

ADMINISTRATOR KONSOLE > DEPLOY CLIENT APPS

Deaktivieren Sie Passwort-Manager im Browser mit Geräteverwaltung

Ansicht im Hilfezentrum:

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

Deaktivieren Sie Passwort-Manager im Browser mit Geräteverwaltung

Dieser Artikel wird Ihnen Anweisungen geben, wie Sie die integrierten Passwort-Manager verschiedener Web-Browser mit Hilfe von Gruppenrichtlinien deaktivieren können. Diese Schritte helfen dabei zu verhindern, dass Zugangsdaten von Unternehmen gespeichert und mit persönlichen Konten synchronisiert werden. Sie könnten auch in Betracht ziehen, die [Bitwarden Browser Erweiterung für alle Browser](#) als Teil dieser gleichen Richtlinie einzusetzen.

Deaktivieren mit Windows GPO

⇒Edge deaktivieren

1. Öffnen Sie den Gruppenrichtlinienverwaltungseditor auf Ihrem verwaltenden Windows-Server.
2. [Laden Sie die entsprechende Edge-Richtlinienvorlage herunter](#) .
3. Im Gruppenrichtlinien-Editor erstellen Sie eine neue GPO für Edge und geben einen passenden Namen.
4. Wählen Sie Ihren gewünschten Umfang.
5. Klicken Sie mit der rechten Maustaste auf das neue Gruppenrichtlinien-Objekt → **Bearbeiten**.
6. Im Gruppenrichtlinienverwaltungs-Editor gehen Sie zu **Benutzerkonfiguration** → **Richtlinien** → **Administrative Vorlagen** → **Microsoft Edge**.
7. Legen Sie die folgenden Richtlinien fest:
 - Öffnen Sie "Passwort-Manager und Schutz", deaktivieren Sie die Richtlinie **Aktivieren Sie das Speichern von Passwörtern im Passwort-Manager**.
 - Deaktivieren Sie die Richtlinie **Automatisches Ausfüllen für Adressen aktivieren**.
 - Deaktivieren Sie die Richtlinie **AutoFill für Zahlungsinstrumente aktivieren**.
 - Optional können Sie die Richtlinie **Deaktivieren der Synchronisation von Daten mit Microsoft-Synchronisationsdiensten** aktivieren.

Nach Abschluss sollten die GPO **Einstellungen** folgendes anzeigen:

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 Einstellungen

8. Stellen Sie sicher, dass der GPO-Link aktiviert ist.

⇒Deaktiviere Chrome

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor auf Ihrem verwaltenden Windows-Server.

2. Laden Sie die administrativen Vorlagen für Google Chrome herunter.

3. In der ADMX Datei, kopieren Sie folgendes:

```
policy_templates\windows\admx\chrome.admx  
und  
policy_templates\windows\admx\google.admx
```

ZU C:\Windows\PolicyDefinitions

4. In der ADML Datei, kopieren Sie folgendes:

```
policy_templates\windows\admx\de-de\chrome.adml  
und  
policy_templates\windows\admx\de-de\google.adml
```

AN C:\Windows \PolicyDefinitions\de-de

5. Im Gruppenrichtlinien-Editor erstellen Sie eine neue GPO für Chrome und geben einen passenden Namen.

6. Wählen Sie Ihren gewünschten Umfang.

7. Rechtsklicken Sie auf das **Gruppenrichtlinienobjekt** → **Bearbeiten**.

8. Gehen Sie zu **Benutzerkonfiguration** → **Richtlinien** → **Administrative Vorlagen** → **Google** → **Google Chrome**.

9. Bearbeiten Sie die folgenden Einstellungen:

- Unter "Passwort-Manager" deaktivieren Sie die Richtlinie **Speichern von Passwörtern im Passwort-Manager ermöglichen**.
- Deaktivieren Sie die Richtlinie **AutoFill für Adressen aktivieren**.
- Deaktivieren Sie die Richtlinie **AutoFill für Kreditkarten aktivieren**.

10. Nach Abschluss sollten die GPO **Einstellungen** folgendes anzeigen:

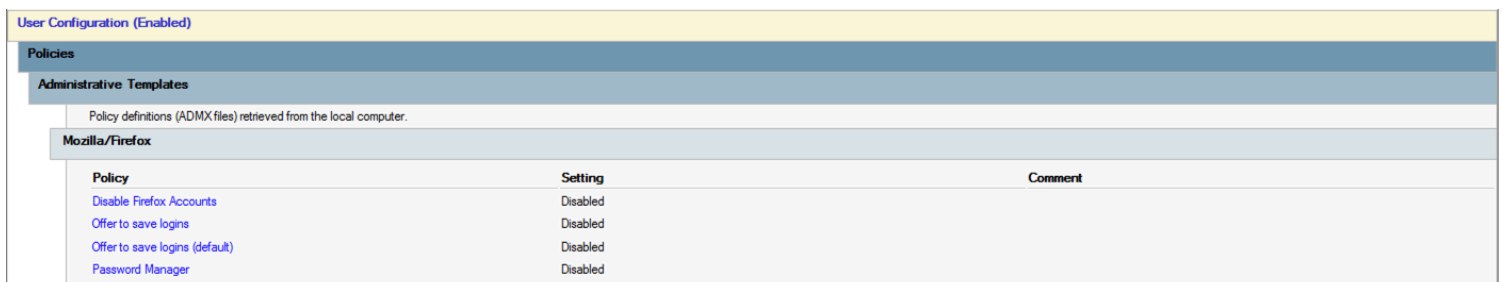
Policy	Setting	Comment
Google/Google Chrome		
Browser sign in settings	Enabled	Disable browser sign-in
Google/Google Chrome/Password manager		
Enable saving passwords to the password manager	Disabled	

Chrome Settings

11. Stellen Sie sicher, dass der GPO-Link aktiviert ist.

⇒Deaktiviere Firefox

1. Öffnen Sie den Gruppenrichtlinien-Editor auf Ihrem verwaltenden Windows-Server.
2. Laden Sie die neueste Firefox Richtlinien Vorlagen .zip Datei herunter.
3. Kopieren Sie die **ADMX** Datei:
AUS dem heruntergeladenen Ordner `policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
ZU `C:\Windows\PolicyDefinitions`
4. Kopieren Sie die **ADML** Datei
VON `policy_templates\windows\de-de\firefox.adml & mozilla.adml`
AN `C:\Windows \PolicyDefinitions\de-de`
5. Im Gruppenrichtlinien-Editor erstellen Sie eine neue GPO für FireFox und geben Sie einen passenden Namen.
6. Wählen Sie Ihren gewünschten Umfang.
7. Rechtsklicken Sie auf die **neue Gruppenrichtlinie** → **Bearbeiten**.
8. Öffnen Sie **Benutzerkonfiguration** → **Richtlinien** → **Administrative Vorlagen** → **Mozilla** → **Firefox**.
9. Suchen und bearbeiten Sie die folgenden Richtlinien:
 - Deaktivieren Sie die Richtlinie **Firefox Konten deaktivieren**.
 - Deaktivieren Sie die Richtlinie **Angebot zum Speichern von Zugangsdaten**.
 - Deaktivieren Sie die Richtlinie **Angebot zum Speichern von Zugangsdaten (Standard)**.
 - Deaktivieren Sie die Richtlinie **Passwort-Manager**.
10. Nach Abschluss sollten die GPO **Einstellungen** folgendes anzeigen:



The screenshot shows the Group Policy Editor interface. At the top, it says 'User Configuration (Enabled)'. Below that, there are sections for 'Policies' and 'Administrative Templates'. Under 'Administrative Templates', it says 'Policy definitions (ADMX files) retrieved from the local computer.' Below that, there is a section for 'Mozilla/Firefox'. At the bottom, there is a table with three columns: 'Policy', 'Setting', and 'Comment'. The table lists four policies, all of which are set to 'Disabled'.

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

Firefox Settings

11. Stellen Sie sicher, dass der GPO-Link aktiviert ist.

Wie kann man überprüfen, ob es funktioniert hat?

Überprüfen Sie, ob die vorherigen Schritte für Ihre Einrichtung korrekt funktioniert haben:

⇒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.

Deaktivieren Sie auf 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.

Deaktivieren auf 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

Verwenden Sie die [Firefox .plist Vorlage](#) und die [Richtlinien README](#) als Referenz.

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**

Jamf-spezifische Hilfe finden Sie in der Microsoft-Dokumentation zum [Konfigurieren von Microsoft Edge-Richtlinieneinstellungen auf macOS mit Jamf](#) .

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