CONSOLA DE ADMINISTRADOR > DEPLOY CLIENT APPS

Desactivar Administradores de Contraseñas del Navegador Usando la Gestión de Dispositivos

Desactivar Administradores de Contraseñas del Navegador Usando la Gestión de Dispositivos

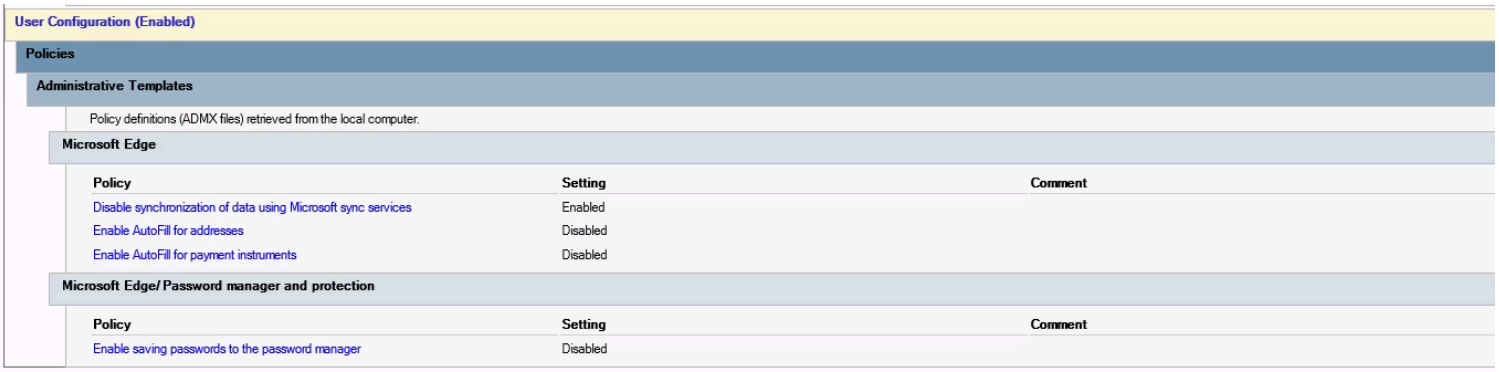
Este artículo te guiará sobre cómo deshabilitar varios administradores de contraseñas integrados en el navegador web utilizando políticas de grupo. Estos pasos ayudarán a prevenir que los inicios de sesión corporativos se guarden y se sincronicen con cuentas personales. También puedes considerar implementar la extensión de navegador Bitwarden en todos los navegadores como parte de esta misma política.

Deshabilitar con Windows GPO

⇒Deshabilitar Edge

1. Abra el Editor de Gestión de Políticas de Grupo en su servidor Windows que está gestionando.
2. Descargue la plantilla de política perimetral adecuada .
3. En el Editor de Políticas de Grupo, crea una nueva GPO para Edge y proporciona un nombre apropiado.
4. Elige tu alcance deseado.
5. Haz clic derecho en el nuevo **Objeto** de Política de Grupo → **Editar**.
6. En el Editor de Gestión de Políticas de Grupo, vaya a **Configuración de Usuario** → **Políticas** → **Plantillas Administrativas** → **Microsoft Edge**.
7. Establezca las siguientes políticas:
   - Abre "Administrador de contraseñas y protección", desactiva la política **Permitir guardar contraseñas en el administrador de contraseñas**.
   - Deshabilita la política **Habilitar AutoFill para direcciones**.
   - Deshabilita la política **Habilitar AutoFill para instrumentos de pago**.
   - Opcionalmente, puedes habilitar la política **Desactivar la sincronización de datos utilizando los servicios de sincronización de Microsoft**.

Una vez completado, los **ajustes** de GPO deberían mostrar lo siguiente:



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	

Ajustes de Edge

8. Asegúrate de que el enlace GPO esté habilitado.

⇒Desactivar Chrome

1. Abra el Editor de Gestión de Políticas de Grupo en su servidor Windows que está gestionando.

2. Descarga las Plantillas Administrativas de Google Chrome.

3. En el archivo ADMX, copia lo siguiente:
   `policy_templates\windows\admx\chrome.admx`
   y
   `policy_templates\windows\admx\google.admx`

   A `C:\Windows\PolicyDefinitions`

4. En el archivo ADML, copia lo siguiente:
   `policy_templates\windows\admx\es-es\chrome.adml`
   y
   `policy_templates\windows\admx\es-es\google.adml`

   A `C:\Windows \PolicyDefinitions\es-us`

5. En el Editor de Políticas de Grupo, crea una nueva GPO para Chrome y proporciona un nombre apropiado.

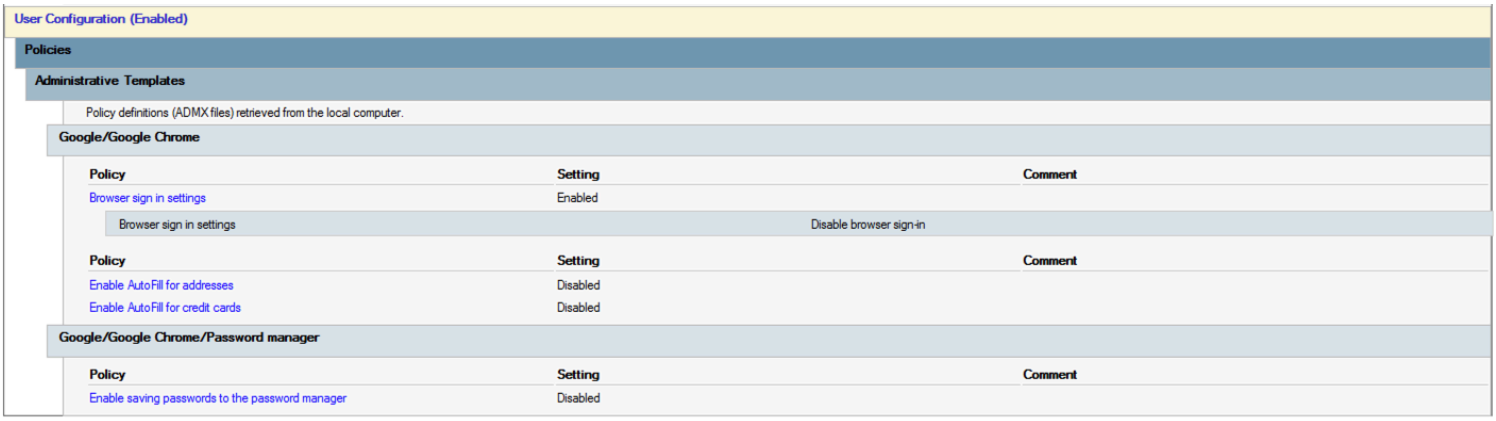
6. Elige tu alcance deseado.

7. Haz clic derecho en el **Objeto de Política de Grupo** → **Editar**.

8. Ve a **Configuración de Usuario** → **Políticas** → **Plantillas Administrativas** → **Google** → **Google Chrome**.

9. Edita los siguientes ajustes:
   - Bajo "Administrador de Contraseñas", deshabilite la política **Permitir guardar contraseñas en el administrador de contraseñas**.
   - Deshabilita la política **Habilitar AutoFill para Direcciones**.
   - Deshabilita la política **Habilitar AutoFill para tarjetas de crédito**.

10. Una vez completado, los **ajustes** de GPO deberían mostrar lo siguiente:



Chrome Settings

11. Asegúrate de que el enlace GPO esté habilitado.

⇒Desactivar Firefox

1. Abra el Editor de Políticas de Grupo en su servidor Windows que está gestionando.

2. Descarga el último archivo .zip de Plantillas de Políticas de Firefox.

3. Copia el archivo **ADMX**:
   DESDE la carpeta descargada `Policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
   A `C:\Windows\PolicyDefinitions`

4. Copia el archivo **ADML**
   DE `plantillas_de_políticas\windows\es-es\firefox.adml & mozilla.adml`
   A `C:\Windows \PolicyDefinitions\es-us`

5. En el Editor de Políticas de Grupo, crea una nueva GPO para FireFox y proporciona un nombre apropiado.

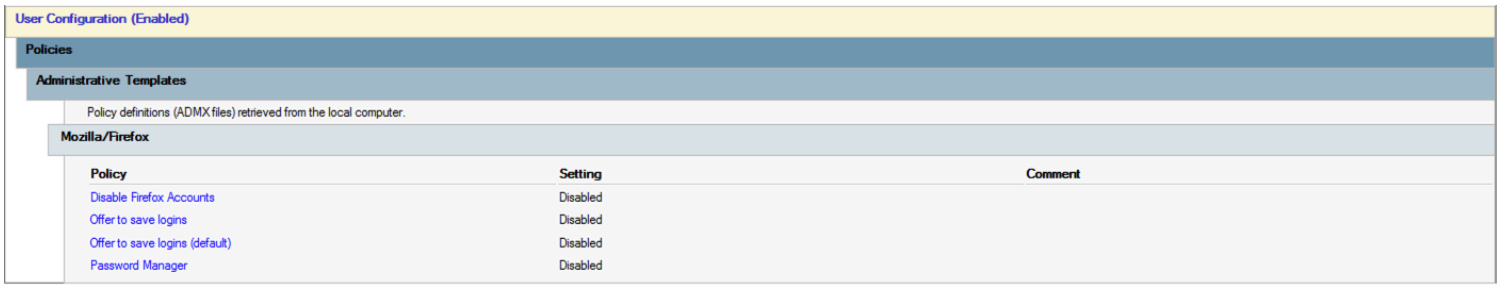
6. Elige tu alcance deseado.

7. Haz clic derecho en la **nueva política de grupo** → **Editar**.

8. Abra **Configuración del Usuario** → **Políticas** → **Plantillas Administrativas** → **Mozilla** → **Firefox**.

9. Ubica y edita las siguientes políticas:
   - Deshabilita la política **Deshabilitar Cuentas de Firefox**.
   - Deshabilita la política **Ofrecer para guardar inicios de sesión**.
   - Deshabilita la política **Ofrecer guardar inicios de sesión (predeterminado)**.
   - Deshabilita la política **Administrador de Contraseñas**.

10. Una vez completado, los **ajustes** de GPO deberían mostrar lo siguiente:



Firefox Settings

11. Asegúrate de que el enlace GPO esté habilitado.

¿Cómo verificar si funcionó?

Verifique que los pasos anteriores funcionaron correctamente para su configuración:

⇒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.

Deshabilitar en 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.

Desactivar en 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**
> Utilice la plantilla .plist de Firefox y la Política README como referencia.

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**
>
> **Para obtener ayuda específica de Jamf** , consulta la documentación de Microsoft sobre Configuración de las políticas de Microsoft Edge en macOS con Jamf .

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