Native Chrome and Firefox integration

Native support for automating web pages and applications in Chrome and Firefox is provided in Blue Prism through the use of browser extensions. The Chrome and Firefox extensions allow Blue Prism to interact with web pages and applications so that business processes that rely on applications presented in those browsers can be modelled.

Install the extensions

The Blue Prism browser extensions should be installed on any machine that will be used to automate Chrome and/or Firefox. The following installation methods are available:

- Install using the Blue Prism installer - The installer applies a registry key that installs an extension the next time Chrome or Firefox are run. Users can run the installer using the graphical interface or the command line. This method ensures the correct version of the extension is installed for the version of the Blue Prism client on the machine.
- Install using Group Policy - This method uses Group Policy or Local Security Policy to create a registry key or to add the appropriate value to an existing key that installs the extension the next time Chrome or Firefox are run.
- Manual Installation (Chrome only) - The Chrome extension is installed directly from the Chrome store using a URL.

Installation considerations

Browser Access

For all installation methods:

- For the Chrome extension, access to the Chrome Store is required.
- For Chrome and Firefox extension, the ability to configure add-ons in the respective browser is required.

Extensions for 32-bit and 64-bit browsers

When installed using the Blue Prism installer or via Group Policy the following behavior is expected:

- **Chrome** - Both 32 and 64-bit versions of the Chrome extension are installed, providing compatibility with both versions of Chrome, whichever Blue Prism installer is used.
- **Firefox** - Installs the extension appropriate to the installed version of Firefox.

Firefox settings

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

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

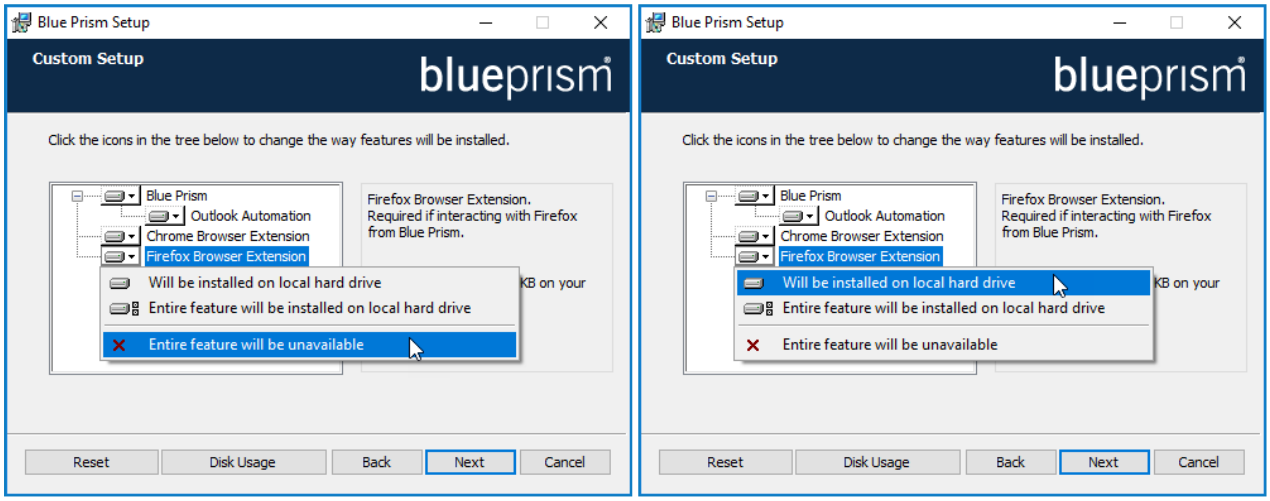
For default Firefox installations, the values are automatically applied when the Blue Prism extension is installed. If Firefox is not installed to the default location, the values must be set manually. Enter *about:config* in the Firefox address bar to access the settings.

Install using the Blue Prism Installer

The Blue Prism installer applies a registry key that installs the Blue Prism extension next time the browser is started.

Run the Blue Prism installer

The registry keys for the browser extensions are set automatically during a default install of Blue Prism. However, a custom installation is available so the Blue Prism components that are not required can be omitted from the installation. Select **Entire feature will be unavailable** from the appropriate drop-down to prevent the installation of a component - the remaining two options both install the component.



Command line installation

The following command line options are available for installing Blue Prism and setting the registry key for the Chrome and Firefox extensions. The example commands are for the 6.4 version of Blue Prism - update the version number as required.

Command	Description
`msiexec /i BluePrism6.4.0_x64 /qn` `msiexec /i BluePrism6.4.0_x86 /qn`	Install Blue Prism and set the Chrome and Firefox extension registry keys.
`msiexec /i BluePrism6.4.0_x64 ADDLOCAL=BluePrism,BPServer /qn` `msiexec /i BluePrism6.4.0_x86 ADDLOCAL=BluePrism,BPServer /qn`	Install Blue Prism without setting the Chrome or Firefox extension registry keys.
`msiexec /i BluePrism6.4.0_x64 ADDLOCAL=ChromePlugin /qn` `msiexec /i BluePrism6.4.0_x86 ADDLOCAL=ChromePlugin /qn`	Adds the Chrome extension registry key to an existing installation of Blue Prism.
`msiexec /i BluePrism6.4.0_x64 ADDLOCAL=FirefoxPlugin /qn` `msiexec /i BluePrism6.4.0_x86 ADDLOCAL=FirefoxPlugin /qn`	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 and Firefox extensions:

```
msiexec /i BluePrism6.4.0_x64 ADDLOCAL=BluePrism,BPServer,ChromePlugin,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 using Group Policy

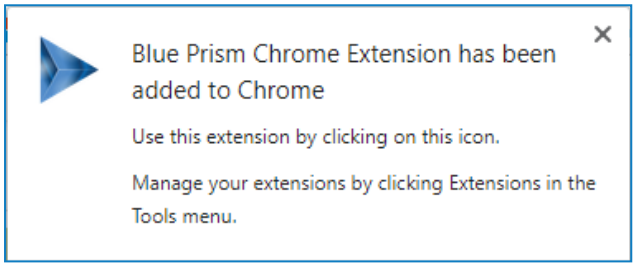
To install the extensions using Group Policy, apply the registry key and value specified in The Blue Prism Chrome registry key.

Manual installation (Chrome only)

An additional installation method is available for Chrome that installs the Blue Prism extension through the Chrome web store using this URL:

https://chrome.google.com/webstore/detail/blue-prism-chrome-extensi/oaflhlmnamdgbgdgakpihkkdfapkebfp

Click the link or paste the URL into the Chrome address bar. When the Blue Prism Extension page displays, 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 Chrome menu.



The Blue Prism extension registry keys

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

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

Chrome

Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist
Name	1
Type	REG_SZ
Data	oaflhlmnamdgbgdgakpihkkdfapkebfp;https://clients2.google.com/service/update2/crx

Firefox

Registry Key	HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\Extensions
Name	{e385850c-828c-4c0e-96fc-c5dcc5bf947f}
Type	REG_SZ
Data	C:\Program Files\Blue Prism Limited\Blue Prism Automate\FirefoxPlugin.xpi

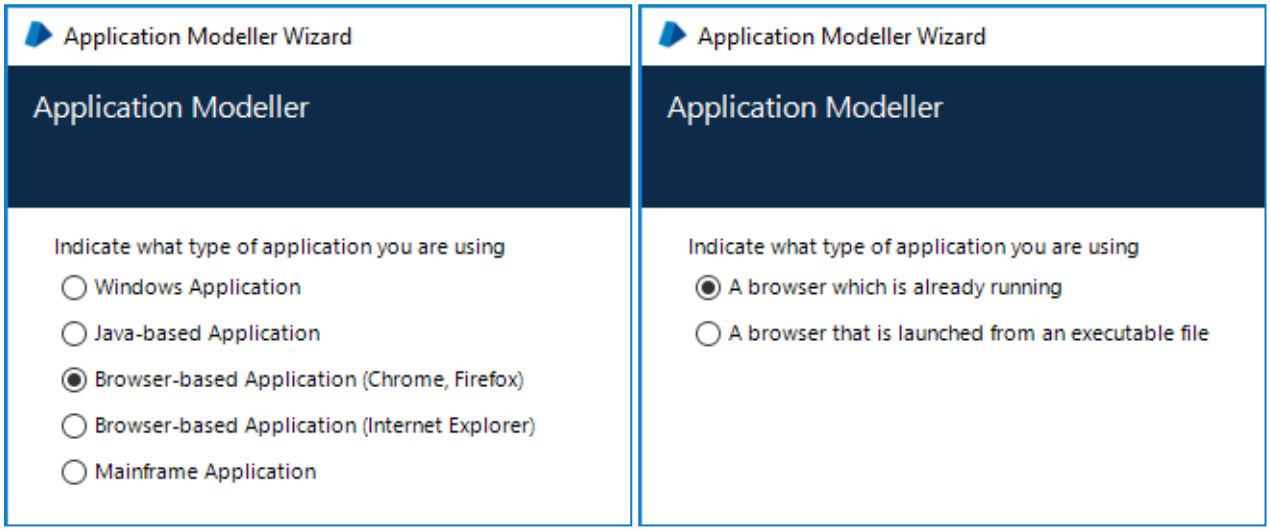
For custom install locations, the path in the data value for the Firefox key is updated accordingly.

Automate Chrome and Firefox with the Application Modeller

A dedicated spy mode is available in the Application Modeller for interacting with Chrome and Firefox.

In the Application Modeller wizard, enter a name for the application model and click **Next**.

Select the **Browser-based Application (Chrome, Firefox)** option. You can then choose to continue using a browser that is already running or by launching a new instance.



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 or Firefox. If the executable path is left blank, an error is thrown if Blue Prism fails to attach.

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

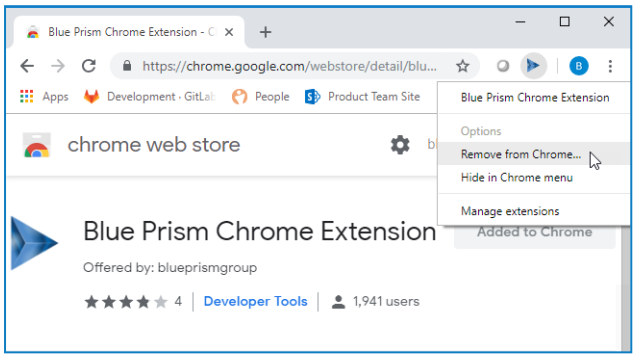
- **Executable path** - The location of the Chrome or Firefox executable required by Blue Prism to open the application. This must be the full path, including the file type.
- **Start page URL** - The address of the browser application or web page to be spied. If a URL is not supplied, the browser opens at the home page set on the machine. Command-line parameters can be appended to a URL, separated by a space.
- **Application manager mode** - The browser extension is only compatible with the *Embedded (Default)* Application Modeller mode when launching or attaching to Chrome or Firefox.

Remove the Blue Prism extension

Manually remove the extension

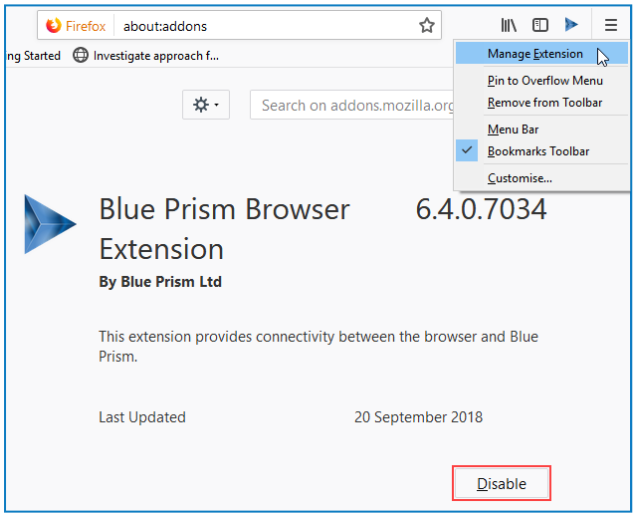
Chrome

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



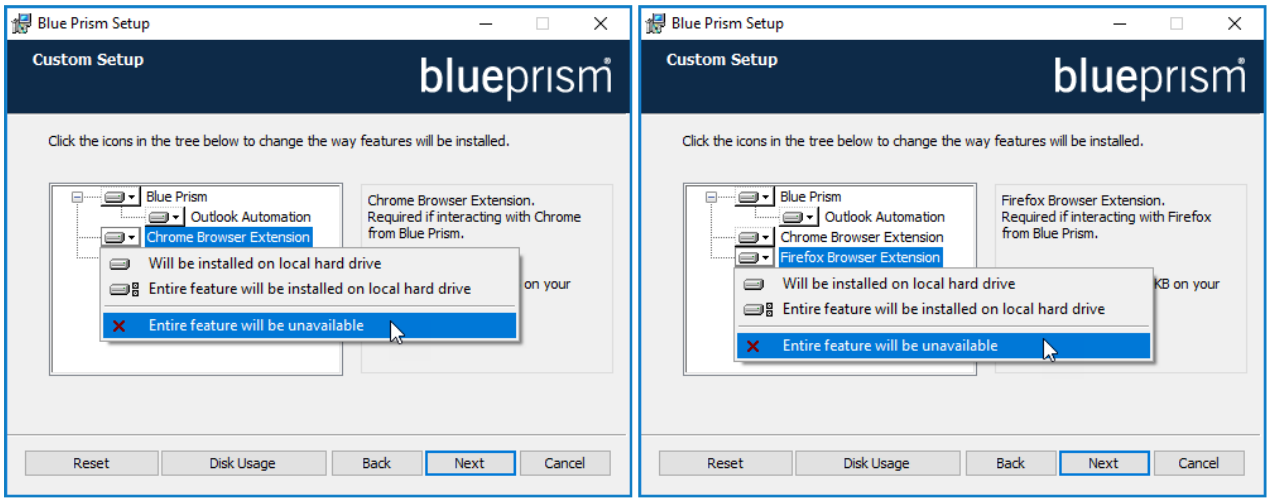
Firefox

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



Remove using the Blue Prism installer

Run the Blue Prism installer and, in the Custom Setup page, select **Entire feature will be unavailable** from the appropriate browser extension drop-down.



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

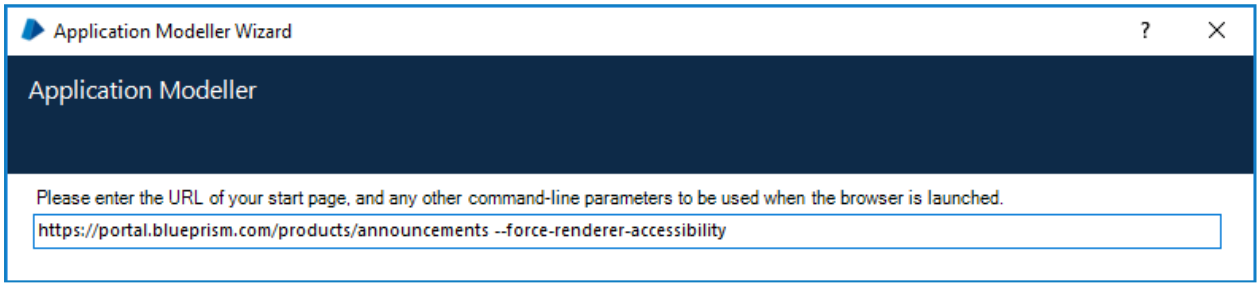
To uninstall the Blue Prism Chrome extension, remove the value from the specified registry key or delete the entire key if none of the associated settings are required.

Automate Chrome with UI Automation (UIA)

For situations where the Chrome 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

To use UIA, accessibility mode must be enabled in Chrome. 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.



Troubleshooting

The following troubleshooting procedures should only be used by advanced users.

Chrome and Firefox

This setting is applicable to both Chrome and Firefox Blue Prism extensions.

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.

How to change the setting

1. Navigate to the Blue Prism install location and open the Automate.exe configuration file in a text editor.
2. 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>
```

3. Relaunch Firefox and navigate to the required website.

Firefox

These settings are only applicable to the Blue Prism Firefox extension.

The 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

Unable to spy websites that use HTTPS

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