

## Guide

SigPlusExtLite 3.0 and Browser Extension GPO Deployment

## Contents

Google Chrome Extension GPO Deployment	2
Prepare Group Policy Editor with Chrome's Policy Template	2
Set-Up Google Chrome with SigPlusExtLite's Chrome Extension	2
Firefox Extension GPO Deployment	4
Prepare Group Policy Editor with Firefox's Policy Templates	4
Set-Up Firefox with SigPlusExtLite's Firefox Extension	5
Edge Chromium Extension GPO Deployment	7
Prepare Group Policy Editor with Edge Chromium's Policy Templates	7
Set-Up Edge Chromium with SigPlusExtLite's Chrome Extension	8

# $\mathbf{V}$

## **Google Chrome Extension GPO Deployment**

#### Prepare Group Policy Editor with Chrome's Policy Template

- 1. Go to https://support.google.com/chrome/a/answer/187202.
- 2. Follow the steps under "Install and configure Chrome policy templates" for your OS.

#### Set-Up Google Chrome with SigPlusExtLite's Chrome Extension

1. After installing and configuring the Chrome policy templates in GPO, open GPO by selecting the "Windows Key + R", typing "gpedit.msc", and then selecting the "Enter" key.

📨 Run	×
۵	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	gpedit.msc ~
	OK Cancel <u>B</u> rowse

2. Under "Computer Configuration", go to "Administrative Templates"  $\rightarrow$  "Classic Administrative Templates"  $\rightarrow$  "Google"  $\rightarrow$  "Google Chrome"  $\rightarrow$  "Extensions".

Iccal Group Policy Editor				_	×
File Action View Help					
🗢 🔿 🙍 📰 🗟 🔝 🍸					
Local Computer Policy	📋 Extensions				
<ul> <li>Computer Configuration</li> <li>Software Settings</li> </ul>	Select an item to view its description.	Setting	State		
> 🧾 Windows Settings		Configure extension installation blacklist	Not configured		
Administrative Templates Control Panel		Configure extension installation whitelist	Enabled		
> 🧮 Network		E Configure extension, app, and user script install sources	Not configured		
Printers		Configure allowed app/extension types	Not configured		
Server		Extension management settings	Not configured		
> System		E blocks external extensions from being installed	Not conligured		
> 📔 Windows Components					
Classic Administrative Temp					
V 🦲 Google					
Content settings					
Default search pr					
Deprecated polici					
Extensions					

SigPlusExtLite Browser Extension GPO Deployment Guide

- 3. In "Extensions", select the "Configure the list of force-installed apps and extensions" setting.
- 4. In the "Configure the list of force-installed apps and extensions" window, select the "Enabled" radio button.

📋 Extensions	
Configure the list of force-installed apps and extensions Edit <u>policy setting</u> Requirer Configure the list of force-installed	State         igure extension installation blacklist       Not configured         igure extension installation whitelist       Not configured         igure the list of force-installed apps and extensions       Enabled         apps and extensions       —
Microso Descript Specifie extensio silently, without which ca disabled Disabled Disabled Disabled	apps and extensions Previous Setting Next Setting
apps/exr Supported on: implicitl includin permissi versions the app/	Microsoft Windows 7 or later
permissi enterpris enterpris enterpris available are not forc This poli a potent Extensio an ap c previous	be silently Specifies a list of apps and extensions that are installed silently, without user interaction, and which cannot be uninstalled nor disabled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future versions of the app/extension. Furthermore, permissions are granted for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These two APIs are not available to apps/extensions that are not force-installed.)
Extende Bundle.	This policy takes precedence over a potentially conflicting ExtensionInstallBlacklist policy. If an app or extension that previously had been force-installed is removed from this list, it is automatically uninstalled by Google Chrome. For Windows instances that are not joined to a Microsoft® Active Directory® domain, forced installation is limited to apps and extensions listed in the Chrome Web Store.
e Config	OK Cancel Apply

5. In the "Configure the list of force-installed apps and extensions" window, select the "Show..." button under "Extensions/App IDs and update URLs to be silently installed."



6. In the "Show Contents" window, add the following value and select the "OK" button: dhcpobccjkdnmibckgpejmbpmpembgco;https://clients2.google.com/service/update2/crx

xten	sion/App IDs and update URLs to be silently installed
	Value
•	dhcpobccjkdnmibckgpejmbpmpembgco;https://clients2.google.com/service/update2

- 7. Select the "Apply" button and exit out of the Local Group Policy Editor.
- 8. Restart Chrome.
- 9. In Chrome, go to Chrome://extensions, and confirm that the SigPlusExtLite extension with ID dhcpobccjkdnmibckgpejmbpmpembgco was added.

## **Firefox Extension GPO Deployment**

#### Prepare Group Policy Editor with Firefox's Policy Templates

- 1. Go to https://github.com/mozilla/policy-templates/releases.
- 2. Locate the latest release section (located at the top).
- 3. Under 'Assets", download the zipped Firefox policy template file and unzip contents. (policy\_template\_v2.01.zip).
- 4. Navigate into the Windows folder within the unzipped folder.
- 5. Copy all the files of this folder to Windows directory's PolicyDefinition folder.

#### Set-Up Firefox with SigPlusExtLite's Firefox Extension

1. After installing and configuring the Firefox policy templates in GPO, open GPO by selecting the "Windows Key + R", typing "gpedit.msc", and then selecting the "Enter" key.

🖅 Run	×
٨	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	gpedit.msc ~
	OK Cancel <u>B</u> rowse

2. Under "Computer Configuration", go to "Administrative Templates" → "Mozilla" → "Firefox" → "Extensions".



3. In "Extensions", select the "Extensions to Install" setting.



4. In the "Extension to Install" window, select the "Enabled" radio button.

Extensions to Inst	all					—		×
Extensions to Inst	all			Previous Setting	Next S	Setting		
O Not Configured	Comment:							^
Enabled								
O Disabled	Constanting							~
	Supported on:	Firefox 60 or lat	er, Firefox 60	ESR or later				^
								~
Options:			Help:					
Show			If this policy or paths the Anytime the If this policy installed.	y is enabled, you c, at will be installed v is list is changed, tl y is disabled or not	an specify a when Firefox he extension configured,	list of exte is started. is will be re	nsion URL: einstalled. iions are	5
				(	OK	Cancel	Арр	ly

5. In the "Extensions to Install" window, select the "Show..." button.



6. In the "Show Contents" window, add the following value and select the "OK" button: https://addons.mozilla.org/firefox/downloads/latest/topaz-sigplusextlite-extension/latest.xpi.

Show	Contents			×
ا				
	Value			
1	tps://addons.mozilla.org/firefox/downloads/latest/topaz-sigplus	extlite-ext	tension/lat	est.xpi
	0	<	Cance	el .

- 7. Select the "Apply" button and exit out of the Local Group Policy Editor.
- 8. Restart Firefox.
- 9. In Firefox, go to about:addons, and confirm that the Topaz SigPlusExtLite extension is installed.

## **Edge Chromium Extension GPO Deployment**

#### Prepare Group Policy Editor with Edge Chromium's Policy Templates

- 1. Go to https://docs.microsoft.com/en-us/DeployEdge/configure-microsoft-edge.
- 2. Follow the steps under "Configure policy settings on Windows".

#### Set-Up Edge Chromium with SigPlusExtLite's Chrome Extension

1. After installing and configuring the Edge policy templates in GPO, open GPO by selecting the "Windows Key + R", typing "gpedit.msc", and then selecting the "Enter" key.

🖅 Run	×
٨	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	gpedit.msc 🗸
	OK Cancel <u>B</u> rowse

2. Under "Computer Configuration", go to "Administrative Templates"  $\rightarrow$  "Classic Administrative Templates"  $\rightarrow$  "Microsoft Edge"  $\rightarrow$  "Extensions".

🧐 Local Group Policy Editor		– 🗆 X
File Action View Help		
← ⇒   2 📰   🗟   🛛 🗊   🍸		
Local Computer Policy	📔 Extensions	
Computer Configuration	Select an item to view its description.	Setting
Software Settings     Windows Settings		Configure allowed extension types
Administrative Templates		E Allow specific extensions to be installed
> 🖺 Control Panel		E Control which extensions cannot be installed
🗸 🚞 Microsoft Edge		E Control which extensions are installed silently
Cast		E Configure extension and user script install sources
Content settings		Configure extension management settings
Default search provider		
Extensions		
Native Messaging		
Password manager and protection		
Printing		
Proxy server		
SmartScreen settings		
📋 Startup, home page and new tab page		

3. In "Extensions", select the "Control which extensions are installed silently" setting.

4. In the "Control which extensions are installed silently" window, select the "Enabled" radio button.

	Extensions			
Co in:	ontrol which extensions are stalled silently	Se	tting Control which e	extensions cannot be installed
Ed	lit <u>policy setting</u>		Allow specific e	extensions to be installed
R	Control which extensions are	install	ed silently	
N V	Control which extensions are	install	ed silently	Previous Setting Next S
S	O Not Configured Comment	:		
ir ir	Enabled			
c ir	O Disabled			
re g ir	Supported	t on:	Microsoft Edge	e version 77, Windows 7 or later
a b e:	Options:			Help:
P e e l	Extension/App IDs and update U installed Show	RLs to I	be silently	Specifies extensions that are installed siler interaction, and that the users can't uninst installed"). All permissions requested by th granted implicitly, without user interactio additional permissions requested by futur extension. Furthermore, permissions are g enterprise.deviceAttributes and enterprise extension APIs. (These two APIs are only a that are force-installed.)
				This policy takes precedence over a poten

5. In the "Control which extensions are installed silently" window, select the "Show..." button under "Extensions/App IDs and update URLs to be silently installed."



6. In the "Show Contents" window, add the following value and select the "OK" button: dhcpobccjkdnmibckgpejmbpmpembgco;https://clients2.google.com/service/update2/crx

	Value
•	dhcpobccjkdnmibckgpejmbpmpembgco;https://clients2.google.com/service/update2/c

- 7. Select the "Apply" button and exit out of the Local Group Policy Editor.
- 8. Restart Edge Chromium.
- 9. In Edge Chromium, go to edge://extensions/, and confirm that the SigPlusExtLite extension with ID dhcpobccjkdnmibckgpejmbpmpembgco was added (Developer mode may need to be toggled on to see the ID of the extension).

## **Additional Information**

If Native Messaging Host application blacklisting is enabled to blacklist all Native Messaging Host applications, then whitelist the Topaz Native Messaging application by adding the "com.topaz.sigplusextlite.win.2" to the GPO Native Messaging Host Whitelisting for the specified browsers GPO settings.