bitwarden | Help Center Article

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

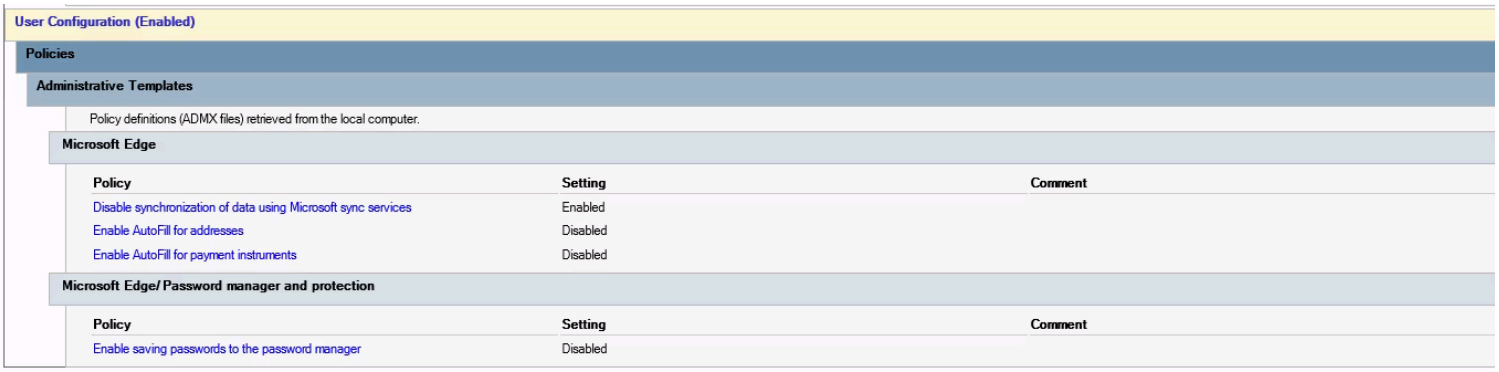
This article will direct you on how to disable various web browser's built-in password managers using group policy. These steps will help prevent corporate logins from being saved and synchronized to personal accounts. You may also consider deploying the Bitwarden browser extension to all browsers as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

Disable with Windows GPO

⇒Inaktivera Edge

1. Öppna Group Policy Management Editor på din hanterande Windows-server.
2. Ladda ner lämplig Edge Policy-mall.
3. Skapa ett nytt GPO för Edge i Group Policy Editor och ange ett lämpligt namn.
4. Välj önskat omfattning.
5. Högerklicka på det nya **grupprincipobjektet** → **Redigera**.
6. I redigeraren för grupprinciphantering, gå till **Användarkonfiguration** → **Policies** → **Administrativa mallar** → **Microsoft Edge**.
7. Ange följande policyer:
   - Öppna "Lösenordshanteraren och skydd", inaktivera policyn **Aktivera spara lösenord i lösenordshanteraren**.
   - Inaktivera principen **Aktivera autofyll för adresser**.
   - Inaktivera policyn **Aktivera autofyll för betalningsinstrument**.
   - Alternativt kan du aktivera principen **Inaktivera synkronisering av data med hjälp av Microsofts synktjänster**.

   När det är klart bör **GPO-inställningarna** visa följande:



Edge Settings

8. Se till att GPO-länken är aktiverad.

⇒Inaktivera Chrome

1. Öppna Group Policy Management Editor på din hanterande Windows-server.

2. Ladda ner Google Chrome administrativa mallar.

3. Kopiera följande i `ADMX-filen`:
   `policy_templates\windows\admx\chrome.admx`
   and
   `policy_templates\windows\admx\google.admx`

   TO `C:\Windows\PolicyDefinitions`

4. Kopiera följande i `ADML-filen`:
   `policy_templates\windows\admx\en-us\chrome.adml`
   and
   `policy_templates\windows\admx\en-us\google.adml`

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

5. Skapa ett nytt GPO för Chrome i Group Policy Editor och ange ett lämpligt namn.

6. Välj önskat omfattning.

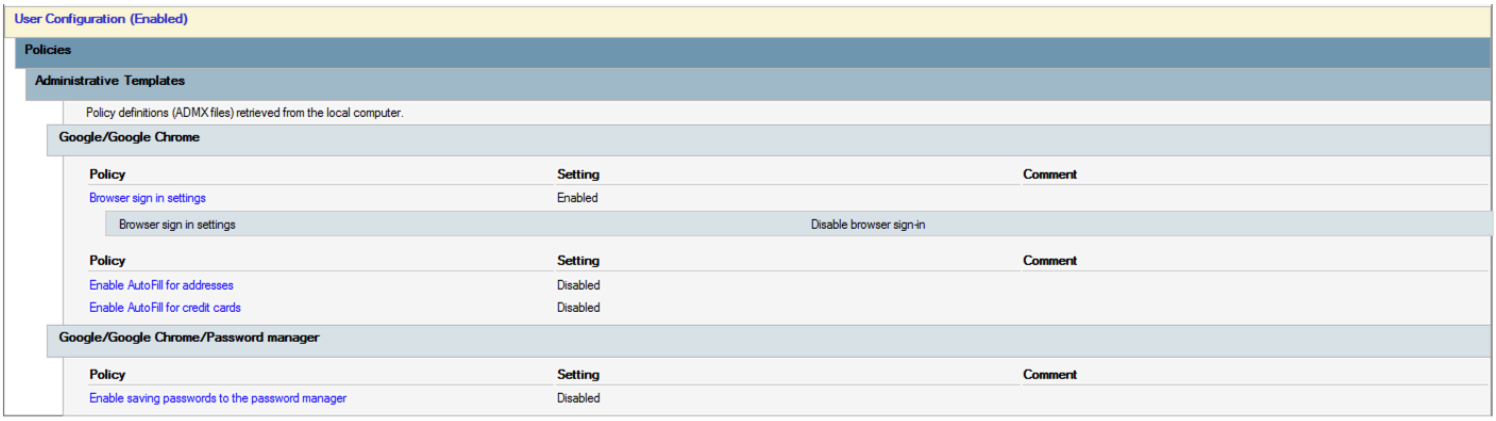
7. Högerklicka på **grupprincipobjektet → Redigera**.

8. Gå till **Användarkonfiguration → Policyer → Administrativa mallar → Google → Google Chrome**.

9. Redigera följande inställningar:

   - Inaktivera policyn **Aktivera spara lösenord i lösenordshanteraren** under "Lösenordshanteraren".
   - Inaktivera principen **Aktivera autofyll för adresser**.
   - Inaktivera policyn **Aktivera autofyll för kreditkort**.

10. När det är klart bör **GPO-inställningarna** visa följande:

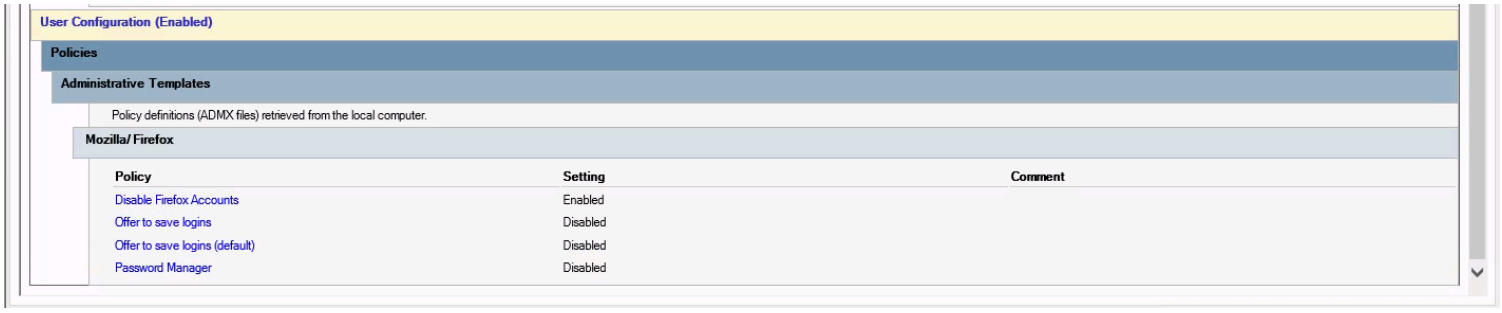


Chrome Settings

11. Se till att GPO-länken är aktiverad.

⇒Inaktivera Firefox

1. Öppna Group Policy Editor på din hanterande Windows-server.
2. Ladda ner den senaste .zip-filen för Firefox Policy Templates.
3. Kopiera **ADMX-filen**:
   FRÅN den nedladdade mappen `policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
   TILL `C:\Windows\PolicyDefinitions`
4. Kopiera **ADML-filen**
   FRÅN `policy_templates\windows\en-us\firefox.adml & mozilla.adml`
   TILL `C:\Windows \PolicyDefinitions\en-us`
5. Skapa ett nytt GPO för FireFox i Group Policy Editor och ange ett lämpligt namn.
6. Välj önskat omfattning.
7. Högerklicka på den **nya grupppolicyn → Redigera**.
8. Öppna **Användarkonfiguration → Politik → Administrativa mallar → Mozilla → Firefox**.
9. Leta reda på och redigera följande policyer:
   - Inaktivera policyn **Inaktivera Firefox-konton**.
   - Inaktivera **policyerbjudandet för att spara inloggningar**.
   - Inaktivera policyn **Erbjudande att spara inloggningar (standard)**.
   - Inaktivera policyn **Password Manager**.
10. När det är klart bör **GPO-inställningarna** visa följande:



Firefox Settings

11. Se till att GPO-länken är aktiverad.

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.deskto
p -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.