ADMIN CONSOLE > DEPLOY CLIENT APPS

Deactivate Browser Password Managers Using Device Management

View in the help center:
https://bitwarden.com/help/deactivate-browser-password-managers/

Deactivate Browser Password Managers Using Device Management

This article will direct you on how to disable various web browser's built-in password managers using group policy. These steps will help prevent corporate logins from being saved and synchronized to personal accounts. You may also consider deploying the Bitwarden browser extension to all browsers as part of this same policy.

Disable with Windows GPO

⇒Disable Edge

1. Open Group Policy Management Editor on your managing Windows server.

2. Download the appropriate Edge Policy Template.

3. In Group Policy Editor, create a new GPO for Edge and provide an appropriate name.

4. Choose your desired scope.

5. Right-click the new Group Policy **Object** → **Edit**.

6. On the Group Policy Management Editor, go to **User Configuration** → **Policies** → **Administrative Templates** → **Microsoft Edge**.

7. Set the following policies:

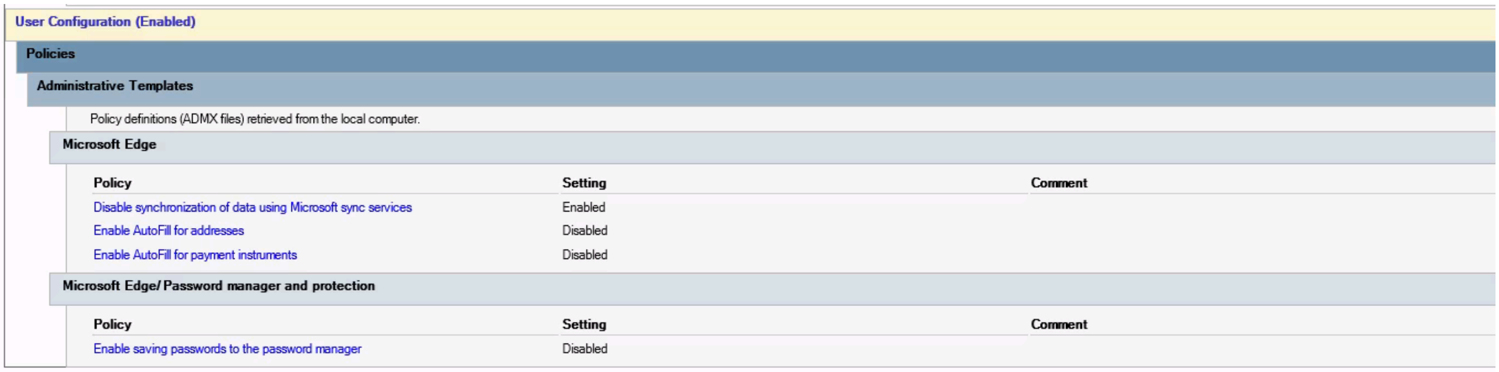
   - Open "Password manager and protection," disable the policy **Enable saving passwords to the password manager**.

   - Disable the policy **Enable AutoFill for addresses**.

   - Disable the policy **Enable AutoFill for payment instruments**.

   - Optionally, you can enable the policy **Disable synchronization of data using Microsoft sync services**.

   Once complete, the GPO **settings** should show the following:



User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Microsoft Edge

Policy	Setting	Comment
Disable synchronization of data using Microsoft sync services	Enabled	
Enable AutoFill for addresses	Disabled	
Enable AutoFill for payment instruments	Disabled	

Microsoft Edge/ Password manager and protection

Policy	Setting	Comment
Enable saving passwords to the password manager	Disabled	

Edge Settings

8. Ensure the GPO link is enabled.

⇒Disable Chrome

1. Open Group Policy Management Editor on your managing Windows server.

2. Download the Google Chrome Administrative Templates.

3. In the `ADMX` file, copy the following:
   `policy_templates\windows\admx\chrome.admx`
   and
   `policy_templates\windows\admx\google.admx`

   TO `C:\Windows\PolicyDefinitions`

4. In the `ADML` file, copy the following:
   `policy_templates\windows\admx\en-us\chrome.adml`
   and
   `policy_templates\windows\admx\en-us\google.adml`

   TO `C:\Windows \PolicyDefinitions\en-us`

5. In Group Policy Editor, create a new GPO for Chrome and provide an appropriate name.

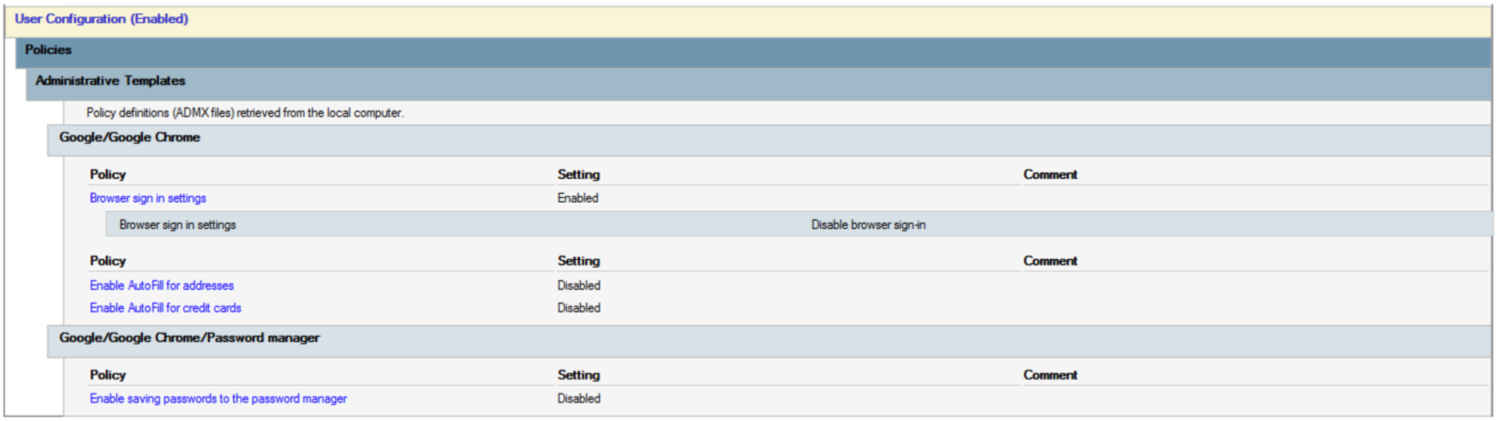
6. Choose your desired scope.

7. Right-click the **Group Policy Object** → **Edit**.

8. Go to **User Configuration** → **Policies** → **Administrative Templates** → **Google** → **Google Chrome**.

9. Edit the following settings:
   - Under "Password Manager," disable the policy **Enable saving passwords to the password manager**.
   - Disable the policy **Enable AutoFill for Addresses**.
   - Disable the policy **Enable AutoFill for credit cards**.

10. Once complete, the GPO **settings** should show the following:



User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Google/Google Chrome

Policy	Setting	Comment
Browser sign in settings	Enabled	
Browser sign in settings	Disable browser sign-in	

Policy	Setting	Comment
Enable AutoFill for addresses	Disabled	
Enable AutoFill for credit cards	Disabled	

Google/Google Chrome/Password manager

Policy	Setting	Comment
Enable saving passwords to the password manager	Disabled	

Chrome Settings

11. Ensure the GPO link is enabled.

⇒Disable Firefox

1. Open Group Policy Editor on your managing Windows server.

2. Download the latest Firefox Policy Templates .zip file.

3. Copy the **ADMX** file:
   FROM the downloaded folder `policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
   TO `C:\Windows\PolicyDefinitions`

4. Copy the **ADML** file
   FROM `policy_templates\windows\en-us\firefox.adml & mozilla.adml`
   TO `C:\Windows \PolicyDefinitions\en-us`

5. In Group Policy Editor, create a new GPO for FireFox and provide an appropriate name.

6. Choose your desired scope.

7. Right-click the **new group policy** → **Edit**.

8. Open **User Configuration** → **Policies** → **Administrative Templates** → **Mozilla** → **Firefox**.

9. Locate and edit the following policies:

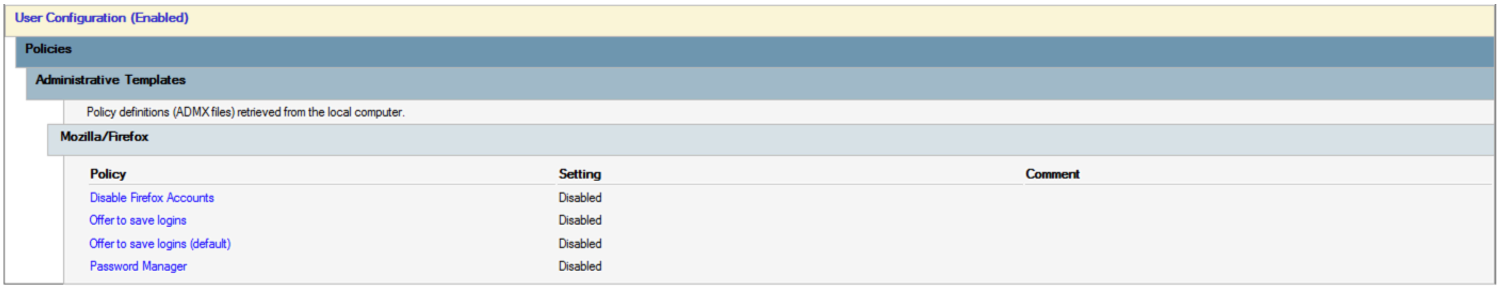
   - Disable the policy **Disable Firefox Accounts**.

   - Disable the policy **Offer to save logins**.

   - Disable the policy **Offer to save logins (default)**.

   - Disable the policy **Password Manager**.

10. Once complete, the GPO **settings** should show the following:



User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Mozilla/Firefox

Policy	Setting	Comment
Disable Firefox Accounts	Disabled	
Offer to save logins	Disabled	
Offer to save logins (default)	Disabled	
Password Manager	Disabled	

Firefox Settings

11. Ensure the GPO link is enabled.

How to check if it worked?

Check that the previous steps worked correctly for your setup:

⇒Edge

1. On a user's computer, Open the command line, and run: `gpupdate /force`.

2. Open Edge, then click the three dots for settings **...** → **Settings** → **Passwords**.

3. Ensure "Offer to save passwords" is turned off and managed by the organization.

> ⓘ **Note**
>
> **Sign-in automatically** is still checked because there is no policy setting to turn this off.
>
> Any logins previously saved in Edge will not be removed and will continue to be displayed to the user, despite autofill being disabled. Be sure to instruct the user to import any saved logins into Bitwarden before deleting them from Edge.

⇒Chrome

1. On a user's computer, Open the command line, and run: `gpupdate /force`.

2. Open Chrome and click the **profile icon** on the top right. See that the user is not signed in.

3. Open Chrome, then click the three dots **...** → **Settings** → **Passwords**. See that **Offer to save passwords** is unchecked and managed by the organization.

⇒Firefox

1. On a user's computer, Open the command line, and run: `gpupdate /force`.

2. Open Firefox and select **Logins and Passwords** from the menu bar.

3. Ensure that a "Blocked Page" message is displayed.

Disable on Linux

⇒Chrome

To disable the Chrome Password Manager via group policy:

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

Plain Text

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

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

   Plain Text

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

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

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

   Plain Text

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

9. Additionally, we recommend admins should add the following to files to prevent modifications to the files themselves:

   Plain Text

   ```
   chmod 644 /etc/opt/chrome/policies/managed/managed_preferences.json
   ```

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

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

⇒Firefox

To disable the Firefox Manager via group policy:

1. Download Firefox for Linux.

2. Open a terminal and navigate to the directory your download has been saved to. For example: `cd ~/Downloads`

3. `Extract to contents of the downloaded file:`

   Plain Text

   ```
   tar xjf firefox-*.tar.bz2
   ```

   The following commands must be executed as root, or preceded by `sudo`.

4. Move the uncompressed Firefox folder to `/opt`:

   Plain Text

   ```
   mv firefox /opt
   ```

5. Create a symlink to the Firefox executable:

   Plain Text

   ```
   ln -s /opt/firefox /usr/local/bin/firefox
   ```

6. Download a copy of the desktop file:

   Plain Text

   ```
   wget https://raw.githubusercontent.com/mozilla/sumo-kb/main/install-firefox-linux/firefox.desktop -P /usr/local/share/applications
   ```

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

   Plain Text

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

8. Create the following directory if it does not already exist:

Plain Text

```
mkdir /opt/firefox/distribution
```

9. Modify the directory with the following:

Plain Text

```
chmod 755 /opt/firefox/distribution
```

10. Additionally, we recommend admins should add the following to files to prevent modifications to the files themselves:

Plain Text

```
chmod 644 /opt/firefox/distribution/policies.json
```

11. Using your preferred software distribution or MDM tool, deploy the following to users' machines:

12. Firefox Browser

13. `/distribution/policies.json`

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

Disable on MacOS

⇒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. To disable Chrome's built-in password manager, add the following to `com.Google.Chrome.plist`:

Plain Text

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

6. Convert the `com.Google.Chrome.plist` file to a configuration profile using a conversion tool of your choice.

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

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

For additional information, see Chrome's documentation for setting up Chrome browser on Mac.

⇒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. To disable Firefox's built-in password manager, add the following to `org.mozilla.firefox.plist`:

   Plain Text

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

5. Convert the `org.mozilla.firefox.plist` file to a configuration profile using a conversion tool of your choice.

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

For additional information, see Firefox's documentation for MacOS configuration profiles.

⇒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:

   Plain Text

   ```
   /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:

Plain Text

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

4. To disable Edge's built-in password manager, add the following to `com.microsoft.Edge.plist`:

Plain Text

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

5. 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.

For additional information, see Edge's documentation for configuration profiles.