [Blue Prism API installation](#).

Upgrade to Hub version 4.7

The required version of Hub has not changed from Desktop version 1.1, so an upgrade may not be necessary. For upgrade steps, see [Upgrade Hub and Interact](#).

Upgrade the Digital Worker API 7.3

To upgrade the Digital Worker API, perform the installation actions as described in [Install and configure the Blue Prism Digital Worker API on the next page](#). The previous version of the Digital Worker API does not need to be removed prior to upgrade.


Upgrade the Desktop client 1.2

To upgrade the Desktop client:

1. Uninstall the previous version of the Desktop client using **Add or remove programs**.
2. Install the latest version of the Desktop client, see [Install and connect the Desktop client on page 19](#) for details.

Install and configure the Blue Prism Digital Worker API


The Blue Prism Digital Worker API provides an interface between Desktop and the Blue Prism database, allowing Desktop to obtain all the information it needs to run automated processes.

 To watch the Blue Prism Digital Worker API installation, see the [Blue Prism Digital Worker API installation and configuration video](#)

Prerequisites

Ensure the following components, required for Desktop to function, are all installed in your Blue Prism environment prior to installing the Digital Worker API:

- Blue Prism Enterprise Edition
- Hub (includes Authentication Server)
- Blue Prism API

 The Blue Prism API needs to be installed in your Desktop environment, however, there is no recommended order in which the APIs need to be installed.

See [Components required for Desktop on page 5](#) for details.


Minimum hardware requirements

See [Blue Prism software and hardware requirements](#) for details of the minimum requirements for the web server onto which the Digital Worker API will be installed.

Web server IIS configuration

The Digital Worker API must be installed as part of the Desktop installation. The API must be installed on an IIS-enabled server, which should have a low latency connection to the Blue Prism database. The Digital Worker API can be installed on the same server as the Blue Prism API, if required.

If you are installing the Digital Worker API on a separate web server to the Blue Prism API, the following configuration must be applied to the web server that will host the API. If you are installing the Digital Worker API on the same server as the Blue Prism API and have already set up the web server, this step does not need to be repeated. This can be configured using the provided PowerShell script, or manually.

 If required, the Digital Worker API can be installed on the same web server as the Blue Prism API, Hub, and Authentication Server.

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 where the Digital Worker API will be installed. It will be used to secure the site that is created. SAN and Wildcard certificates are supported. The certificate must be present on the machine that hosts the API and should be stored in the Trusted Root certificate store. 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

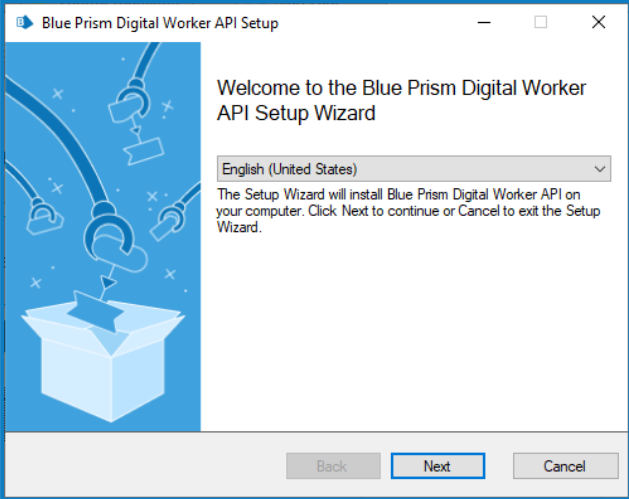
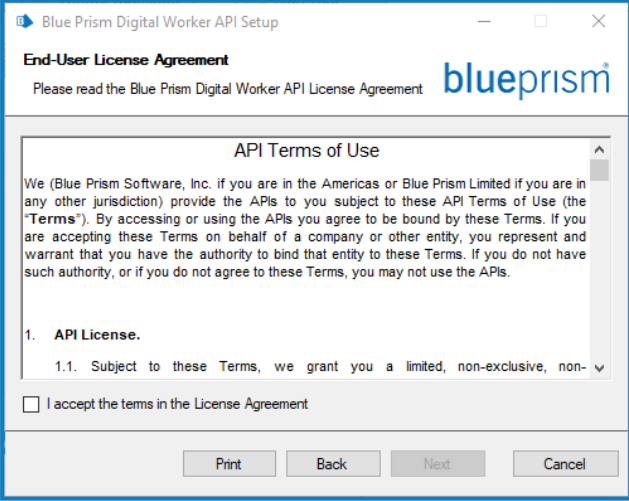
To enable authentication against the API, your Blue Prism environment must be configured to use Authentication Server, and Authentication Server must be enabled in the interactive client.

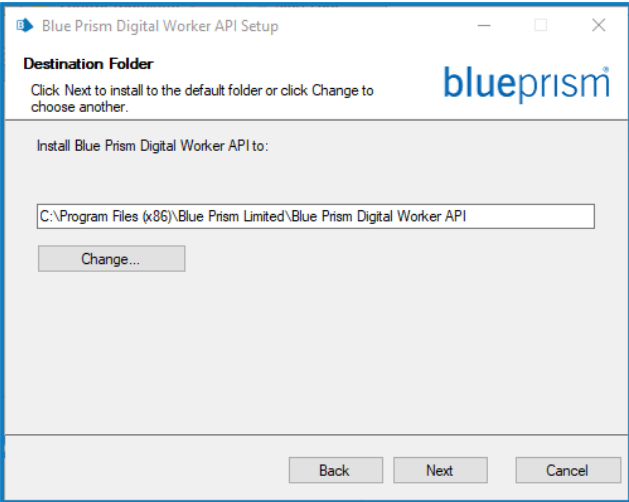
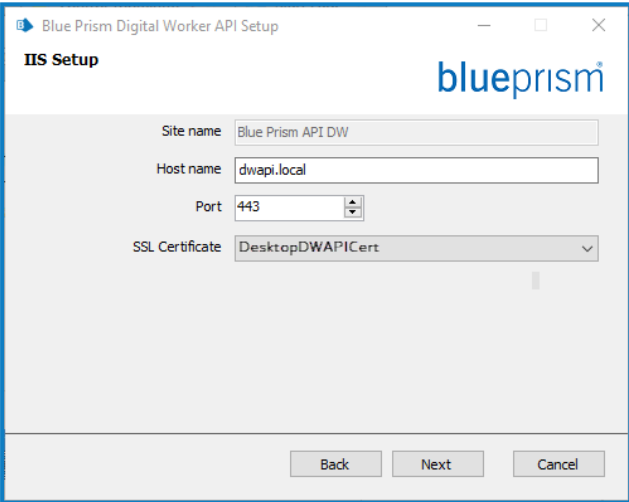

- Authentication Server must be installed using the Hub installer, see the [Hub installation guide](#).
- In addition to the configuration described in the [Hub installation guide](#), an Authentication Server user must be created in Hub first, and then assigned the Desktop User role in Blue Prism. This is done by adding the Authentication Server user to the Desktop Users role via System > Security > User Roles.
- For information on how to configure your Blue Prism environment to use Authentication Server, see the [Authentication Server configuration guide](#).

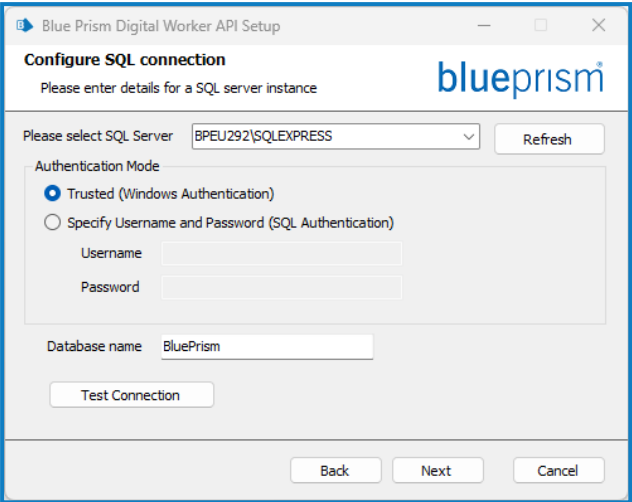


Install the Digital Worker API

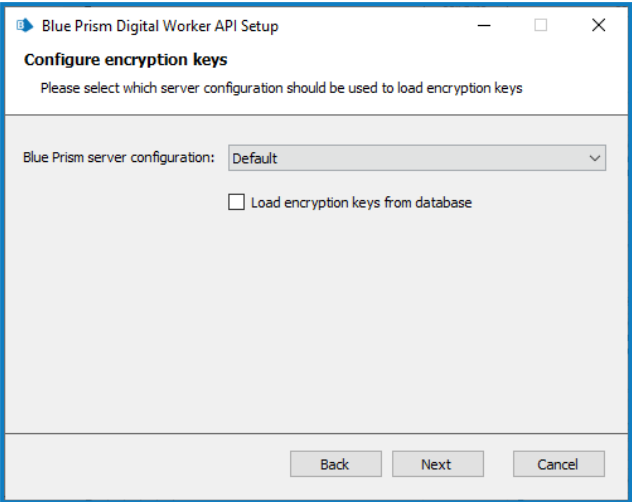

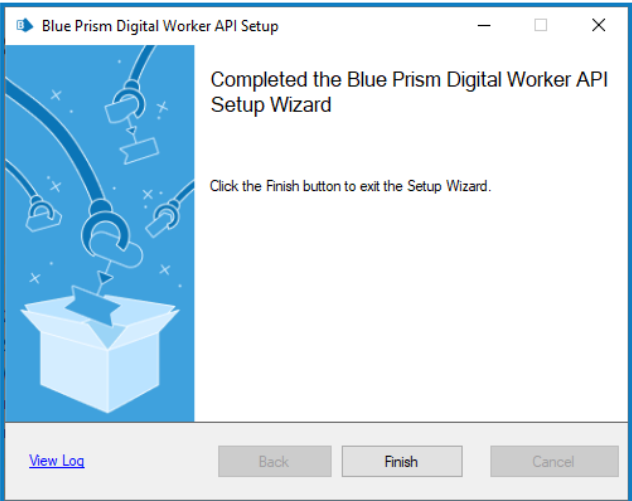
After you have installed Hub, Authentication Server, and Blue Prism Enterprise, you can now install the Digital Worker API.

To install the Digital Worker API, download and run the Blue Prism Digital Worker API installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below. The installer must be run with administrator rights.

Step	Installer screen	Details
<p>1</p>		<p>Welcome</p> <p>If required, select another language for the installer from the drop-down list. The default language is English (United States).</p> <p>Click Next.</p>
<p>2</p>		<p>License agreement</p> <p>Read the End-User License Agreement and if you agree to the terms, select the check box.</p> <p>Click Next.</p>

Step	Installer screen	Details
<p>3</p>		<p>Destination folder</p> <p>Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism\Blue Prism Digital Worker API, but you can choose your own using the Change button.</p> <p>Click Next.</p>
<p>4</p>		<p>IIS Setup</p> <p>Configure the Internet Information Service (IIS) for the Digital Worker API.</p> <ul style="list-style-type: none"> • Site name – This defaults to <i>Blue Prism API DW</i> and cannot be amended. • Host name – Enter the URL of the Digital Worker API website. This URL must also match the site included in the required certificate. • Port – Enter the port number for the machine that you are installing the Digital Worker API onto. The default port number is 443. <div style="border: 1px solid #00a0e3; padding: 5px; margin: 10px 0;"> <p> If the Blue Prism API is installed on the same server and you have already used the default port number, you must enter a different port number here.</p> </div> <ul style="list-style-type: none"> • SSL Certificate – Select the appropriate Secure Sockets Layer (SSL) certificate, issued for the website specified for Host name. <p>Click Next.</p>

Step	Installer screen	Details
<p>5</p>		<p>Configure SQL connection</p> <p>Configure the SQL database connection for the Digital Worker API.</p> <ul style="list-style-type: none"> • SQL Server – Enter the SQL server host name or IP address. <div data-bbox="1023 528 1461 725" style="border: 1px solid #00a0e3; padding: 5px;"> <p> If using a non-standard SQL port, enter the SQL server host name, followed by the port. For example: SQLSERVER1,1434.</p> </div> <ul style="list-style-type: none"> • Authentication Mode – Select your authentication mode for the account that the API will use to connect to the Blue Prism database: <ul style="list-style-type: none"> • For Windows Authentication (default), this is the identity of the IIS application pool associated with the site. • For SQL Authentication, enter the username and password. • Database name – Enter the name of your Blue Prism database. <div data-bbox="983 1267 1461 1503" style="border: 1px solid #00a0e3; padding: 5px;"> <p> The minimum SQL requirements must be granted to the user who will connect to the Blue Prism database in order for the API to function correctly.</p> </div> <p>Click Test Connection to check that a connection can be established with the SQL Server.</p> <p>Click Next.</p>


Step	Installer screen	Details
<p>6</p>		<p>Configure encryption keys</p> <p>Select the location from which to load the encryption keys.</p> <ul style="list-style-type: none"> • Blue Prism server configuration (recommended) – Select an existing Blue Prism server configuration from which to load the encryption keys. <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p> The options available in the drop-down list are taken from the Blue Prism application server configuration. The web server does not need to be able to communicate with a running Blue Prism application server, but the server configuration file must be present on the web server.</p> </div> <ul style="list-style-type: none"> • Load encryption keys from database – Select this option if the encryption keys are stored in the Blue Prism database. This is commonly appropriate for scenarios where no application server is deployed. <p>Click Next to install the Digital Worker API. A progress bar displays during the installation of the API.</p>
<p>7</p>		<p>Installation complete</p> <p>If the installation has completed successfully, click Finish to exit the installer.</p> <p>If the installation fails, click View Log to see the error that was encountered.</p>

Configure DNS record

Once the Digital Worker 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

 This section applies to Windows Authentication only.

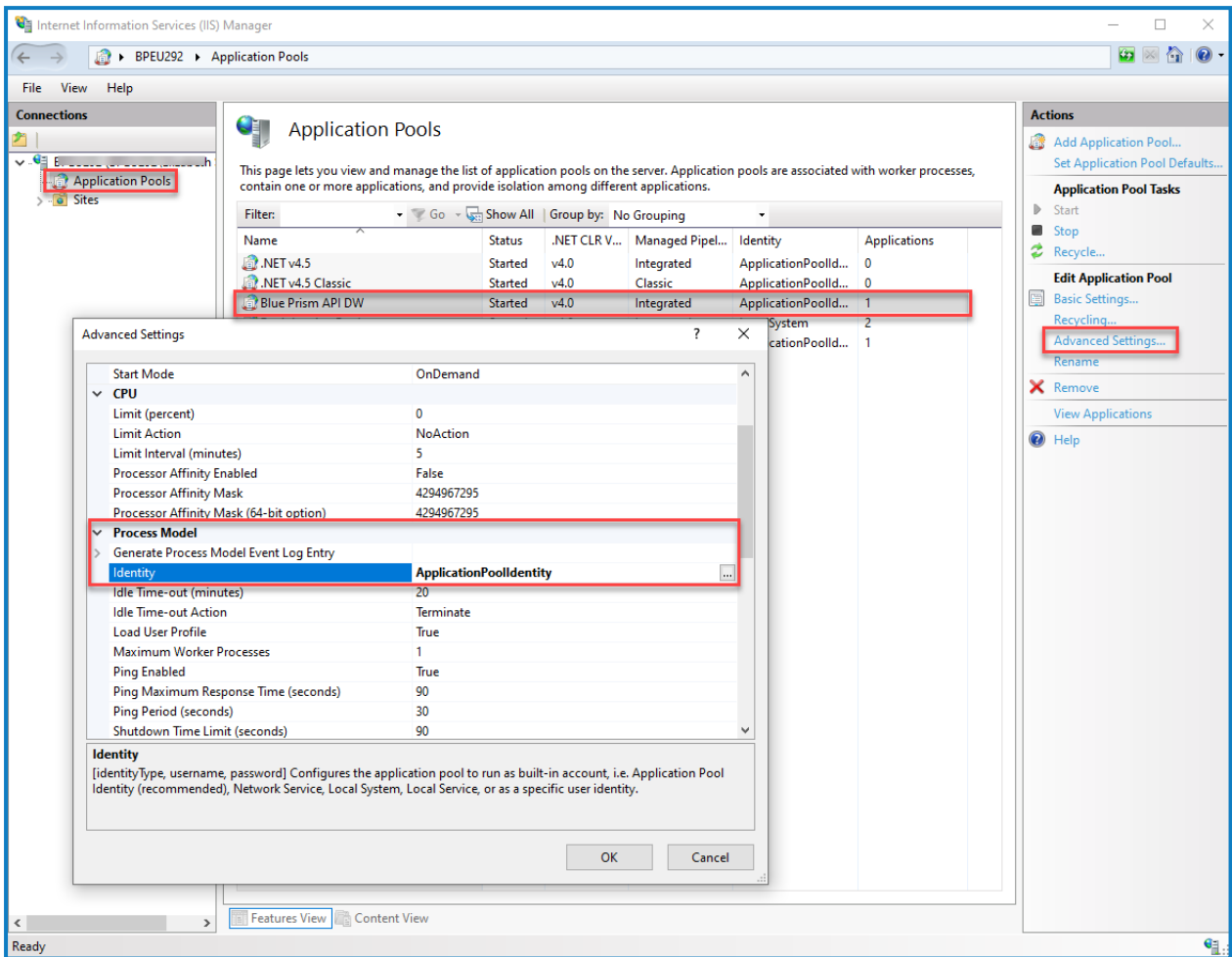
After you have successfully installed the Digital Worker API, you will need to complete the following Internet Information Service (IIS) configuration:

If the Digital Worker API has been configured to use Windows Authentication, the Blue Prism Digital Worker 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:

 Application pool identities are most commonly set to service accounts.


1. Launch the Internet Information Services Manager from the Windows Start menu.
2. In the Connections pane, click **Application Pools**.
The Application Pools window displays.
3. Select **Blue Prism API DW**.
4. In the Actions pane, click **Advanced Settings**.

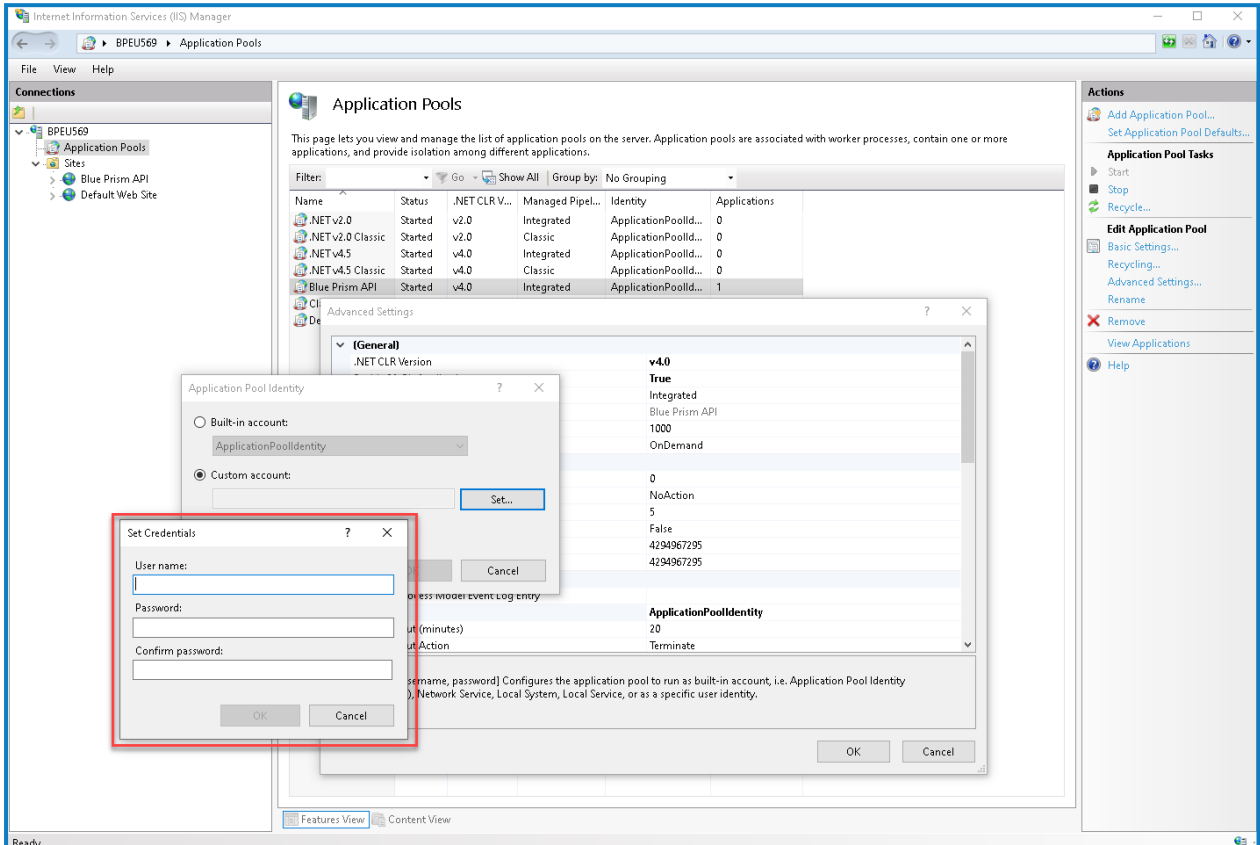
- In the Advanced Settings dialog, expand **Process Model** and click the ellipsis (...) next to **ApplicationPoolIdentity**.



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

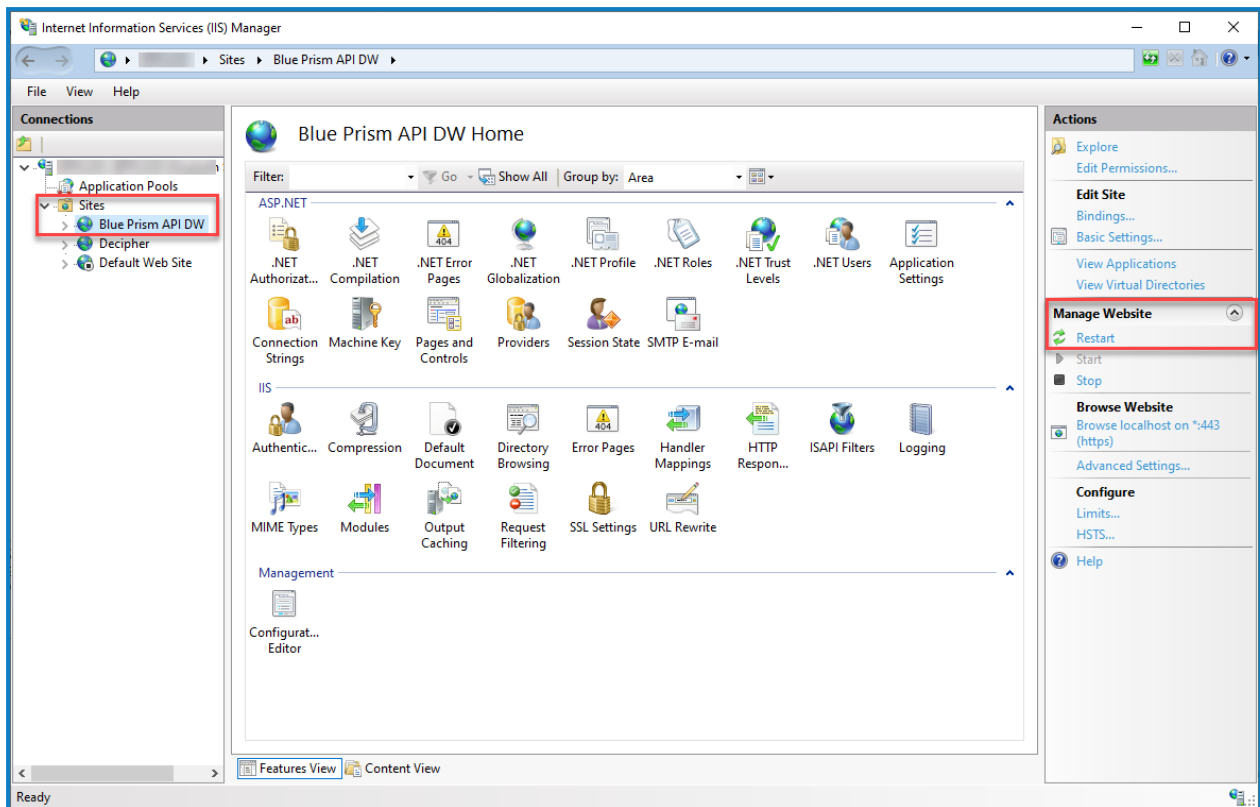
- In the Set Credentials dialog, enter the Windows login credentials service account that has access to the Blue Prism database and click **OK**.

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



- In the Connections panel, expand the **Sites** node and select **Blue Prism API DW**. The Blue Prism API DW Home window displays.

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



After you have successfully installed and configured the Digital Worker API, you need to install the Blue Prism Desktop client and configure a connection for use by the Desktop users. See [Install and connect the Desktop client on page 19](#) for details.

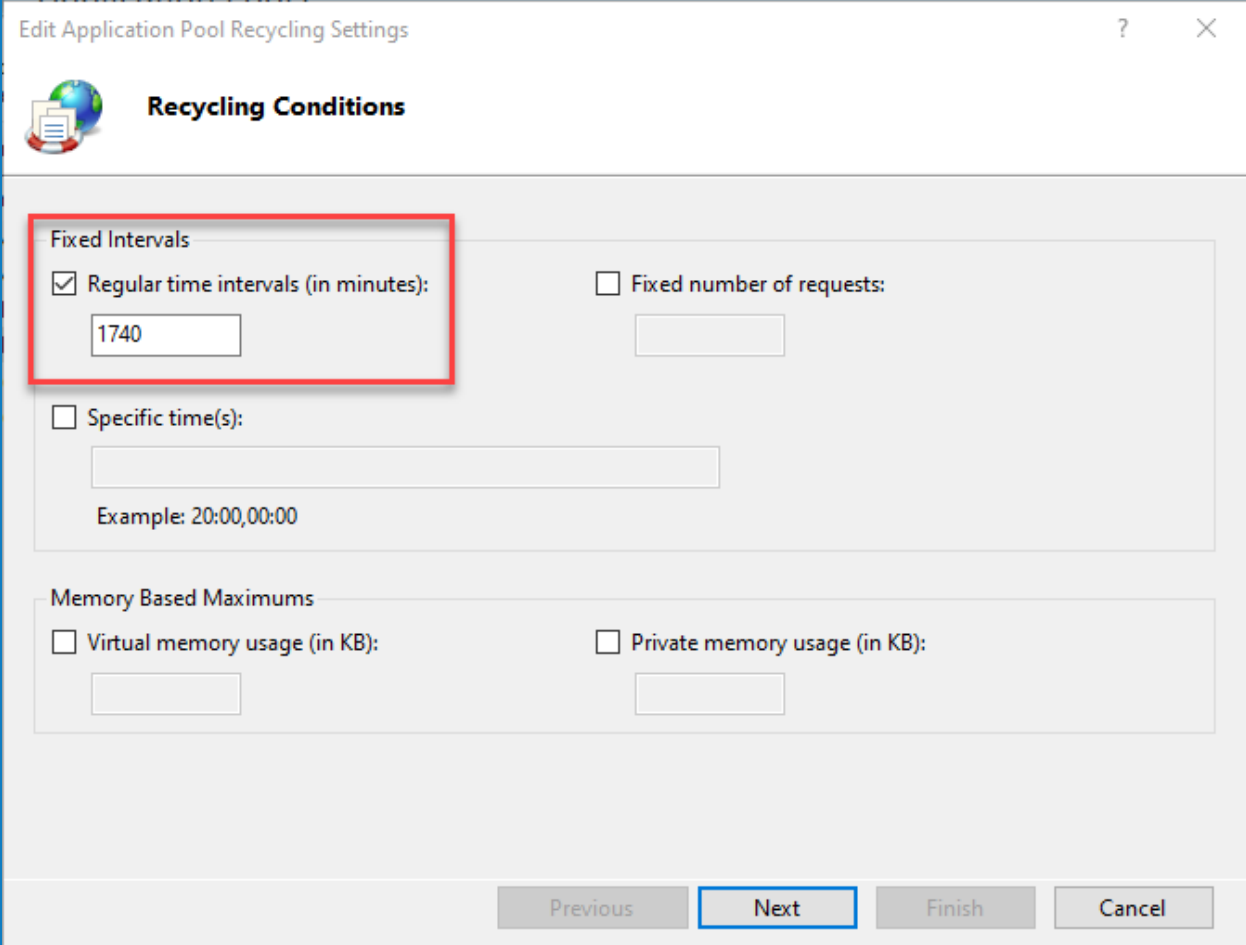
Configure IIS application pool for high usage (optional)

If the Desktop environment is accessed by more than 750 highly active users, then the Digital Worker API may time out, resulting in error messages being displayed. To prevent this from happening, it is recommended that the **Regular time intervals (in minutes)** setting in the Internet Information Service (IIS) application pool is decreased from 1740 to 180.

To amend this setting in IIS:

1. Launch IIS from the Windows Start menu.
2. In the Connections pane, click **Application Pools**.
The Application Pools window displays.
3. Select **Blue Prism API DW**.
4. In the Actions pane, click **Recycling**.

5. In the Edit Application Pool Recycling Settings dialog, change the value of the **Regular time intervals (in minutes)** field to 180.



Edit Application Pool Recycling Settings

Recycling Conditions

Fixed Intervals

Regular time intervals (in minutes):

Fixed number of requests:

Specific time(s):

Example: 20:00,00:00

Memory Based Maximums

Virtual memory usage (in KB):

Private memory usage (in KB):

Previous **Next** Finish Cancel

6. Click **Next**, then click **Finish** to apply the changes.

Install and connect the Desktop client

The Desktop client needs to be installed on the machines of the users running processes.

▶ To watch the Desktop client installation, see the [Blue Prism Desktop installation and configuration video](#)

Prerequisites

Ensure the following components, required for Desktop to function, are all installed in your Blue Prism environment prior to installing the SS&C | Blue Prism Desktop client:

- Blue Prism Enterprise
- Blue Prism API
- Hub (includes Authentication Server)
- Digital Worker API

See [Components required for Desktop on page 5](#) for details.

Desktop licenses

A Desktop license will need to be applied to the Blue Prism database before a user is able to sign in and use the Desktop client. See [Desktop installation overview on page 5](#) for details.



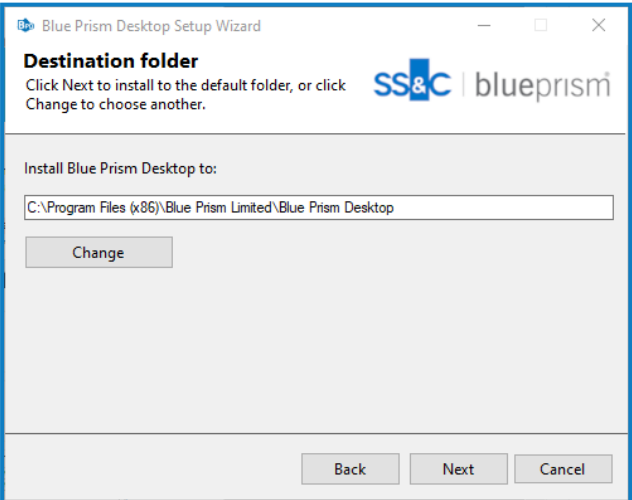
The *Concurrent Blue Prism Desktop Sessions* dashboard view on the Analytics screen in Blue Prism Enterprise shows the total number of concurrent Desktop sessions available, the number of sessions currently in use, and the number of sessions not currently in use.

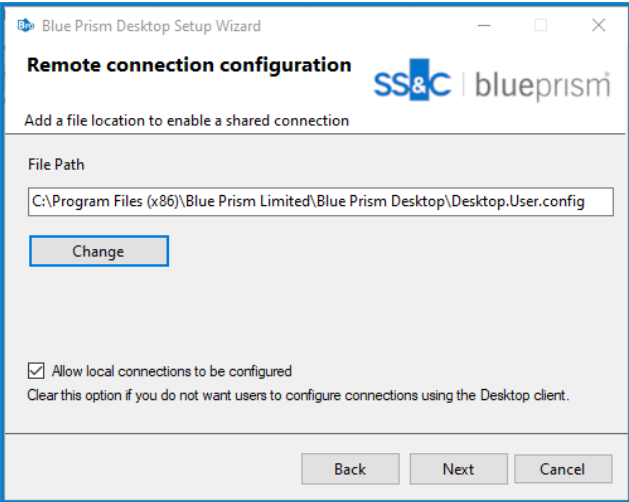

Minimum hardware requirements

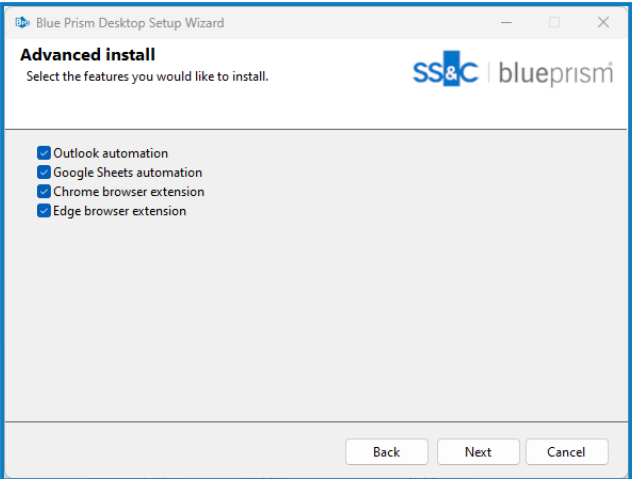
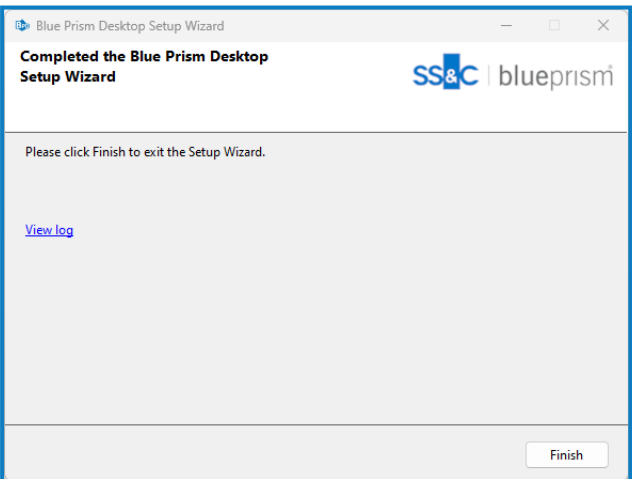
See [Blue Prism software and hardware requirements](#) for details of the minimum requirements for the computer running the Blue Prism Desktop client.

Install the Desktop client

To install the Desktop client, download and run the Desktop installer, available from the [Blue Prism Portal](#), and progress through the installer as shown below:

Step	Installer screen	Details
<p>1</p>		<p>Welcome</p> <p>If required, select another language for the installer from the drop-down list. The default language is English (United States).</p> <p>Click Next.</p>
<p>2</p>		<p>License agreement</p> <p>Read the End User License Agreement and if you agree to the terms, select the check box.</p> <p>Click Next.</p>
<p>3</p>		<p>Destination folder</p> <p>Specify the required installation folder. The default location is C:\Program Files (x86)\Blue Prism\Blue Prism Desktop, but you can choose your own using the Change button.</p> <p>Click Next.</p>

Step	Installer screen	Details
<p>4</p>		<p>Remote connection configuration</p> <p>Desktop users can connect to Desktop environments using one or both of the following options:</p> <ul style="list-style-type: none"> • Shared connection file – Specify the location and name of the shared connection file. If you enter an invalid location and file name, a warning will display. If you leave the field blank, a shared connection file will not be configured. • Local connection files – Select Allow local connections to be configured to enable configuration of Desktop client connections using the Desktop client. <p>For details on Desktop connection files, see Configure a Desktop client connection on page 23.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> It is strongly recommended that Desktop client connections are configured by a Blue Prism system administrator.</p> </div>

Step	Installer screen	Details
<p>5</p>		<p>Advanced install</p> <p>Select the additional components you would like to install. All available options are selected by default.</p> <ul style="list-style-type: none"> • Outlook automation – Required on devices where the Blue Prism MS Outlook Email VBO will be executed. • Google Sheets automation – Required on devices where the Blue Prism Google Sheets VBO will be executed. • Chrome browser extension – Required to enable Blue Prism to interact with Chrome-based applications and web pages. • Edge browser extension – Required to enable Blue Prism to interact with Edge-based applications and web pages. <p>Click Install to install Desktop. A progress bar displays during the installation of the application.</p>
<p>6</p>		<p>Installation complete</p> <p>If the installation has completed successfully, click Finish to exit the installer.</p> <p>If the installation fails, click View Log to see details of the error that was encountered.</p>

Configure a Desktop client connection

It is strongly recommended that Desktopclient connections are configured by a Blue Prism system administrator.

When installing the Desktop client, users can choose to connect to the Desktop environment using at least one or both of the following options:

- [Configure a shared connection](#) – Connect to a shared configuration file, which can only be modified by a system administrator.
- [Configure a local connection](#) – Connect to a local configuration file, which can be modified by the Desktop user, if required.

Configure a shared connection

If your organization wants Desktop client users to connect to a Desktop environment using a shared connection file, the location of the shared file will need to be entered when installing the Desktop client. The creation and configuration of the shared connection file should be carried out by a system administrator. Desktop client users cannot edit or delete shared connections. See [Configuring environment connections for Blue Prism Desktop](#) for details.

Desktop.User.config backup file

When a Desktop user has successfully connected to a Desktop environment using a shared connection file, a .desktop.shared.config.bak file is automatically generated and stored locally in C:\Users\\AppData\Roaming\Blue Prism Limited\Desktop. This connection file is then used to establish a connection with the Desktop environment, removing the need to connect to the shared file each time the user accesses Desktop.

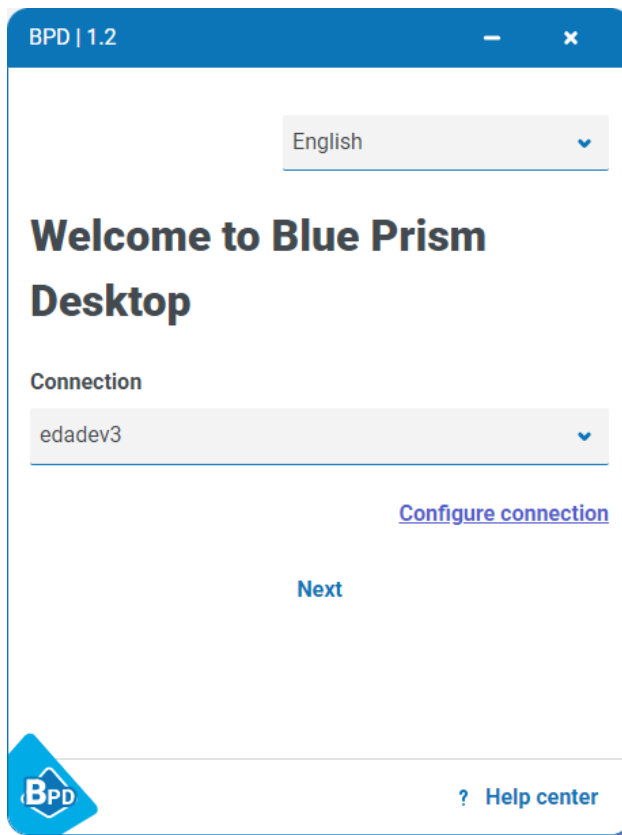
Configure a local connection

Details of how users can import and connect to existing Desktop connections can be found in [Configuring environment connections for Blue Prism Desktop](#).

The Desktop.User.config file, which is located in C:\Users\\AppData\Roaming\Blue Prism Limited\Desktop on each computer, points to the location of the Blue Prism API, the Digital Worker API, and Authentication Sever. This file can be edited directly if necessary, or configured via the Desktop user interface (recommended), as described below.

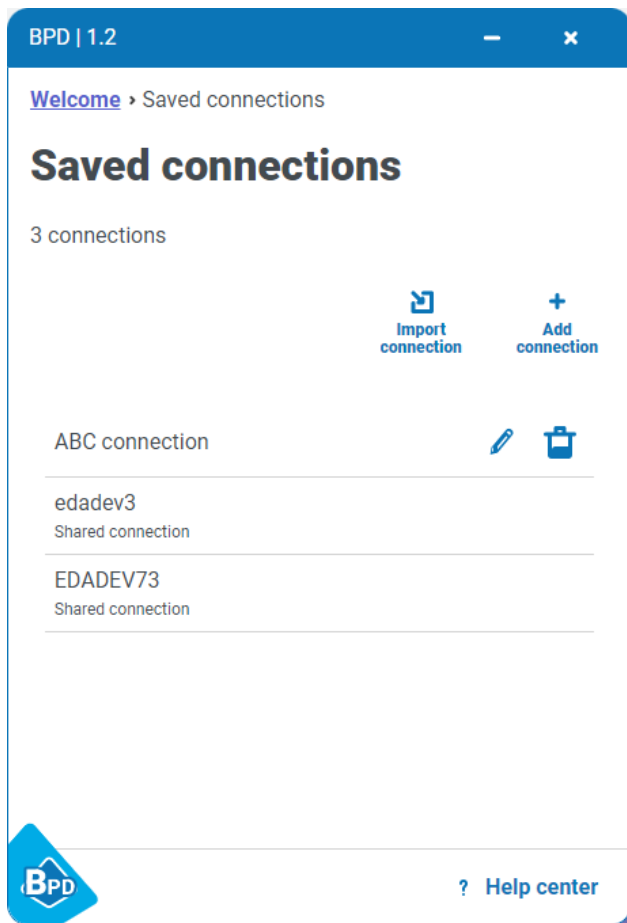
1. Open the Desktop application.


The Welcome to Desktop screen displays.



2. Click **Configure connection**.

The Saved connections screen displays.





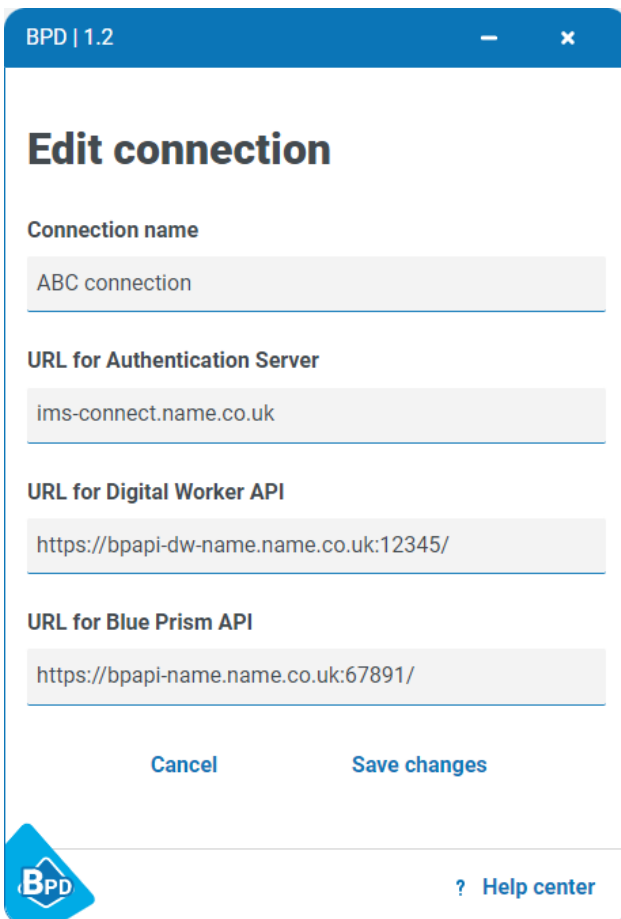
 The available connections and options on this screen are dependent on each user's installation of the Desktop client.

3. The Create new connection screen displays:

The screenshot shows a window titled "BPD | 1.2" with a close button. The main heading is "Create new connection". Below this are four text input fields, each with a label above it: "Connection name", "URL for Authentication Server", "URL for Digital Worker API", and "URL for Blue Prism API". At the bottom of the form area are two buttons: "Cancel" and "Create". In the bottom-left corner is a blue diamond-shaped logo with "BPD" inside. In the bottom-right corner is a link that says "? Help center".

4. Enter the connection details, as prompted. All the fields are mandatory.

Field name	Information required
Connection name	<p>Enter a name for this connection. Connection names must be unique, and are case-sensitive.</p> <p> If you try to create a new connection with the same name as an existing one, a warning message displays and you cannot save the connection.</p>
URL for Authentication Server	<p>Enter the Authentication Server URL.</p> <p> To ensure a secure connection is used, all Authentication Server URLs must include https://. If you do not include https:// in the URL, it will be added automatically.</p>
URL for Digital Worker API	Enter the URL of the Digital Worker API to which you want to connect.
URL for Blue Prism API	Enter the URL of the Blue Prism API to which you want to connect.



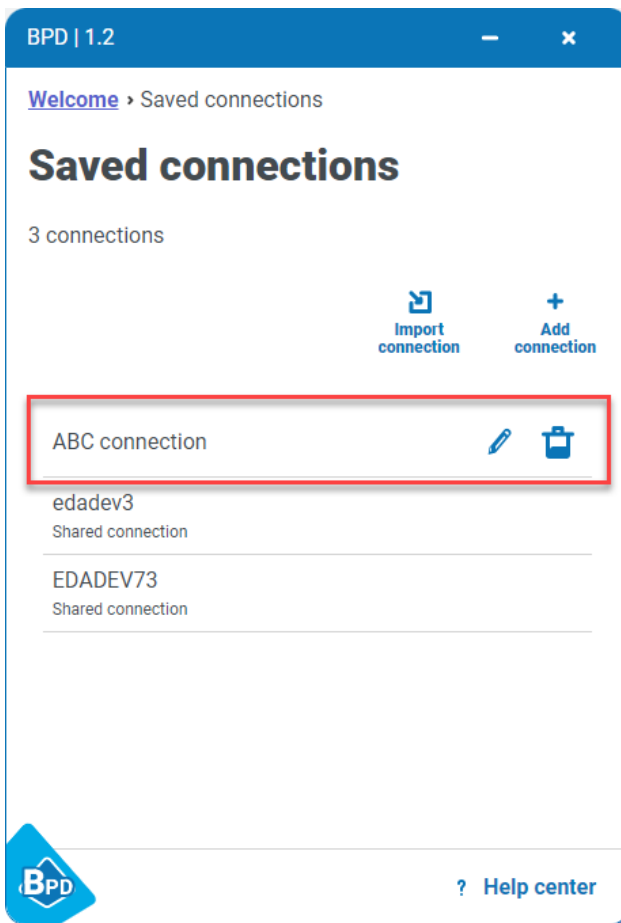
The screenshot shows a window titled 'BPD | 1.2' with a close button. The main heading is 'Edit connection'. Below this are four input fields:

- Connection name:** ABC connection
- URL for Authentication Server:** ims-connect.name.co.uk
- URL for Digital Worker API:** https://bpapi-dw-name.name.co.uk:12345/
- URL for Blue Prism API:** https://bpapi-name.name.co.uk:67891/

At the bottom of the form are two buttons: 'Cancel' and 'Save changes'. In the bottom left corner is the BPD logo, and in the bottom right corner is a link for '? Help center'.

5. Click **Create** to add the new connection.

The connection is created and displays on the Saved connections screen.



The configuration is updated in the Desktop.User.config file, which is located in C:\Users\Import connection on the Saved connections screen on each Desktop user's computer. See [Configure Blue Prism Desktop connections](#) for details.


Although the functionality is available to do so, it is not expected that Desktop users will create, edit, or delete their own connections. It is expected that this information will be provided to them by system administrators. However, because the connection configuration information is stored in their user settings, they will need to import the configuration file themselves. When rolling out Desktop to end users, it is recommended that system administrators create and distribute a centrally-controlled Desktop.User.config file to be imported by Desktop users.

Example Desktop.User.config file


The following example shows a typical Desktop.User.config file:

```
{
  "Environments": {
    "Production Environment": {
      "ConfigurationName": "Production Environment",
      "ApiUrl": "https://xxapi-edadev2.site.co.uk:12121",
      "DigitalWorkerApiUrl": "https://ttapi-dw-edadev2.site.co.uk:54441",
      "AuthenticationServerDomain": "ims-prod.aadeuops.co.uk",
      "ClientName": "bpd"
    },
    "ABC connect": {
      "ConfigurationName": "ABC connect",
      "ApiUrl": "https://xxapi-edadev2.site.co.uk:12634",
      "DigitalWorkerApiUrl": "https://uuapi-dw-edadev2.site.co.uk:54455",
      "AuthenticationServerDomain": "ims-aaadev2.site.co.uk",
      "ClientName": "bpd"
    }
  },
  "Selected": "edadev2"
}
```

Desktop silent installation and configuration

 Downloading and installing any of the Blue Prism Enterprise components, including by silent installation via command line, means that you accept the [End User License Terms](#).

The installation of Desktop client and the installation and configuration of the Blue Prism Digital Worker 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 Digital Worker 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 Digital Worker API installation are also applicable to a Digital Worker API silent installation. For information on installing the required software, see [Prerequisites on page 8](#).

Desktop client silent installation commands

Install Desktop

```
msiexec /i "BluePrismDesktop-1.2.0.msi" /quiet /qn /norestart
```

Uninstall Desktop

```
msiexec /x "BluePrismDesktop-1.2.0.msi" /quiet /qn /norestart
```

Digital Worker 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.

Component	Description						
<code>API_SQL_DATABASE_NAME</code>	The name of the Blue Prism database.						
<code>API_SQL_AUTH_MODE</code>	<p>SQL authentication mode. 0 - Windows authentication mode; 1 - SQL authentication mode.</p> <p>If <code>API_SQL_AUTH_MODE</code> is set to 1 the following details also need to be supplied:</p> <table border="1"> <thead> <tr> <th>Component</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><code>API_SQL_USERNAME</code></td> <td>Username to access the Blue Prism database.</td> </tr> <tr> <td><code>API_SQL_PASSWORD</code></td> <td>Password to access the Blue Prism database.</td> </tr> </tbody> </table>	Component	Description	<code>API_SQL_USERNAME</code>	Username to access the Blue Prism database.	<code>API_SQL_PASSWORD</code>	Password to access the Blue Prism database.
Component	Description						
<code>API_SQL_USERNAME</code>	Username to access the Blue Prism database.						
<code>API_SQL_PASSWORD</code>	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:

- Install the API to D:\DWAPI to listen on dwapi.example.com:4343
- Use the certificate thumbprint E3AEFC6DCB900469E1E6288202B12DA3BD1EDD4D
- Use the BPD database on sql.example.com, with SQL authentication, using the sa account and password SQLP@ssw0rd
- Use the BluePrismDigitalWorkerAPI-7.3.0.msi

```
mmsiexec /i BluePrismDigitalWorkerAPI-7.3.0.msi /qn INSTALLDIR='D:\DWAPI' API_IIS_
HOSTNAME=dwapi.example.com API_IIS_
PORT=4343 API_SSL_CERTIFICATE_ID=E3AEFC6DCB900469E1E6288202B12DA3BD1EDD4D API_SQL_
SERVER=sql.example.com API_SQL_DATABASE_NAME=BPD API_SQL_AUTH_MODE=1 API_SQL_USERNAME=sa API_SQL_
PASSWORD=SQLP@ssw0rd
```

Digital Worker API configuration scripts


Following the installation of the Digital Worker 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 DW\' -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 Digital Worker 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 DW ', 'Read', 'Allow'))
Set-Acl -Path $KeyPath -AclObject $Acl
```