securly

Chromebook best practices

Table of contents

Overview

Security is a key requirement of any 1:1 Chromebook program—ensuring students are using their devices safely and productively.

This document addresses several aspects of the Google Apps for Education Admin Console that are important to configure correctly for a successful 1:1 experience. The Google Apps cloud-based policy consists of:

Device settings

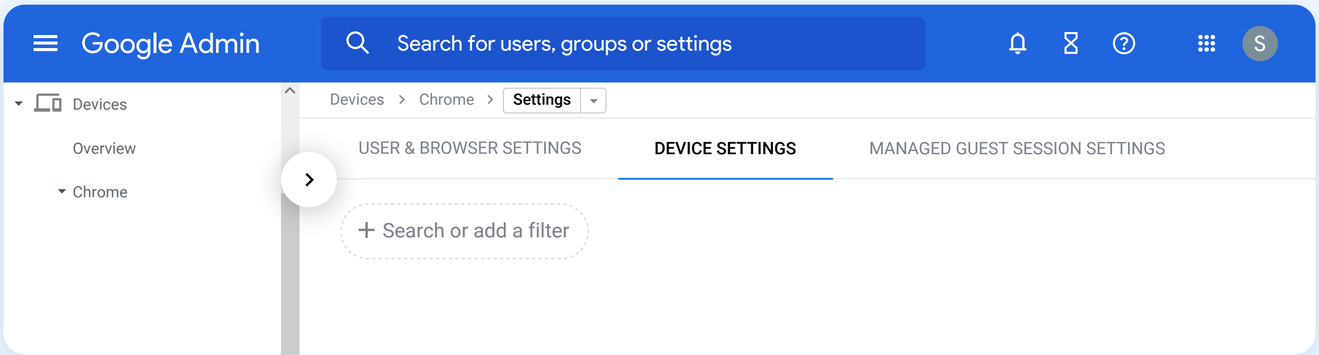
User settings

While the User Settings are pushed down to the Chrome browser regardless of the device when as the user logs in, the Device Settings are only pushed down to the Chromebook device if the device is enrolled into the school's enterprise policy as configured via the admin console.

To learn more about Google's Chrome Policy Management and the various policies for users and browsers, check out the **Knowledge Base** more broadly.

Device settings

The primary navigation for all device settings in this section is **Device management > Chrome management > Device settings** after logging in to your G Suite admin console.

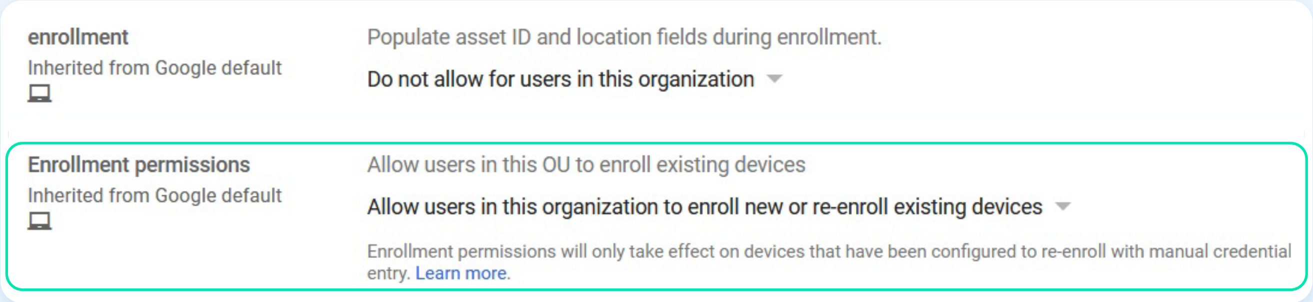


Enrolling devices

Enrolling the Chromebook device in your school policy is necessary to push Device Settings down to that device. The Device Settings can include important pieces such as guest mode access or sign-in restrictions. To enroll your Chromebooks in the school policy, ensure that the device is enrolled in the enterprise policy. To do this:

1. Navigate to **Device Management** > **Chrome Management** > **Device Settings**

2. Select **'Force device to re-enroll into this domain after wiping'** from the dropdown for the **'Forced Re-enrollment'** field.



enrollment
Inherited from Google default

Populate asset ID and location fields during enrollment.
Do not allow for users in this organization

Enrollment permissions
Inherited from Google default

Allow users in this OU to enroll existing devices
Allow users in this organization to enroll new or re-enroll existing devices

Enrollment permissions will only take effect on devices that have been configured to re-enroll with manual credential entry. Learn more.

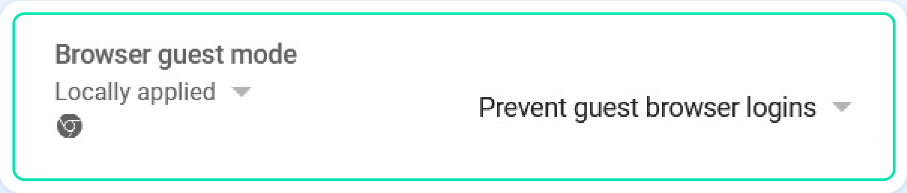
Note that this should be done for for OUs with devices that need to be managed by the admin console.

When, when your Chromebooks first arrive, your students can log in with their admin console-created credentials. This will automatically enroll the Chromebooks into the enterprise policy for the school—without the admins needing to individually log in to each of these devices.

Disabling guest mode

The guest mode for Chromebooks allows users to bypass the school district's filtering policy and expose them to inappropriate content. It is therefore recommended that you disable the guest mode for all your devices. The guest mode is similar to the incognito mode in Chrome browsers which we also recommend disabling. To disable guest mode:

1. Navigate to **Device Management** > **Chrome Management** > **Device Settings**
2. Scroll down to **Sign-in Settings**
3. Select the **'Do not allow guest mode'** option from the dropdown for the guest mode field.

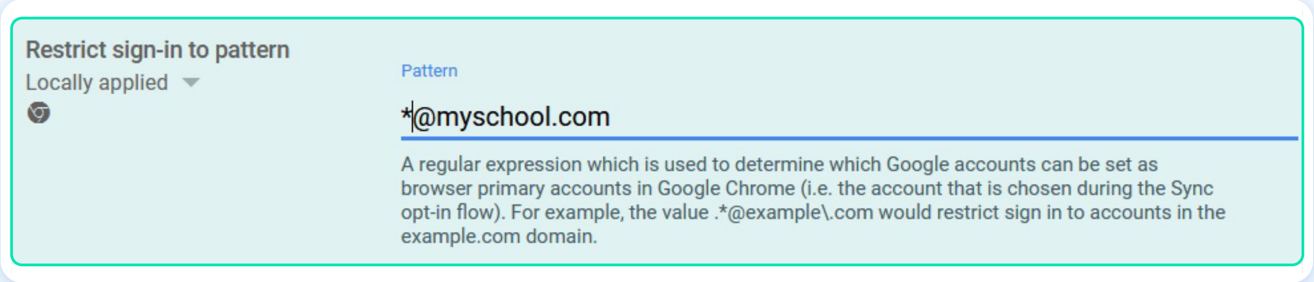


Browser guest mode
Locally applied
Prevent guest browser logins

Implementing sign-in restrictions

You may want to restrict users from logging in using their personal Gmail IDs on school-owned Chromebooks. Personal Gmail IDs can lead to evasion of filtering and auditing of the Chromebook. To restrict login:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Sign-in Settings** > **Restrict sign-in to pattern**
3. In the text box enter the domain you want to allow sign-ins from. For example, ***@k12publicschools.org** will restrict logins to only **k12publicschools.org** and prevent users from signing in using their Gmail address.



Restrict sign-in to pattern
Locally applied

Pattern
*@myschool.com

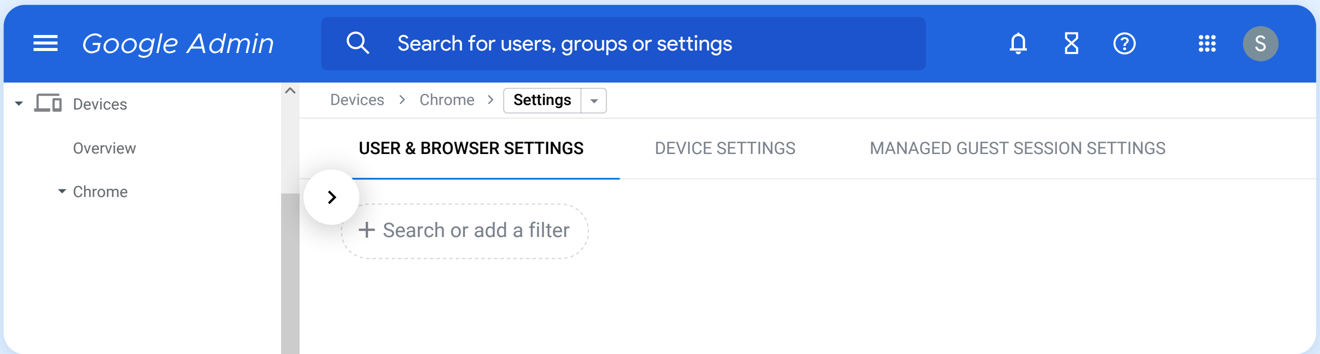
A regular expression which is used to determine which Google accounts can be set as browser primary accounts in Google Chrome (i.e. the account that is chosen during the Sync opt-in flow). For example, the value .*@example\.com would restrict sign in to accounts in the example.com domain.

Make sure that you do not restrict access to **https://accounts.google.com/AccountChooser** to allow teachers to switch between accounts and use the **temporary allow sites** feature seamlessly.

Securly also allows you to customize access to personal Gmail on school devices. Click **here** to learn how.

User settings

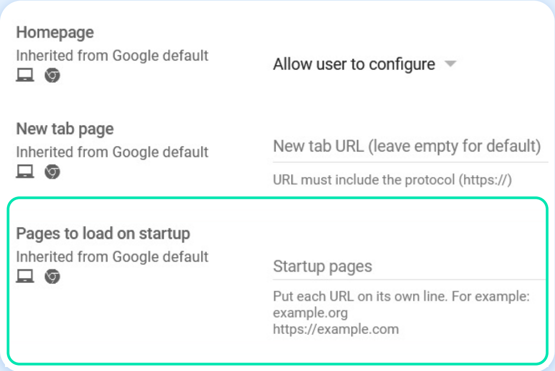
The primary navigation for all user settings is **Device Management** > **Chrome Management** > **User Settings** after you log in to your G Suite admin console.



Customizing start-up display pages

It is possible to predefine the web pages that should be displayed automatically to the users when they start up their Chromebooks and begin browsing. It is recommended that you display pages such as your school's Acceptable Use Policy (AUP) here so that students are reminded of following proper online conduct and other school policies they are bound by. To do this:

1. Navigate to **Device to Device** > **Chrome** > **Settings**
2. Scroll down to **Startup.** In the text box for Pages to Load on Startup enter the web pages you want to first display upon startup. For example: **www.k12publicschools.org/aup.html**


Homepage
Inherited from Google default
Allow user to configure

New tab page
Inherited from Google default
New tab URL (leave empty for default)
URL must include the protocol (https://)

Pages to load on startup
Inherited from Google default
Startup pages
Put each URL on its own line. For example:
example.org
https://example.com

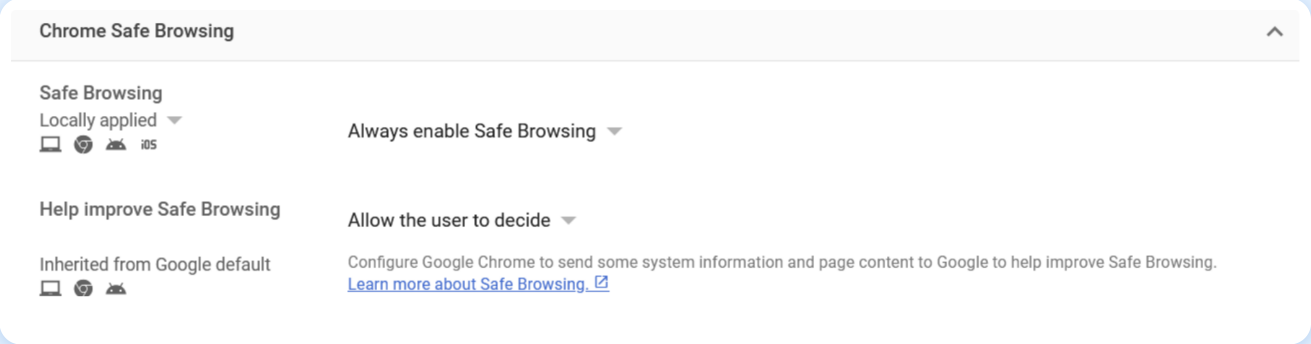
Enabling Safe Browsing and Safe Search

Chromebooks are generally known to be immune against most malware and therefore good at protecting kids from malicious websites. However, to ensure extra security for students it is recommended that you enable Safe Browsing, Safe Search, and malicious sites settings in G Suite.

Safe Search helps you ensure that your users are always displayed safe search results and protected from age-inappropriate content and images. As they are user-level settings, they not only protect users on Chromebooks but also on Chrome browsers when the user logs into a different device.

Furthermore, malicious sites can also include phishing or other sites that involve platform independent vulnerabilities that target the user directly—e.g. identity theft, financial theft, password theft, etc. To enable safe browsing and malicious sites protection:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Chrome Safe Browsing**
3. Select the **"Always enable Safe Browsing"** option from the dropdown list for the Safe Browsing field.



Chrome Safe Browsing

Safe Browsing
Locally applied
iOS

Always enable Safe Browsing

Help improve Safe Browsing

Allow the user to decide

Inherited from Google default

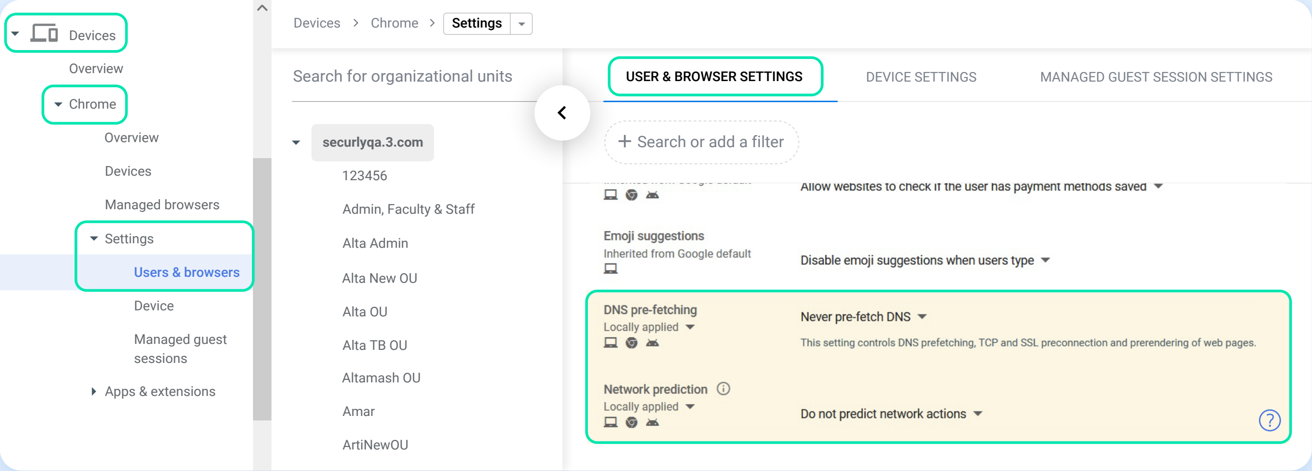
Configure Google Chrome to send some system information and page content to Google to help improve Safe Browsing.
Learn more about Safe Browsing.

Bypass DNS pre-fetching

Sometimes, websites tend to be logged as user activity even if they do not actually visit a website. For example, a user searches for Facebook login on google.com. The user may or may not actually click the search result link for the Facebook login page, but as browsers tend to pre-fetch sites it is logged as user activity with Securly. This can lead to some incorrect representation of user activity at times.

To avoid this:

1. Navigate to **Devices** > **Chrome** > **Settings** > **Users and browsers**
2. Scroll down to **User experience**
3. Select **'DNS pre-fetching'** and choose **'Never pre-fetch DNS'** from the dropdown.
4. For the **'Network prediction'** field select **'Do not predict network actions'** from the dropdown.



Inherited from Google default — Allow websites to check if the user has payment methods saved

Emoji suggestions
Inherited from Google default — Disable emoji suggestions when users type

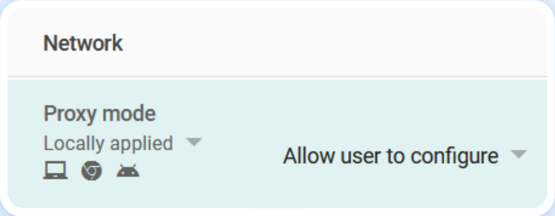
DNS pre-fetching
Locally applied — Never pre-fetch DNS
This setting controls DNS prefetching, TCP and SSL preconnection and prerendering of web pages.

Network prediction
Locally applied — Do not predict network actions

Proxy settings

Setting the Chrome Proxy settings to **'Allow User To Configure'** ensures that the Chrome browser will always respect SmartPac settings on Windows and Mac devices and keep that traffic filtered. To set the proxy settings:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Network**
3. Select the **'Allow user to configure'** option from the dropdown for the Proxy Settings field.

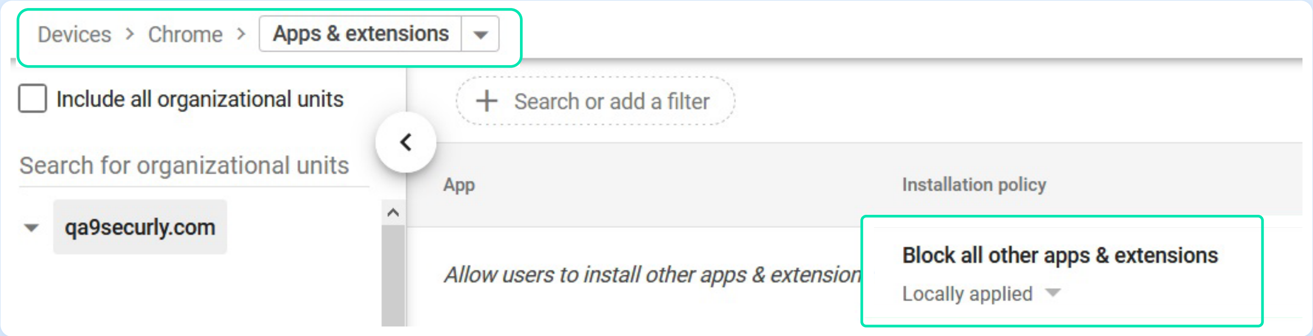

Network

Proxy mode
Locally applied — Allow user to configure

Managing apps and extensions

Many students will attempt to download games and other non-educational apps to their school-issued Chromebooks. Schools may decide to enforce restrictions on app installations, to help keep students focused on learning. To restrict app installations:

1. Navigate to **Devices** > **Chrome** > **Apps and Extensions**
2. Select the **"Block all other apps and extensions"** option from the dropdown for the Allow or Block Apps and Extension field.


Devices > Chrome > Apps & extensions

□ Include all organizational units

Search for organizational units

qa9securly.com

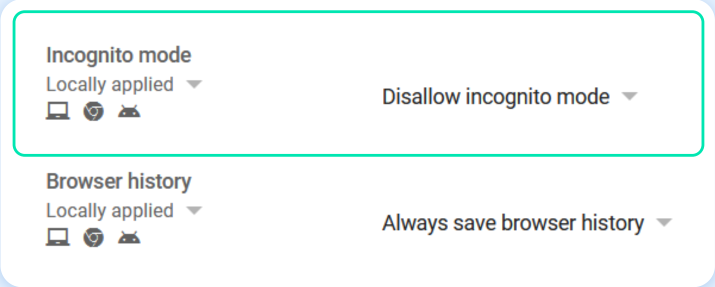
Search or add a filter

App	Installation policy
Allow users to install other apps & extension	Block all other apps & extensions Locally applied

Disabling Incognito mode

Similar to the guest mode in Chromebooks, it is recommended that you disable the Incognito mode for Chrome browsers. Users can bypass filtering using the Incognito mode, potentially exposing them to harmful and age-inappropriate content. To disable the Incognito mode:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Security**
3. Select the **'Disallow Incognito mode'** option from the dropdown for the Incognito mode field.


Incognito mode
Locally applied
Disallow incognito mode

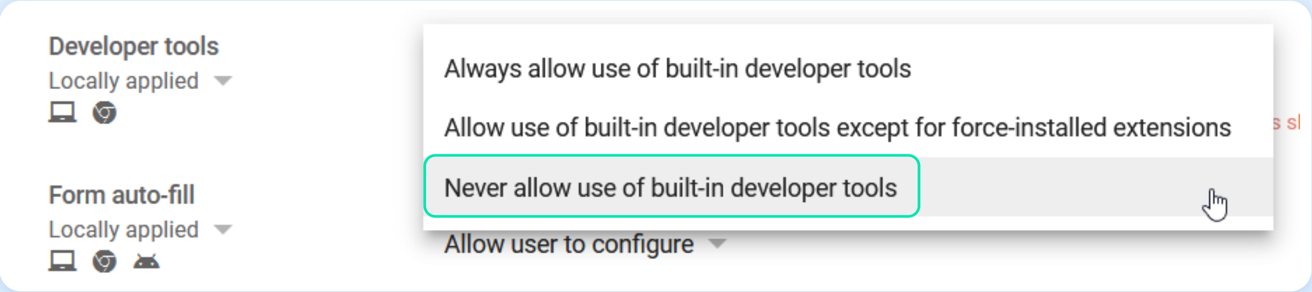
Browser history
Locally applied
Always save browser history

Disabling developer tools for Chromebooks

One of the many ways that students can bypass filtering is by tampering with scripts and apps using developer tools. Developer tools allow users to debug network, scripts, apps, and other issues.

It is also possible to gain an unfair advantage over other students by reverse engineering edtech applications that transmit insecure data or have confidential information hidden away in the code. It is therefore recommended that you always disable developer tools for your Chromebooks. To do this:

1. Navigate to **Device** > **Chrome** > **Settings**
2. Scroll down to **User Experience** > **Developer Tools**
3. Select the 'Never allow use of built-in developer tools' option from the dropdown.



Developer tools
Locally applied

Always allow use of built-in developer tools
Allow use of built-in developer tools except for force-installed extensions
Never allow use of built-in developer tools

s sl

Form auto-fill
Locally applied

Allow user to configure

Blocking URLs

There are various ways students can attempt to bypass filtering set by the school. One such way is to stop or disable extensions or to modify settings for their Chromebooks. It is possible to ensure that students do not disable extensions or modify settings by blocking certain URLs in your user settings. To do this:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Content** > **URL Blocking** > **URL Blacklist**
3. Input the following URLs in the text field:

chrome://**certificate-manager**

chrome://**extensions**

chrome://**addresses**

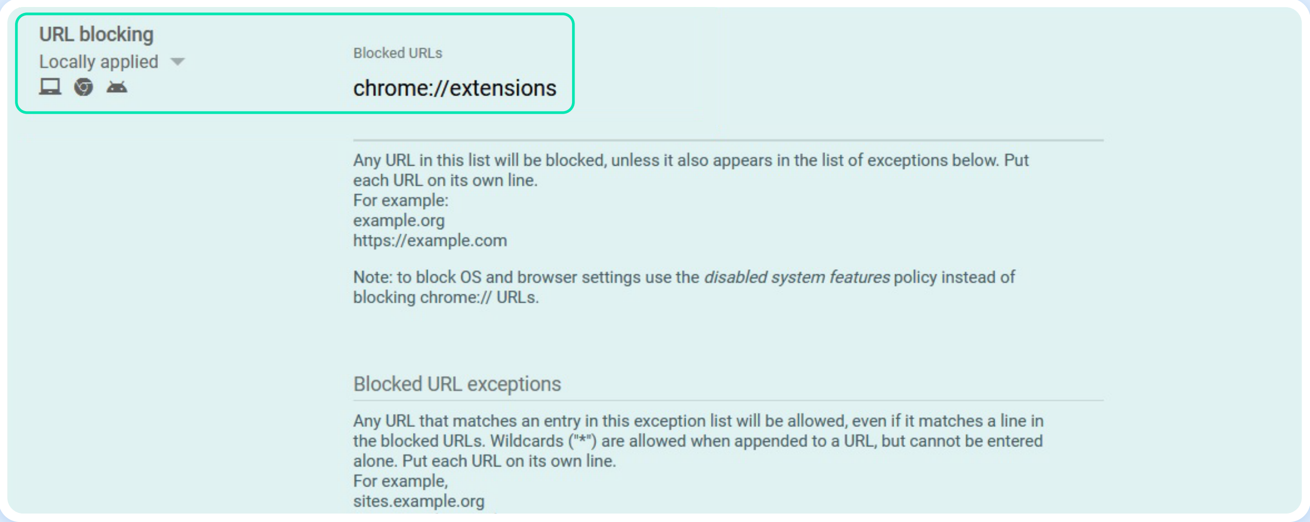
chrome://**settings/signOut**

chrome://**kill**

chrome://**hang**

javascript://*

4 You can add more such URLs to the URL blocking field depending upon the pages you want students to stay away from.



URL blocking
Locally applied

Blocked URLs
chrome://extensions

Any URL in this list will be blocked, unless it also appears in the list of exceptions below. Put each URL on its own line.
For example:
example.org
https://example.com

Note: to block OS and browser settings use the *disabled system features* policy instead of blocking chrome:// URLs.

Blocked URL exceptions

Any URL that matches an entry in this exception list will be allowed, even if it matches a line in the blocked URLs. Wildcards ("*") are allowed when appended to a URL, but cannot be entered alone. Put each URL on its own line.
For example,
sites.example.org

Securly also allows you to block or allow specific web pages, websites, and keywords to help you manage your students' access effectively. To learn more, click here.

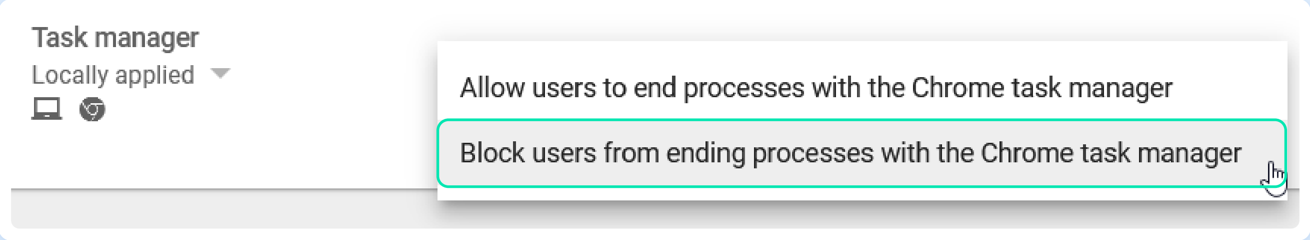
Disabling Task Manager for students

It is possible for students to disable Chrome extensions and other processes that are essential to ensuring a safe online experience for them. All they need is access to the Task Manager to do this. Giving students the ability to access the Task Manager is disruptive to schools' ability to manage and secure Chromebooks. It is therefore recommended that you disable the Task Manager for students on their Chromebooks.

1 Navigate to **Devices** > **Chrome** > **Settings**

2 Scroll down to **Apps and Extensions** > **Task Manager**

3 Select the **'Block user from ending processes with the Chrome task manager'** option from the dropdown.



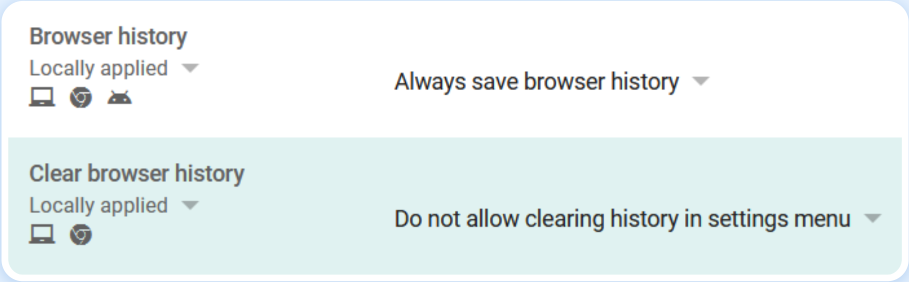
Task manager
Locally applied

Allow users to end processes with the Chrome task manager
Block users from ending processes with the Chrome task manager

Managing Browser history

It is recommended that you do not allow users to clear their browsing history. This can be done by disabling users' ability to clear browsing history. To do this:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Security**
3. Select **'Always save browser history'** option for the Browser History field.
4. Select **'Do not allow clearing history in settings menu'** option from the dropdown for the **'Clear Browser History'** field.



Browser history
Locally applied
Always save browser history

Clear browser history
Locally applied
Do not allow clearing history in settings menu

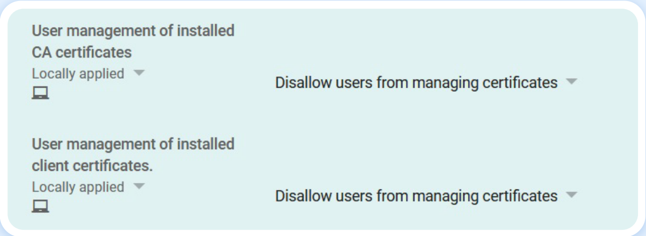
Managing user access to certificates

It is recommended that you do not allow users to edit certificates installed on their devices. To do this:

1. Navigate to **Devices** > **Chrome** > **Settings**
2. Scroll down to **Security**
3. Select **'Disallow users from managing certificates'** option for the following fields:

A. User management of installed CA certificates

B. User management of installed client certificates



User management of installed CA certificates
Locally applied
Disallow users from managing certificates

User management of installed client certificates.
Locally applied
Disallow users from managing certificates

YouTube Restricted Mode

The YouTube Restricted Mode helps you limit students' access to inappropriate content on YouTube. Setting up the YouTube Restricted Mode will give you greater flexibility with the administration of videos and channels. You can allow specific videos for specific groups of students to suit their educational requirements.

Note that it is necessary to enable YouTube Restricted Mode from G Suite so that students get it when they sign in using their school credentials. To do this:

1 Navigate to **Apps** > **Additional Google services**

2 Scroll down to **YouTube**

Note that YouTube service needs to be enabled for these features to work. This is as per OU setting.

3 Click on Permissions and select the OU you would like to change permissions for. This is set at each OU or inherited.

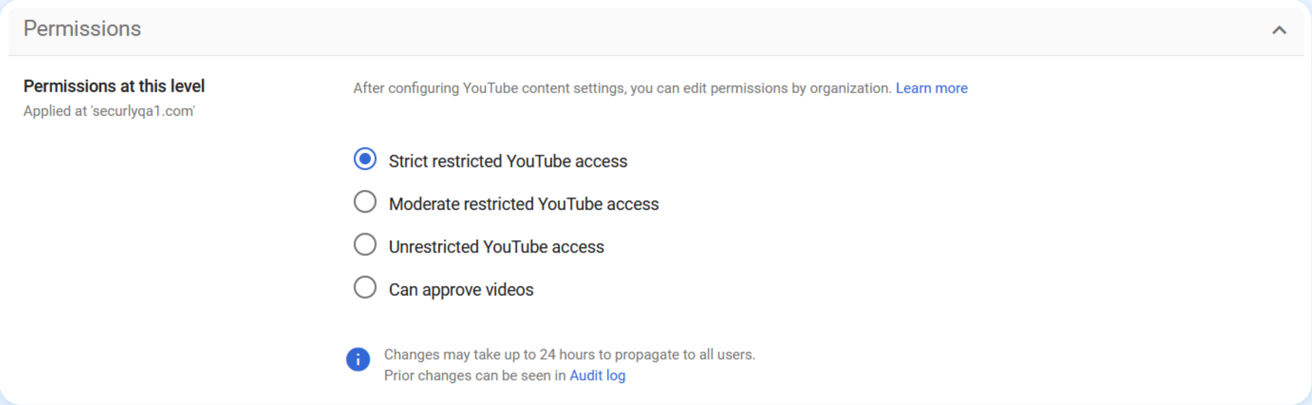
4 Set the level of permission for this OU.

A **Strict Restricted YouTube access**—Enabled by default only when you choose the option "restrict content for logged-in users in your organization.

B **Moderate Restricted YouTube access**—Users can only watch restricted and approved videos. This offering is similar to the Restricted Mode setting in the YouTube app and offers a larger corpus of videos than the Strict offering.

C **Unrestricted YouTube access**—Users can browse all of YouTube when signed-in even if you have also set network-level restrictions.

D **Can approve videos**—You can designate individuals or organizational units to approve videos so that signed-in users in their organization can watch them.



Permissions

Permissions at this level

Applied at 'securlyqa1.com'

After configuring YouTube content settings, you can edit permissions by organization. Learn more

● Strict restricted YouTube access

○ Moderate restricted YouTube access

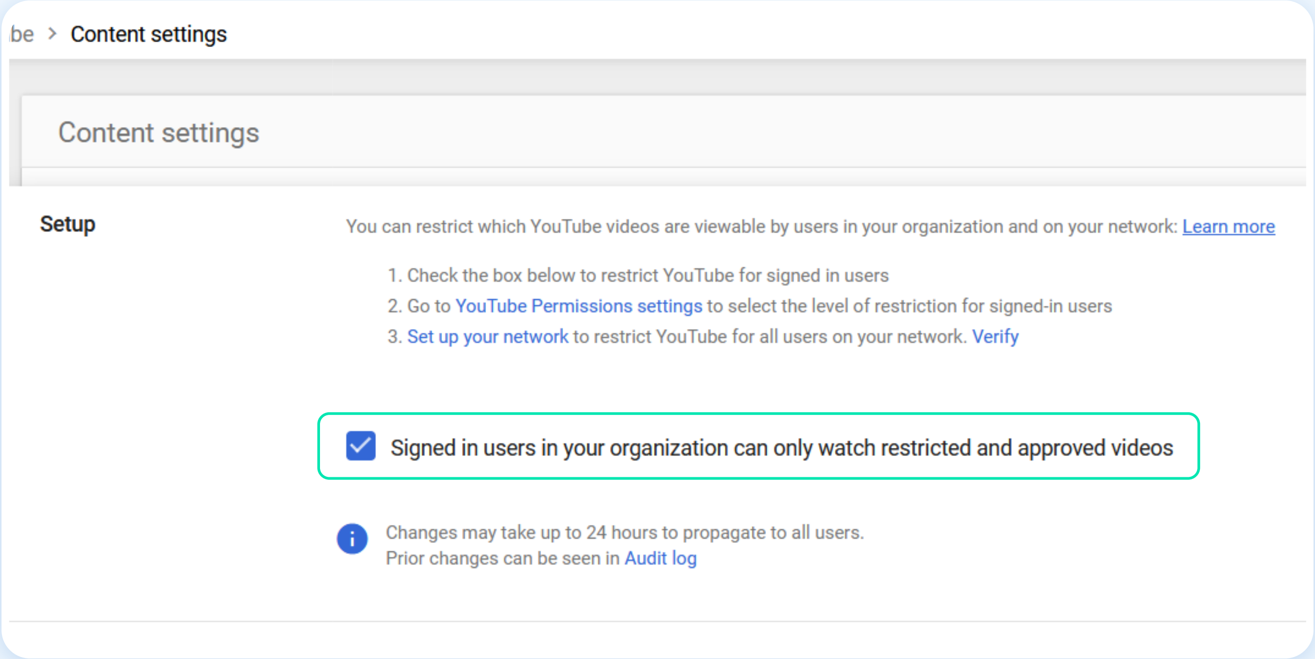
○ Unrestricted YouTube access

○ Can approve videos

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

5 After you are done with setting permission levels on all OUs, click Content Settings.

6 **"Signed in users in your organization can only watch restricted and approved videos"** needs to be checked to enable approval or restrictions from these settings.


be > Content settings

Content settings

Setup

You can restrict which YouTube videos are viewable by users in your organization and on your network: Learn more

1. Check the box below to restrict YouTube for signed in users
2. Go to YouTube Permissions settings to select the level of restriction for signed-in users
3. Set up your network to restrict YouTube for all users on your network. Verify

☑ Signed in users in your organization can only watch restricted and approved videos

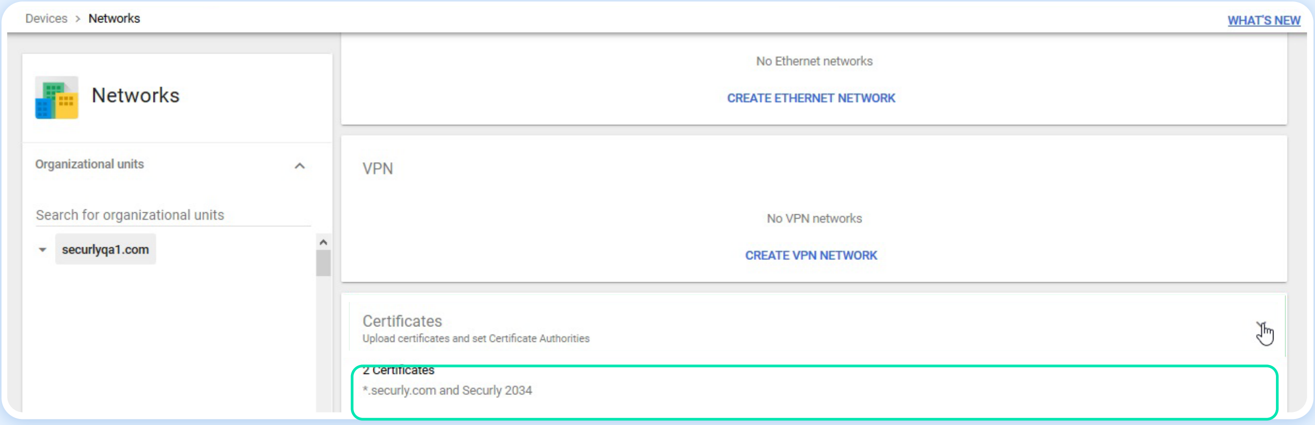
Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log

Securly Chrome extension & SSL certificate

Installing the Securly SSL certificate

You should install the Securly SSL certificate to ensure the best browsing experience and prevent errors on sites that Securly decrypts. The certificate does not control the level of filtering or what sites are allowed. Without the certificate, sites like Google.com and Facebook.com will show privacy errors, users will perceive this as the internet being **"broken"**.

Download the SSL certificate. Or you could also ask a Securly sales engineering or support executive. Then simply navigate to **Devices** > **Chrome Devices** and select **Networks** from the Device dropdown. Scroll down to **Certificates** and select **Add Certificates**. For details and latest Securly SSL certificate click **here**.


Devices > Networks

WHAT'S NEW

Networks

Organizational units

Search for organizational units

securlyqa1.com

No Ethernet networks

CREATE ETHERNET NETWORK

VPN

No VPN networks

CREATE VPN NETWORK

Certificates

Upload certificates and set Certificate Authorities

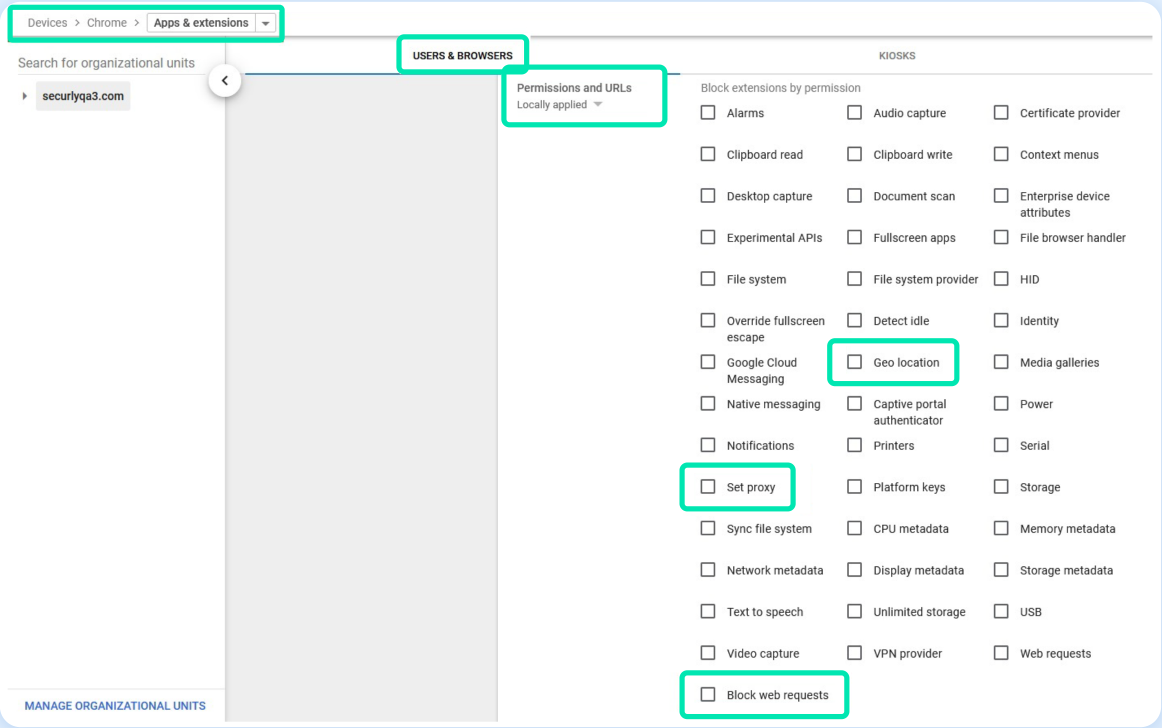
2 Certificates

*.securly.com and Securly 2034

Installing the Securly Chrome Extension

The Securly Chrome extension can be installed from your **Google Admin Console.** The 5-minute installation process will push the extension to all Chromebooks belonging to the OU selected. Before starting the installation process, ensure that your school **domain/subdomains** are registered with Securly.

To ensure that the Securly extension loads seamlessly you would need to watch out for the **'Block Extensions by Permission'** field under Apps & Extensions. Make sure that the checkboxes for **'Geolocation'**, **'Web Requests'**, and **'Set Proxy'** are unchecked.



Devices > Chrome > Apps & extensions

USERS & BROWSERS | KIOSKS

Search for organizational units

securlyqa3.com

Permissions and URLs
Locally applied

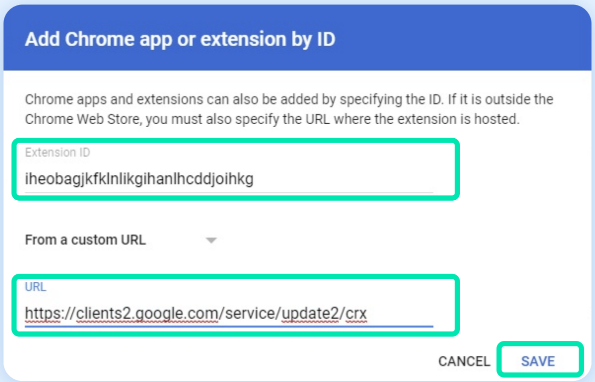
Block extensions by permission

□ Alarms □ Audio capture □ Certificate provider
□ Clipboard read □ Clipboard write □ Context menus
□ Desktop capture □ Document scan □ Enterprise device attributes
□ Experimental APIs □ Fullscreen apps □ File browser handler
□ File system □ File system provider □ HID
□ Override fullscreen escape □ Detect idle □ Identity
□ Google Cloud Messaging □ Geo location □ Media galleries
□ Native messaging □ Captive portal authenticator □ Power
□ Notifications □ Printers □ Serial
□ Set proxy □ Platform keys □ Storage
□ Sync file system □ CPU metadata □ Memory metadata
□ Network metadata □ Display metadata □ Storage metadata
□ Text to speech □ Unlimited storage □ USB
□ Video capture □ VPN provider □ Web requests
□ Block web requests

MANAGE ORGANIZATIONAL UNITS

Input your ID and URL with the details below and click "Save".

1. Extension ID: iheobagjkfklnlikgihanlhcddjoihkg
2. URL: https://clients2.google.com/service/update2/crx



Add Chrome app or extension by ID

Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.

Extension ID
iheobagjkfklnlikgihanlhcddjoihkg

From a custom URL

URL
https://clients2.google.com/service/update2/crx

CANCEL SAVE

Conclusion

Following the best practices outlined in this guide will help you manage Chromebooks effectively and ensure online student safety for your 1:1 program.

Securly is committed to providing schools with all the tools required to protect students from harmful content online on any device, anywhere they connect.

Please contact a Securly sales representative for more information.

securly

✉ sales@securly.com

☎ 1-855-SECURLY

🌐 www.securly.com