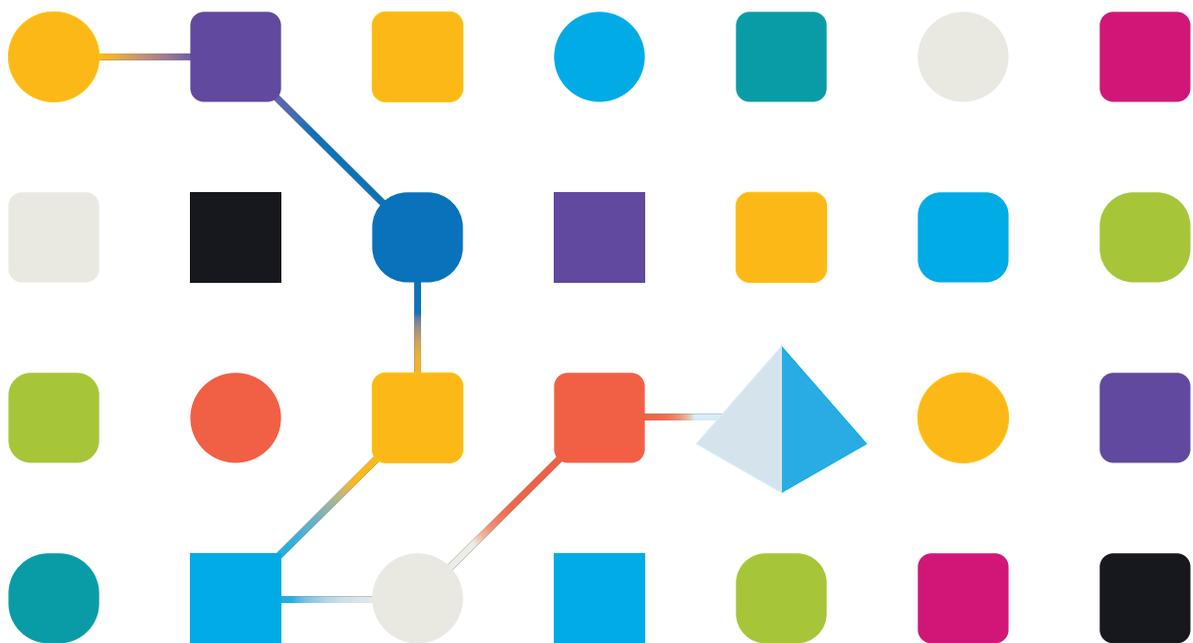




Blue Prism 7.1

Chrome, Edge, and Firefox Integration

Document Revision: 7.0



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

- Chrome, Edge, and Firefox integration** 4
 - Manifest V2 and V3 support 4
 - Browser extension compatibility 4
- Chrome browser extension** 5
 - Prerequisites 5
 - Install the Chrome browser extension using the Blue Prism installer 6
 - Install the Chrome browser extension from the web store 8
 - Install the Chrome browser extension using an offline package 9
 - Chrome browser extension registry keys 10
 - Remove the Chrome Blue Prism extension 11
- Edge browser extension** 12
 - Prerequisites 12
 - Install the Edge browser extension using the Blue Prism installer 13
 - Install the Edge browser extension from the web store 15
 - Install the Edge browser extension using an offline package 16
 - Edge browser extension registry key 17
 - Remove the Edge browser extension 18
- Firefox browser extension** 19
 - Prerequisites 19
 - Install the Firefox browser extension using the Blue Prism installer 19
 - Install the Firefox browser extension using an offline package 22
 - Firefox browser extension registry keys 23
 - Remove the Firefox browser extension 24
- Automate Chrome, Edge, and Firefox with the Application Modeller** 25
 - Use Tracking ID to automate multiple browser instances of the same type from a single Blue Prism instance 26
 - Automate multiple browser instances of the same type from multiple Blue Prism instances 28
- Automate Chrome and Edge with UI Automation (UIA)** 29
 - Use UIA to model Chrome and Edge 29
- Disable browser extension automatic updates** 30
 - Sideload an extension 30
 - Local Group Policy 32
 - Additional information 36
- Troubleshooting browser integration** 37
 - Configure browser timeout parameters 37
 - Unable to spy elements on a web site 38
 - The Firefox extension does not load 39
 - Unable to spy websites that use HTTPS in Firefox 39
 - The browser extension is not detected 39
 - The browser extension is not compatible with the Blue Prism version 40

Chrome, Edge, and Firefox integration

Native support for automating web pages and applications in Google Chrome, the Chromium-based version of Microsoft Edge, and Mozilla Firefox web browsers is provided in Blue Prism® using Blue Prism browser extensions. The extensions allow Blue Prism to interact with web pages and applications presented in these browsers, so that business processes that rely on such applications and web pages can easily be modelled.

The Blue Prism extensions establish connectivity with Blue Prism, allowing Blue Prism to interact with web pages in Chrome, Edge, and Firefox, so data can be exchanged and elements manipulated.

Blue Prism uses a native messaging host application to communicate with the browser extension. When a browser is launched from Blue Prism, a native messaging host application is started behind the scenes that listens for any incoming messages from Blue Prism and sends them to the browser extension.

The Blue Prism installer automatically installs the configuration settings for the native messaging host, regardless of whether the user selects to install any of the browser extensions or not. An additional registry key for the native messaging host is created and points to a JSON file which provides details on the allowed extensions and the location of the executable.

There are three Blue Prism browser extensions:

- **Chrome** – Used to automate applications and web pages in Google Chrome.
- **Firefox** – Used to automate applications and web pages in Mozilla Firefox.
- **Edge** – Used to automate applications and web pages in Microsoft Edge.

Browser-based applications can also be automated natively via a [Citrix virtual desktop environment](#) in which Blue Prism has been installed with the browser extensions enabled.

Manifest V2 and V3 support

For the Chrome and Edge extensions, we differentiate between Manifest V2 and V3 support according to Google's and Microsoft's guidance. For more information, see the guidance from [Google](#) and [Microsoft](#).

Mozilla have not announced a date by which they will remove support for MV2 browser extensions so the Blue Prism Firefox browser extension still uses Manifest V2 and is therefore not impacted by this change.

The following Manifest V2 and V3 support applies to Blue Prism 7 versions:

- Native Manifest V2 browser extension support is provided by default in Blue Prism version 7.0.
- Manifest V3 browser extension support via the [Blue Prism Browser Automation Agent](#) (with Insert/Invoke JavaScript functionality) is available in Blue Prism versions 7.0 and 7.1.
- Native Manifest V3 browser extension support is provided in Blue Prism versions 7.1 and 7.2 as follows:
 - In Blue Prism version 7.1, native Manifest V3 support is provided without Insert/Invoke JavaScript functionality. For more information, see the [Blue Prism 7.1 upgrade notices](#).
 - From Blue Prism version 7.2, the Insert/Invoke JavaScript functionality previously provided only via the [Blue Prism Browser Automation Agent](#) is included with the Manifest V3 browser extension by default.

Browser extension compatibility

For up-to-date testing and compatibility data about the Blue Prism browser extensions, see the [Browser extension compatibility matrix](#).

Chrome browser extension

The Blue Prism Chrome browser extension establishes connectivity with Blue Prism, allowing Blue Prism to interact with Chrome applications and web pages so data can be exchanged and elements manipulated.

The Blue Prism browser extensions should be installed on any machine that will be used to automate Chrome.

 For details of browser extension and Blue Prism versions, see [browser extension compatibility](#).

Prerequisites

The following are required:

- Access to the Chrome web store for online installations.
- Extension package for offline installations.
- The ability to configure Chrome add-ons.
- The Windows Process Performance Counters must be enabled.

 This affects Blue Prism versions 7.0 to 7.1.1 only, see [The browser extension is not detected on page 39](#) and [this Knowledge Base article](#) for details on how to address it.

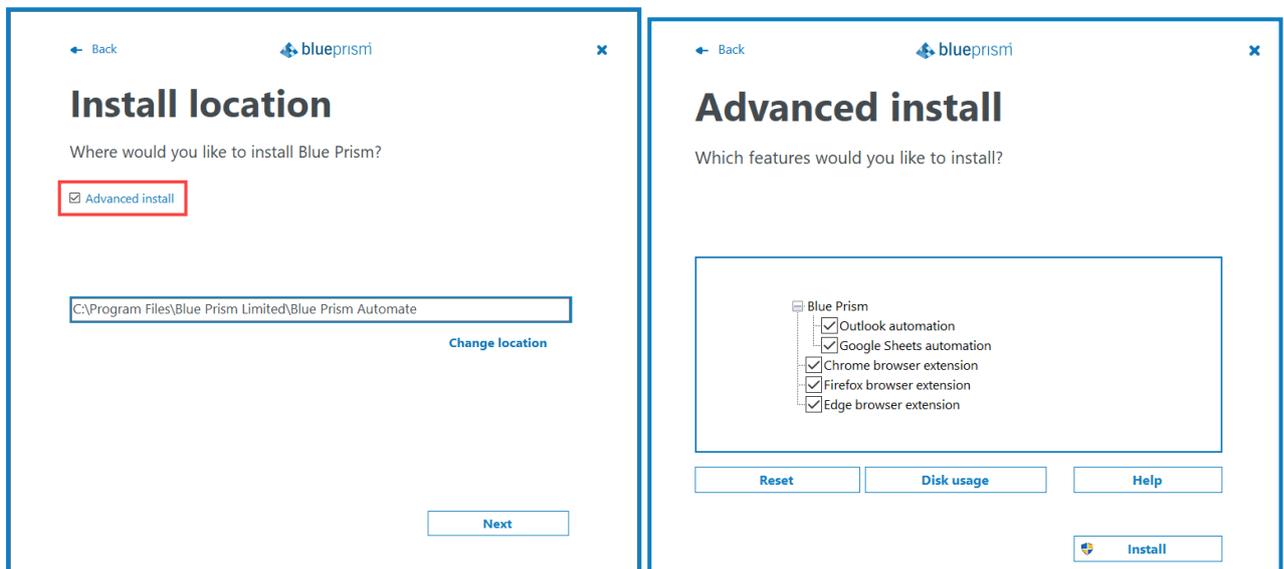
Install the Chrome browser extension using the Blue Prism installer

The Blue Prism installer applies a [registry key](#) that installs the Blue Prism extension the next time the browser is started. The installer can be run using the graphical user interface or from the command line. An additional registry key is created for the native messaging host and points to a JSON file which provides details on the allowed extensions and the location of the executable.

Install from the Blue Prism installer

Using the advanced installation option, you can determine which browser extensions (and other optional features) to install.

1. Run the appropriate Blue Prism installer for your system – 32-bit or 64-bit.
2. Select **Advanced install** from the Install location page of the install wizard.
3. Click **Next** and select the Chrome browser extension and any other features you want to install.



4. Click **Install** and complete the installation.

 During an upgrade, the settings already applied for the current installation are maintained unless edited in the advanced install options.

Install from the command line

The following command line options are available for installing Blue Prism and setting the registry key for the Chrome extension. The example commands are for the 7.1 version of Blue Prism – update the version number as required.

Command	Description
<pre>msiexec /i BluePrism7.1_x64 /qn msiexec /i BluePrism7.1_x86 /qn</pre>	Installs Blue Prism and sets the Chrome extension registry key.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=BluePrism,BPServer /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=BluePrism,BPServer /qn</pre>	Installs Blue Prism without setting the browser extension registry keys.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=ChromePlugin /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=ChromePlugin /qn</pre>	Adds the Chrome extension registry key to an existing installation of Blue Prism.

The ADDLOCAL property allows you to install multiple Blue Prism components. These must be separated by a comma. For example, the following command installs 64-bit versions of Blue Prism, and the Chrome, Edge, and Firefox extensions:

```
msiexec /i BluePrism7.1_x64  
ADDLOCAL=BluePrism,BPServer,ChromePlugin,EdgePlugin,FirefoxPlugin /qn
```

 The *BluePrism* and *BPServer* components must both be specified to install or upgrade Blue Prism when using the ADDLOCAL parameters. They cannot be used in isolation.

Install the Chrome browser extension from the web store

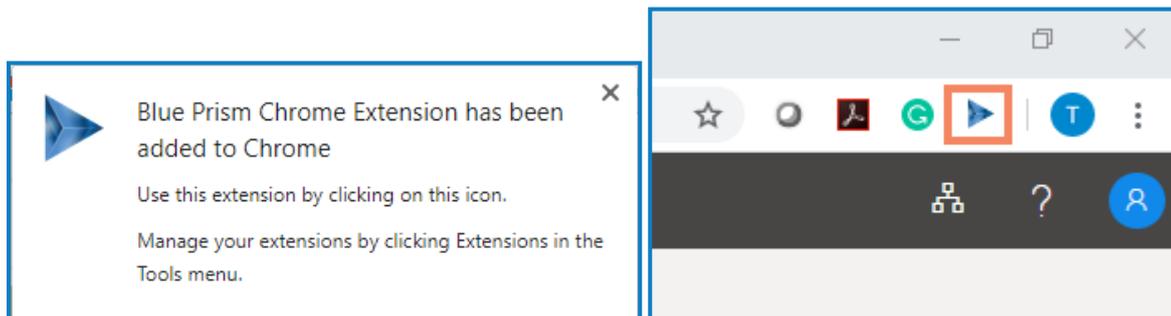
You can install the Blue Prism Chrome extension from the Chrome web store using the appropriate URL for your version of Blue Prism.

Blue Prism version	Compatible browser extension version
7.1.2	https://chrome.google.com/webstore/detail/blue-prism-712-browser-ext/bpgakglmlggfnkikkmimonpdgipdnaha
7.1.1	https://chrome.google.com/webstore/detail/blue-prism-71-browser-ext/koibfinjpefmmmdmmdicglmhfehjjlhn/
7.1	https://chrome.google.com/webstore/detail/blue-prism-71-browser-ext/koibfinjpefmmmdmmdicglmhfehjjlhn/
7.0.2	https://chrome.google.com/webstore/detail/blue-prism-701-browser-ext/hpaajmgfhgakaamoopdhieneihpmeapm
7.0.1	https://chrome.google.com/webstore/detail/blue-prism-701-browser-ext/hpaajmgfhgakaamoopdhieneihpmeapm
7.0	https://chrome.google.com/webstore/detail/blue-prism-70-browser-ext/lbnooplepikajpiphjgfoniaakpclemh/

To install the browser extension for Chrome:

1. Open Chrome.
2. Enter the URL for the required version into the address bar of the browser.
3. Click **Add to Chrome** and confirm the installation when prompted.

A notification displays when installation is complete, and the Blue Prism extension icon is added to the browser toolbar.



Install the Chrome browser extension using an offline package

If the browser extension has already been installed, updated extensions that are made available after a Blue Prism release are automatically updated when the browser is loaded if there is an active internet connection. For devices that are not connected to the internet, the Blue Prism Chrome extension can be installed offline using an independent package. The extension will need to be installed separately for each user on each device that needs to use the extension.

To install the browser extension for Chrome:

1. Download the required extension package from the web store, see URLs for applicable Blue Prism version [above](#).
2. Create a ZIP file of the downloaded extension.

Extensions are stored in the folder C:\Users\Username\AppData\Local\extension-path', for example for Blue Prism 7.0.0: C:\Users\Username\AppData\Local\Google\Chrome\User Data\Default\Extensions\bnnoolepikajpiphjgfoniaakpclemh

Select all files in the 7.0.0.0_0 folder and add them to a ZIP file.

3. Open Chrome.
4. Click the menu (...) icon and select **More Tools > Extensions**.

<chrome://extensions> displays with the existing extensions.



If you have installed Blue Prism using the installer, you will see a Blue Prism extension on this page. This is a managed extension (indicated with the managed icon), as such, you cannot remove or turn off the extension from this page.

5. Switch the page into **Developer mode** using the slider.
6. In Windows Explorer, navigate to the extension ZIP file then drag and drop it into the Chrome Developer page.

The extension installs and displays on the page.

7. Switch the page back into standard mode using the **Developer mode** slider.



Ensure you turn off **Developer mode** after installing the extension. Leaving your browser in **Developer mode** can be a security risk.

Chrome browser extension registry keys

The following registry keys are applied when installing the browser extension with the Blue Prism installer to instruct the browser to add the Blue Prism extension.

For situations where the browser extension is to be installed independently or, where the registry value applied by the installer is prevented from persisting, such as if network restrictions override them, the setting can be applied using an alternative deployment method, such as Group Policy or Local Security Policy.

Fresh installs: If no keys are in the force install list -> 1

Change features: If we find an previously installed -> same key as the previously installed extension

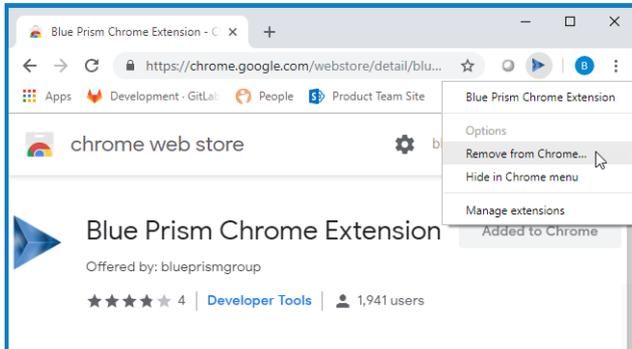
If there is already a key in the force install list (virus scanner)it increments the key number automatically

Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Google\Chrome\ExtensionInstallForcelist
Name	1 (Or the next available number)
Type	REG_SZ
Data	<p>7.1.2: bpgakglmlggfnkikkmimonpdgipdnaha;https://clients2.google.com/service/update2/crx</p> <p>7.1.1: koibfinjpefmdmmdiicglmhfehjjlhn;https://clients2.google.com/service/update2/crx</p> <p>7.1.0: koibfinjpefmdmmdiicglmhfehjjlhn;https://clients2.google.com/service/update2/crx</p>
Registry Key for Native Messaging Host	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Chrome\NativeMessagingHosts\com.blueprism.messaging
Name	default
Type	REG_SZ
Data	C:\ProgramData\Blue Prism Limited\Blue Prism\com.blueprism.messaging-manifest.json

Remove the Chrome Blue Prism extension

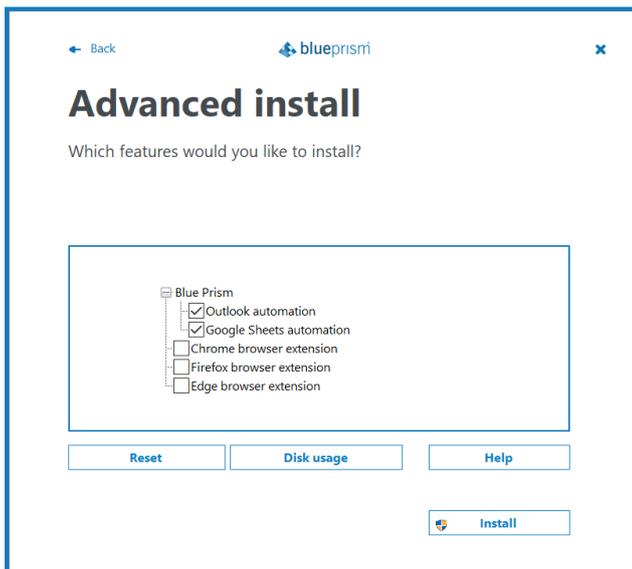
Remove using browser options

Select **Remove from Chrome** from the extension options.



Remove using the Blue Prism installer

Run the Blue Prism installer and on the Advanced install page, select **Change features** and clear the selection for the Chrome extension.



The registry key is deleted and the extension is removed. Alternatively, delete the registry key manually using a registry editor.

Remove using Local Security Policy or Group Policy

To uninstall the Blue Prism Chrome extension, remove the value from the [specified registry key](#) or delete the entire key if none of the associated settings are required.

Edge browser extension

The Blue Prism Edge browser extension establishes connectivity with Blue Prism, allowing Blue Prism to interact with Chromium-based Edge applications and web pages so data can be exchanged and elements manipulated.

The Blue Prism browser extension should be installed on any machine that will be used to automate Edge.

 For details of browser extension and Blue Prism versions, see [browser extension compatibility](#).

Prerequisites

The following are required:

- Access to the Edge web store for online installations
- Extension package for offline installations
- The ability to configure Edge add-ons
- The Windows Process Performance Counters must be enabled.

 This affects Blue Prism versions 7.0 to 7.1.1 only, see [The browser extension is not detected on page 39](#) and [this Knowledge Base article](#) for details on how to address it.

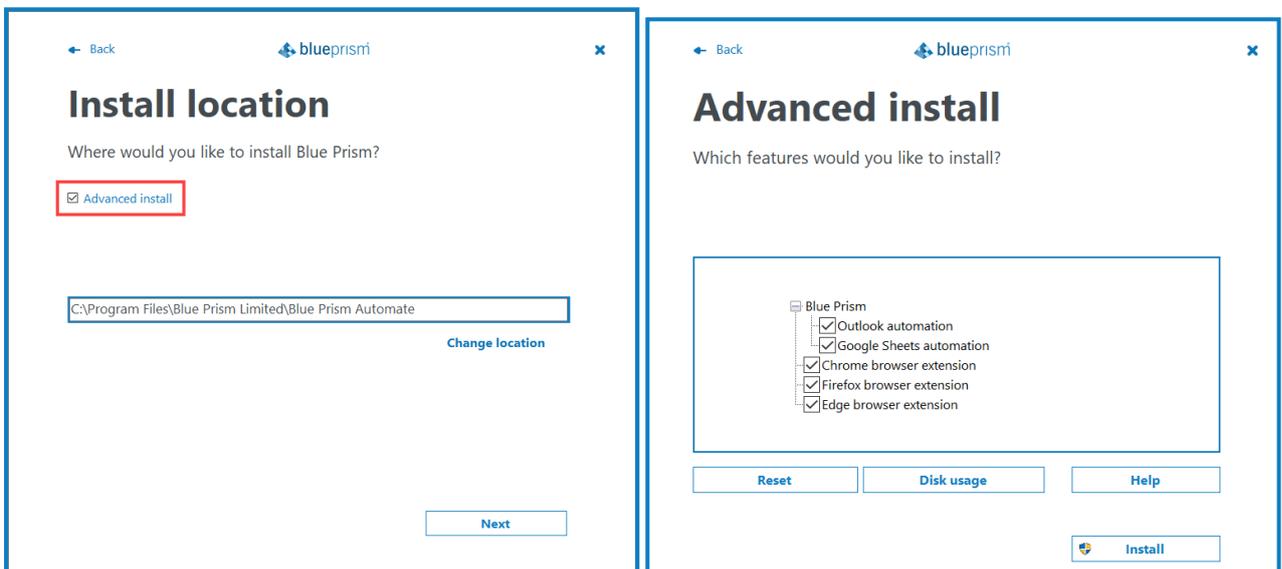
Install the Edge browser extension using the Blue Prism installer

The Blue Prism installer applies a [registry key](#) that installs the Blue Prism extension the next time the browser is started. The installer can be run using the graphical user interface or from the command line. An additional registry key is created for the native messaging host and points to a JSON file which provides details on the allowed extensions and the location of the executable.

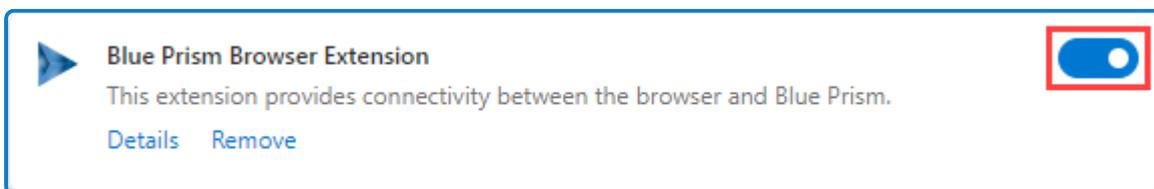
Install from the Blue Prism installer

Using the advanced installation option, you can determine which browser extensions (and other optional features) are installed.

1. Run the appropriate Blue Prism installer for your system – 32-bit or 64-bit.
2. Select **Advanced install** from the Install location page of the install wizard.
3. Click **Next** and select the Edge browser extension and any other features you want to install.



4. Click **Install**.
5. When installation is complete, open Edge and type `edge://extensions` in the address bar.
6. Enable the browser extension using the slider.



 During an upgrade, the settings already applied for the current installation are maintained unless edited in the advanced install options.

Install from the command line

The following command line options are available for installing Blue Prism and setting the registry key for the Edge extension. The example commands are for the 7.1 version of Blue Prism – update the version number as required.

Command	Description
<pre>msiexec /i BluePrism7.1_x64 /qn msiexec /i BluePrism7.1_x86 /qn</pre>	Installs Blue Prism and sets Edge extension registry key.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=BluePrism,BPServer /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=BluePrism,BPServer /qn</pre>	Installs Blue Prism without setting the browser extension registry keys.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=EdgePlugin /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=EdgePlugin /qn</pre>	Adds the Edge extension registry key to an existing installation of Blue Prism.

The ADDLOCAL property allows you to install multiple Blue Prism components. These must be separated with a comma. For example, the following command installs 64-bit versions of Blue Prism, and the Chrome, Edge, and Firefox extensions:

```
msiexec /i BluePrism7.1_x64  
ADDLOCAL=BluePrism,BPServer,ChromePlugin,EdgePlugin,FirefoxPlugin /qn
```

 The *BluePrism* and *BPServer* components must both be specified to install or upgrade Blue Prism when using the ADDLOCAL parameters. They cannot be used in isolation.

Enable the Edge extension

When installation is complete, open Edge and type `edge://extensions` in the address bar. Enable the extension using the slider.

Install the Edge browser extension from the web store

You can install the Blue Prism Edge browser extension from the Microsoft Edge add-ons store using the following URL:

Blue Prism version	Compatible browser extension version
7.1.2	https://microsoftedge.microsoft.com/addons/detail/blue-prism-712-browser-ex/ajkifijhcgbnobfbhckepbaffdknmng
7.1.1	https://microsoftedge.microsoft.com/addons/detail/blue-prism-71-browser-ex/alphbcchbekpcfaknckinfapdaiiol
7.1	https://microsoftedge.microsoft.com/addons/detail/blue-prism-71-browser-ex/alphbcchbekpcfaknckinfapdaiiol
7.0.2	https://microsoftedge.microsoft.com/addons/detail/blue-prism-701-browser-/chgmlbmnlliciejdidnllecifgjhepe
7.0.1	https://microsoftedge.microsoft.com/addons/detail/blue-prism-701-browser-/chgmlbmnlliciejdidnllecifgjhepe
7.0	https://microsoftedge.microsoft.com/addons/detail/blue-prism-70-browser-ex/jecmlbbpjadglfjggkpkckhheoblfdohf

To install the browser extension for Edge:

1. Open Microsoft Edge.
2. Enter the URL for the required version into the address bar of the browser.
3. Click **Get** and confirm the installation when prompted.

A notification displays when installation is complete and the Blue Prism extension icon is added to the browser toolbar.

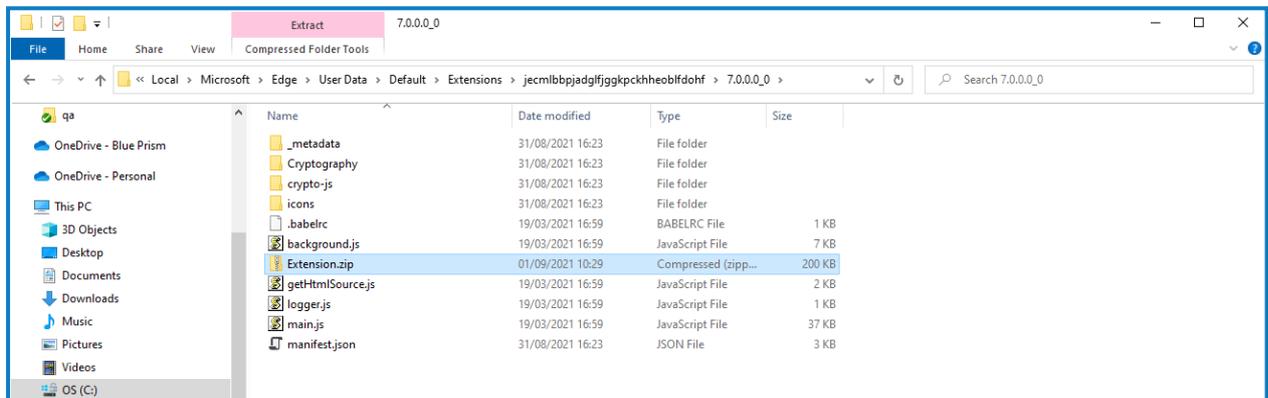
Install the Edge browser extension using an offline package

If the browser extension has already been installed, updated extensions that are made available after a Blue Prism release are automatically updated when the browser is loaded if there is an active internet connection. For devices that are not connected to the internet, the Blue Prism Edge extension can be installed offline using an independent package. The extension will need to be installed separately for each user on each device that needs to use the extension.

To install the browser extension for Edge:

1. Download the required extension package from the web store, see URLs for applicable Blue Prism version [above](#).
2. Create a ZIP file of the downloaded extension.

Extensions are stored in the folder C:\Users\'Username'\Appdata\Local\'path', for example for Blue Prism 7.0.0: C:\Users\'Username'\Appdata\Local\Microsoft\Edge\User Data\Default\Extensions\jecmlbbpjadglfjggkpkkhheoblfdohf



Select all files in the 7.0.0.0_0 folder and add them to a ZIP file.

3. Open Edge.
4. Click the menu (...) icon and select **Extensions**.
edge://extensions displays with the existing extensions.

 If you have installed Blue Prism using the installer, you will see a Blue Prism extension on this page.

5. Switch the page into **Developer mode** using the slider.
6. In Windows Explorer, navigate to the extension ZIP file then drag and drop it into the Edge Developer page.
The extension installs and displays on the page.
7. Switch the page back into standard mode using the **Developer mode** slider.

 Ensure you turn off **Developer mode** after installing the extension. Leaving your browser in **Developer mode** can be a security risk.

Edge browser extension registry key

The following registry keys are applied when installing the browser extension with the Blue Prism installer to instruct the browser to add the Blue Prism extension.

For situations where the browser extension is to be installed independently or, where the registry value applied by the installer is prevented from persisting, such as if network restrictions override them, the setting can be applied using an alternative deployment method, such as Group Policy or Local Security Policy.

Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Edge\ExtensionInstallForcelist
Name	1 (Or the next available number)
Type	REG_SZ
Data	<p>7.1.2: ajkifijhcgbnobfbhckepbaffdknmg</p> <p>7.1.1: alphbcchbekpcfaknckinfpapdaiiol</p> <p>7.1.0: alphbcchbekpcfaknckinfpapdaiiol</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Your organization's GPO requirements may require the extension ID (the Data value) to be appended with an 'update' URL to control where updates are downloaded from. You can use the Microsoft Edge Add-ons website update URL, which must be separated from the extension ID by a semicolon(;). For more information, see Microsoft's FAQ for Microsoft Edge extensions.</p> </div>

Registry Key for Native Messaging Host	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Edge\NativeMessagingHosts\com.blueprism.messaging
Name	default
Type	REG_SZ
Data	C:\ProgramData\Blue Prism Limited\Blue Prism\com.blueprism.messaging-manifest.json

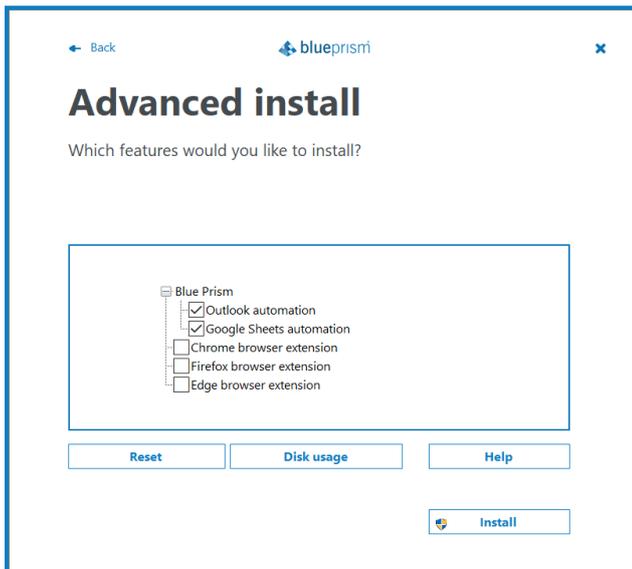
Remove the Edge browser extension

Remove using browser options

Select **Remove from Microsoft Edge** from the extension options.

Remove using the Blue Prism installer

Run the Blue Prism installer and on the Advanced install page, select **Change features** and deselect the Edge extension.



The registry key is deleted and the extension is removed. Alternatively, delete the registry key manually using a registry editor.

Remove using Local Security Policy or Group Policy

To uninstall the Blue Prism Edge extension, remove the value from the specified registry key or delete the entire key if none of the associated settings are required.

Firefox browser extension

The Blue Prism Firefox browser extension establishes connectivity with Blue Prism, allowing Blue Prism to interact with Firefox applications and web pages so data can be exchanged and elements manipulated.

The Blue Prism browser extensions should be installed on any machine that will be used to automate Firefox.

 Mozilla no longer hosts the Blue Prism Firefox browser extension in their web store. As such, you can only install the extension using the Blue Prism installer, or by downloading the package from the Blue Prism Portal.

For details of browser extension and Blue Prism versions, see [browser extension compatibility](#).

Prerequisites

The following are required:

- Extension package (available on the [Blue Prism Portal](#))
- The ability to configure Firefox add-ons
- The Windows Process Performance Counters must be enabled

 This affects Blue Prism versions 7.0 to 7.1.1 only, see [The browser extension is not detected on page 39](#) and [this Knowledge Base article](#) for details on how to address it.

Firefox settings

The Blue Prism Firefox extension requires the following Firefox settings to be applied:

Setting	Value
extensions.autoDisableScopes	0
network.websocket.allowInsecureFromHTTPS	true

For default Firefox installations, the values are automatically applied when the Blue Prism extension is installed. If Firefox is not installed to the default location, the values must be set manually. Enter *about:config* in the Firefox address bar to access the settings.

Install the Firefox browser extension using the Blue Prism installer

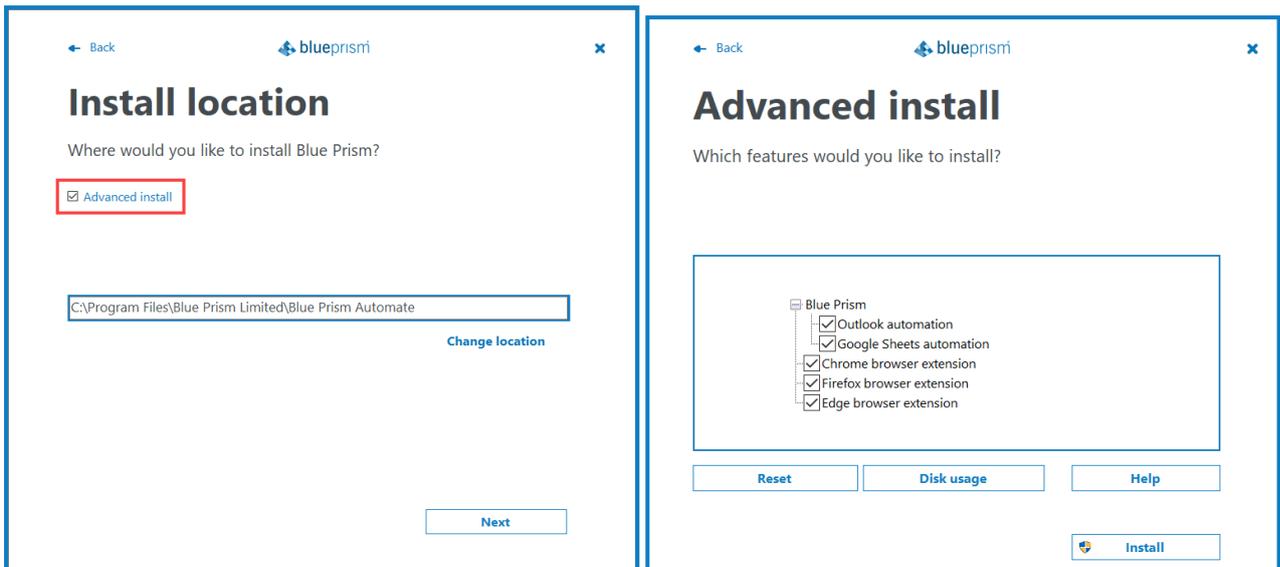
The Blue Prism installer applies a [registry key](#) that installs the Blue Prism extension the next time the browser is started. The installer can be run using the graphical user interface or from the command line. An additional registry key is created for the native messaging host and points to a JSON file which provides details on the allowed extensions and the location of the executable.

Install from the Blue Prism installer

Using the advanced installation option, you can determine which browser extensions (and other optional features) are installed.

1. Run the appropriate Blue Prism installer for your system – 32-bit or 64-bit.
2. Select **Advanced install** from the Install location page of the install wizard.

3. Click **Next** and select the Firefox browser extension and any other features you want to install.



4. Click **Install**.
5. A notification displays prompting you to add the Firefox browser extension. Click **Add**.
6. Complete the installation.

 During an upgrade, the settings already applied for the current installation are maintained unless edited in the advanced install options.

Install from the command line

The following command line options are available for installing Blue Prism and setting the registry key for the Firefox extension. The example commands are for the 7.1 version of Blue Prism – update the version number as required.

Command	Description
<pre>msiexec /i BluePrism7.1_x64 /qn msiexec /i BluePrism7.1_x86 /qn</pre>	Installs Blue Prism and sets Firefox extension registry key as well as those for Chrome and Edge.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=BluePrism,BPServer /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=BluePrism,BPServer /qn</pre>	Installs Blue Prism without setting the browser extension registry keys.
<pre>msiexec /i BluePrism7.1_x64 ADDLOCAL=FirefoxPlugin /qn msiexec /i BluePrism7.1_x86 ADDLOCAL=FirefoxPlugin /qn</pre>	Adds the Firefox extension registry key to an existing installation of Blue Prism.

The ADDLOCAL property can also be used to install multiple Blue Prism components by separating them with a comma. The following command installs 64-bit versions of Blue Prism, and the Chrome, Edge, and Firefox extensions:

```
msiexec /i BluePrism7.1_x64
ADDLOCAL=BluePrism,BPServer,ChromePlugin,EdgePlugin,FirefoxPlugin /qn
```

 The *BluePrism* and *BPServer* components must both be specified to install or upgrade Blue Prism when using the ADDLOCAL parameters. They cannot be used in isolation.

Install the Firefox browser extension using an offline package

If the browser extension has already been installed, updated extensions that are made available after a Blue Prism release are automatically updated when the browser is loaded if there is an active internet connection. For devices that are not connected to the internet, the Blue Prism Firefox extension can be installed offline using an independent package. The extension will need to be installed separately for each user on each device that needs to use the extension. The xpi file for the extension is available from the Blue Prism installation folder.

To install the browser extension for Firefox:

1. Download the required extension package from the [Blue Prism Portal](#).

 A Blue Prism customer portal account is required to access the Blue Prism Portal.

2. In Windows Explorer, navigate to the Blue Prism installation location, for example, C:/Program Files/Blue Prism Limited/Blue Prism Automate/ and locate Firefox Plugin.xpi.

If the file is not there, you will need to:

- a. From Start, open Add or Remove Programs, find Blue Prism and select **Modify**. The Blue Prism Change, fix, remove wizard displays.
- b. Click **Change features**.
- c. Select **Firefox browser extension**, click **Install** and complete the installation.

3. Open Firefox.

4. Click the menu icon and select **Options**.
about:preferences displays.

5. Click **Extensions & Themes** and then click **Extensions**.
about:addons displays with the existing and recommended extensions.

 If you have installed Blue Prism using the installer, you will see a Blue Prism extension on this page.

6. Drag and drop the Firefox Plugin.xpi from Windows Explorer to the Extensions page.
A confirmation message displays.
7. Click **Add**.
The extension installs and displays on the page.

Firefox browser extension registry keys

The following registry keys are applied when installing the browser extension with the Blue Prism installer to instruct the browser to add the Blue Prism extension.

For situations where the browser extension is to be installed independently or, where the registry value applied by the installer is prevented from persisting, such as if network restrictions override them, the setting can be applied using an alternative deployment method, such as Group Policy or Local Security Policy.

The following registry keys can be applied using a Group Po

Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\Extensions
Name	7.1.2: {6ef886df-5a6b-48c2-966d-8f4313563944} 7.1.1: {3f6df374-a2a7-4698-921c-94a7dec8ba9b} 7.1.0: {3f6df374-a2a7-4698-921c-94a7dec8ba9b}
Type	REG_SZ
Data	7.1.2: C:\Program Files\Blue Prism Limited\Blue Prism Automate\FirefoxPlugin.xpi 7.1.1: C:\Program Files\Blue Prism Limited\Blue Prism Automate\FirefoxPlugin.xpi 7.1.0: C:\Program Files\Blue Prism Limited\Blue Prism Automate\FirefoxPlugin.xpi

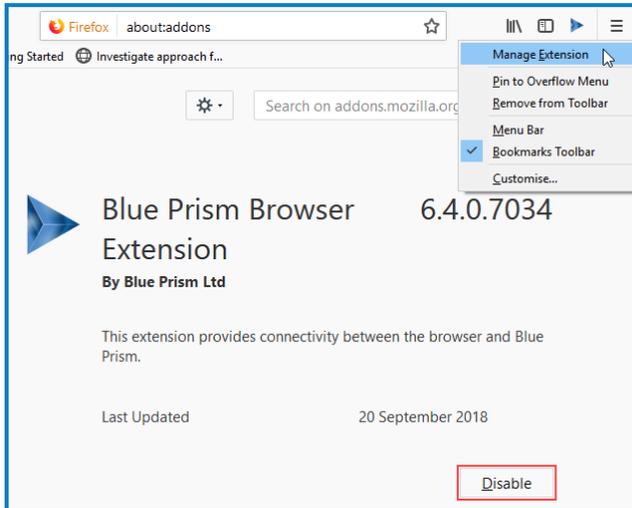
Registry Key for Native Messaging Host	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mozilla\NativeMessagingHosts\com.blueprism.messaging
Name	default
Type	REG_SZ
Data	C:\ProgramData\Blue Prism Limited\Blue Prism\com.blueprism.messaging-firefox-manifest.json

 For custom install locations the path in the data value for the Firefox key is updated accordingly.

Remove the Firefox browser extension

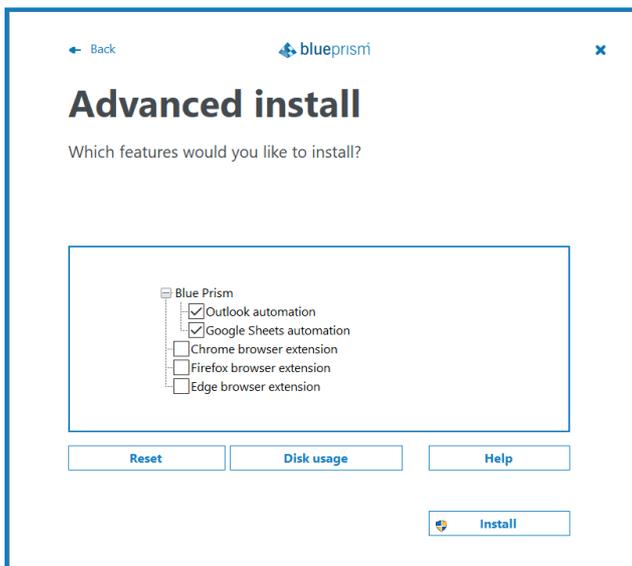
Remove using browser options

Click **Disable** from the Manage Extension options.



Remove using the Blue Prism installer

Run the Blue Prism installer and on the Advanced Install page, select **Change features** and deselect the Firefox extension.



The registry key is deleted and the extension is removed. Alternatively, delete the registry key manually using a registry editor.

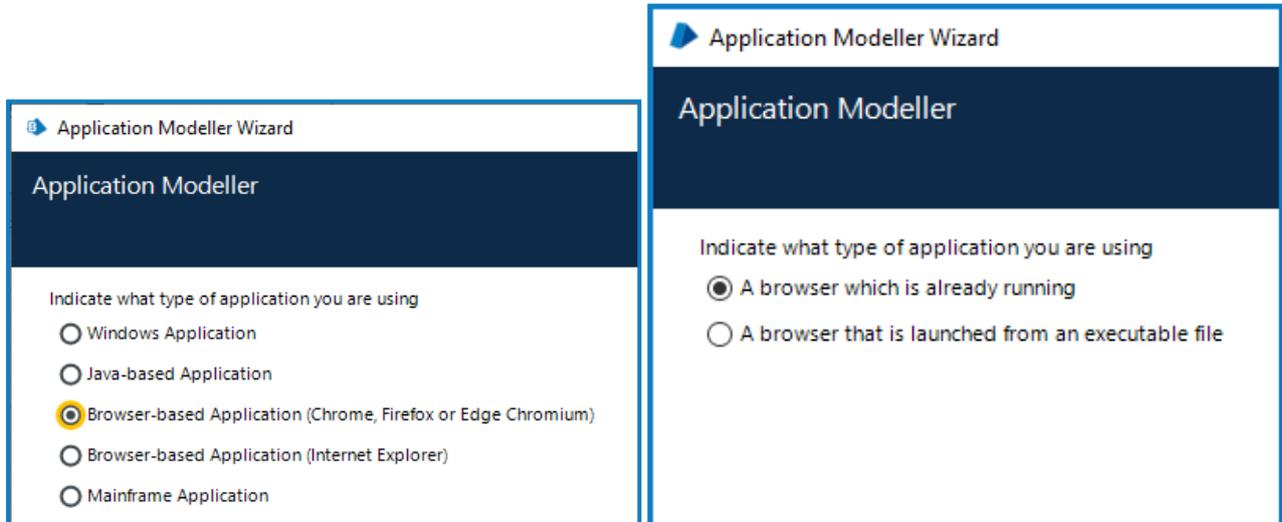
Remove using Local Security Policy or Group Policy

To uninstall the Blue Prism Firefox extension, remove the value from the [specified registry key](#) or delete the entire key if none of the associated settings are required.

Automate Chrome, Edge, and Firefox with the Application Modeller

The Application Modeller provides a dedicated spy mode for interacting with Chrome, Edge, and Firefox.

1. In the Application Modeller wizard, enter a name for the application model and click **Next**.
2. Select the **Browser-based Application (Chrome, Firefox or Edge Chromium)** option. You can then choose to continue using a browser that is already running or a browser launched from an executable.



3. Continue through the wizard, completing the following fields:
 - **Target page title** – When configuring the Application Modeller using a browser that is already running, the window title can be specified. This ensures that the correct tab or window is identified when attaching to the browser. The visible window title is sometimes appended with further text that is not visible to users. Blue Prism adds a * wildcard at the end of the entered text to ensure that the window can be correctly identified. If the window title is not found for attaching, Blue Prism uses the executable to open Chrome, Edge, or Firefox. If the executable path is left blank, an error occurs if Blue Prism fails to attach.

 This option is only available when modelling a browser that is running.

- **Executable path** – The location of the Chrome, Edge, or Firefox executable required by Blue Prism to open the application. This must be the full path, including the file type.
- **Start page URL** – The address of the browser application or web page to be spied. Several URLs can be added, separated by a space. Command line parameters can be appended to a URL, also separated by a space.

If a URL is not entered, the browser opens an about:blank URL and the user must replace it with a valid URL.

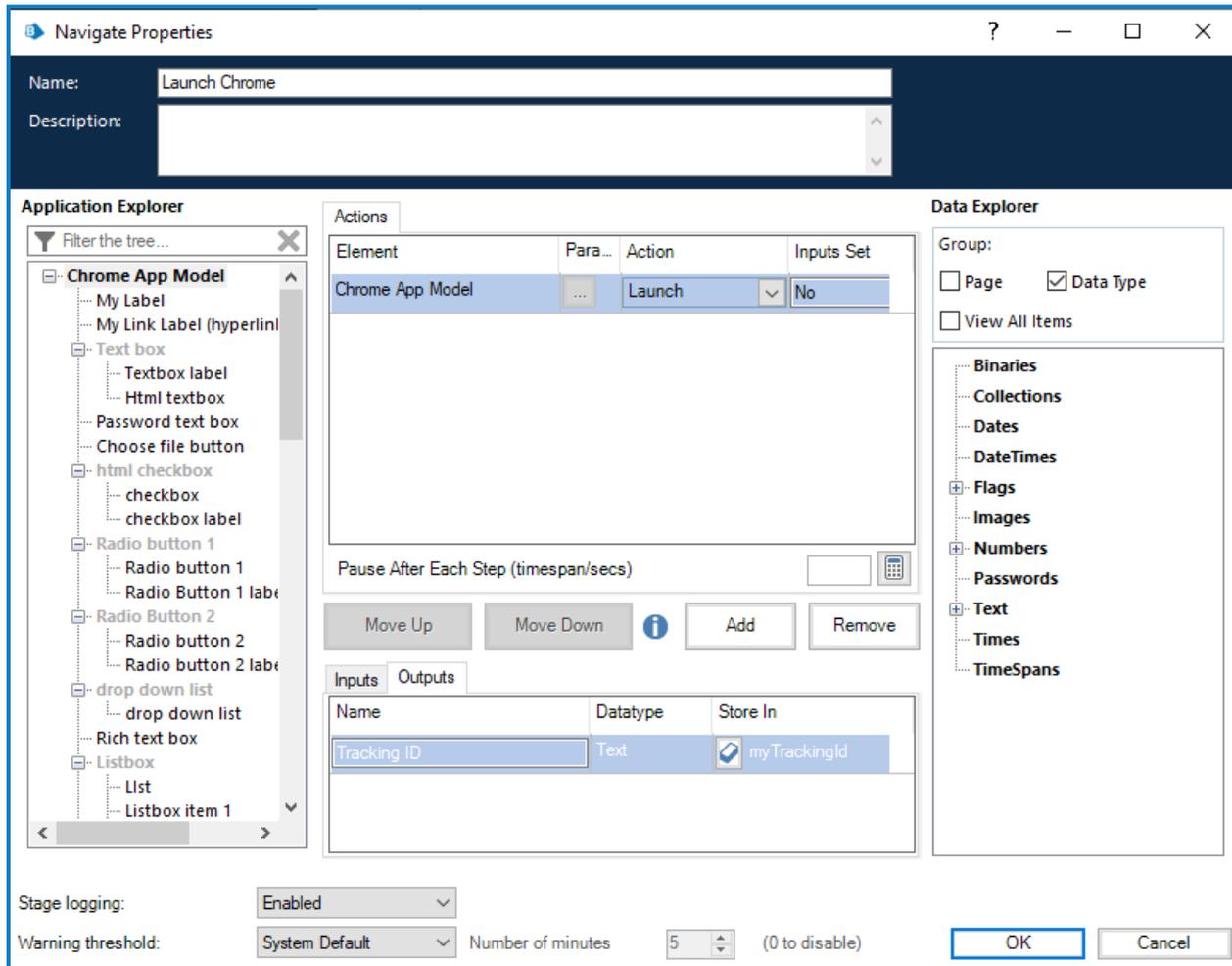
- **Application manager mode** – The browser extension is only compatible with the **Embedded (default)** Application Modeller mode when launching or attaching to Chrome, Edge, or Firefox.

A list of web page attributes and their descriptions for Chrome, Edge, or Firefox automation is available [here](#).

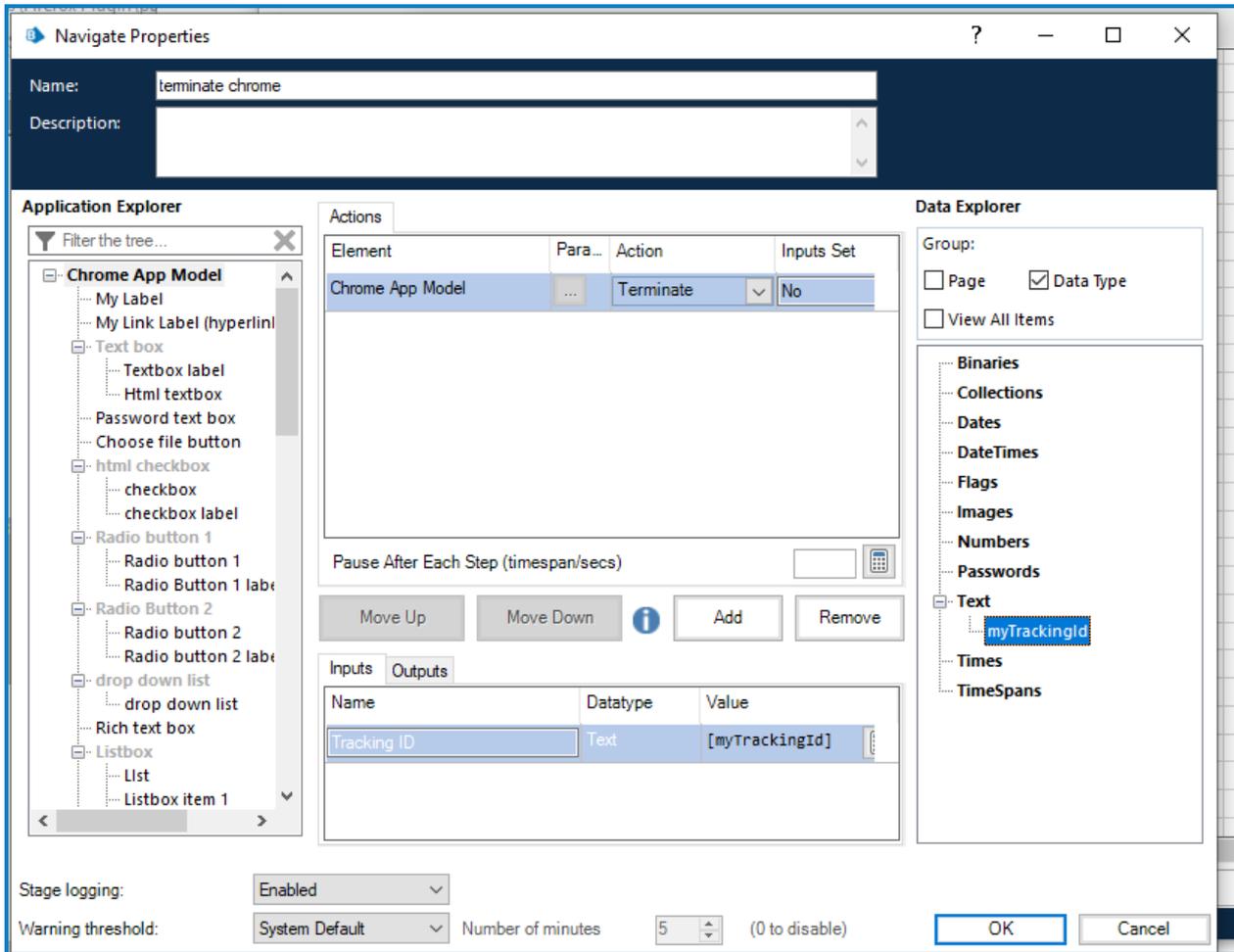
Use Tracking ID to automate multiple browser instances of the same type from a single Blue Prism instance

The spy mode used for interacting with Chrome, Edge, or Firefox can interact with multiple browser instances of the same type (Chrome, Edge, or Firefox) from a single instance of Blue Prism. A unique Tracking ID field can be used in the input or output parameters of various stages to restrict spying to a specific browser.

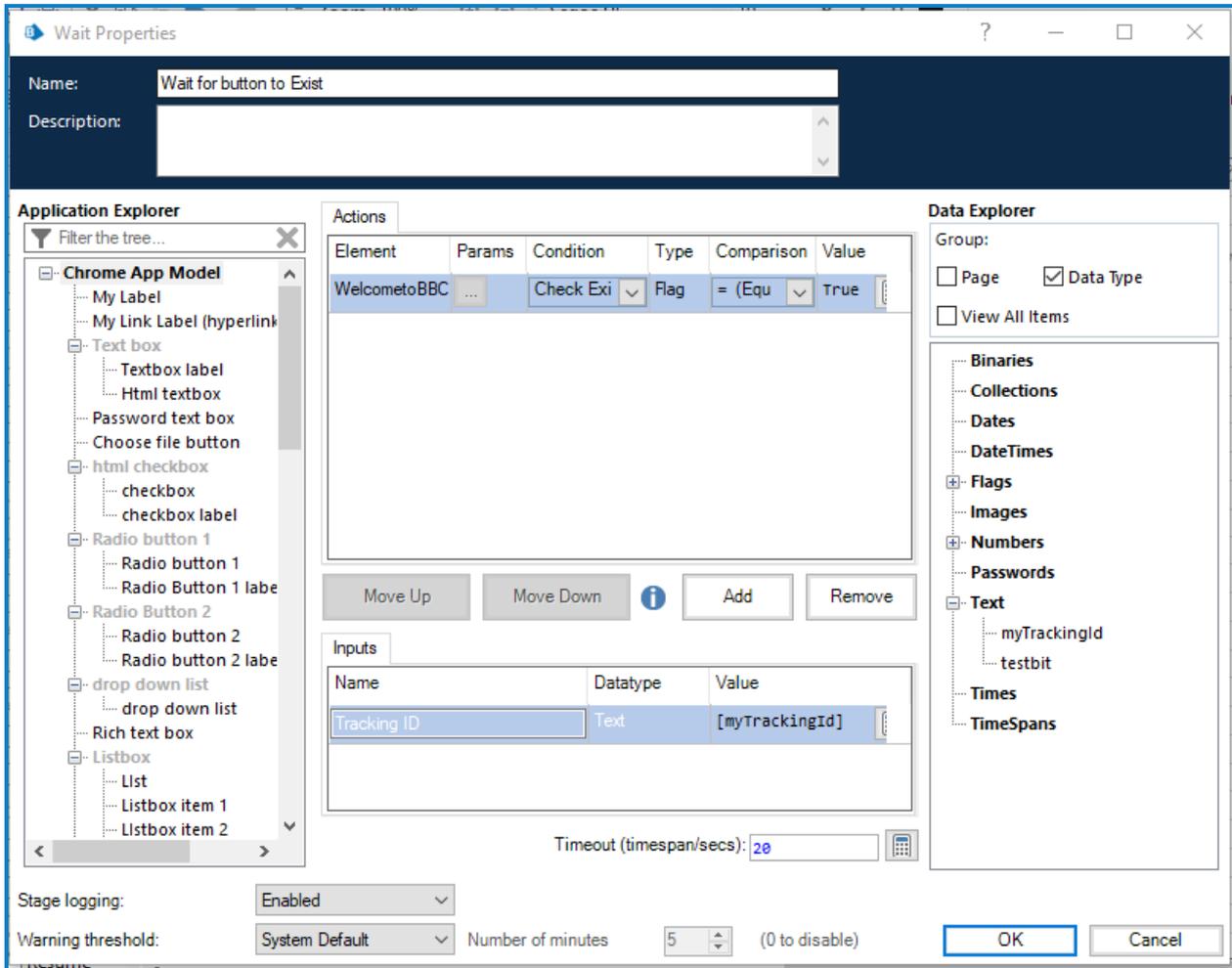
When launching a browser instance, a tracking ID can be applied as an output parameter in the Navigate stage and stored in a Text data item.



When detaching or terminating a browser instance, a tracking ID can be applied as an input parameter in the Navigate stage and only that instance of the browser will be detached/terminated.



The tracking ID can be used in Read, Write, and Wait stages to restrict Blue Prism to only interact with the browser instance that was created in the Launch action matching the tracking ID. This is useful if you have a process that needs to interact with two instances of the same Single Page Application (SPA), as controls in the first browser instance will also appear on the second instance of the browser resulting in spying errors. If using a tracking ID, only the instance of the browser you want to interact with will respond.



Automate multiple browser instances of the same type from multiple Blue Prism instances

You can open multiple instances of Blue Prism and spy multiple browser instances of the same type on the same device without conflict. If a user has two or more separate instances of Blue Prism on the same Windows environment, they can launch a browser from each Blue Prism instance and only spy the browsers launched by a particular instance. This can be combined with tracking IDs to further limit the spying to individual instances of the browser being spied.

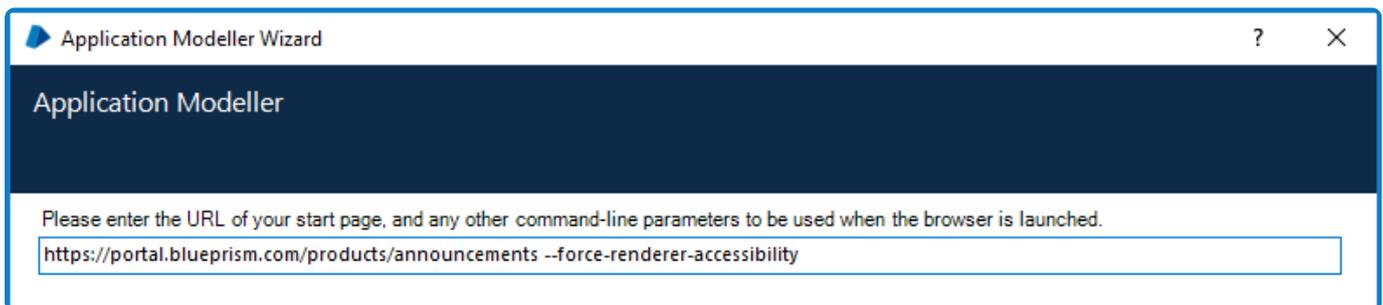
▶ This [video](#) demonstrates how to spy and automate multiple browser windows at the same time.

Automate Chrome and Edge with UI Automation (UIA)

For situations where the Chrome, Edge, or Firefox extensions are not available or if a different approach is required, UIA can be used to automate Chrome. However, using this method is typically not as performant as using the Blue Prism extensions.

Use UIA to model Chrome and Edge

To use UIA, accessibility mode must be enabled in Chrome and Edge browsers. Append the start page URL with the `--force-renderer-accessibility` parameter to open the browsers in accessibility mode. When launched using this parameter, the UIA spy mode can be used to model and interact with Chrome and Edge browsers.



Disable browser extension automatic updates

By default, browser extensions update to the latest version automatically. However, this is not always desirable, for example, if testing or investigations are being carried out in a specific version.

There are two recommended methods that can be used in Chrome, Edge, and Firefox to safely disable the automatic update of extensions by the browser:

- [Sideload an extension below](#) – Sideloaded allows you to install an extension without using a default common installer. It gives an individual user more control over their extensions, so is often used by developers and testers.
- [Local Group Policy on page 32](#) – This method allows rules for extensions to be applied to specific groups of users inside an organization. The rules determine how extensions can be managed, and who can make changes. Using a Local Group Policy is the recommended method for controlling automatic updates for your whole organization.

In addition to these methods, Firefox also contains an option to disable all automatic updates without additional customization, as follows:

1. In Firefox, click the **Open application menu** icon , then select **Add-ons and themes > Extensions**.
2. Click the **Tools for all add-ons** icon  and disable the **update Add-ons automatically** option.

Sideload an extension

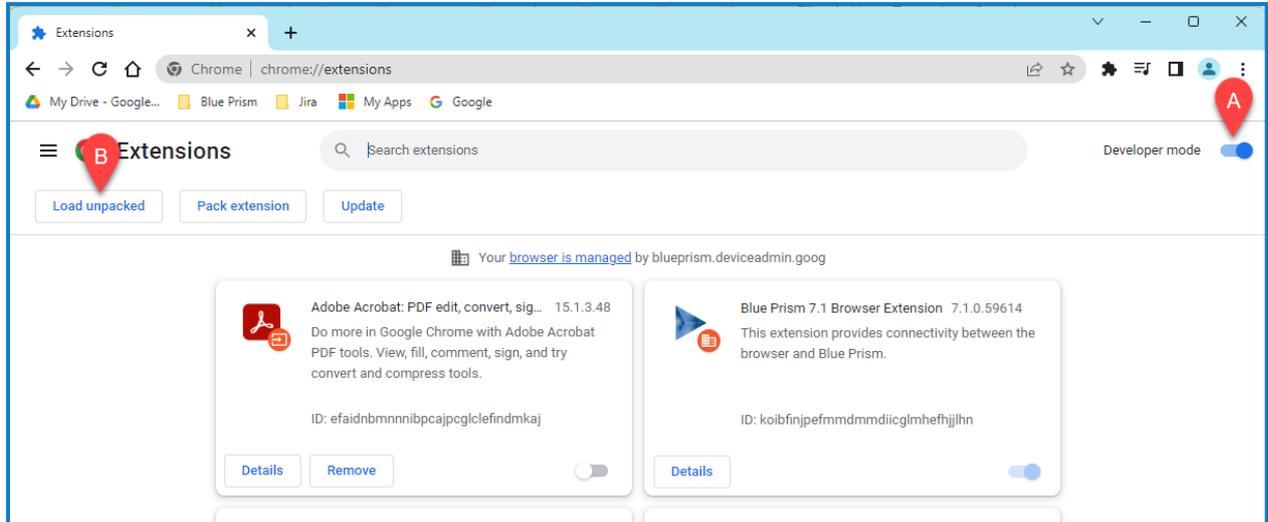
Sideloaded an extension involves manually installing a specific version of an extension. If you use this method, the browser cannot automatically update the extension to another version, or make any changes to it.

See the following browser-specific sections:

- [Chrome](#)
- [Edge](#)
- [Firefox](#)

Chrome

1. In a Chrome browser, click the **Customise and control Google Chrome** icon , then select **More tools > Extensions**, or open a new tab and enter *chrome://extensions*.
2. Enable **Developer mode** (A), and click **Load unpacked** (B).

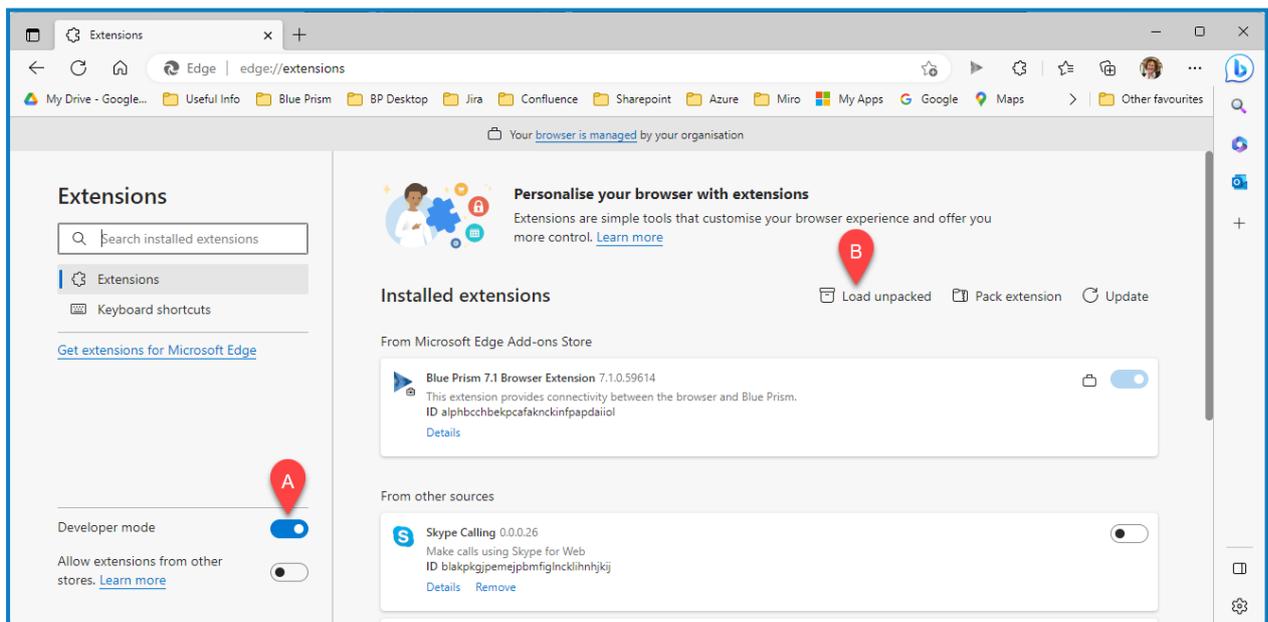


The Select the extension directory file browser opens.

3. Browse to the required file and click **OK** to install the extension.

Edge

1. In an Edge browser, click the **Settings and more** icon , then select **Extensions > Manage extensions**, or open a new tab and enter *edge://extensions*.
2. Enable **Developer mode** (A), and click **Load unpacked** (B).



The Select the extension directory file browser opens.

3. Browse to the required file and click **OK** to install the extension.

Firefox

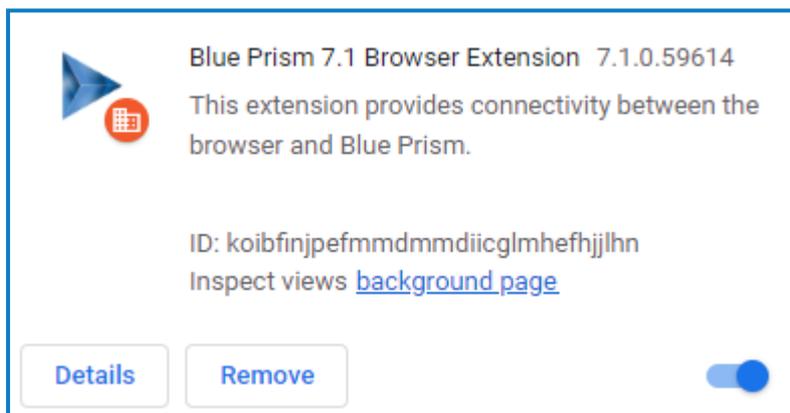
1. In a Firefox browser, click the **Open application menu** icon ☰, then select **Add-ons and themes > Extensions**, or open a new tab and enter *about:addons*.
2. Click the Tools for all add-ons icon ⚙️ and select **Install Add-on from File...**
The Select add-on to install file browser opens.
3. Browse to the required file and click **Open** to install the extension.

Local Group Policy

A Local Group Policy uses rules to control settings for larger groups of users across your organization. You can create Group Policy rules to prevent automatic browser updates in a domain controller or on your local machine, using custom JSON data options that have been defined for each browser.

Before carrying out the browser-specific steps below, you must do the following:

1. Download and install the Group Policy templates for each browser, available through these links:
 - Chrome – [Set policies](#)
 - Edge – [Configure Microsoft Edge policy settings on Windows devices](#)
 - Firefox – [Customizing Firefox Using Group Policy \(Windows\)](#)
2. Fetch the relevant browser extension ID. The ID is displayed in the extension manager of your browser as shown in this example from Chrome, where the extension ID is koibfinjpefmmdmmdiicglmhefhjllhn:



See the following browser-specific sections:

- [Chrome](#)
- [Edge](#)
- [Firefox](#)

Chrome

Use the following JSON data (this is based on examples in the official [Chrome extension configuration documentation](#)), substituting your extension ID and a suitable invalid URL for the placeholders:

```
{ "Your extension ID":  
  {  
    "installation_mode": "normal_installed",  
    "update_url": "Any invalid address",  
    "override_update_url": true  
  }  
}
```

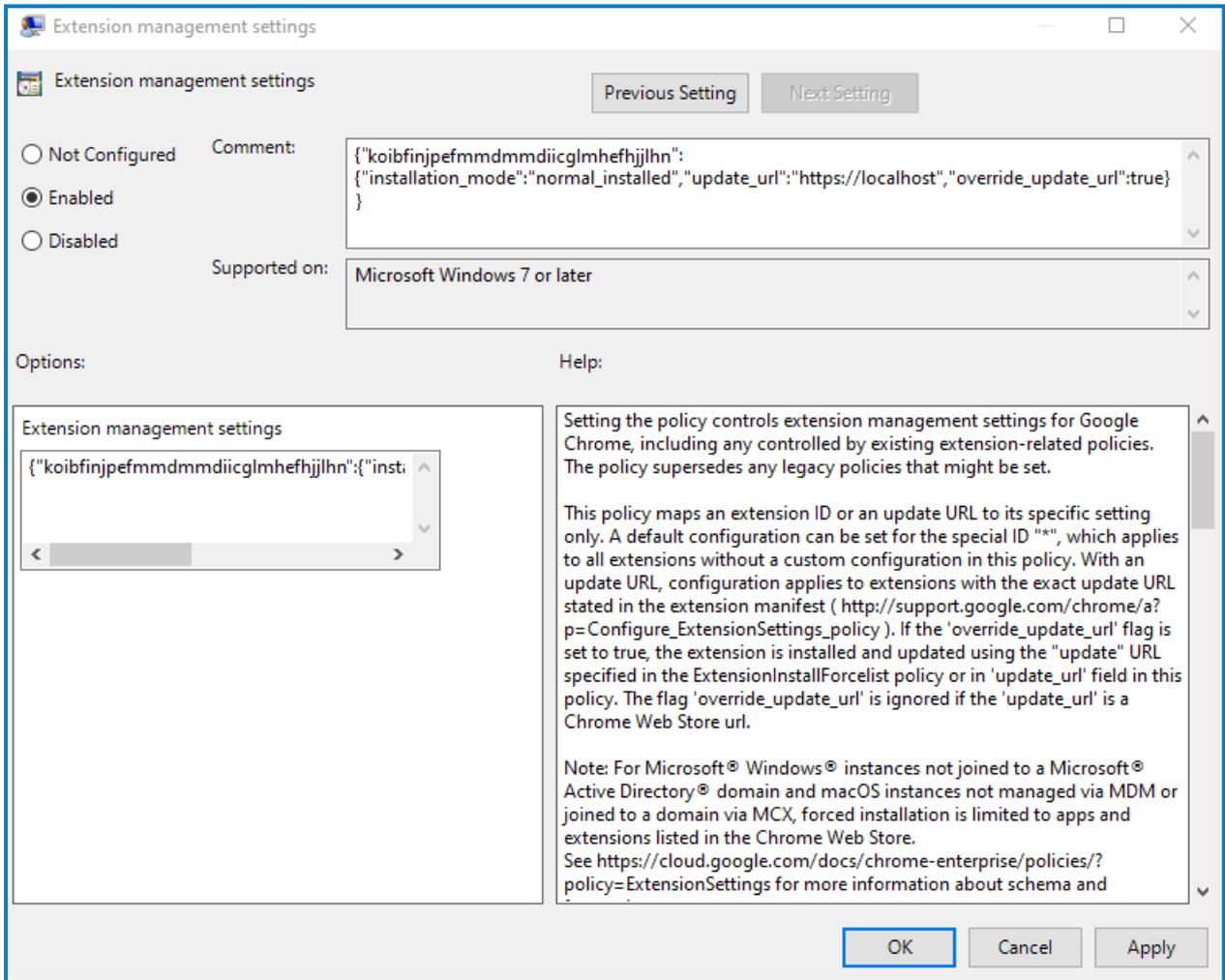
 The `override_update_url` option is set to true, which forces the browser to look at `update_url`. This has an invalid http address, therefore no update is downloaded.

1. Open the Local Group Policy Editor.
2. Go to **User Configuration > Administrative Templates > Google > Google Chrome > Extensions**, and double-click **Extension management settings**.
The Extension management settings window opens.
3. Select **Enabled**, and paste the JSON data with your chosen extension ID into the **Options** field. This must be entered as a single line with no line breaks. This example is for the scenario where the extension ID is `koibfinjpefmmddiicglmhefhjllhn`, and the invalid address is `https://localhost`:

```
{"koibfinjpefmmddiicglmhefhjllhn":{"installation_mode":"normal_installed","update_url":"https://localhost","override_update_url":true}}
```

4. Optionally, you can also paste the JSON data into the Comment field for reference, and include any other appropriate comments.

5. Click **Apply**, then **OK** to update the Group Policy settings for the Chrome browser extension.



Edge

Use the following JSON data (this is based on examples in the official [Edge extension configuration documentation](#)), substituting your extension ID and a suitable invalid URL for the placeholders:

```
{ "Your extension ID":
  {
    "installation_mode": "normal_installed",
    "update_url": "Any invalid address",
    "override_update_url": true
  }
}
```

 The `override_update_url` option is set to true, which forces the browser to look at `update_url`. This has an invalid http address, therefore no update is downloaded.

1. Open the Local Group Policy Editor.
2. Go to **User Configuration > Administrative Templates > Microsoft Edge > Extensions**, and double-click **Configure extension management settings**.

The Configure extension management settings window opens.

3. Select **Enabled**, and paste the JSON data with your chosen extension ID into the **Options** field. This must be entered as a single line with no line breaks. This example is for the scenario where the extension ID is *alphbcchbekpcfaknckinfapdaiiol*, and the invalid address is *https://localhost*:

```
{"alphbcchbekpcfaknckinfapdaiiol":{"installation_mode":"normal_installed","update_url":"https://localhost","override_update_url":true}}
```

4. Optionally, you can also paste the JSON data into the Comment field for reference, and include any other appropriate comments.
5. Click **Apply**, then **OK** to update the Group Policy settings for the Edge browser extension.

Firefox

Use the following JSON data (this is based on examples in the official [Firefox extension configuration documentation](#)), substituting your extension ID and a suitable invalid URL for the placeholders:

```
{"Your extension ID":  
  {  
    "installation_mode":"normal_installed",  
    "install_url":"Any invalid address",  
    "updates_disabled":true  
  }  
}
```

 The `updates_disabled` option is set to true, which forces the browser to look at `install_url`. This has an invalid http address, therefore no update is downloaded.

1. Open the Local Group Policy Editor.
2. Go to **User Configuration > Administrative Templates > Mozilla > Firefox > Extensions**, and double-click **Extension Management**.

The Extension Management window opens.

3. Select **Enabled**, and paste the JSON data with your chosen extension ID into the **Options** field. This must be entered as a single line with no line breaks. This example is for the scenario where the extension ID is *{3f6df374-a2a7-4698-921c-94a7dec8ba9b}*, and the invalid address is *https://localhost*:

```
{"{3f6df374-a2a7-4698-921c-94a7dec8ba9b}":{"installation_mode":"normal_installed","install_url":"https://localhost","updates_disabled":true}}
```

4. Optionally, you can also paste the JSON data into the Comment field for reference, and include any other appropriate comments.
5. Click **Apply**, then **OK**.
6. Open the Command Prompt as Administrator, and run `gpupdate /force`.
7. Carry out a hard refresh of the Firefox browser (Ctrl + F5), or close and open it.

Additional information

See also the following browser-specific information:

- Chrome – An [administration console](#) allows you to define a specific setup for extensions for your organization. For more information about managing extensions for the Chrome browser, see [Managing Extensions in Your Enterprise](#).
- Microsoft Edge – A [self-host guide](#) provides guidance for building packages and deploying them in your organization.

Troubleshooting browser integration

Configure browser timeout parameters

 This functionality is only available from Blue Prism 7.1.2 onwards.

Browser timeout parameters used in Blue Prism extensions may need to be amended if the default configuration is causing issues in a particular environment, or to optimize browser automations across environments.

If individual browser user profiles are used and you want to apply these settings across multiple environments, you must apply them on each user's machine post installation. You can set up shared browser profiles to apply the settings to multiple environments by default. For more information, see [Use Chrome with multiple profiles](#), [Chrome storage](#), and [Create multiple profiles in Microsoft Edge](#).

 Any changes should only be made under guidance from Blue Prism and tested in a Development environment.

The following timeout parameters can be configured in the browser extensions by updating the value in the Current Value column:

- **Native messaging host waits for pages to close** – The amount of time the native messaging host waits for pages to disconnect after the browser has closed. The default value is 30000 milliseconds.
- **Extension logging level** – The logging level used for the extension. Log entries below the current value will not be transmitted to the Chrome DevTools console.
 - 0 = Trace
 - 1 = Debug
 - 2 = Info
 - 3 = Error
- **Maximum connection attempts to service worker** – The maximum number of times the page will attempt to connect to the service worker. The default is 300 attempts.
- **Timeout when creating service worker connection** – The time between attempts to send a connection message to the service worker to establish the connection between Blue Prism and the page. This applies to every page or iframe that comes into existence and connects to the service worker. The default is 1000 milliseconds.
- **Timeout when connecting to a service worker** – The time between attempts to connect to the service worker when a new page loads. This applies to every page or iframe that comes into existence and connects to the service worker. The default value is 100 milliseconds.
- **Message transmit interval** – The amount of time between messages queued for transmission when the service worker is sending messages to Blue Prism via the native messaging host. The default is 10 milliseconds.
- **Timeout when connecting to native messaging host** – The amount of time the extension waits before attempting to connect to the native messaging host in the event of a disconnection. The default is 100 milliseconds.

- **Maximum connection attempts to native messaging host** – The maximum number of times the service worker will attempt to reconnect to the native messaging host in the event of a disconnection. The default is 300 attempts.

Timeout Configuration			
Names	Default	Current Value	
Native messaging host waits for pages to close	30000	30000	
Extension Logging Level	Info	Trace	▼
Maximum Connection Attempts to service worker	300	300	
Timeout when creating Service Worker Connection	1000	1000	
Timeout when Connecting to a service worker	100	100	
Message transmit interval	10	10	
Timeout When connecting to Native Messaging Host	100	100	
Maximum Connection Attempts to Native Messaging Host	300	300	

All values are stored in:

- The Chrome local storage (chrome.storage.local.get)
- The appman_config.xml file located in C:\Users\\AppData\Roaming

Unable to spy elements on a web site

Using the browser extensions to automate web pages relies on a connection between the extension and Blue Prism. Situations where elements of a website cannot be spied can be improved by increasing the timeout between Blue Prism and the browser to allow sufficient time to make the connection.

To troubleshoot this:

1. Navigate to the Blue Prism install location and open the Automate.exe configuration file in a text editor.

- Increase the BrowserAutomation.DefaultCommunicationTimeout value.

The default value is 3000 milliseconds – the optimum value is dependent on the responsiveness of the browser.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7" />
  </startup>
  <appSettings>
    <add key="BrowserAutomation.DefaultCommunicationTimeout" value="3000"/>
  </appSettings>
  <runtime>
```

- Relaunch the browser and navigate to the required website.

 Browser automations should not be run by runtime resources with elevated permissions as this might affect the interaction with the application that is being automated. The permissions of the runtime resources must match those of the user context of the browser extension's native messaging host (NMH).

The Firefox extension does not load

A Firefox advanced setting can prevent new extensions from being enabled.

Enter *about:config* in the Firefox address bar and ensure the following value is applied:

Setting	Value
extensions.autoDisableScopes	0

 This setting is only applicable to the Blue Prism Firefox extension.

Unable to spy websites that use HTTPS in Firefox

A Firefox advanced setting can prevent the extension communicating with Blue Prism from a site that uses the HTTPS protocol.

Enter *about:config* in the Firefox address bar and ensure the following value is applied:

Setting	Value
network.websocket.allowInsecureFromHTTPS	true

 This setting is only applicable to the Blue Prism Firefox extension.

The browser extension is not detected

When launching a Chrome, Edge, or Firefox browser from the Application Modeller, Blue Prism attempts to detect whether the browser extension has been installed or enabled for that browser. If no browser extension is found, a message notifies the user that the browser extension has not been installed or enabled.

This message may also appear in the following scenarios:

- Where the browser extension is not compatible with the Blue Prism version installed (see [The browser extension is not compatible with the Blue Prism version below](#)).
- When the Startup Boost mode is enabled in Edge Chromium browsers.
- When the Windows Performance Counters are not enabled. This affects Blue Prism version 7.0 to 7.1.1 only.

 See [this Knowledge Base article](#) for more details on how to troubleshoot the browser extensions when they are not detected.

The browser extension is not compatible with the Blue Prism version

Users are notified if the browser extension they are using is not compatible with their installed version of Blue Prism. From 6.10 onwards, the versioning of the Blue Prism browser extensions follow the Blue Prism software versioning pattern, for example 6.10.0 for the first release of Blue Prism 6.10.

See also [Troubleshooting - Browser integration](#).