

BEHEERCONSOLE > DEPLOY CLIENT APPS

Browserwachtwoordbeheer deactiveren met apparaatbeheer

Weergeven in het Helpcentrum:

<https://bitwarden.com/help/deactivate-browser-password-managers/>

Browserwachtwoordbeheer deactiveren met apparaatbeheer

Dit artikel leert je hoe je verschillende ingebouwde wachtwoordmanagers van webbrowsers kunt uitschakelen met behulp van groepsbeleid. Deze stappen helpen voorkomen dat bedrijfslogins worden opgeslagen en gesynchroniseerd met persoonlijke accounts. U kunt ook overwegen om de Bitwarden browserextensie in te zetten [in alle browsers](#) als onderdeel van ditzelfde beleid.

Uitschakelen met Windows GPO

⇒Rand uitschakelen

1. Open de Group Policy Management Editor op je Windows-server.
2. [Download het juiste Edge-beleidssjabloon](#).
3. Maak in Group Policy Editor een nieuwe GPO aan voor Edge en geef deze een geschikte naam.
4. Kies je gewenste bereik.
5. Klik met de rechtermuisknop op het nieuwe **Groepsbeleidobject** → **Bewerken**.
6. Ga in de groepsbeleidbeheereditor naar **Gebruikersconfiguratie** → **Beleid** → **Administratieve sjablonen** → **Microsoft Edge**.
7. Stel de volgende beleidsregels in:
 - Open "Wachtwoordbeheer en -beveiliging" en schakel het beleid **Wachtwoorden opslaan in de wachtwoordbeheerder inschakelen** uit.
 - Schakel het beleid **Enable AutoFill for addresses (Automatisch invullen voor adressen inschakelen)** uit.
 - Schakel het beleid **Enable AutoFill voor betaalinstrumenten** uit.
 - Optioneel kun je het beleid **Synchronisatie van gegevens met Microsoft synchronisatieservices uitschakelen** inschakelen.

Enmaal voltooid zouden de **GPO-instellingen** het volgende moeten tonen:

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	

Randinstellingen

8. Zorg ervoor dat de GPO link is ingeschakeld.

⇒Chrome uitschakelen

1. Open de Group Policy Management Editor op je Windows-server.

2. Download de beheersjablonen voor Google Chrome.

3. Kopieer het volgende in het **ADMX**-bestand:
`policy_templates\windowsadmx\chrome.admx`
en
`policy_templates\windowsadmx\google.admx`

naar `C:\WindowsPolicyDefinitions`

4. Kopieer het volgende in het **ADML**-bestand:
`policy_templates\windowsadmx\en-uschrome.adml`
en
`policy_templates\windowsadmx\en-usgoogle.adml`

NAAR `C:\Windows beleidsdefinities \en-us`

5. Maak in Group Policy Editor een nieuwe GPO aan voor Chrome en geef deze een geschikte naam.

6. Kies je gewenste bereik.

7. Klik met de rechtermuisknop op het **Groepsbeleidobject** → **Bewerken**.

8. Ga naar **Gebruikersconfiguratie** → **Beleid** → **Administratieve sjablonen** → **Google** → **Google Chrome**.

9. Bewerk de volgende instellingen:

- Schakel onder "Wachtwoordbeheer" het beleid **Wachtwoorden opslaan in wachtwoordbeheer inschakelen** uit.
- Schakel het beleid **Enable AutoFill for Addresses (Automatisch invullen voor adressen inschakelen)** uit.
- Schakel de optie **Automatisch invullen voor creditcards** uit.

10. Eenmaal voltooid zouden de **GPO-instellingen** het volgende moeten tonen:

Policy	Setting	Comment
Google/Google Chrome		
Browser sign in settings	Enabled	
Browser sign in settings		
Disable browser sign-in		
Enable AutoFill for addresses	Disabled	
Enable AutoFill for credit cards	Disabled	
Google/Google Chrome/Password manager		
Enable saving passwords to the password manager	Disabled	

Chrome Settings

11. Zorg ervoor dat de GPO link is ingeschakeld.

⇒Firefox uitschakelen

1. Open de Groepsbeleideditor op je Windows-server.
2. Download het nieuwste Firefox Policy Templates .zip-bestand.
3. Kopieer het **ADMX-bestand**:
UIT de gedownloade map `policy_templates_v1.##windowsvuurvos.admx & mozilla.admx`
NAAR `C:\Windows\beleidsdefinities`
4. Kopieer het **ADML-bestand**
VAN `policy_templates-usfirefox.adml & mozilla.adml`
NAAR `C:\Windows\beleidsdefinities\en-us`
5. Maak in Group Policy Editor een nieuwe GPO aan voor FireFox en geef deze een geschikte naam.
6. Kies je gewenste bereik.
7. Klik met de rechtermuisknop op het **nieuwe groepsbeleid** → **Bewerken**.
8. Open **Gebruikersconfiguratie** → **Beleidsregels** → **Administratieve sjablonen** → **Mozilla** → **Firefox**.
9. Zoek en bewerk de volgende beleidsregels:
 - Schakel het beleid **Firefox-accounts uitschakelen** uit.
 - Schakel het beleid **Aanbod om aanmeldingen op te slaan** uit.
 - Schakel het **beleidsaanbod uit om aanmeldingen op te slaan (standaard)**.
 - Schakel het beleid **Password Manager** uit.
10. Eenmaal voltooid zouden de **GPO-instellingen** het volgende moeten tonen:

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

Firefox Settings

11. Zorg ervoor dat de GPO link is ingeschakeld.

Hoe controleer ik of het werkt?

Controleer of de vorige stappen correct werkten voor jouw opstelling:

⇒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.

Uitschakelen op 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.

Uitschakelen op 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

Gebruik de [Firefox .plist-sjabloon](#) en [Policy README](#) als referentie.

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**

Raadpleeg **voor Jamf-specifieke** hulp de documentatie van Microsoft over [Microsoft Edge-beleidsinstellingen configureren op macOS met Jamf](#).

For additional information, see [Edge's documentation](#) for configuration profiles.