The Library Network
Libraries working together.

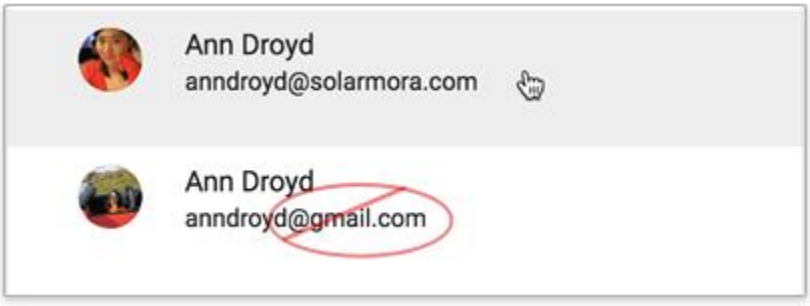
Google Chrome Enterprise Help

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*

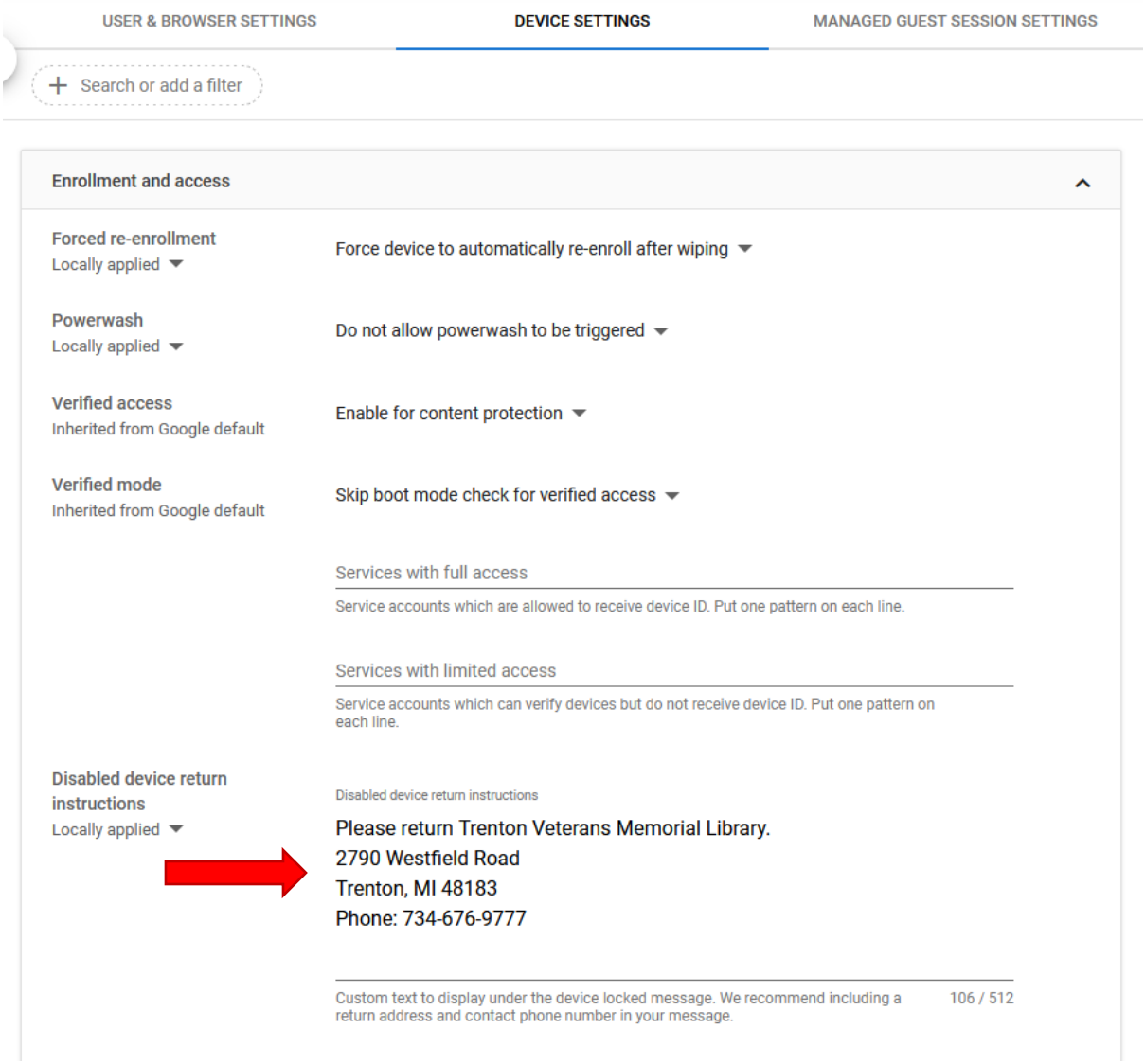
- From the Admin Console Home page, go to **Devices**.
- Click **Networks** and then **> Wi-Fi.**
- To apply the setting to all devices, leave the top organizational unit selected. Otherwise, select a child organizational unit.
- Click **Add Wi-Fi.**
- Under Platform access, select **Chromebooks (by 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.

The Library Network
Libraries working together.

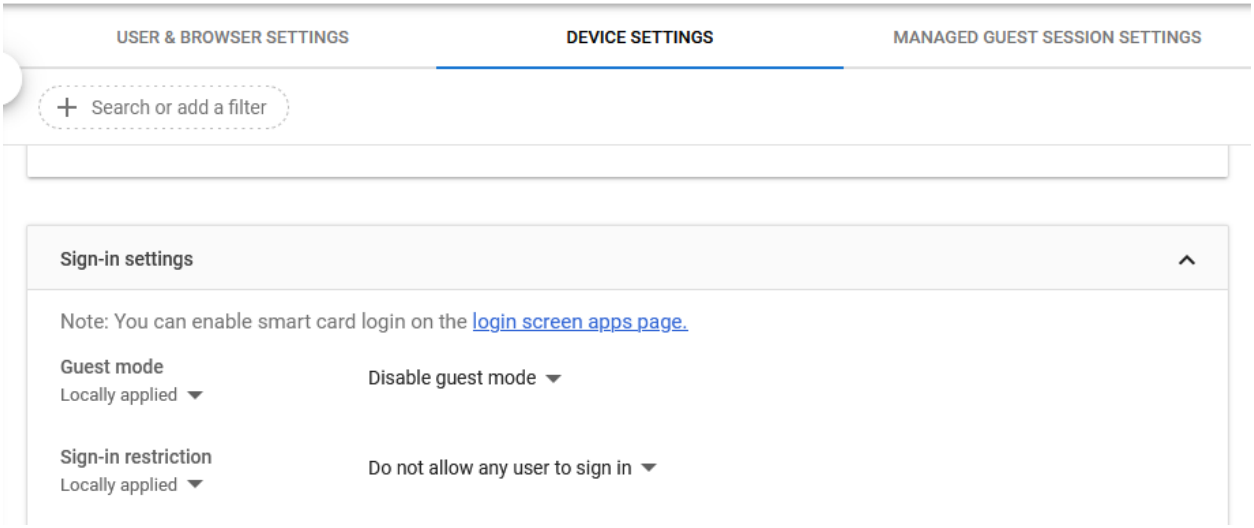
Google Chrome Enterprise Help



- 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.

The Library Network
Libraries working together.

Google Chrome Enterprise Help



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.**

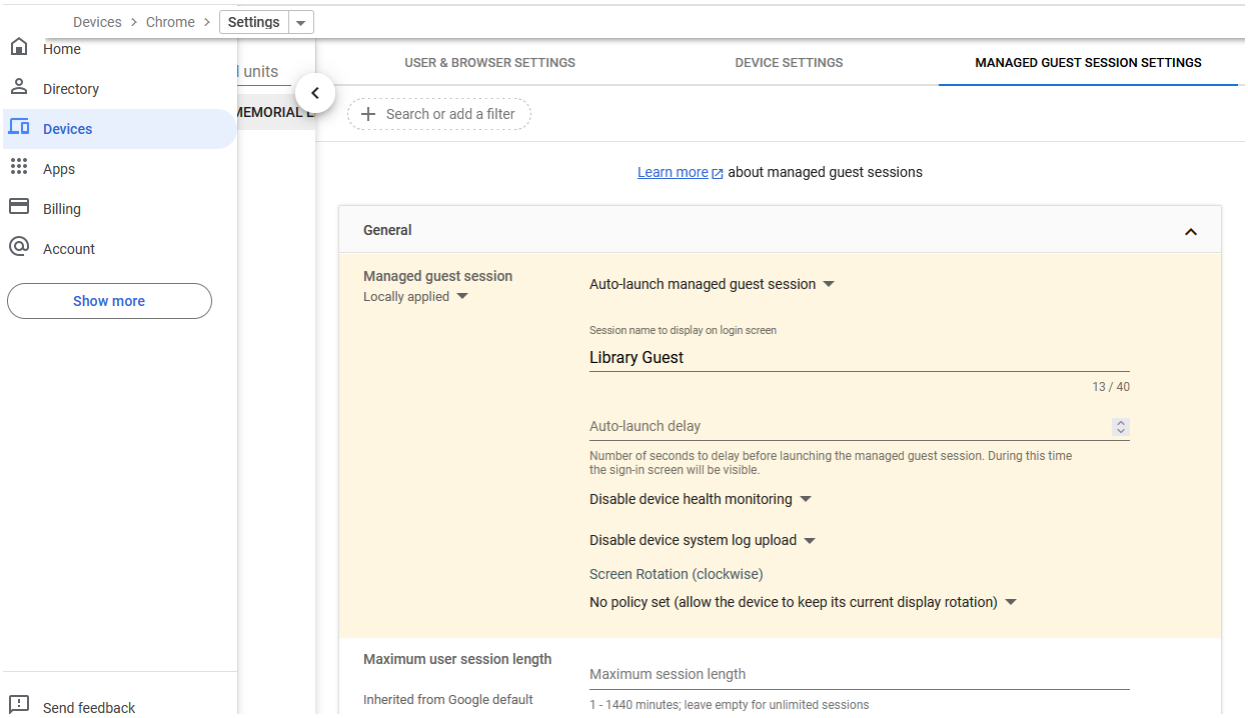
The Library Network
Libraries working together.

Google Chrome Enterprise Help

7. Managed Guest Sessions Settings

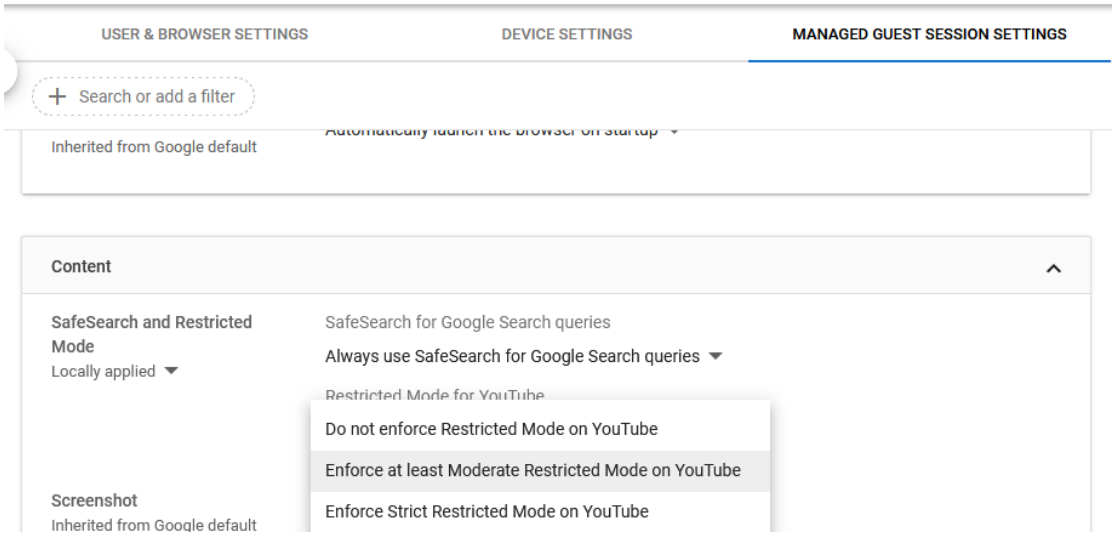
- From within the Admin console, select the **Main Menu**.
- Select the **Devices** dropdown. From there select **Chrome > Settings > Managed Guest Sessions.**

Set managed guest sessions to auto-launch.

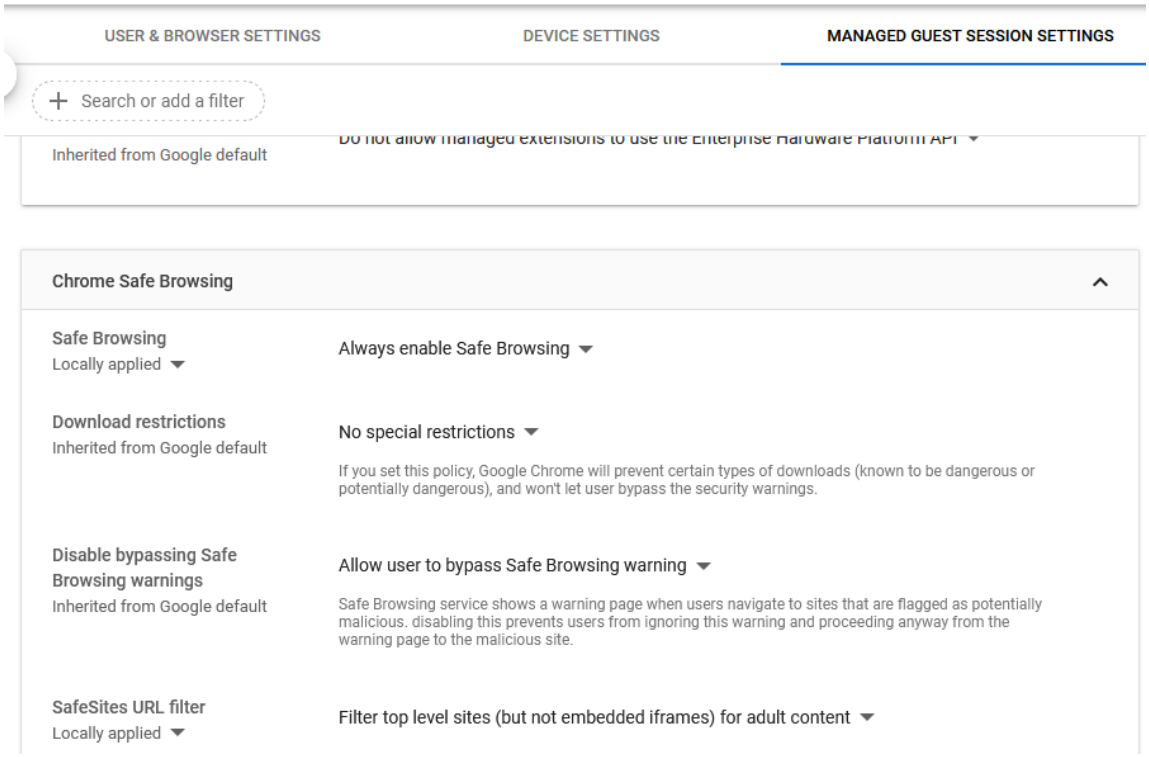


Google Chrome Enterprise Help

- Enable SafeSearch for Google search results.



- Enable SafeSites URL Filter.



The Library Network
Libraries working together.

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

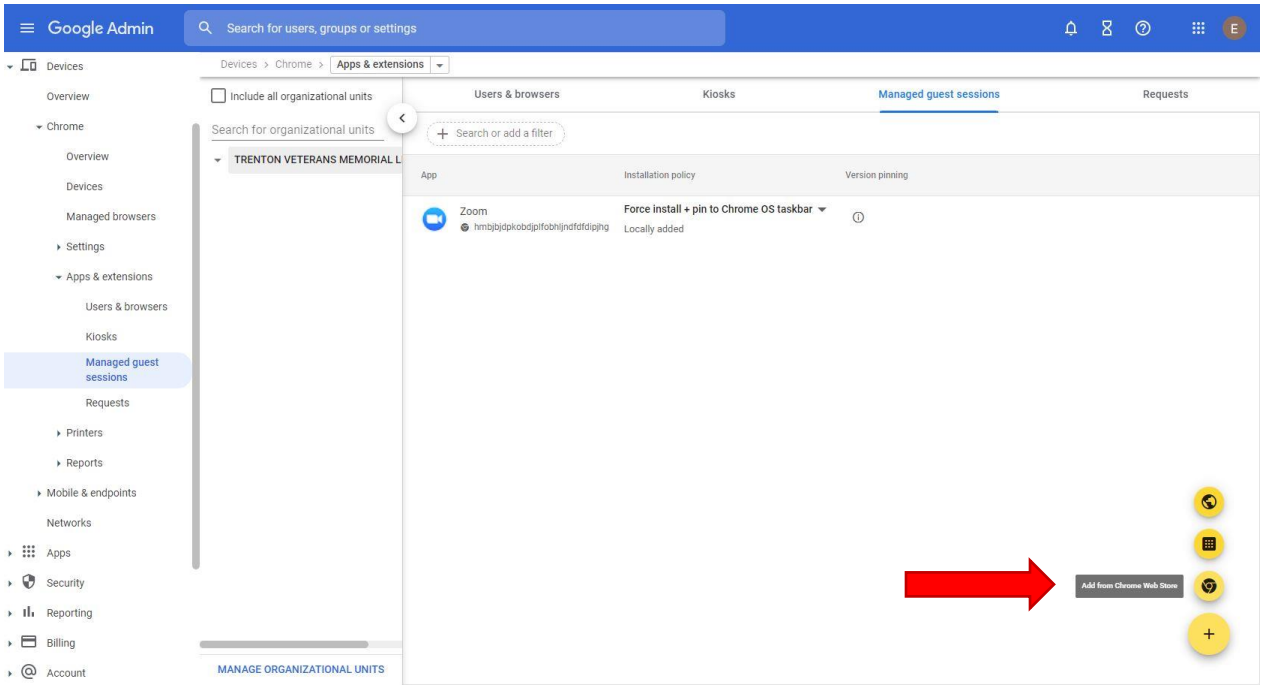
The Library Network
Libraries working together.

Google Chrome Enterprise Help

CleanBrowsing Installation Steps - Chromebooks

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

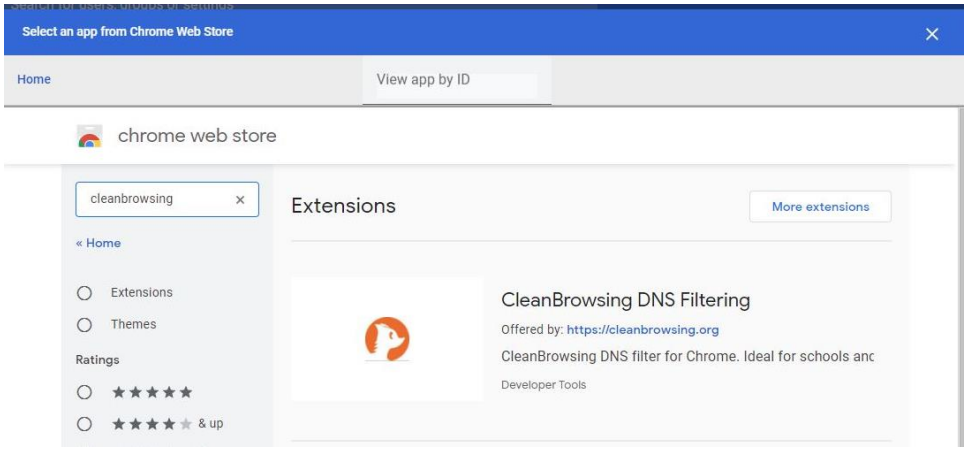
- Under the **Devices > Chrome > Apps & extensions > Managed Guest Sessions.**
  - At the bottom right of the window, select **Add from Chrome Web Store.**



The Library Network
Libraries working together.

Google Chrome Enterprise Help

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



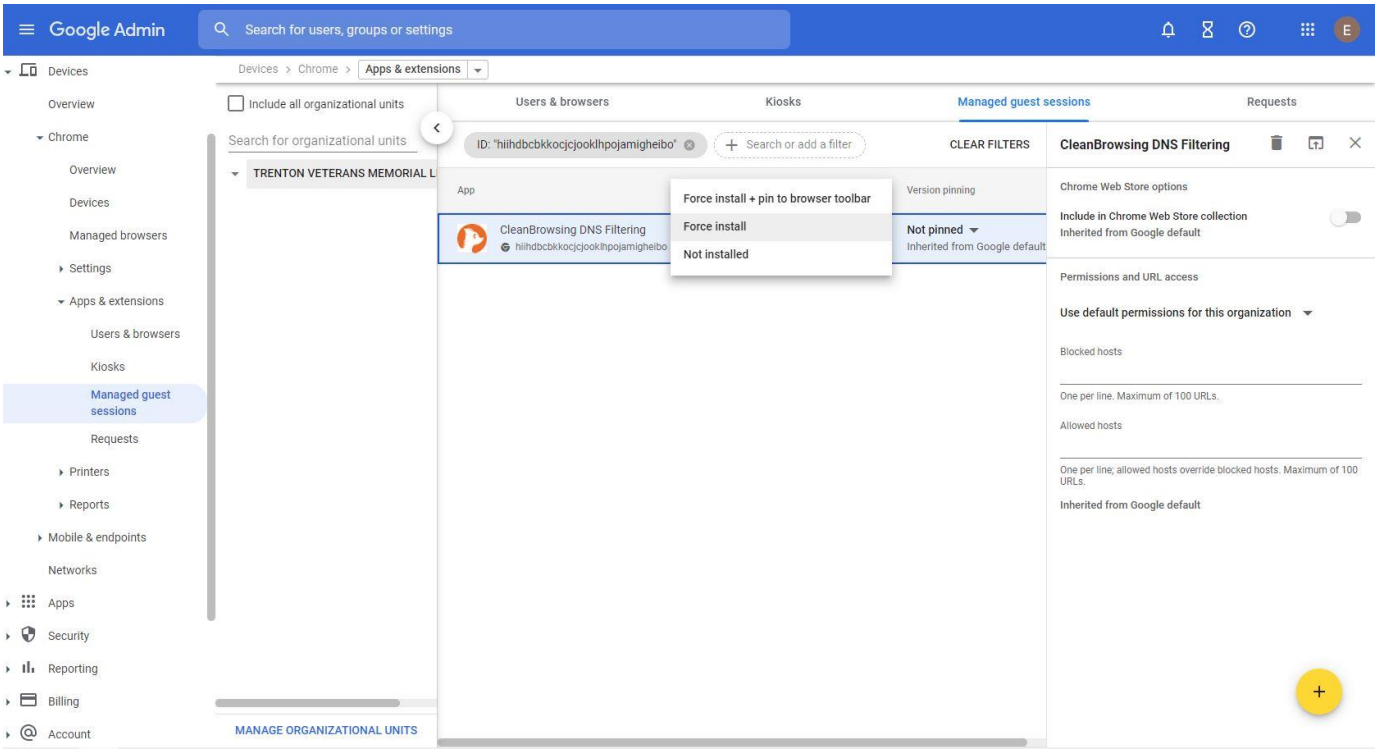
and hit **ENTER**.

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

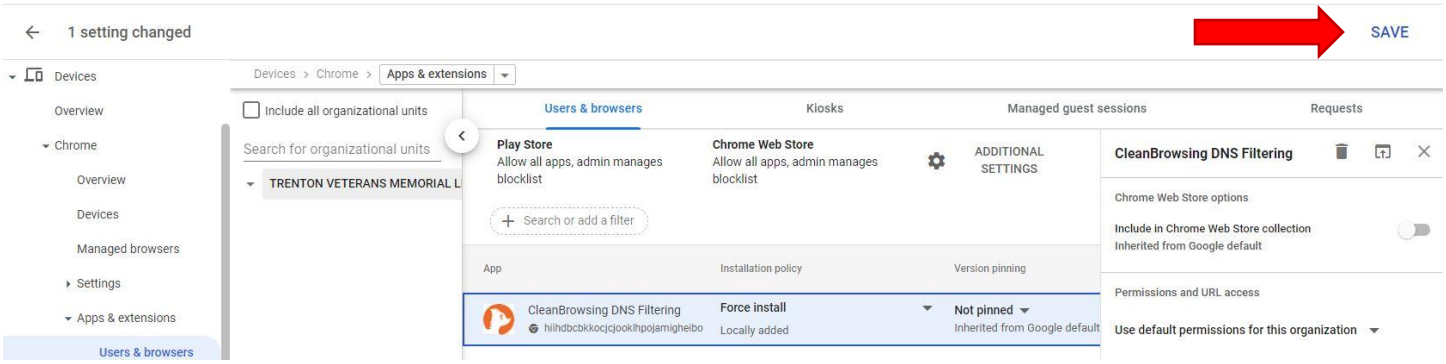
The Library Network
Libraries working together.

Google Chrome Enterprise Help

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

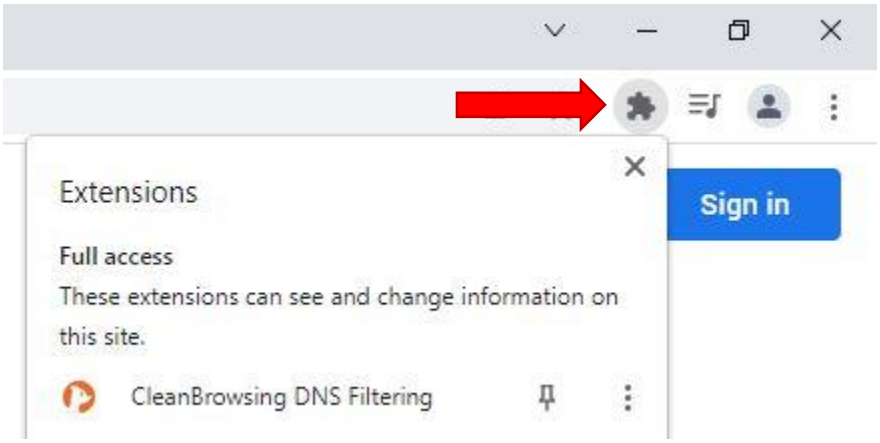


- Save your change with the **SAVE** button in the top right corner.

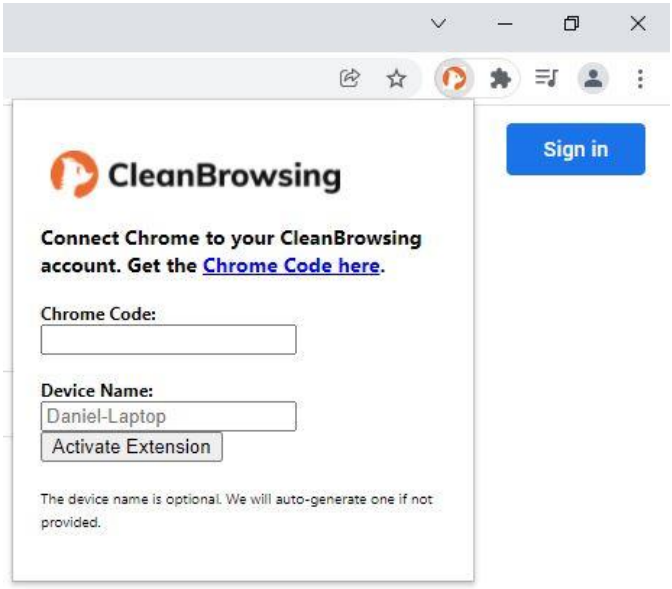


4. Enable the CleanBrowsing browser extension on the Chromebook.

- 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.



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