GAT for Chrome Extension – Installed Extensions Explained

Chrome Audit & Management · https://gatlabs.com/knowledge/tech-tips/gat-for-chrome-extension-installed-extensions-explained/

Definitions

Type

- **Extension** - An application installed in Chrome with a large amount of access to Chrome features. They use a permission system to request access to subsets of those features. Depending on the permissions they request, they can add icons to your toolbar or inside the address bar, they can open and close tabs and windows, they have full access to every page you visit and all data sent to the web(even if you use HTTPS), and more besides. GAT Chrome Stats helps you identify extensions that request permissions for potentially malicious features. An example would be Adblock, which runs on every page you visit and monitors what resources the page loads, and can block requests for advertisements.
- **Chrome App** - An application installed on ChromeOS(Chromebook or Chromebox). These have a high level of access to the device they are installed on. Treat these as you would any software program installed on a traditional operating system(such as Photoshop, an Office program, etc.). They can have a user interface that is separate from that of Chrome itself.
- **Hosted App** - An app that acts as a shortcut to an online web app(such as Gmail, Google Docs, etc). It appears in your New Tab page or at chrome://apps/. When you click the hosted app it launches a browser session to the web app. The web app itself has no special permissions or elevated access to Chrome. The app can also run in the background. This creates essentially an ‘invisible’ tab that can do work while you use other tabs - i.e a file storage site that uploads large files in the background; a ‘radio’ site that streams and plays music in the background. The background age has no special permissions or elevated access to Chrome.
- **Legacy Packaged App** - An older version of Chrome Apps. These do not have as much access to ChromeOS and local device features as current Chrome Apps.

Install Method

- **Admin** - The extension was installed by your organization's administrator via ‘enterprise policy’. When you sign into Chrome, this extension is automatically installed, and you cannot remove or disable it without signing out of your organization's account.
- **Normal** - The extension was installed either through the Chrome Web Store or by manually installing an extension file.
- **Sideload** - The extension was installed by other software on your PC. For example, a piece of software may add an extension to Chrome as part of its installation process, and then use the extension to integrate with the user’s browser.
- **Development** - The extension was installed by manually loading it in developer mode. If you do not actively develop Chrome extensions, you should not have any extensions with this install method.
- **Other** - The extension was installed by other means.

Access Requested

- None
- Low
- Medium
- High

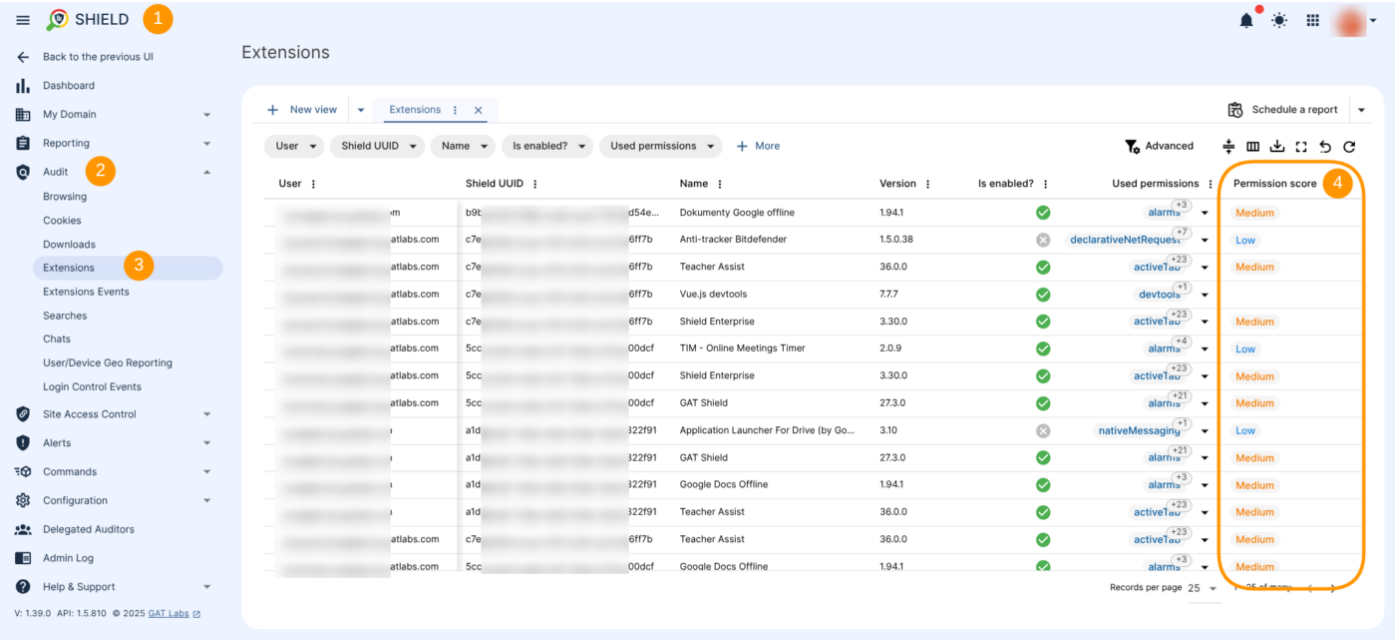
Rating System

In the GAT Chrome Extension, we rate all installed extensions, including our own, based on the amount of access to your environment that they require. The rating system works based on a permission level. The permission level can be viewed in two ways, the highest level required and the combined total score.

Permission score:

- Low
- Medium
- High

To audit the Extensions Used permissions ratings, navigate to **GAT Shield (1)→ Audit (2)→ Extensions (3) -> Permission score (4)**



All extensions that have at least one access permission request of 3 are marked in Red (High), those whose highest level of access for any permission is a 2 are marked in Orange (Medium), and so on.

However, for example, an extension can have many requests for permissions of 2, and if 2 is always the highest it will be marked in orange (medium), while the combined score may be a 6 or even an 8.

In short, the color under the **Permission score** shows the severity level of the requested access and can be used for easily identification of the potentially maltious software installed, and the **Used permissions** shows the total number of permissions.

In short, the color under the **Permission score** shows the severity level of the requested access and can be used to easily identify potentially malicious software installed, while **Used permissions** column shows the total number of permissions.

A detailed list of the Permissions available to extensions, their shortcodes, and their permission level scores (as judged by us) are outlined below.

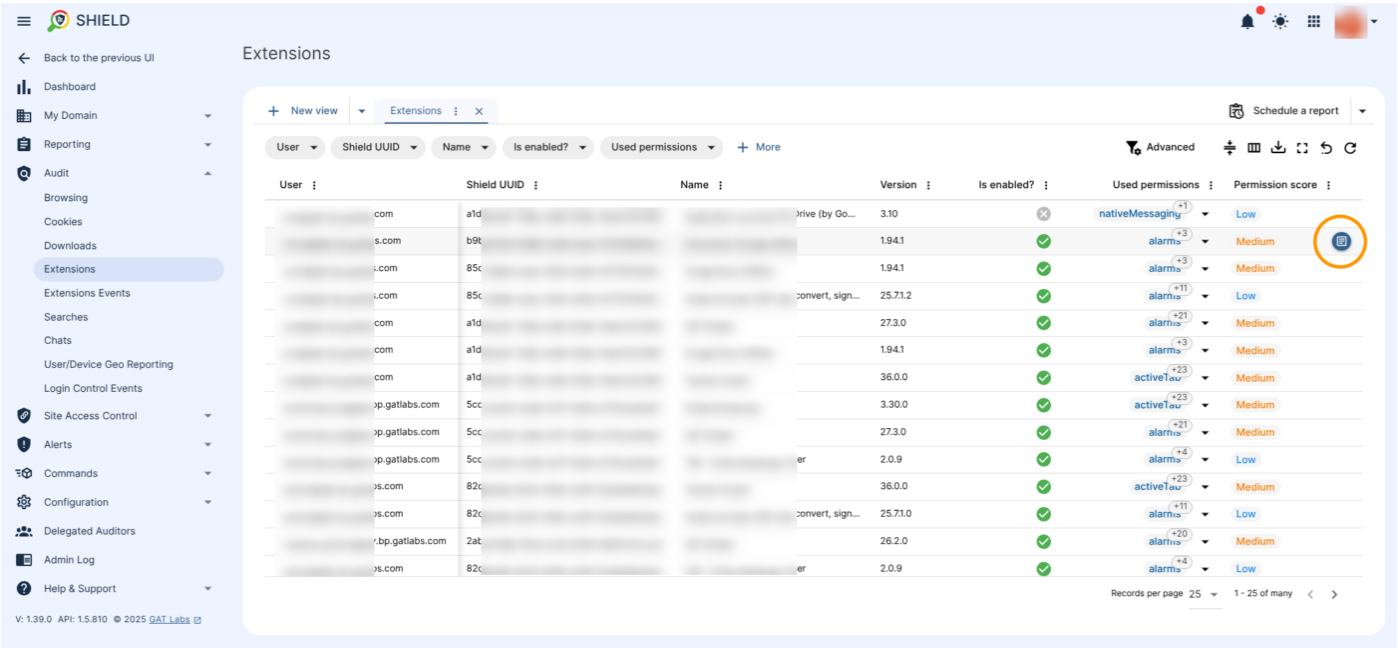
Permission Short Code	**Permission level**	**Permission Description**
"alarms"	0	Gives your app access to the chrome.alarms API.
"audio"	0	Gives your app access to the chrome.audio API.

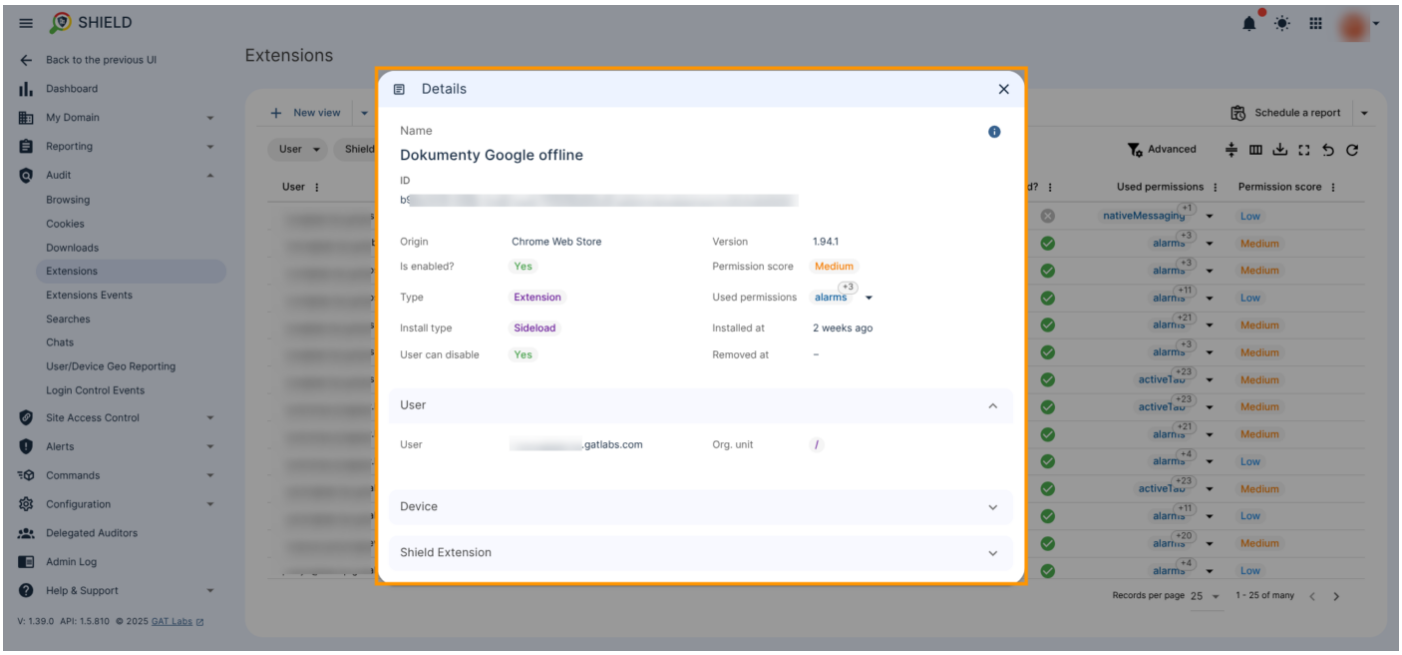
"audioCapture"	3	Requests that the app be granted permissions to capture audio directly from the user's Microphone via the getUserMedia API.
"browser"	3	Gives your app access to the chrome.browser API.
"clipboardRead"	2	Required if the extension or app usesdocument.execCommand('paste').
"clipboardWrite"	1	Indicates the extension or app usesdocument.execCommand('copy') ordocument.execCommand('cut'). This permission is required for hosted apps; it's recommended for extensions and packaged apps.
"contextMenus"	0	Gives your app access to thechrome.contextMenus API.
"desktopCapture"	3	Gives your app access to thechrome.desktopCapture API.
"diagnostics"	0	Gives your app access to the chrome.diagnosticsAPI.
"dns"	0	Gives your app access to the chrome.dns API.
"experimental"	0	Required if the extension or app uses anychrome.experimental.* APIs.
"fileBrowserHandler"	0	Gives your app access to thechrome.fileBrowserHandler API.
"fileSystem"	2	Gives your app access to the chrome.fileSystemAPI.
"fileSystemProvider"	3	Gives your app access to thechrome.fileSystemProvider API.
"gcm"	3	Gives your app access to the chrome.gcm API.
"geolocation"	2	Allows the extension or app to use the proposed HTML5 geolocation API without prompting the user for permission.
"hid"	0	Gives your app access to the chrome.hid API.
"identity"	0	Gives your app access to the chrome.identity API.
"idle"	0	Gives your app access to the chrome.idle API.
"infobars"	0	Gives your app access to the chrome.infobars API.
"location"	0	Gives your app access to the chrome.location API.
"mediaGalleries"	0	Gives your app access to thechrome.mediaGalleries API.

"nativeMessaging"	2	Gives your app access to the native messaging API.
"notificationProvider"	1	Gives your app access to thechrome.notificationProvider API.
"notifications"	1	Allows the extension to use the proposed HTML5notification API without calling permission methods (such as checkPermission()). For more information see Desktop Notifications.
"pointerLock"	1	Required to use Pointer Lock via calls torequestPointerLock or Pepper's Mouse Lock API. See Other APIs for behavior differences.
"power"	2	Gives your app access to the chrome.power API.
"pushMessaging"	2	Gives your app access to thechrome.pushMessaging API.
"serial"	0	Gives your app access to the chrome.serial API.
"signedInDevices"	0	Gives your app access to thechrome.signedInDevices API.
"socket"	2	Gives your app access to the chrome.socket API.
"storage"	2	Gives your app access to the chrome.storage API.
"syncFileSystem"	3	Required if the app uses thechrome.syncFileSystem API to save and synchronize data on Google Drive.
"system.cpu"	1	Gives your app access to the chrome.system.cpuAPI.
"system.display"	3	Gives your app access to thechrome.system.display API.
"system.memory"	3	Gives your app access to thechrome.system.memory API.
"system.network"	3	Gives your app access to thechrome.system.network API.
"system.storage"	3	Gives your app access to thechrome.system.storage API.
"tts"	3	Gives your app access to the chrome.tts API.
"unlimitedStorage"	3	Provides an unlimited quota for storing HTML5 client-side data, such as databases and local storage files. Without this permission, the extension or app is limited to 5 MB of local storage.Note: This permission applies only to Web SQL Database and application cache (see issue 58985). Also, it doesn't currently work with wildcard subdomains such ashttp://*.example.com.

"usb"	2	Gives your app access to the chrome.usb API.
"videoCapture"	3	Requests that the app be granted permissions to capture video directly from the user's Web Cam via the getUserMedia API.
"wallpaper"	0	Gives your app access to the chrome.wallpaperAPI.
"webview"	1	Required if the app uses the Webview Tag to embed live content from the web in the packaged app.
"webRequest"	1	Monitor all network requests made by Chrome
"webRequestBlocking"	1	As above, but also able to stop, redirect and modify requests
"tabs"	0	Lets the extension get info on tabs and their status, open and close tabs
"management"	3	Lets the extension view information on other installed extensions and potentially uninstall thems
"history"	2	Get details of a user's history over the last 35 days
"identity"	0	Get the signed in Chrome user's name
"downloads"	2	View details of a user's downloads

To review each Extension log details, hover the cursor over the right side of each record. The "**Details**" icon will appear and allow you to view the details.




SHIELD
Back to the previous UI
Dashboard
My Domain
Reporting
Audit
Browsing
Cookies
Downloads
Extensions
Extensions Events
Searches
Chats
User/Device Geo Reporting
Login Control Events
Site Access Control
Alerts
Commands
Configuration
Delegated Auditors
Admin Log
Help & Support
V: 1.39.0 API: 1.5.810 © 2025 GAT Labs
Extensions
New view
Schedule a report
Advanced
User
Shield
Used permissions
Permission score
Details
Name
Dokumenty Google offline
ID
Origin
Chrome Web Store
Version
1.94.1
Is enabled?
Yes
Permission score
Medium
Type
Extension
Used permissions
alarms
Install type
Sideload
Installed at
2 weeks ago
User can disable
Yes
Removed at
-
User
User
Org. unit
/
Device
Shield Extension
Records per page 25
1 - 25 of many