bitwarden | Help Center Article

ADMIN CONSOLE > DEPLOY CLIENT APPS >

Deploy Browser Extensions using GPOs, Linux Policies, & .plist Files

View in the help center:
https://bitwarden.com/help/browserext-deploy/

Deploy Browser Extensions using GPOs, Linux Policies, & .plist Files

When operating Bitwarden in a business setting, administrators may want to automate deployment of Bitwarden browser extensions to users with an endpoint management platform or group policy. This article will cover how to use GPOs and other templates to automate deployment of Bitwarden browser extensions to users with an endpoint management platform.

Windows

Deploying Bitwarden browser extensions to browsers on Windows generally require using Windows Group Policy to target managed computers an ADMX policy template. The procedure is slightly different for each browser:

⇒Chrome

To deploy the browser extension on Windows and Google Chrome:

1. Download and unzip the Chrome Enterprise Bundle for Windows.
2. From the unzipped directory:
   - Copy `\Configuration\admx\chrome.admx` to `C:\Windows\PolicyDefinitions`
   - Copy `\Configuration\admx\en-US\chrome.adml` to `C:\Windows\PolicyDefinitions\en-US`
3. Open the Windows Group Policy Manager and create a new GPO for Bitwarden browser extension installation.
4. Right-click on the new GPO and select **Edit...**, and proceed to navigate to **Computer Configuration** → **Policies** → **Administrative Templates** → **Google Chrome** → **Extensions**.
5. In the right-hand settings area, select **Configure the list of force-installed apps and extensions**. In the dialog, toggle the **Enabled** option.
6. Select the **Show...** button and add the following:

   ```Bash
   nngceckbapebfimnlniiiahkandclblb;https://clients2.google.com/service/update2/crx
   ```

   Click **OK**.
7. Still in **...Administrative Templates** → **Google Chrome**, select **Password manager** from the file tree.
8. In the right-hand settings area, right-click **Enable saving passwords to the password manager** and select **Edit**. In the dialog, toggle the **Disabled** option and select **OK**.
9. Repeat **Step 8** for the **Enable Autofill for addresses** and **Enable Autofill for credit cards** options, found in settings area for **...Administrative Templates** → **Google Chrome**.
10. Apply the newly-configured GPO to your desired scope.

⇒Firefox

To deploy the browser extension on Windows and Firefox:

1. Download and unzip the Firefox ADMX Template file.
2. From the unzipped directory:
   - Copy `\policy_templates_<version>\windows\firefox.admx` to `C:\Windows\PolicyDefinitions`
   - Copy `\policy_templates_<version>\windows\en-US\firefox.adml` to `C:\Windows\PolicyDefinitions\en-US`
3. Open the Windows Group Policy Manager and create a new GPO for the Bitwarden browser extension installation.
4. Right-click on the new GPO and select **Edit...**, and proceed to navigate to **Computer Configuration → Policies → Administrative Templates → Firefox → Extensions**.
5. In the right-hand settings area, select **Extensions to Install**. In the dialog, toggle the **Enabled** option.
6. Select the **Show...** button and add the following:

   ```
   Bash

   https://addons.mozilla.org/firefox/downloads/latest/bitwarden-password-manager/latest.xpi
   ```

   Click **OK**.
7. Back in the file tree select **Firefox**. In the right-hand settings area, **Edit...** and disable both the **Offer to save logins** and **Offer to save logins (default)** options.
8. Apply the newly-configured GPO to your desired scope.

⇒Edge

To deploy the browser extension on Windows and Edge:

1. Download and unzip the Microsoft Edge Policy Files.
2. From the unzipped directory:
   - Copy `\windows\admx\msedge.admx` to `C:\Windows\PolicyDefinitions`
   - Copy `\windows\admx\en-US\msedge.adml` to `C:\Windows\PolicyDefinitions\en-US`
3. Open the Windows Group Policy Manager and create a new GPO for the Bitwarden browser extension installation.
4. Right-click on the new GPO and select **Edit...**, and proceed to navigate to **Computer Configuration → Policies → Administrative Templates → Microsoft Edge → Extensions**.
5. In the right-hand settings area, select **Control which extensions are installed silently**. In the dialog, toggle the **Enabled** option.
6. Select the **Show...** button and add the following:

```Bash
jbkfoedolllekgbhcbcoahefnbanhhlh;https://edge.microsoft.com/extensionwebstorebase/v1/crx
```

Click **OK**.

7. Still in **..Administrative Templates → Microsoft Edge**, select **Password manager and protection** from the file tree.
8. In the right-hand settings area, right-click **Enable saving passwords to the password manager** and select **Edit**. In the dialog, toggle the **Disabled** option and select **OK**.
9. Repeat **Step 8** for the **Enable Autofill for addresses** and **Enable Autofill for payment instruments** options, found in settings area for **...Administrative Templates → Microsoft Edge**.
10. Apply the newly-configured GPO to your desired scope.

Linux

Deploying Bitwarden browser extensions to browsers on Linux generally involves using a `.json` file to set configuration properties. The procedure is slightly different for each browser:

⇒Chrome

To deploy the browser extension on Linux and Google Chrome:

1. Download the Google Chrome .deb or .rpm for Linux.
2. Download the Chrome Enterprise Bundle.
3. Unzip the Enterprise Bundle (`GoogleChromeEnterpriseBundle64.zip` or `GoogleChromeEnterpriseBundle32.zip`) and open the `/Configuration` folder.
4. Make a copy of the `master_preferences.json` (in Chrome 91+, `initial_preferences.json`) and rename it `managed_preferences.json`.
5. Add the following to `managed_preferences.json`:

```Bash
{
  "policies:" {
  "ExtensionSettings": {
    "nngceckbapebfimnlniiiahkandclblb": {
      "installation_mode": "force_installed",
      "update_url":
         "https://clients2.google.com/service/update2/crx"
      }
    }
  }
}
```

In this JSON object, `"nngceckbapebfimnlniiiahkandclblb"` is the application identifier for the Bitwarden browser extension. Similarly, `"https://clients2.google.com/service/update2/crx"` signals Chrome to use the Chrome Web Store to retrieve the identified application.

> **ⓘ Note**
>
> You may also configure forced installations using the ExtensionInstallForcelist policy, however the ExtensionSettings method will supersede ExtensionInstallForceList.

6. (**Recommended**) To disable Chrome's built-in password manager, add the following to `managed_preferences.json` inside of `"policies": { }`:

```Bash
{
  "PasswordManagerEnabled": false
}
```

7. Create the following directories if they do not already exist:

```Bash
mkdir /etc/opt/chrome/policies
mkdir /etc/opt/chrome/policies/managed
```

8. Move `managed_preferences.json` into `/etc/opt/chrome/policies/managed`.

9. As you will need to deploy these files to users' machines, we recommend making sure only admins can write files in the `/managed` directory:

```
Bash

chmod -R 755 /etc/opt/chrome/policies
```

10. Using your preferred software distribution or MDM tool, deploy the following to users' machines:
    - Google Chrome Browser
    - `/etc/opt/chrome/policies/managed/managed_preferences.json`

> **Tip**
> For more help, refer to Google's Chrome Browser Quick Start for Linux guide.

⇒Firefox

To deploy the browser extension on Linux and Firefox:

1. Download Firefox for Linux.
2. Create a `distribution` directory within the Firefox installation directory.
3. In the `distrubition` directory, create a file `policies.json`.
4. Add the following to `policies.json`:

```
Bash

{
"policies": {
 "ExtensionSettings": {
   "446900e4-71c2-419f-a6a7-df9c091e268b": {
     "installation_mode": "force_installed",
     "install_url": "https://addons.mozilla.org/firefox/downloads/latest/bitwarden-password-mana
ger/latest.xpi"
      }
    }
  }
}
```

In this JSON object, `"446900e4-71c2-419f-a6a7-df9c091e268b"` is the extension ID for the Bitwarden browser extension. Similarly, `"https://addons.mozilla.org/firefox/downloads/latest/bitwarden-password-manager/latest.xpi"` signals Firefox to use the extension store to retrieve the extension.

5. (**Recommended**) To disable Firefox's built-in password manager, add the following to `policies.json` inside of `"policies": { }`:

```
Bash

{
 "PasswordManagerEnabled": false
}
```

6. Using your preferred software distribution or MDM tool, deploy the following to users' machines:
   - Firefox Browser
   - `/distribution/policies.json`

> **Tip**
> For more help, refer to Firefox's policies.json Overview or Policies README on Github.

MacOS

Deploying Bitwarden browser extensions to browsers on macOS generally involves using a property list (`.plist`) file. The procedure is slightly different for each browser:

⇒Chrome

To deploy the browser extension on macOS & Google Chrome:

1. Download the Google Chrome .dmg or .pkg for macOS.
2. Download the Chrome Enterprise Bundle.
3. Unzip the Enterprise Bundle (`GoogleChromeEnterpriseBundle64.zip` or `GoogleChromeEnterpriseBundle32.zip`).
4. Open the `/Configuration/com.Google.Chrome.plist` file with any text editor.
5. Add the following to the `.plist` file:

```Bash
<key>ExtensionSettings</key>
<dict>
  <key>nngceckbapebfimnlniiiahkandclblb</key>
  <dict>
    <key>installation_mode</key>
    <string>force_installed</string>
    <key>update_url</key>
    <string>https://clients2.google.com/service/update2/crx</string>
  </dict>
 </dict>
```

In this codeblock, `nngceckbapebfimnlniiiahkandclblb` is the application identifier for the Bitwarden browser extension. Similarly, `https://clients2.google.com/service/update2/crx` signals Chrome to use the Chrome Web Store to retrieve the identified application.

> **Note**
> You may also configure forced installations using the ExtensionInstallForcelist policy, however the ExtensionSettings method will supersede ExtensionInstallForceList.

6. (**Recommended**) To disable Chrome's built-in password manager, add the following to `com.Google.Chrome.plist`:

```Bash
<key>PasswordManagerEnabled</key>
<false />
```

7. Convert the `com.Google.Chrome.plist` file to a configuration profile using a conversion tool like mcxToProfile.
8. Deploy the Chrome `.dmg` or `.pkg` and the configuration profile using your software distribution or MDM tool to all managed computers.

> **Tip**
> For more help, refer to Google's Chrome Browser Quick Start for Mac guide.

⇒Firefox

To deploy the browser extension on MacOS and Firefox:

1. Download and install Firefox for Enterprise for macOS.
2. Create a `distribution` directory in `Firefox.app/Contents/Resources/`.

3. In the created `/distribution` directory, create a new file `org.mozilla.firefox.plist`.

> **Tip**
>
> Use the Firefox .plist template and Policy README for reference.

4. Add the following to `org.mozilla.firefox.plist`:

```
Bash

<key>ExtensionSettings</key>
<dict>
   <key>446900e4-71c2-419f-a6a7-df9c091e268b</key>
   <dict>
     <key>installation_mode</key>
     <string>force_installed</string>
     <key>update_url</key>
     <string>https://addons.mozilla.org/firefox/downloads/latest/bitwarden-password-manager/late
st.xpi</string>
   </dict>
 </dict>
```

In this codeblock, `446900e4-71c2-419f-a6a7-df9c091e268b` is the extension ID for the Bitwarden browser extension. Similarly, `https://addons.mozilla.org/firefox/downloads/latest/bitwarden-password-manager/latest.xpi` signals Firefox to use the extension store to retrieve the application.

5. (**Recommended**) To disable Firefox's built-in password manager, add the following to `org.mozilla.firefox.plist`:

```
Bash

<dict>
  <key>PasswordManagerEnabled</key>
  <false/>
</dict>
```

6. Convert the `org.mozilla.firefox.plist` file to a configuration profile using a conversion tool like mcxToProfile.

7. Deploy the Firefox `.dmg` and the configuration profile using your software distribution or MDM tool to all managed computers.

⇒Edge

To deploy the browser extension on macOS and Microsoft Edge:

1. Download the Microsoft Edge for macOS .pkg file.

2. In Terminal, use the following command to create a `.plist` file for Microsoft Edge:

```
Bash

/usr/bin/defaults write ~/Desktop/com.microsoft.Edge.plist RestoreOnStartup -int 1
```

3. Use the following command to convert the `.plist` from binary to plain text:

```
Bash

/usr/bin/plutil -convert xml1 ~/Desktop/com.microsoft.Edge.plist
```

4. Open `com.microsoft.Edge.plist` and add the following:

```
Bash

<key>ExtensionSettings</key>
<dict>
  <key>jbkfoedolllekgbhcbcoahefnbanhhlh</key>
  <dict>
    <key>installation_mode</key>
    <string>force_installed</string>
    <key>update_url</key>
    <string>https://edge.microsoft.com/extensionwebstorebase/v1/crx</string>
  </dict>
</dict>
```

In this codeblock, `jbkfoedolllekgbhcbcoahefnbanhhlh` is the application identifier for the Bitwarden browser extension. Similarly, `https://edge.microsoft.com/extensionwebstorebase/v1/crx` signals Edge to use the Edge Add-On Store to retrieve the identified application.

> **Note**
>
> You may also configure forced installations using the ExtensionInstallForceList, however the ExtensionSettings method will supersede ExtensionInstallForceList.

5. (**Recommended**) To disable Edge's built-in password manager, add the following to `com.microsoft.Edge.plist`:

```
Bash

<key>PasswordManagerEnabled</key>
<false/>
```

6. Convert the `com.microsoft.Edge.plist` file to a configuration profile using a conversion tool like mcxToProfile.

7. Deploy the Edge `.pkg` and the configuration profile using your software distribution or MDM tool to all managed computers.

> **Tip**
>
> **For Jamf-specific** help, refer to Microsoft's documentation on Configuring Microsoft Edge policy settings on macOS with Jamf.