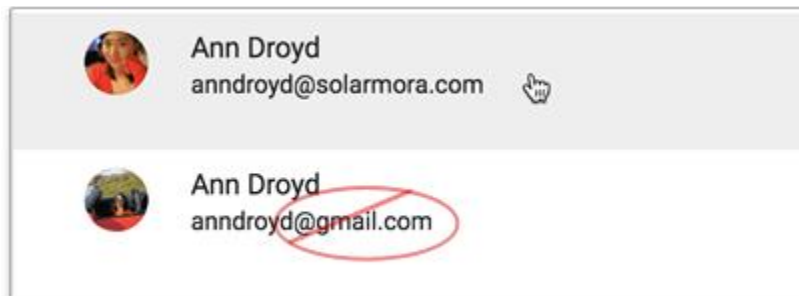


Google Chrome Enterprise Help

Chrome OS Device Management Steps

1. Access Prerequisites

- Before any management of your devices can be accomplished, the library must have an administrator account to Google's cloud-based Admin console: admin.google.com
If you have access to an administrator (or admin) account, you can sign in to the Google Admin console. The Admin console is where administrators manage Google services for people in an organization. This admin account does not end in @gmail.com



2. Domain Ownership

- Domain ownership must be claimed with Google in order to enable Chrome device management policies in the Google Admin console and to gain access to the Google Cloud Support Center. Administrator access to primary domain will be needed.
 - a. Check out [this video](#) to see how to verify your domain.

3. Buy Chrome Enterprise Upgrade or Chrome Education Upgrade

- To manage standalone devices that run Chrome OS in your business or educational environment, you need Chrome Enterprise Upgrade or Chrome Education Upgrade. You need to buy it for every Chrome device you want to manage.

4. Initial Device Setup - Add Wi-Fi network

- Sign in to your [Google Admin console](#). **Note:** *This must be an administrator account*



Google Chrome Enterprise Help

- From the Admin Console Home page, go to **Devices**.
- Click **Networks** and then > **Wi-Fi**.
- To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit.
- Click **Add Wi-Fi**.
- Under Platform access, select **Chromebooks (by device)**.
- Enter the details for your organization's Wi-Fi network and set it to **Automatically connect**.
- Confirm that the Wi-Fi configuration options are correct and click **Save**.
 - a. **Tip:** In particular, pay attention to the SSID and passphrase, both are case-sensitive.
 - b. Connect to an open or unfiltered network temporarily while you set up your devices. You can remove this network from the list of preferred networks later by following the instructions to forget a network at Manage Wi-Fi networks.
 - c. Apply Wi-Fi networks by device instead of by user. This ensures that devices can access your Wi-Fi network at the sign-in screen.

5. Device Settings - Enrollment and access

- From within the Admin console, select the **Main Menu**.
- Select the **Devices** dropdown. From there select **Chrome > Settings > Device**.
- To reduce risk of theft, enable **Forced re-enrollment**.
 - a. This will prevent a user from wiping a device and using it on their own on in another domain.
- Next, select the option to **Do not allow powerwash to be triggered**.
- We also recommend adding **Disabled device return instructions** in case a Chromebook is lost or stolen. You can add your personal here message so that patrons are given instructions on returning the disabled device. This should include (but not limited to) the library address and contact information.

Google Chrome Enterprise Help

USER & BROWSER SETTINGS

DEVICE SETTINGS

MANAGED GUEST SESSION SETTINGS

+ Search or add a filter

Enrollment and access ^

Forced re-enrollment
Locally applied ▼ Force device to automatically re-enroll after wiping ▼

Powerwash
Locally applied ▼ Do not allow powerwash to be triggered ▼

Verified access
Inherited from Google default Enable for content protection ▼

Verified mode
Inherited from Google default Skip boot mode check for verified access ▼

Services with full access
Service accounts which are allowed to receive device ID. Put one pattern on each line.

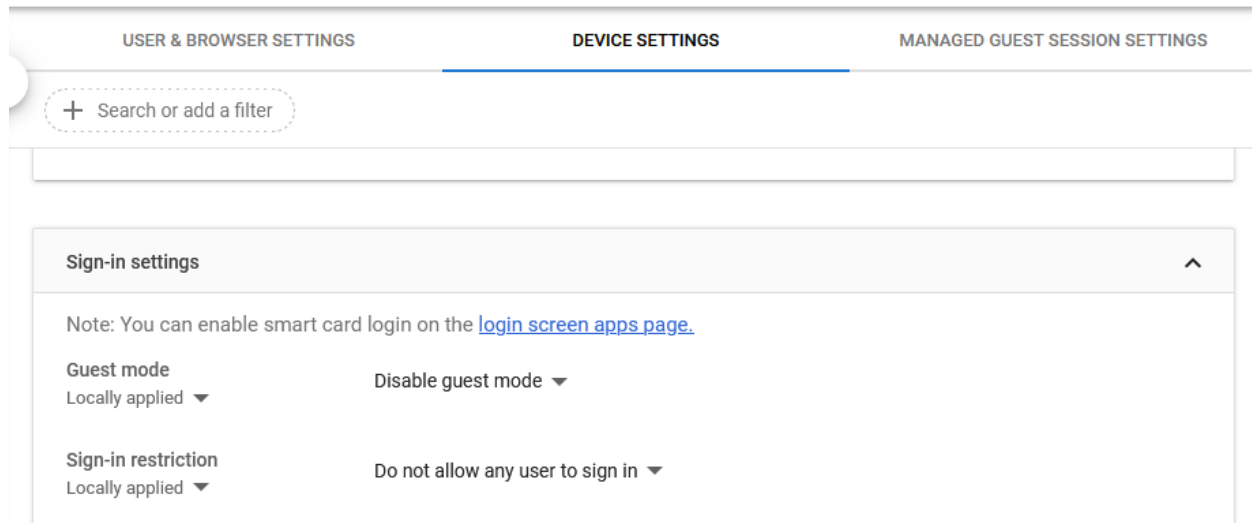
Services with limited access
Service accounts which can verify devices but do not receive device ID. Put one pattern on each line.

Disabled device return instructions
Locally applied ▼ Disabled device return instructions
Please return Trenton Veterans Memorial Library.
2790 Westfield Road
Trenton, MI 48183
Phone: 734-676-9777

Custom text to display under the device locked message. We recommend including a return address and contact phone number in your message. 106 / 512

- First, disable guest mode and set sign-in restriction to **Do not allow any user to sign in**. This policy allows for patrons to use the Chromebook without a device sign-in.

Google Chrome Enterprise Help



The screenshot shows the Google Chrome Enterprise Admin console interface. At the top, there are three tabs: "USER & BROWSER SETTINGS", "DEVICE SETTINGS" (which is selected and underlined), and "MANAGED GUEST SESSION SETTINGS". Below the tabs is a search bar with a plus icon and the text "Search or add a filter". The main content area displays the "Sign-in settings" section, which is expanded to show a note and two settings. The note states: "Note: You can enable smart card login on the [login screen apps page](#)." The first setting is "Guest mode", currently set to "Locally applied" with a dropdown arrow, and a sub-setting "Disable guest mode" with a dropdown arrow. The second setting is "Sign-in restriction", currently set to "Locally applied" with a dropdown arrow, and a sub-setting "Do not allow any user to sign in" with a dropdown arrow.

6. User & Browser Settings - Sign-in settings

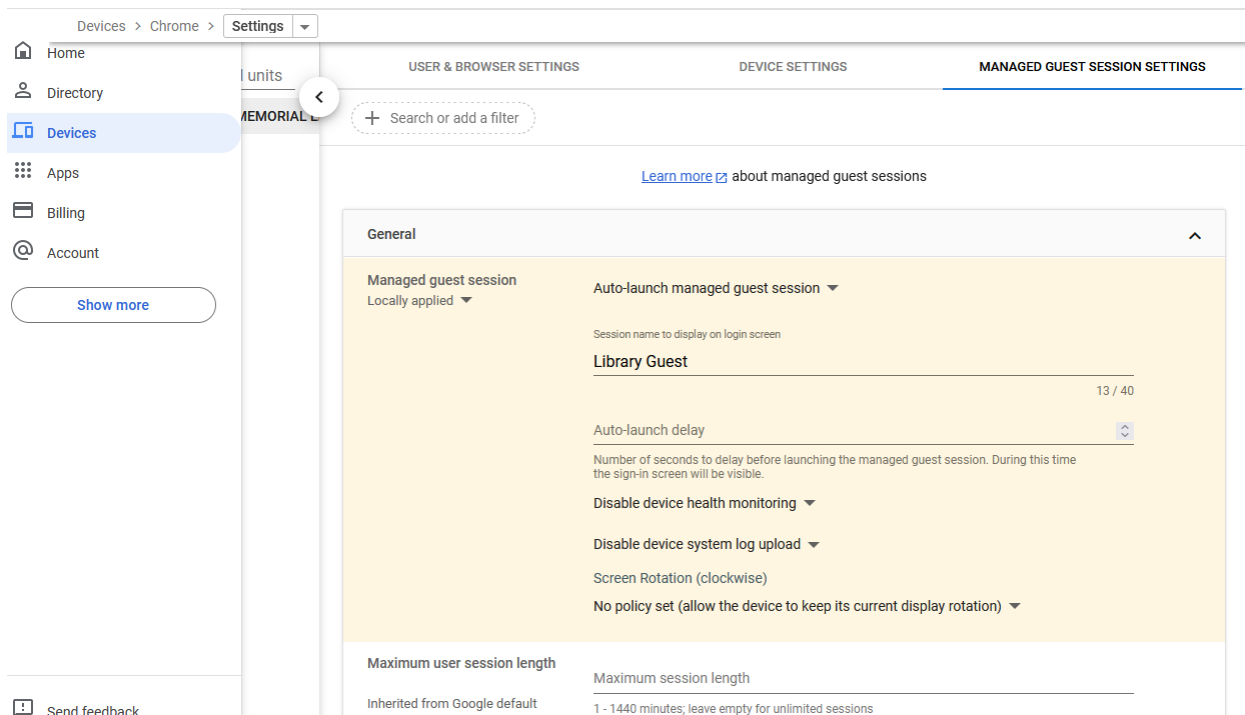
- From within the Admin console, select the **Main Menu**.
- Select the **Devices** dropdown. From there select **Chrome > Settings > User & Browser**.
- Under the **Display password button** section, select **Do not show the display password button on the login and lock screen**.
- Enrollment permissions - select **Allow users in this organization to enroll new or re-enroll existing devices**.

Google Chrome Enterprise Help

7. Managed Guest Sessions Settings

- From within the Admin console, select the **Main Menu**.
- Select the **Devices** dropdown. From there select **Chrome > Settings > Managed Guest Sessions**.

Set managed guest sessions to auto-launch.



The screenshot displays the Google Chrome Enterprise Admin console interface. The breadcrumb navigation at the top reads "Devices > Chrome > Settings". The left-hand navigation menu includes "Home", "Directory", "Devices" (which is highlighted), "Apps", "Billing", and "Account". Below the menu is a "Show more" button and a "Send feedback" link at the bottom.

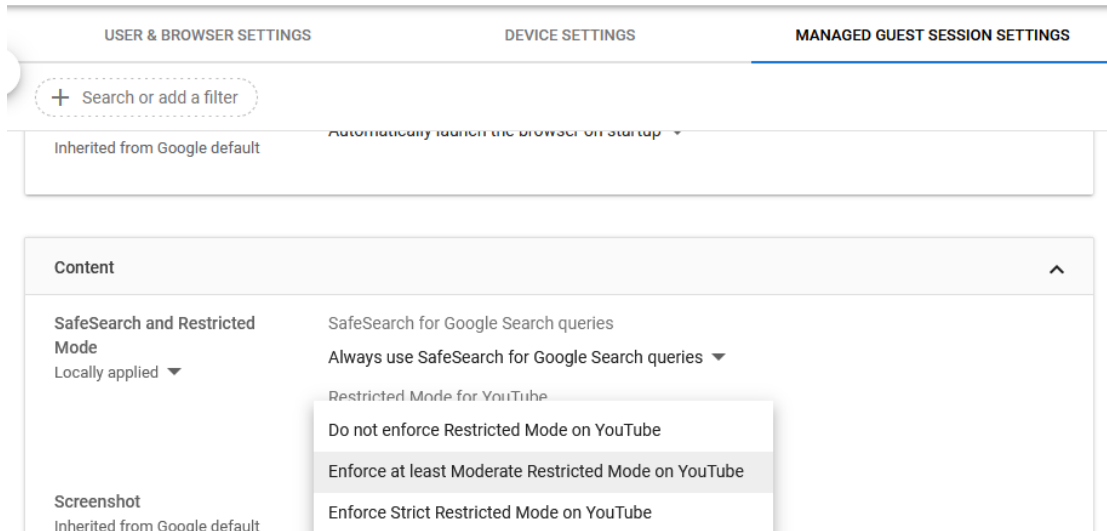
The main content area is titled "MANAGED GUEST SESSION SETTINGS" and includes a search bar with the placeholder text "+ Search or add a filter". A link for "[Learn more](#) about managed guest sessions" is present. The "General" section is expanded, showing the following settings:

- Managed guest session:** Locally applied
- Auto-launch managed guest session:** A dropdown menu is set to "Auto-launch managed guest session".
- Session name to display on login screen:** "Library Guest" (with a character count of 13 / 40).
- Auto-launch delay:** A dropdown menu.
- Disable device health monitoring:** A dropdown menu.
- Disable device system log upload:** A dropdown menu.
- Screen Rotation (clockwise):** "No policy set (allow the device to keep its current display rotation)".

At the bottom, the "Maximum user session length" section shows "Maximum session length" set to "1 - 1440 minutes; leave empty for unlimited sessions", which is noted as being "Inherited from Google default".

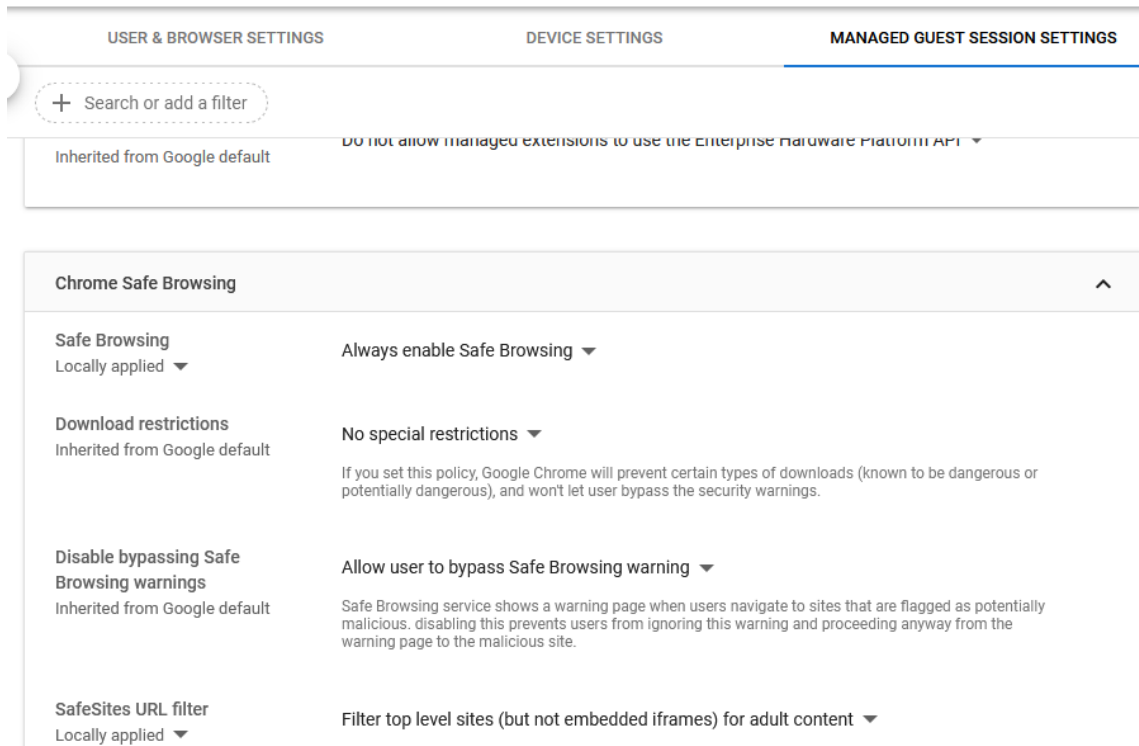
Google Chrome Enterprise Help

- Enable SafeSearch for Google search results.



The screenshot shows the 'MANAGED GUEST SESSION SETTINGS' tab in Google Chrome Enterprise. A search bar at the top contains the text '+ Search or add a filter'. Below it, a search bar contains the text 'Automatically launch the browser on startup'. The 'Content' section is expanded, showing 'SafeSearch and Restricted Mode' set to 'Locally applied'. A dropdown menu is open for 'SafeSearch for Google Search queries', showing options: 'Always use SafeSearch for Google Search queries', 'Restricted Mode for YouTube', 'Do not enforce Restricted Mode on YouTube', 'Enforce at least Moderate Restricted Mode on YouTube', and 'Enforce Strict Restricted Mode on YouTube'. The 'Screenshot' section shows 'Inherited from Google default'.

- Enable SafeSites URL Filter.



The screenshot shows the 'MANAGED GUEST SESSION SETTINGS' tab in Google Chrome Enterprise. A search bar at the top contains the text '+ Search or add a filter'. Below it, a search bar contains the text 'Do not allow managed extensions to use the Enterprise Hardware Platform API'. The 'Chrome Safe Browsing' section is expanded, showing 'Safe Browsing' set to 'Always enable Safe Browsing', 'Download restrictions' set to 'No special restrictions', 'Disable bypassing Safe Browsing warnings' set to 'Allow user to bypass Safe Browsing warning', and 'SafeSites URL filter' set to 'Filter top level sites (but not embedded iframes) for adult content'. The 'Screenshot' section shows 'Inherited from Google default'.



Google Chrome Enterprise Help

CIPA compliant content filtering with CleanBrowsing

TLN has tested and verified that the product [CleanBrowsing](#) offers web content filtering to ensure CIPA compliance for all library loaned devices.

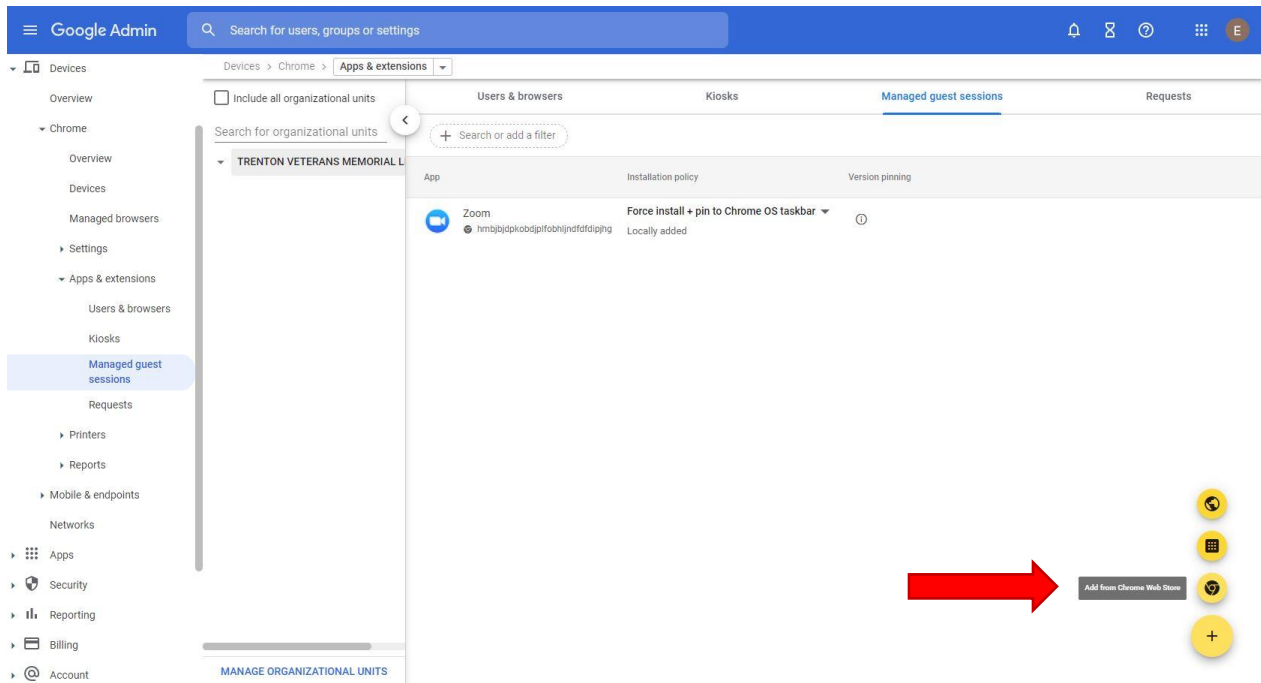
- Since this is a web-based DNS solution, all settings are configured within the CleanBrowsing web portal then enabled on activated devices. Once the device you need monitored has the assigned CleanBrowsing DNS IP address set, it can be used outside the library and remain filtered.
- CleanBrowsing key features include:
 - Predefine Filters - Over 19 predefined filters to quickly filter by entire categories (e.g., Pornography, Partial-Nudity, Malicious, Mixed Content, etc...)
 - Custom whitelist/blacklist - Easily add custom domains to the custom "allow" or "block" lists to create custom rules on your network.
 - Activity Monitoring - A modern, simplified, dashboard experience allows you to quickly see, and parse, daily activity to see what is happening on the network.
 - Data Retention - Choose how long to store your logs. Options include extreme configurations that include "no-logs" to storage as long as 90 days.
- Please visit <https://cleanbrowsing.org/pricing/> for all pricing options.
- CleanBrowsing works with Windows, Google Chrome, Apple, MacOS products.
 - For Windows, Android and Apple products, download the app. Only Google requires extra steps

Google Chrome Enterprise Help

CleanBrowsing Installation Steps - Chromebooks

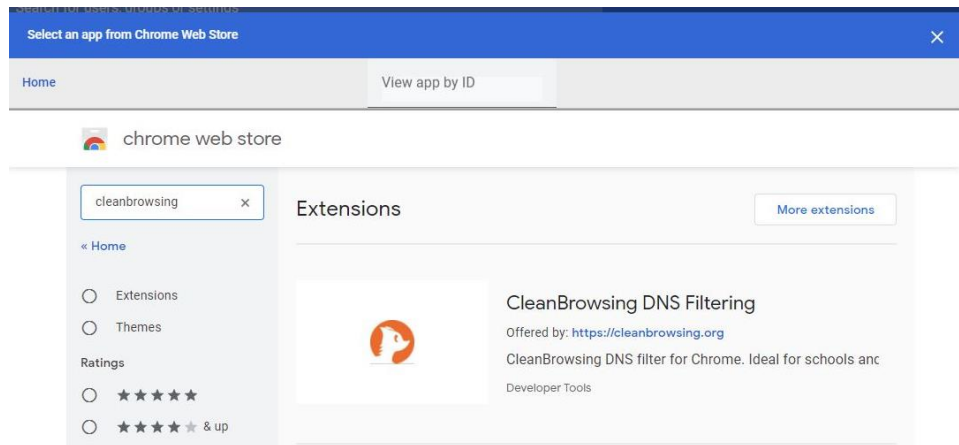
1. After purchasing your CleanBrowsing device licenses, you must sign to your [Google Admin console](#).

- Under the **Devices > Chrome > Apps & extensions > Managed Guest Sessions**.
 - At the bottom right of the window, select **Add from Chrome Web Store**.



Google Chrome Enterprise Help

2. Once the Chrome Web Store window appears, type “cleanbrowsing” in the search field

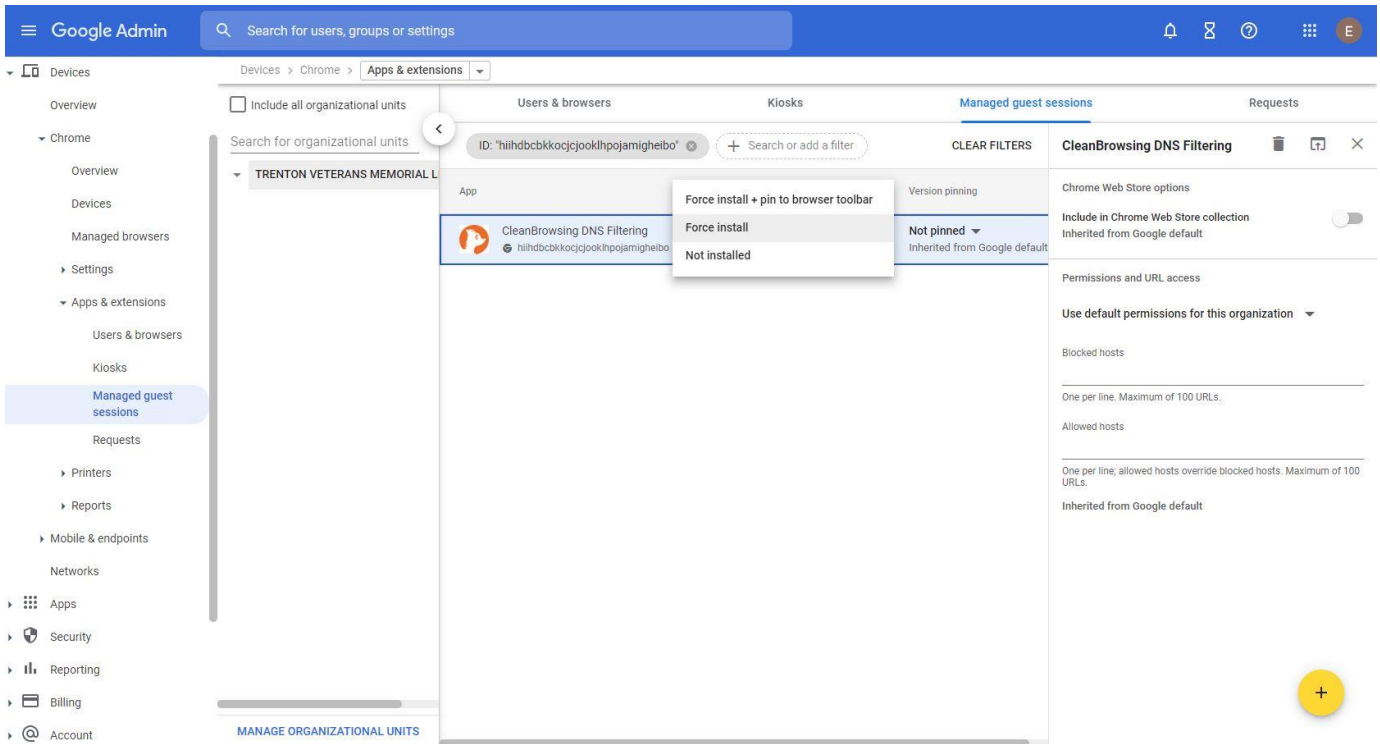


and hit **ENTER**.

3. Select **CleanBrowsing DNS Filtering** extension from the list and click the blue **Select** button on the top right corner of the window.

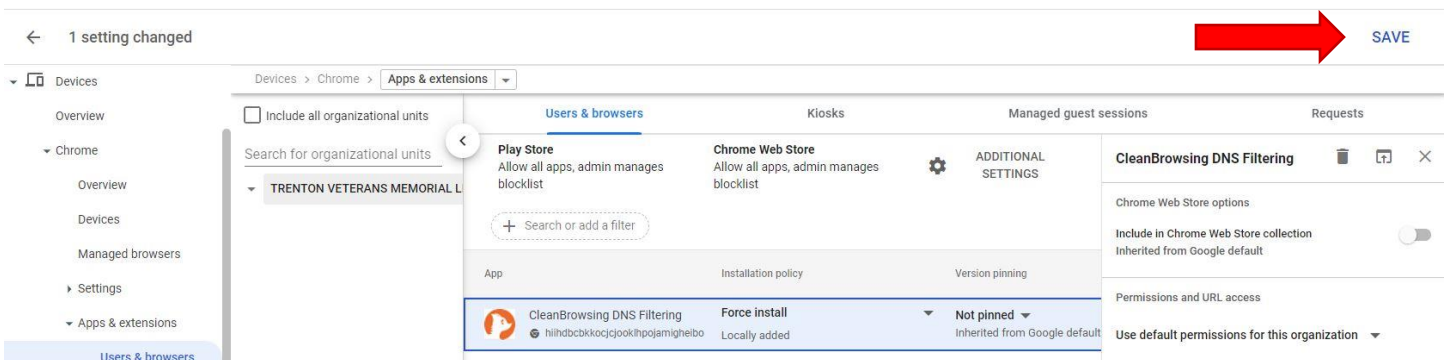
Google Chrome Enterprise Help

- Click on the app within the list and select **Force install**.



The screenshot shows the Google Admin console interface. The left sidebar contains navigation options like Overview, Chrome, Managed browsers, Settings, Apps & extensions, Users & browsers, Kiosks, Managed guest sessions, Requests, Printers, Reports, Mobile & endpoints, Networks, Apps, Security, Reporting, Billing, and Account. The main content area is titled 'Apps & extensions' and shows a list of apps for the organization 'TRENTON VETERANS MEMORIAL L'. The 'CleanBrowsing DNS Filtering' app is selected, and a context menu is open over it, showing options: 'Force install + pin to browser toolbar', 'Force install', and 'Not installed'. The 'Force install' option is highlighted. The right side of the screen shows the app's configuration details, including 'CleanBrowsing DNS Filtering' settings, 'Chrome Web Store options', and 'Permissions and URL access'.

- Save your change with the **SAVE** button in the top right corner.

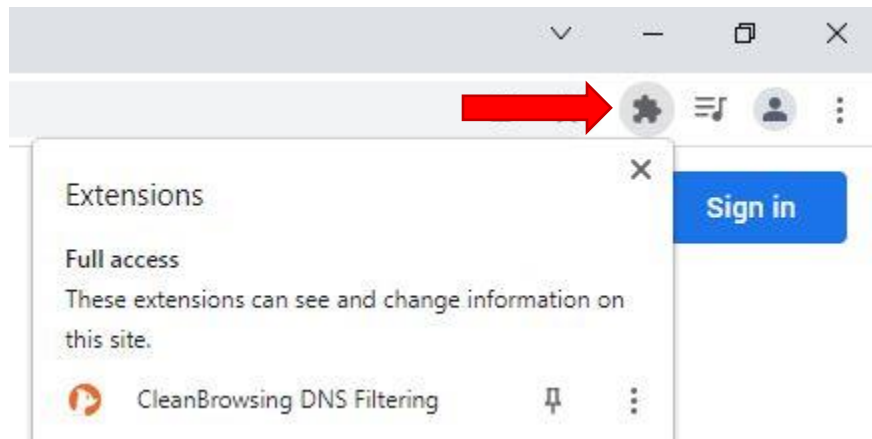


The screenshot shows the Google Admin console interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Users & browsers' and shows a list of apps for the organization 'TRENTON VETERANS MEMORIAL L'. The 'CleanBrowsing DNS Filtering' app is selected, and its configuration details are visible. A red arrow points to the 'SAVE' button in the top right corner of the page. The top of the page shows a notification '1 setting changed'.

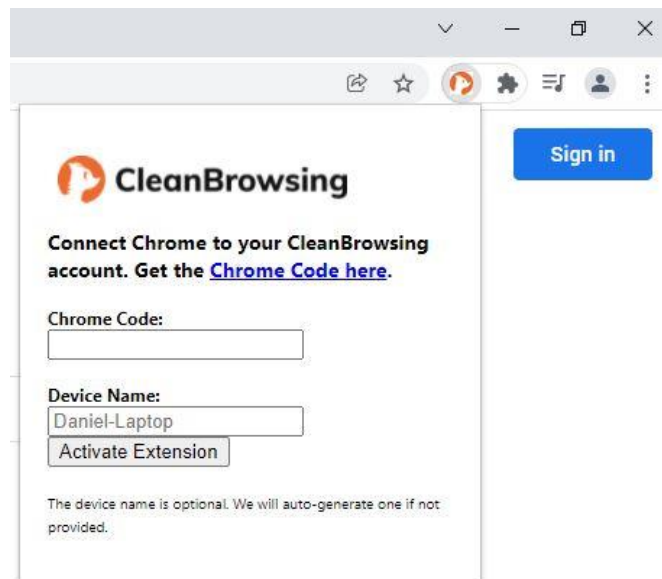
Google Chrome Enterprise Help

4. Enable the CleanBrowsing browser extension on the Chromebook.

- Turn on your Chromebook and open Google Chrome.
- Now that the Admin Console settings are saved, you should now see CleanBrowsing DNS Filtering as a web extension option. Select the **extension icon** in the toolbar.



- Select **CleanBrowsing DNS Filtering** from the extensions list. The app will then ask for your account code and to enter a unique device name. If you do not know this code, you can select the option in the dialog box to get this info from [here](#).





Google Chrome Enterprise Help

- Once the app has been activated, the device is ready to deploy for patron use.