

管理者コンソール > DEPLOY CLIENT APPS

デバイス管理を使用してブラウザのパスワードマネージャーを無効化する

ヘルプセンターで表示:

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

デバイス管理を使用してブラウザのパスワードマネージャーを無効化する

この記事では、グループポリシーを使用して、さまざまなウェブブラウザの組み込みパスワードマネージャーを無効にする方法について説明します。これらの手順は、企業のログインが保存されて個人のアカウントに同期されるのを防ぐのに役立ちます。この同じポリシーの一部として、[すべてのブラウザにBitwardenブラウザ拡張機能をデプロイすること](#)も検討してみてください。

Windows GPOを無効にする

⇒エッジを無効にする

1. あなたの管理Windowsサーバーでグループポリシー管理エディタを開きます。
2. [適切なエッジ ポリシー テンプレートをダウンロード](#)します。
3. グループポリシーエディターで、Edgeの新しいGPOを作成し、適切な名前を付けてください。
4. あなたの望む範囲を選択してください。
5. 新しいグループポリシーオブジェクトを右クリック → **編集**。
6. グループポリシー管理エディターで、**ユーザー設定** → **ポリシー** → **管理テンプレート** → **Microsoft Edge**に移動します。
7. 次のポリシーを設定します：
 - 「パスワードマネージャーと保護」を開き、ポリシー「**パスワードマネージャーへのパスワードの保存を有効にする**」を無効にします。
 - ポリシー**住所の自動入力**を有効にするを無効にしてください。
 - ポリシー**支払い手段のための自動入力**を有効にするを無効にしてください。
 - 必要に応じて、ポリシー**Microsoft同期サービスを使用したデータの同期を無効にする**を有効にすることができます。

完了後、GPOの**設定**は次のように表示されるべきです：

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	

エッジの設定

8. GPOリンクが有効になっていることを確認してください。

⇒Chromeを無効にする

1. あなたの管理Windowsサーバーでグループポリシー管理エディタを開きます。

2. [Google Chrome管理テンプレート](#)をダウンロードしてください。

3. **ADMX** ファイルで、以下をコピーしてください：

`policy_templates\windows\admx\chrome.admx`

と

`policy_templates\windows\admx\google.admx`

）

へ `C:\Windows\PolicyDefinitions`

4. **ADML** ファイルで、次のものをコピーしてください：

`policy_templates\windows\admx\en-us\chrome.adml`

そして

`policy_templates\windows\admx\en-us\google.adml`

宛先 `C:\Windows \PolicyDefinitions\ja-jp`

5. グループポリシーエディターで、Chrome用の新しいGPOを作成し、適切な名前を付けてください。

6. あなたの望む範囲を選んでください。

7. **グループ ポリシー オブジェクト**を右クリック → **編集**。

8. **ユーザー設定** → **ポリシー** → **管理テンプレート** → **Google** → **Google Chrome**に移動します。

9. 次の設定を編集してください：

- 「パスワードマネージャー」の下で、**ポリシーパスワードマネージャーへのパスワード保存を有効にする**を無効にします。
- ポリシー住所の自動入力**を**有効にする**を無効にしてください。
- ポリシーを無効にする クレジットカードのための自動入力**を**有効にする**。

10. 完了後、GPOの**設定**は次のように表示されるべきです：

User Configuration (Enabled)		
Policies		
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Google/Google Chrome		
Policy	Setting	Comment
Brower sign in settings	Enabled	
Brower sign in settings	Disabled	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. GPOリンクが有効になっていることを確認してください。

⇒Firefoxを無効にする

1. あなたの管理Windowsサーバーでグループポリシーエディタを開きます。
2. [最新のFirefoxポリシーテンプレート.zip](#)ファイルをダウンロードしてください。
3. **ADMX** ファイルをコピーします:
ダウンロードしたフォルダーから、 `policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
宛先 `C:\Windows\PolicyDefinitions`
4. **ADML** ファイルをコピーしてください。
から `policy_templates\windows\ja-jp\firefox.adml & mozilla.adml`
宛先 `C:\Windows \PolicyDefinitions\ja-jp`
5. グループポリシーエディターで、FireFoxの新しいIGPOを作成し、適切な名前を付けてください。
6. あなたの望む範囲を選んでください。
7. 右クリックして新しいグループポリシー → **編集**。
8. **ユーザー設定**を開く → **ポリシー** → **管理テンプレート** → **Mozilla** → **Firefox**。
9. 次のポリシーを探して編集してください：
 - ポリシー**Firefoxアカウントを無効にする**を無効にします。
 - ポリシー**ログインの保存を提案する**を無効にします。
 - ポリシー**ログインを保存するオファー（デフォルト）**を無効にしてください。
 - ポリシー**パスワードマネージャー**を無効にします。

10. 完了後、GPOの**設定**は次のように表示されるべきです：

User Configuration (Enabled)		
Policies		
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Mozilla/ Firefox		
Policy	Setting	Comment
Disable Firefox Accounts	Enabled	
Offer to save logins	Disabled	
Offer to save logins (default)	Disabled	
Password Manager	Disabled	

Firefoxの設定

11. GPOリンクが有効になっていることを確認してください。

それが機能しているかどうかを確認する方法は何ですか？

あなたのセットアップに対して前のステップが正しく機能したか確認してください:

⇒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.

Linuxで無効にする

⇒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.

MacOSで無効にする

⇒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

[Firefox .plistテンプレートとポリシーREADME](#)を参考にしてください。

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 固有のヘルプについては、「[Jamf を使用した macOS での Microsoft Edge ポリシー設定の構成](#)」に関する Microsoft のドキュメントを参照してください。

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