MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Cyber Security in Schools

New Zealand Government

Presenters

Danielle Vandendungen
Security Advisor – Ministry of Education

Steve Smith / Jared Mayer
Education Advisors – Google

REC Please note this session is being recorded.

Please have your microphone on mute.

Use the chat function to record questions.

Use the raise hand function to ask questions.

Today's agenda

1. Cyber Security in Schools programme
2. The Security Sessions
3. Episode Four – Device Management
    - Management options
    - Recommended technical settings
    - Questions

Cyber security in schools

The Ministry has created a new team – Cyber Security in Schools - to empower schools to improve their cyber security. We'll do that through a mix of best practice advice, templates, and services.

At present we're focused on some key areas including:

- Backups
- Email filtering
- Cyber insurance
- Education and awareness raising

Get in touch with the Cyber Security in Schools team:

Subscribe to our newsletter
https://bit.ly/DigitalDownloadNZ

Send us an email with any questions (big or small)
cyber.security@education.govt.nz

Previous training videos will be available on our website:
www.education.govt.nz/cyber-security-in-schools-training/

The Security Sessions

These webinars are designed help you to improve your cyber security and reduce your IT admin overhead.

We're working in collaboration with Google and Microsoft to help you configure your domain to protect against threats.

The settings we're recommending today aren't compulsory; **they’re best practice advice recommended by the Ministry.**

The Security Sessions - Episodes

1. Identity and Authentication - If you missed it, find a recording here
2. File Management and Storage - Recording, Slidedeck
3. Mail, Calendar and Contacts - Recording, Slidedeck
4. **Device Management - Today**
5. Administration, Reporting and Applications

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Episode Four:

Device Management

New Zealand Government

Device Management

Google's mission is to maximize user productivity while keeping data secure.

More than
110 million
30DA devices under management*

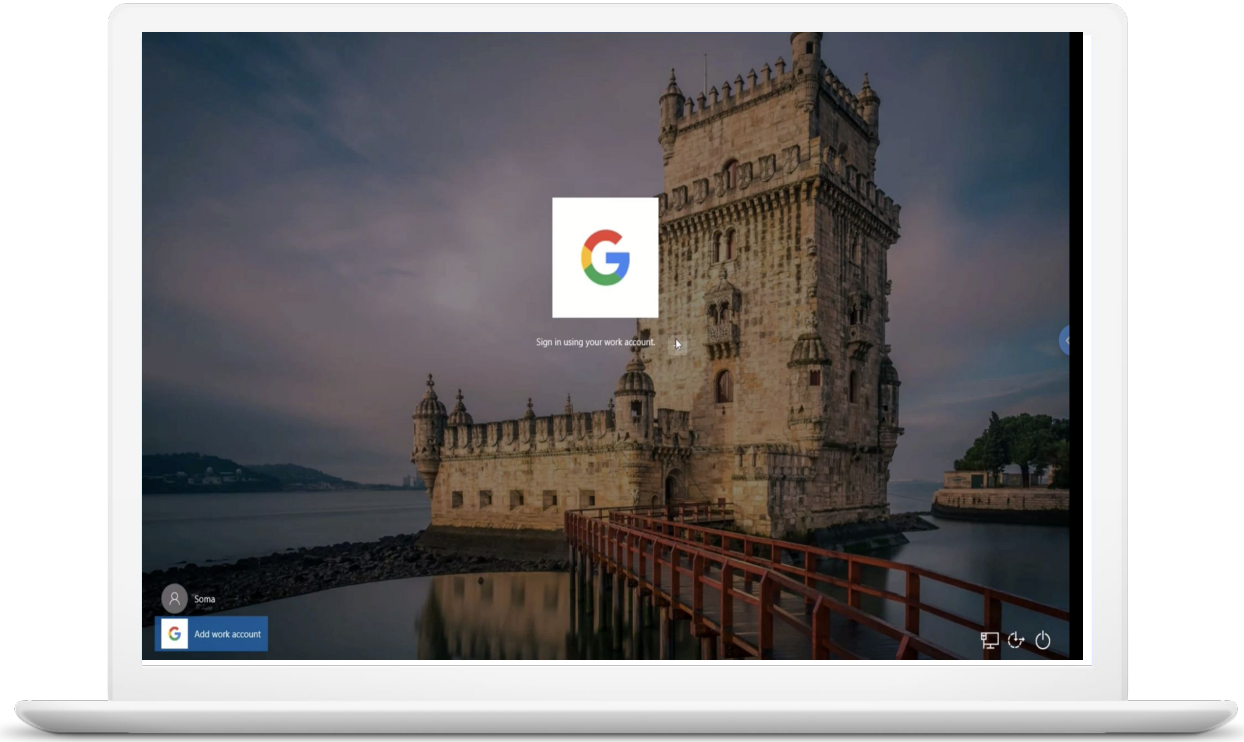
Helping to keep your data **secure** with easy to set-up management for:

- Chrome OS
- Android
- iOS
- Desktops

*As of 04/22/2020; includes devices that are licensed through Google Workplace, Cloud Identity, and Chrome Enterprise

Enhanced Desktop Security for Windows

- Add an extra layer of security for Windows 10 devices that access Google Workspace
- Use existing Google account credentials to login to Windows 10 devices and easily access apps and services with SSO
- Protect user accounts with anti-hijacking, and suspicious login detection technologies
- Ensure that all Windows 10 devices used to access Google Workspace are updated, secure, and within compliance



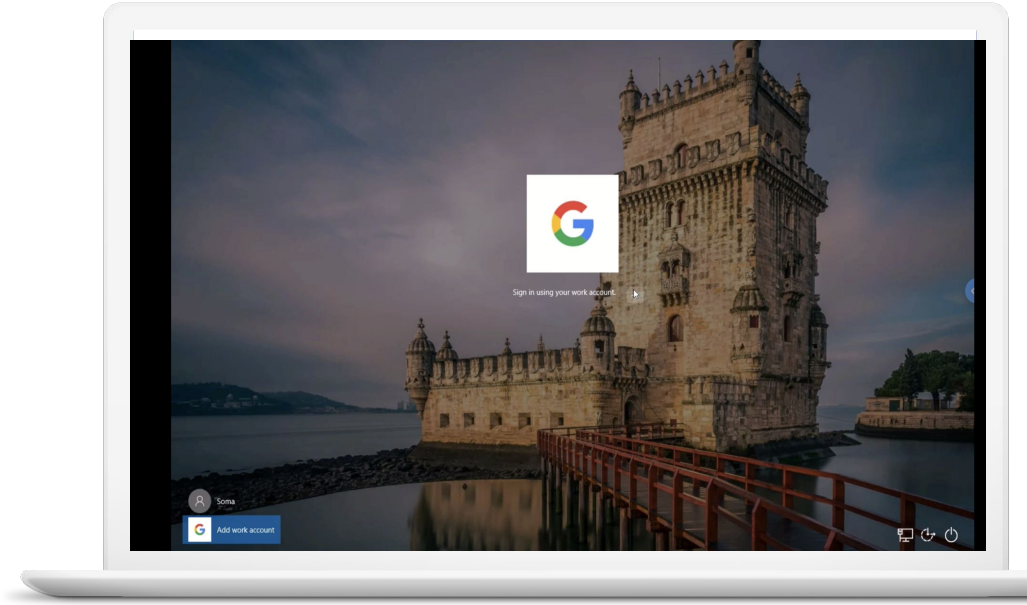
Enhanced Desktop Security for Windows
Key Components

- Google Credentials Provider for Windows (GCPW)
- Windows device management*

*Requires Education Plus

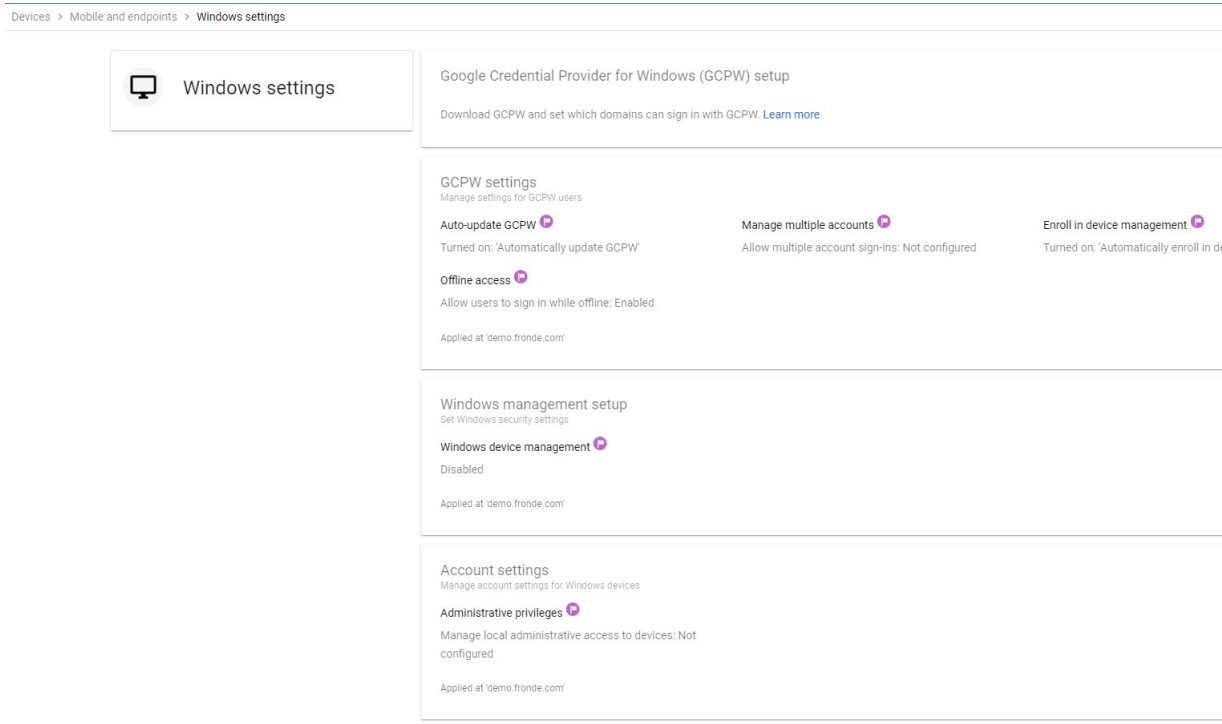
Enhanced Desktop Security for Windows
Google Credentials Provider for Windows

- Log into Windows 10 devices using Google credentials
- Seamless SSO experience
  - Web-based Google services
  - Thousands of 3P apps (SAML, OIDC, Password Vaulted apps)
  - Desktop Google apps (e.g., Meet, Drive FileStream)
- Synchronizes Google password with Active Directory / local Windows profiles
- Auto-enrolls the current device in Windows device management



Enhanced Desktop Security for Windows
Windows Device Management

- Enforce Windows settings
  - Pushing windows settings. E.g., Windows updates, account settings, device encryption
  - Apply custom settings
- Inventory Management
  - Managing the Windows 10 device inventory
  - Admin actions (Wipe device, unenroll device, remote sign out)
- Audit & Device logs

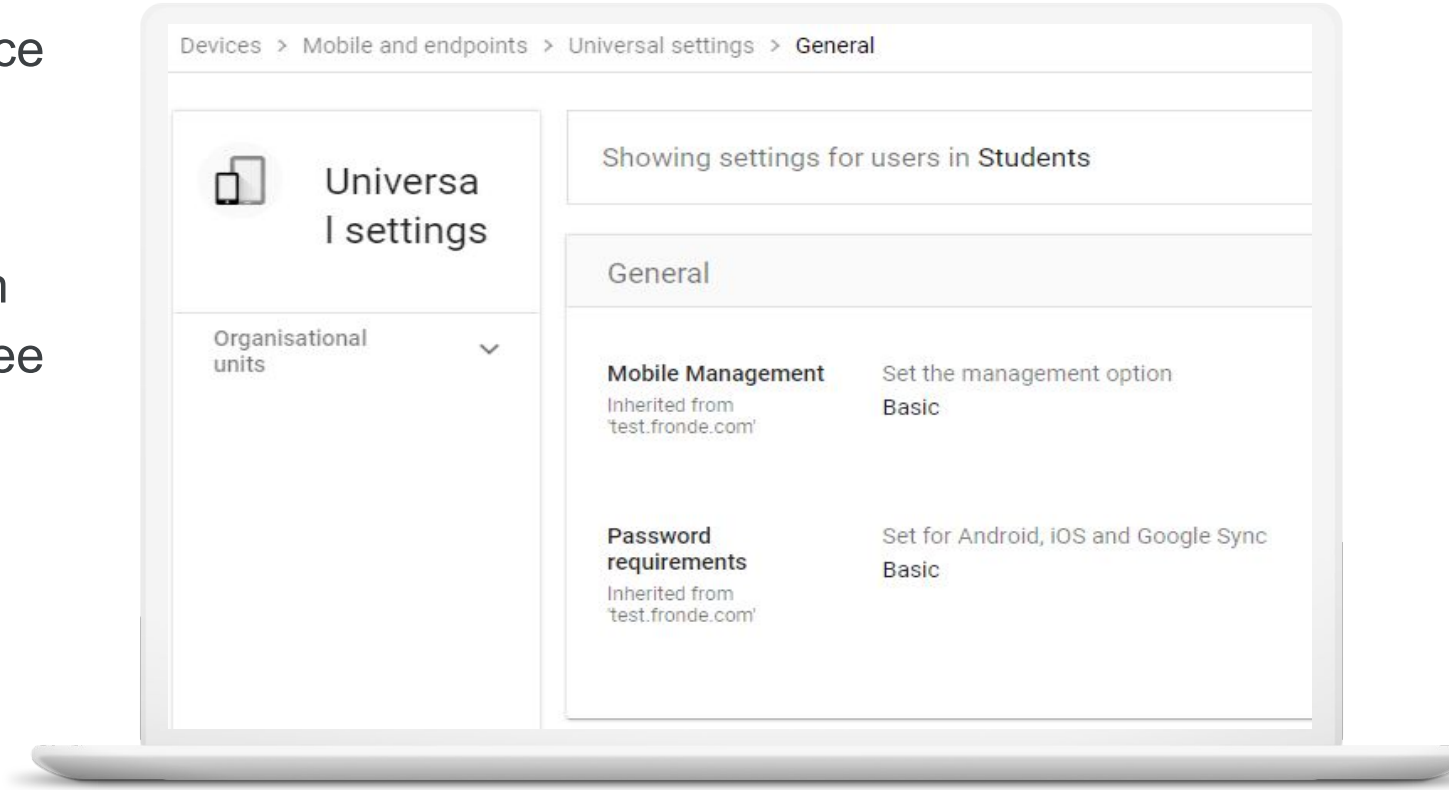


Mobile Management
Basic Management

Use basic mobile management to enforce passwords on devices and keep your school's data safe.

You can also wipe corporate information from lost or stolen devices or you can see which devices are accessing your school's data.

Basic management is now enabled by default to 100% of devices and it's agentless management.

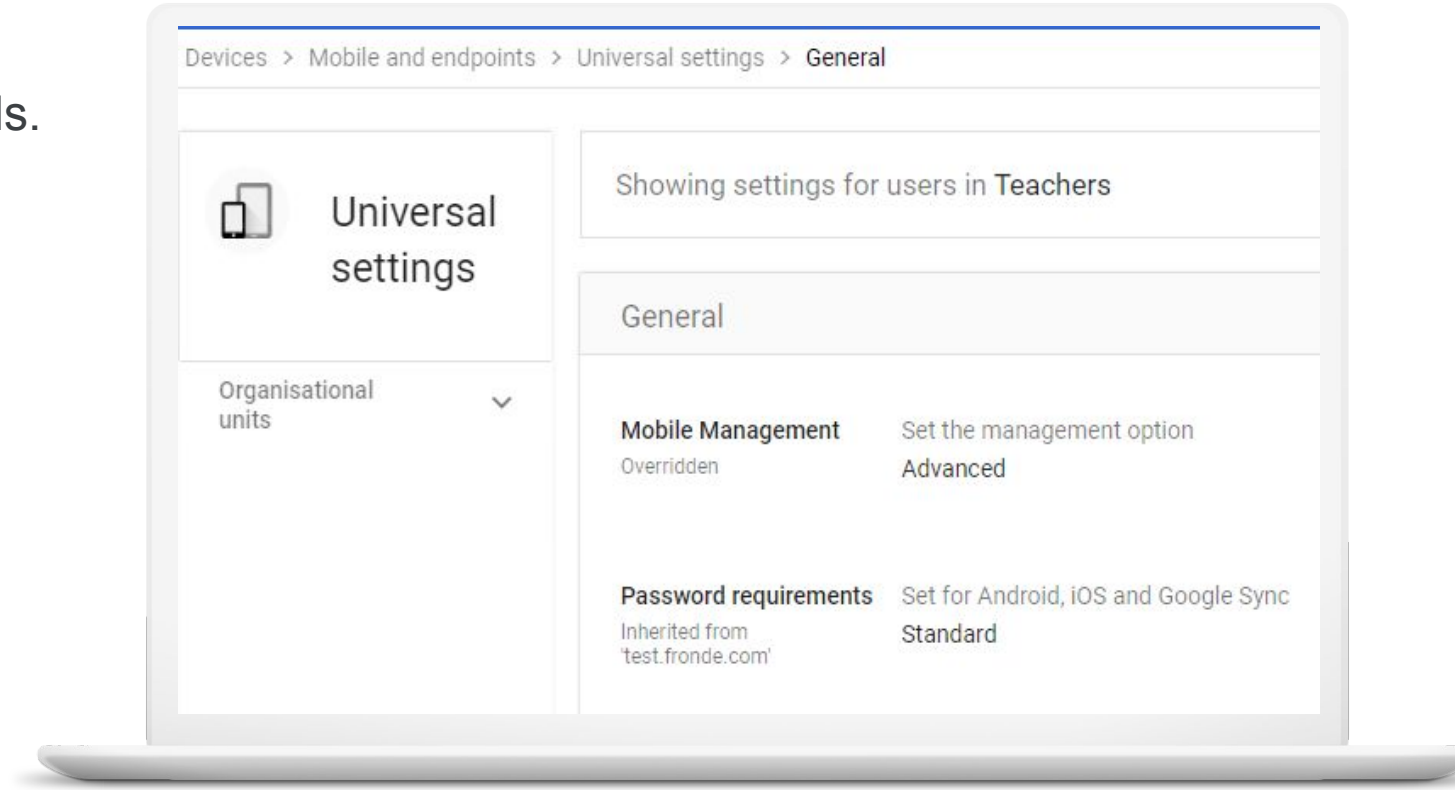


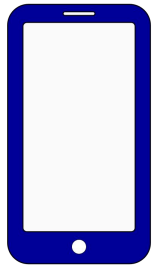
Mobile Management
Advance Management

Use advanced management for more control over device policies and passwords.

Advanced app management or for the ability to wipe all data from devices.

An app needs to be installed on each managed device to be able to enforce the policies.





Recommended Technical Settings

Advanced Mobile Management

Area	Setting	Ref	Best Practice Recommendation
Universal Settings	Allow sync on Android devices	HC	Enable
	Allow sync on iOS devices		Enable
	Allow sync via ActiveSync	HC	Disable
	Require device encryption	HC	Enable
	Block compromised devices	HC	Enable
Password policies	Password Policy	HC	Standard or Strong
	Wipe device after failed attempts		~7 attempts
Android Settings	Block apps from unknown sources		Enable

ChromeOS Management

400+ policies available to be configured on devices to enhance the user experience, and enforce security controls.

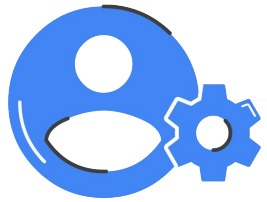
User Based Policies

- Does not matter where the user has logged in eg input tools for macrons eg for the word ākonga

Device Based Policies

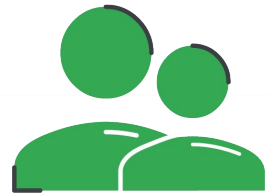
- Apply to managed/enrolled devices only eg off hours, USB blocking

Managed access puts admins in control



Login controls stop end users from logging into Chromebooks with unauthorized accounts.

Site blocking prohibits access to social media platforms or unmonitored content.



Managed guest sessions enable shared, identity-free sessions in libraries and other shared environments.

Google for Education

Advanced security keeps your data safe

Persistent enrollment ensures devices are always enrolled to your domain.

Lost and stolen protections prevent data theft by remotely disabling devices.

Kiosk mode keeps high-stakes testing data safe.

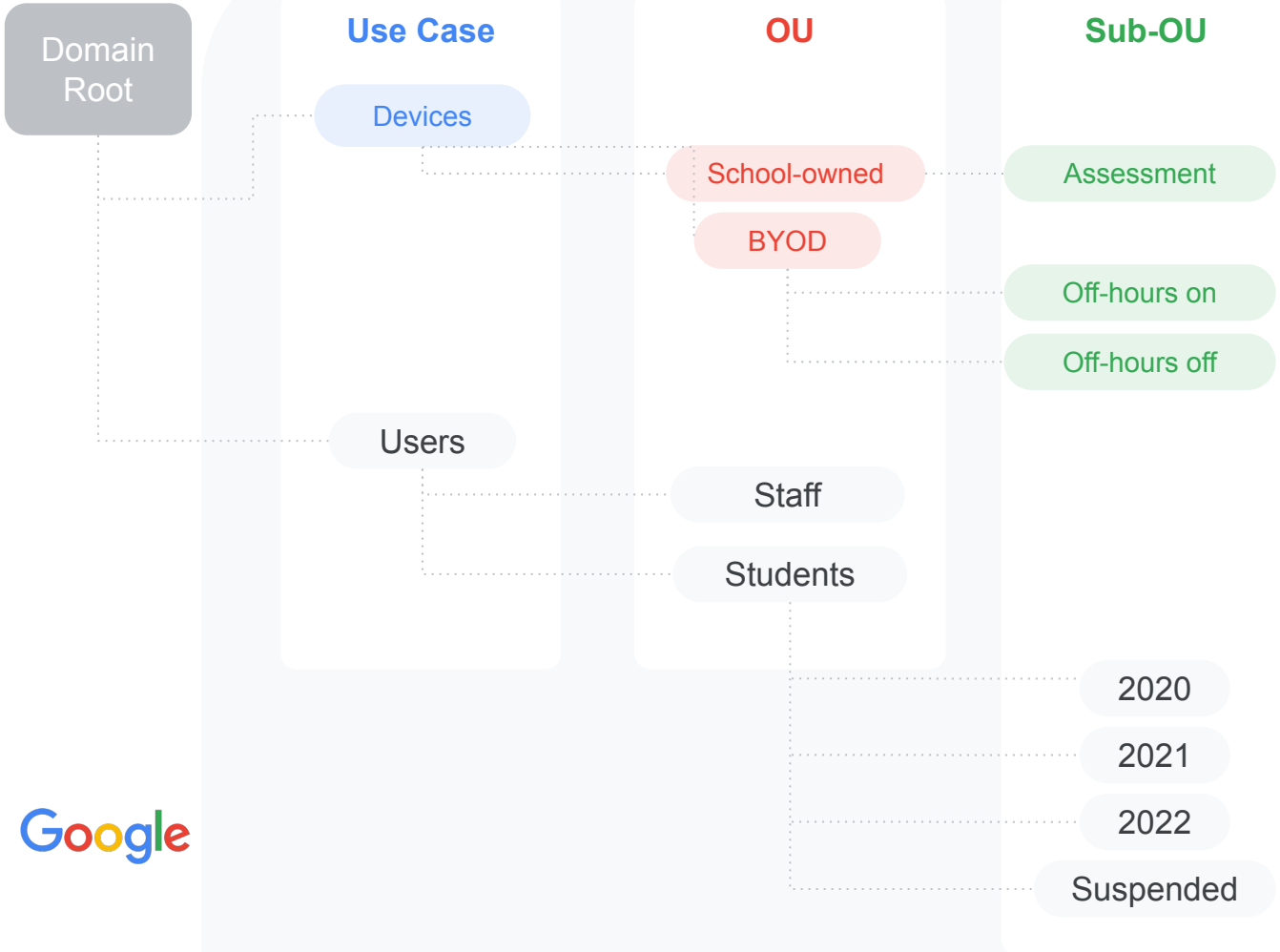
Locked mode prevents students from navigating away from a test until it’s done.

Ephemeral mode ensures user data is wiped upon log out.

Application verified access allows third-party apps to understand Chrome devices and provide a service.

Google for Education

Recommended Organizational Unit (OU) structure



This is an example of how you could set up OUs for devices in your school. Different OUs can have different settings, so devices can be sorted into OUs depending on what settings they need.

Note: This shows how schools may want to structure their OUs in a BYOD environment, utilising the off-hour sign-in settings. For schools wanting to create a secure testing environment, you may want to create a Sub-OU called 'Assessment'.

Google

User settings

Create a custom, school-wide experience on each and every device, no matter who signs in.

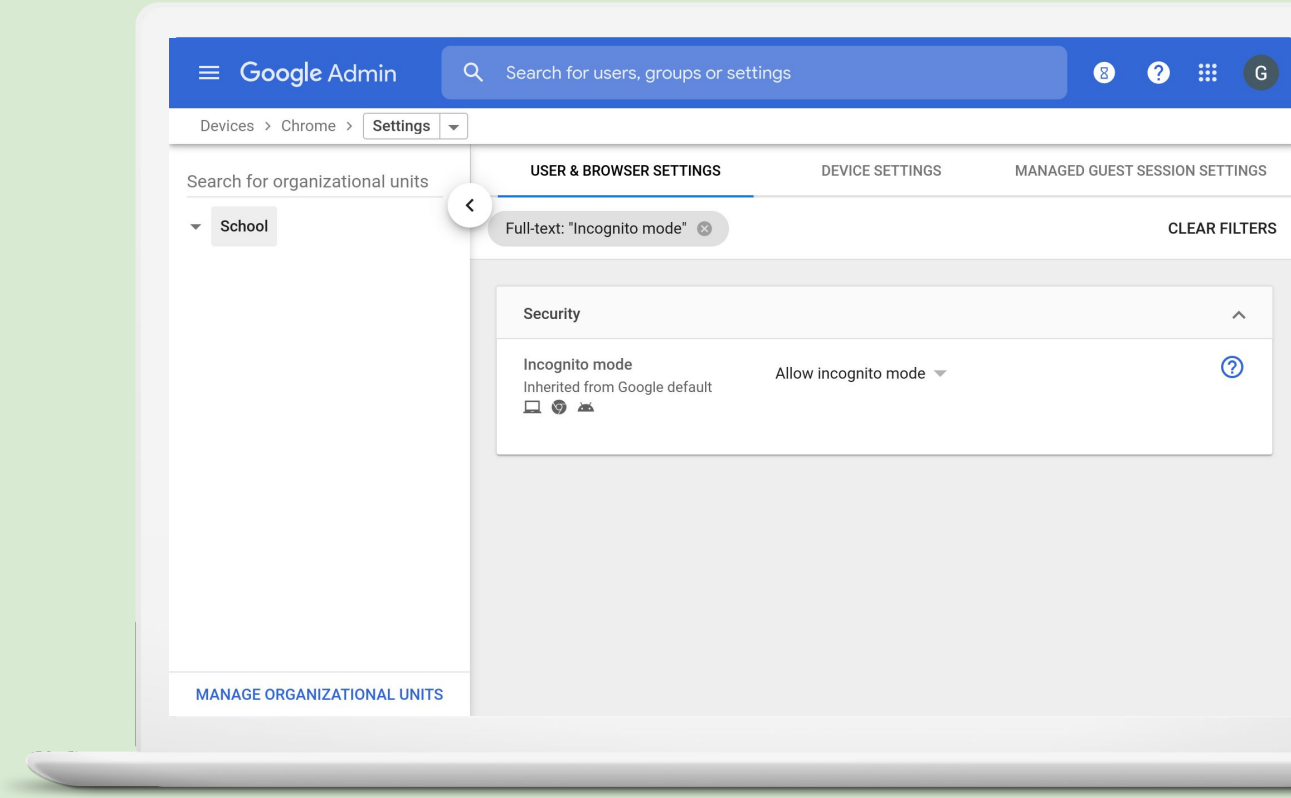
User settings help maintain control over who can sign in on your Chromebooks. For example, you can create a policy that only allows users within your domain to sign in.

User settings

Incognito Mode and Browser History

Admins can select to ‘Disallow Incognito Mode’ to prevent users from opening new incognito windows. Browser History can be toggled on or off so teachers can view what sites students have visited.

Recommendation: Disallow Incognito Mode

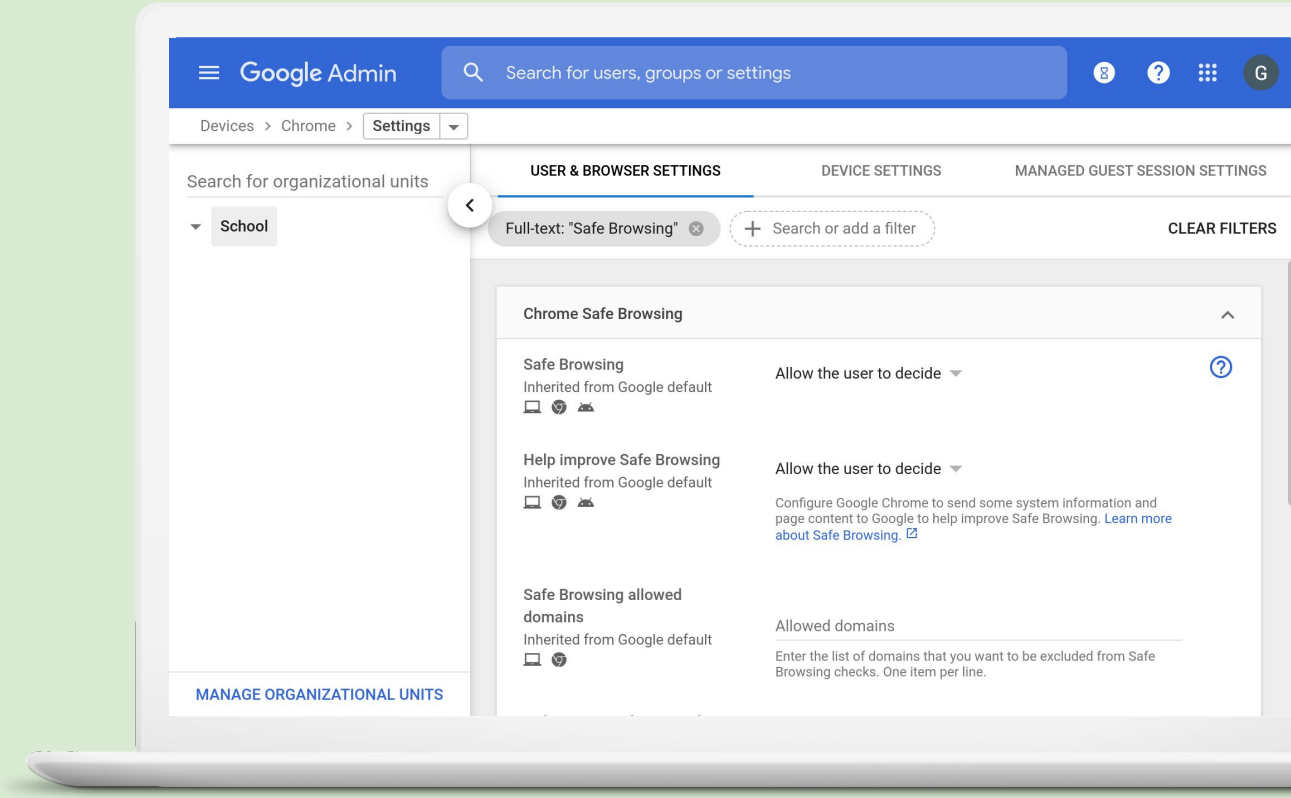


User settings

Safe Browsing

Safe Browsing in Chrome helps protect users from websites that may contain malware or phishing content. The default setting allows users to decide whether to use Safe Browsing or not.

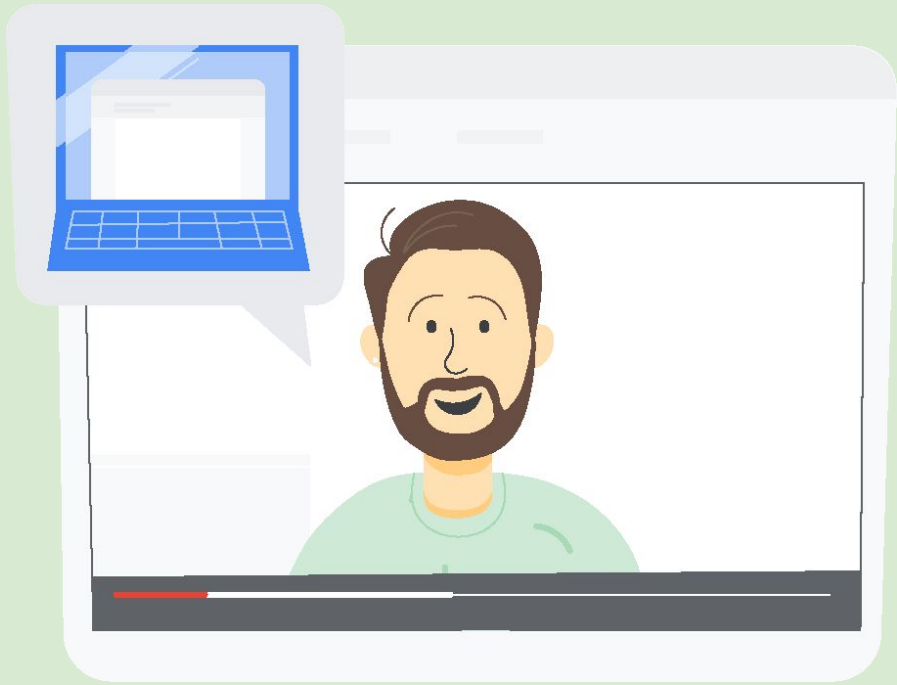
Recommendation: Enforce



User settings

Safe Search and YouTube Restricted Mode

Activate Google Safe Search for web search queries and Restricted Mode for YouTube to make sure the content students are exposed to is appropriate and safe.

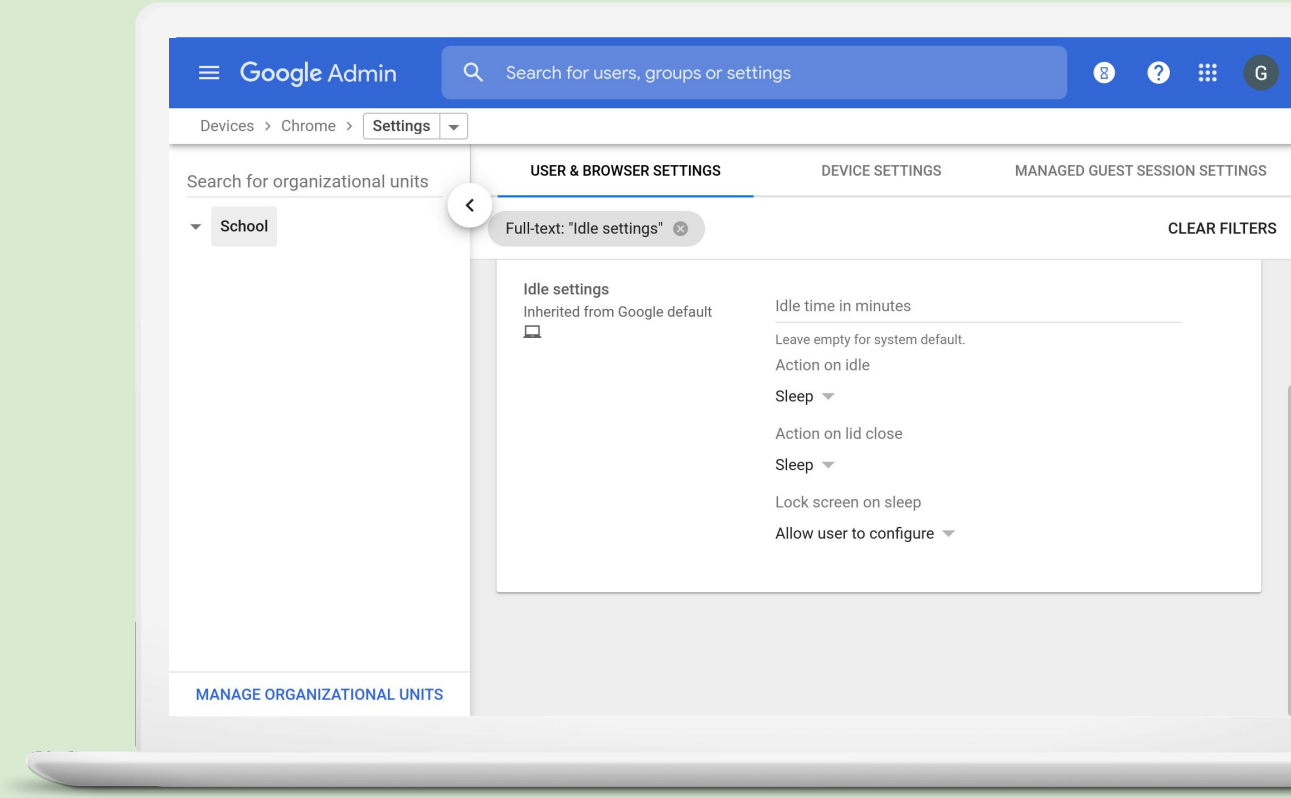


User settings

Idle settings

Specify the amount of idle time before a user's device goes to sleep or signs them out.

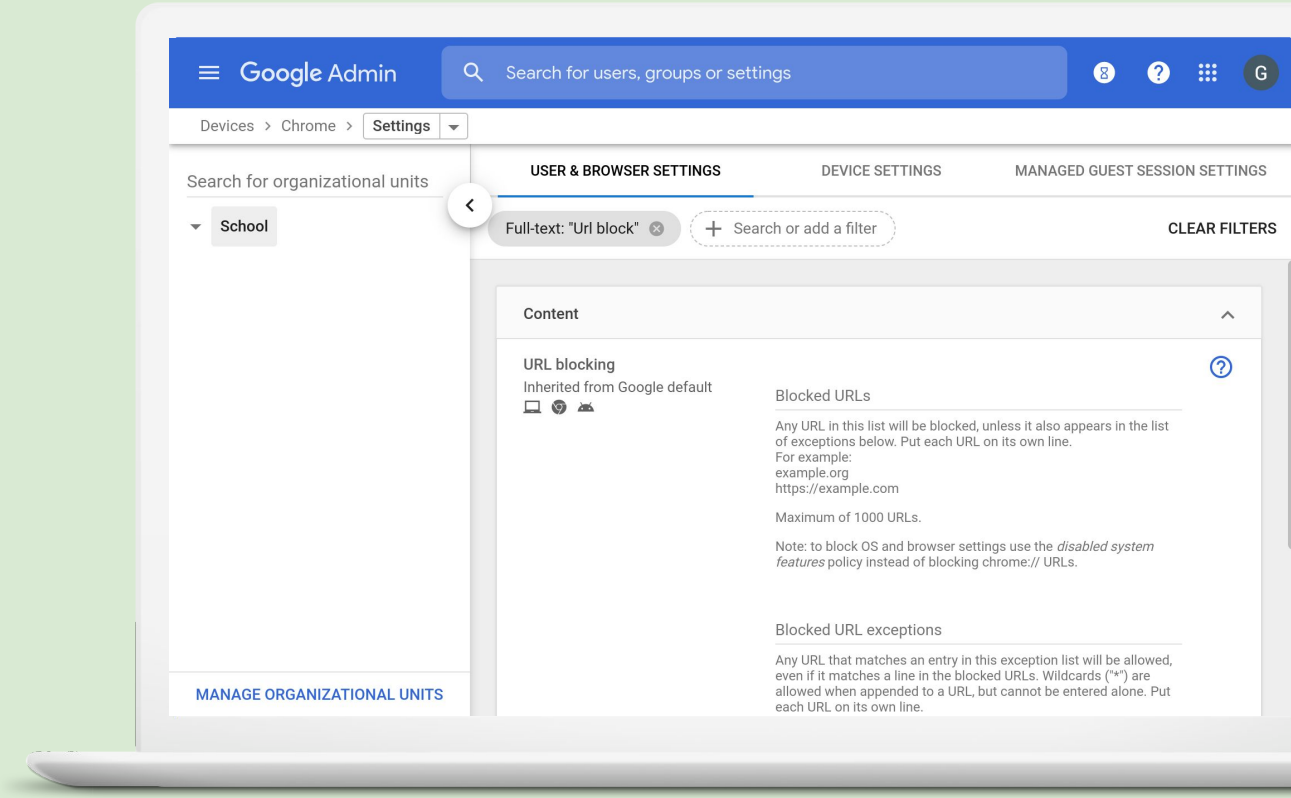
Recommended: 10mins



User settings

URL blocking

Create a deny list that prevents Chrome users from accessing specific URLs.



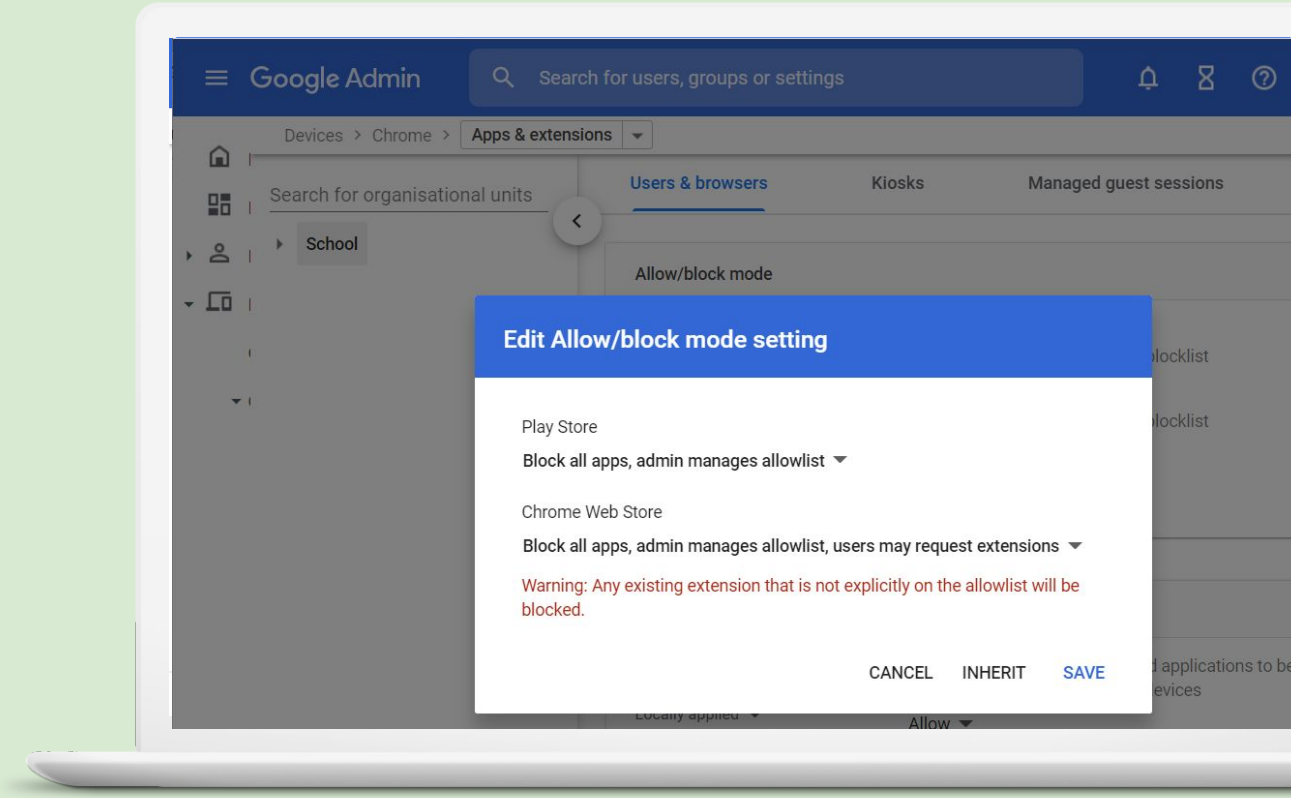
User settings

Apps & Extension Management

Adjust the Allow/Block Mode to enable administrators to control an allow list, and end users to request access to specific extensions.

Ensure extensions are suitable for students.

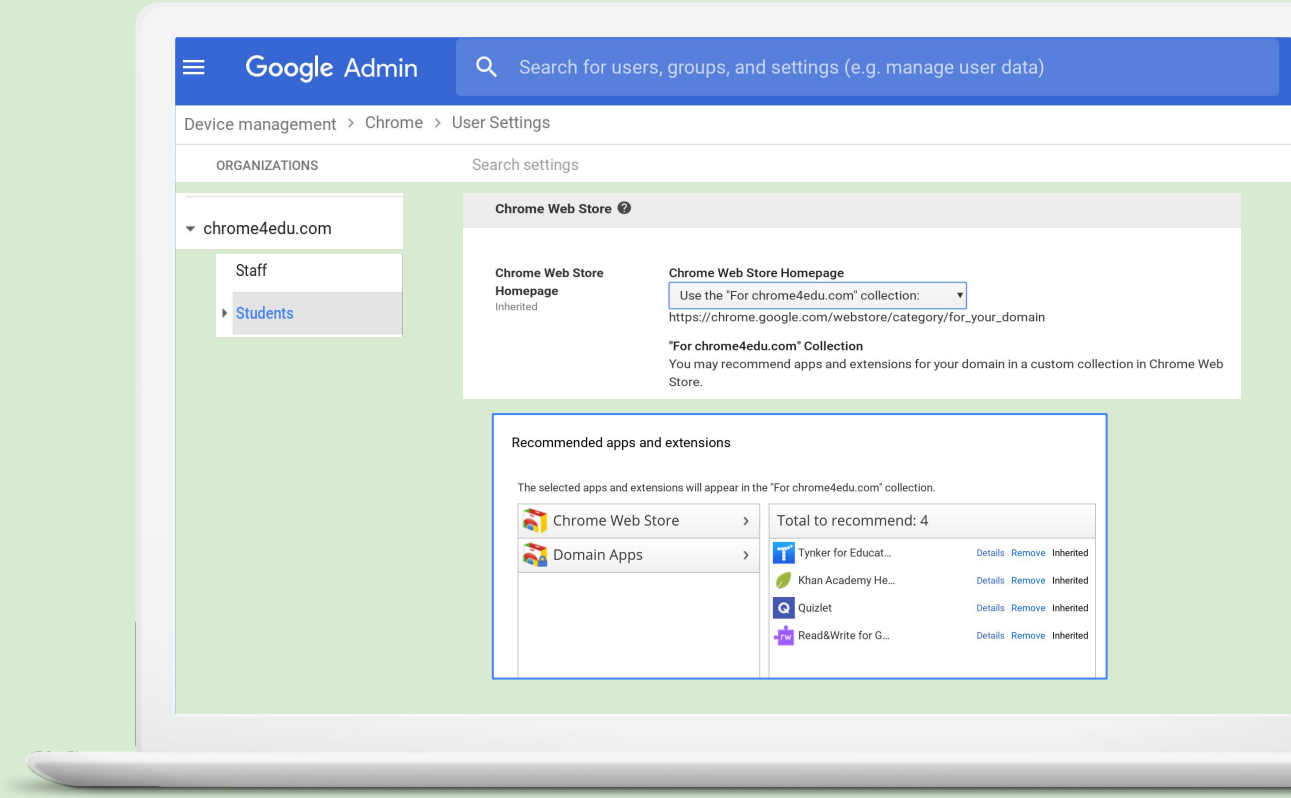
As a Chrome Enterprise admin, you can use your Admin console to set policies for a specific web app, Chrome app or extension, or supported Android app. For example, you might force-install an app and pin it to users' Chrome taskbar.



Chrome Web Store

You can change the Chrome Web Store Homepage to a custom homepage for your users when they're signed in.

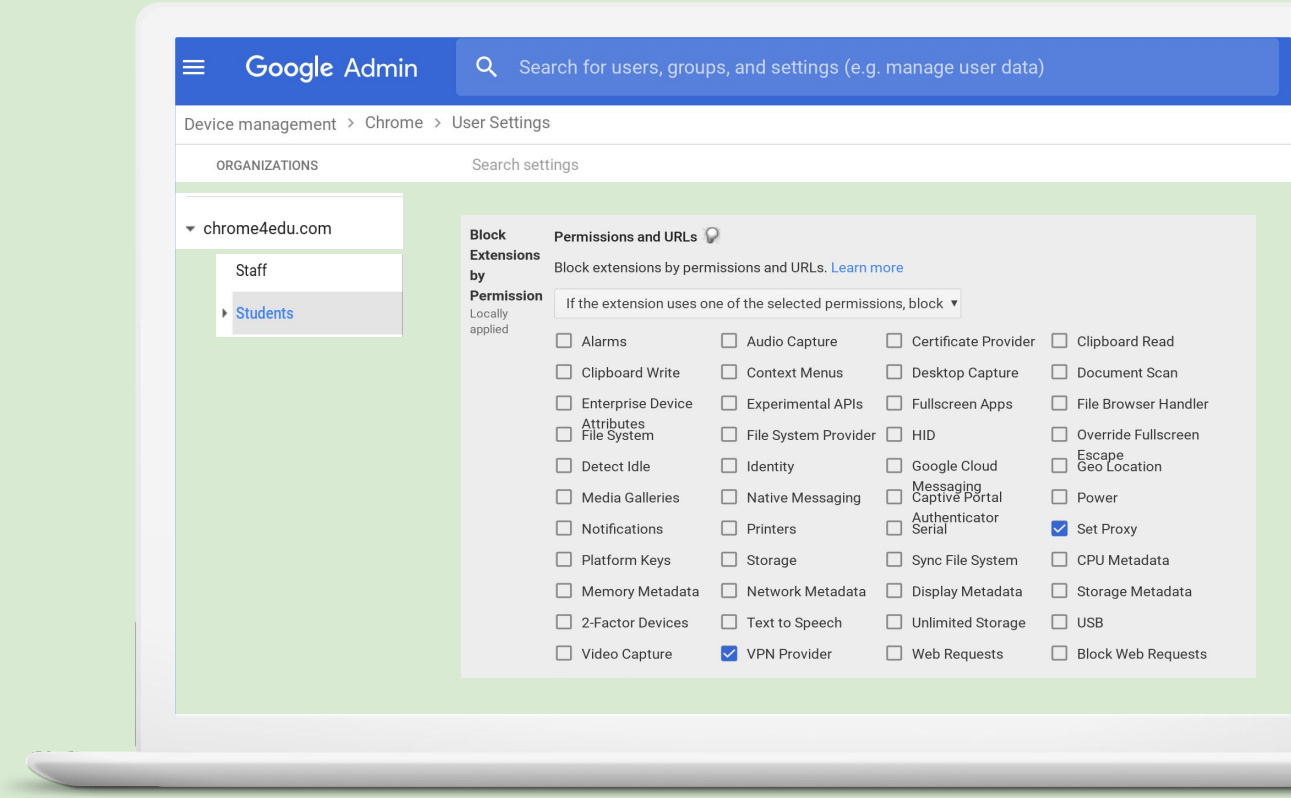
Recommend apps and extensions for your domain in a custom collection named after your domain in the Chrome Web Store.



Block extensions by permission

Prevent users from running extensions that request certain permissions that your organization doesn't allow.

Select whether to allow or block apps that request specific permissions. Check the permissions to allow or block.

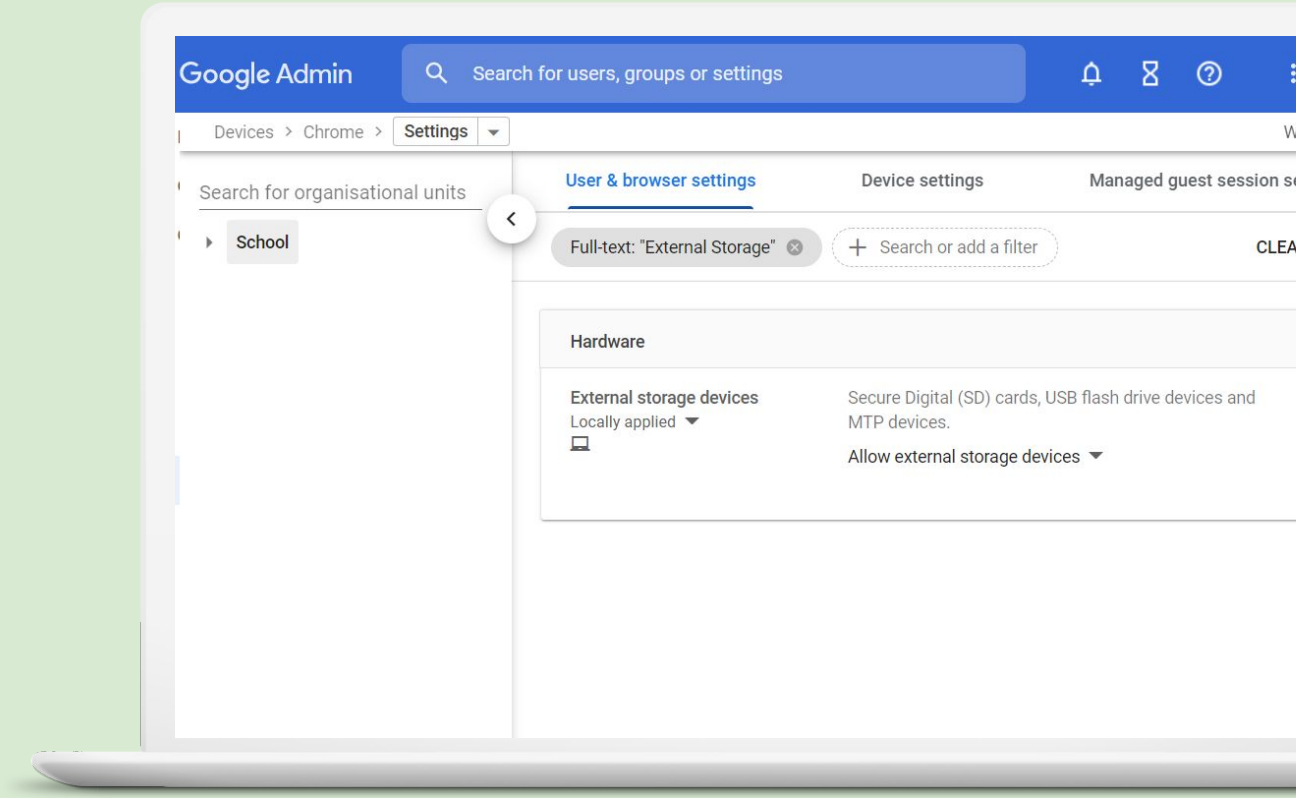


User settings

External Storage

Block the ability to utilise USB external storage devices on Chrome devices.

Limit non-auditable data sharing, file sharing and data leakage.

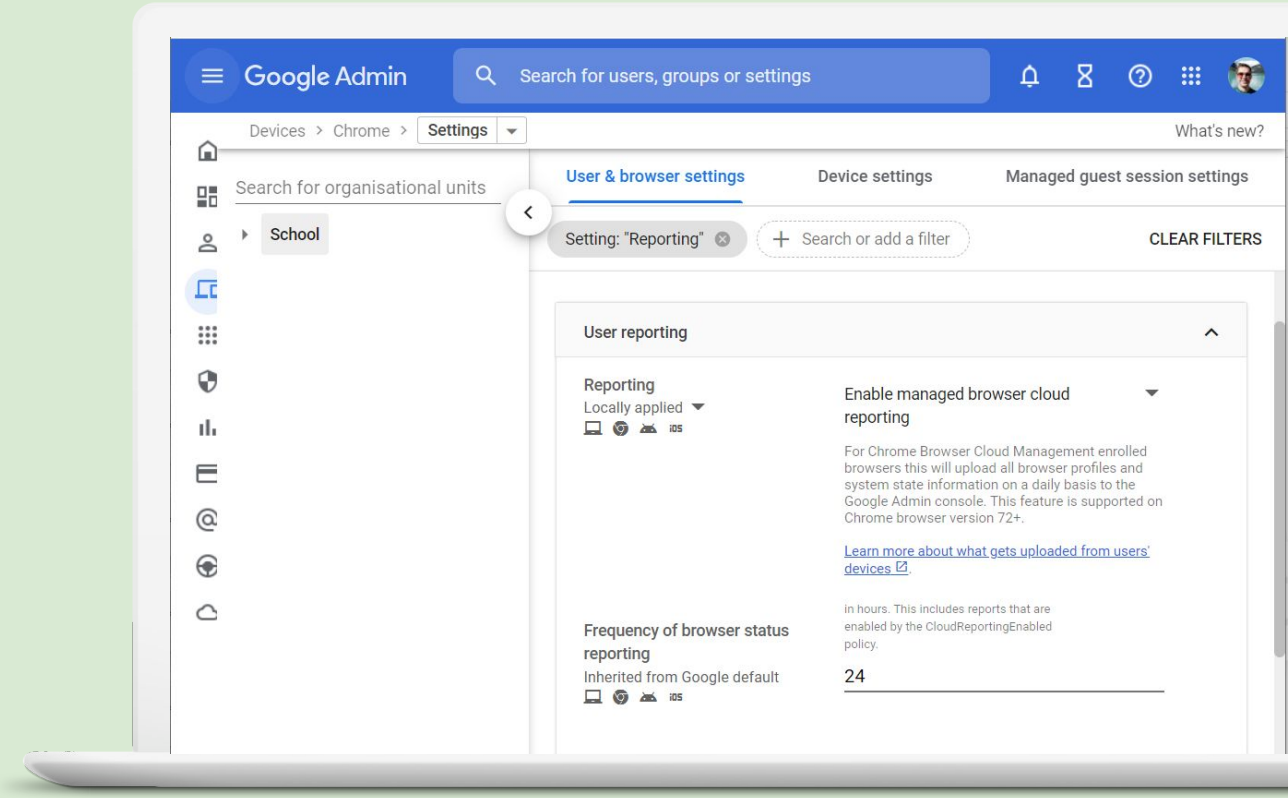


User settings

Reporting

Enable managed browser cloud reporting to receive additional device and user reports within the Admin Console

- Chrome Version
- Stable / Beta Channel
- Profiles present
- Extensions installed
- Device information
- Other policies configured



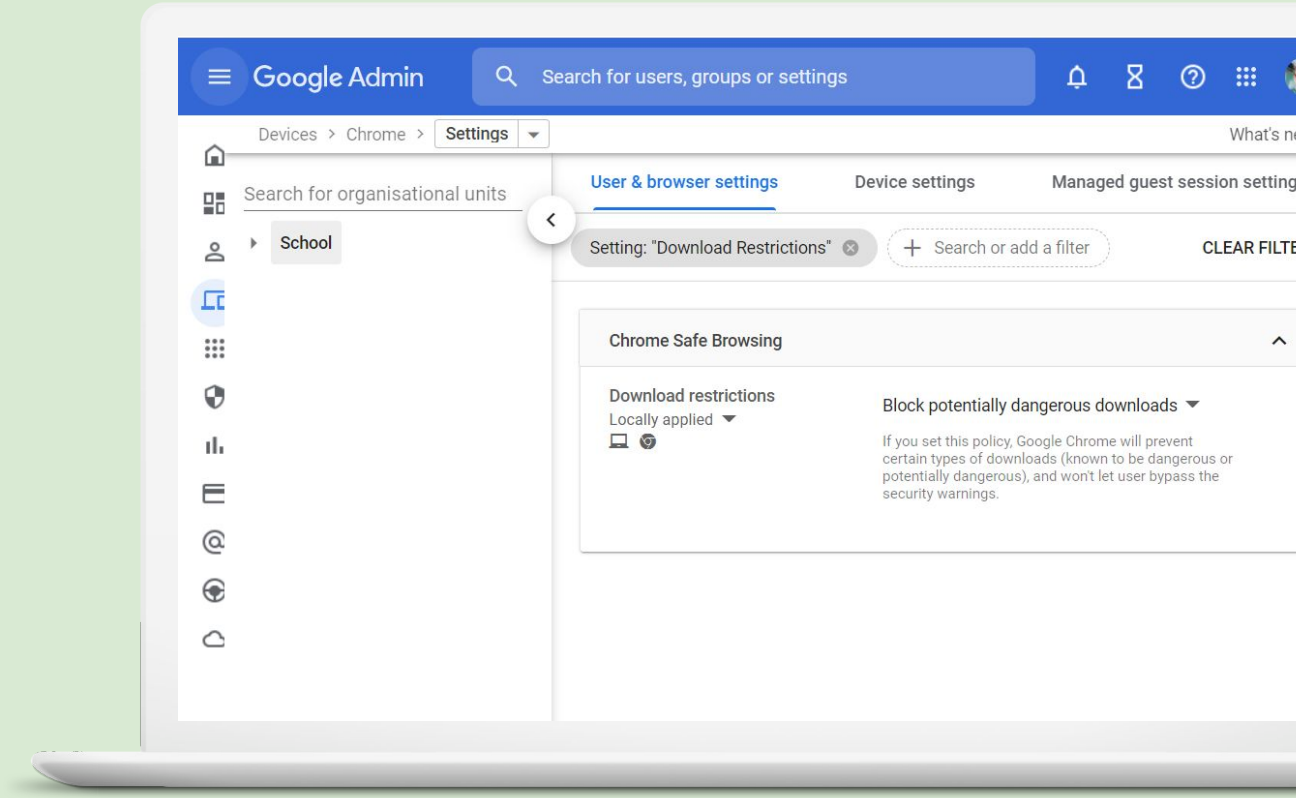
User settings

Download Restrictions

Prevents users from downloading dangerous files, such as malware or infected files. You can prevent users from downloading all files or those that Google Safe Browsing identifies as dangerous. If users try downloading dangerous files, Safe Browsing shows them a security warning.

Number of options available:

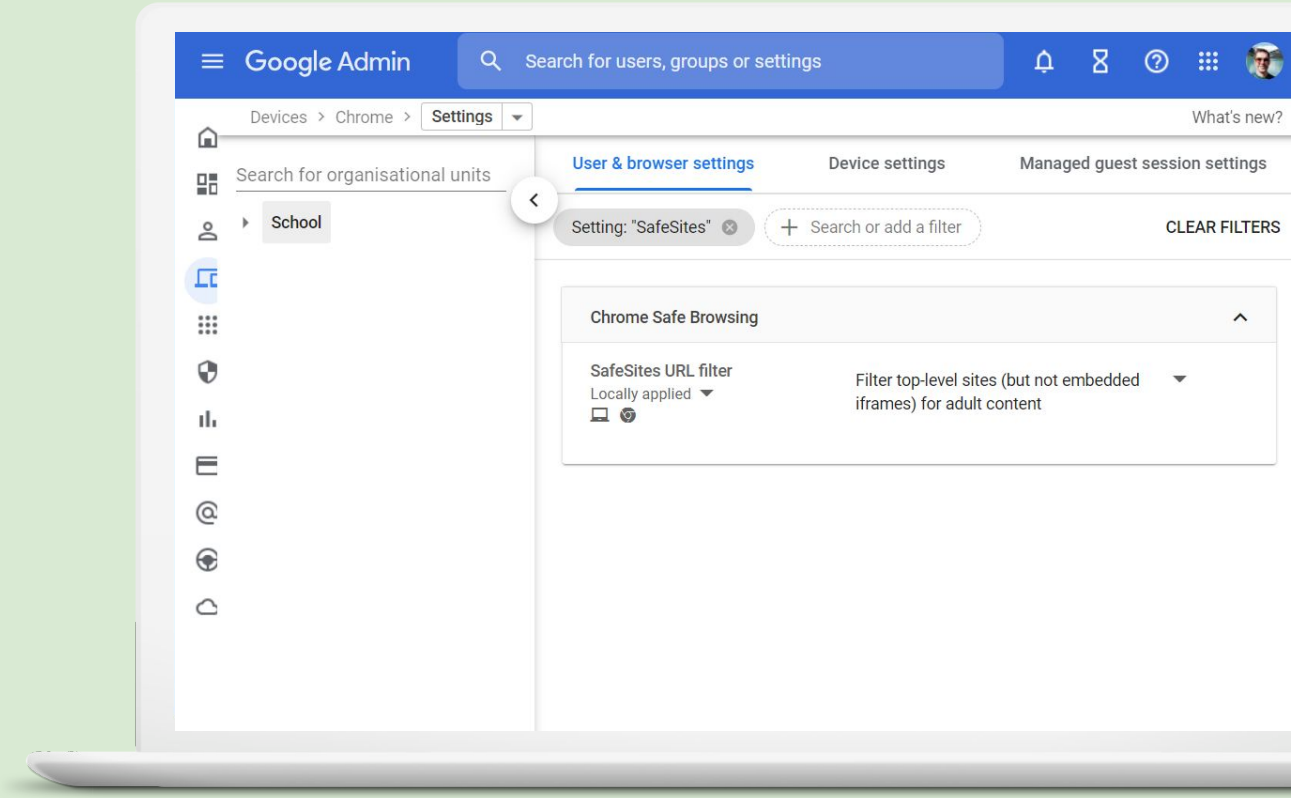
- Block all downloads
- Block all malicious downloads
- Block dangerous downloads
- Block potentially dangerous downloads



User settings

Safe Sites URL Filter

Allows you to turn on or off the SafeSites URL filter. This filter uses the Google Safe Search API to classify URLs as pornographic or not.

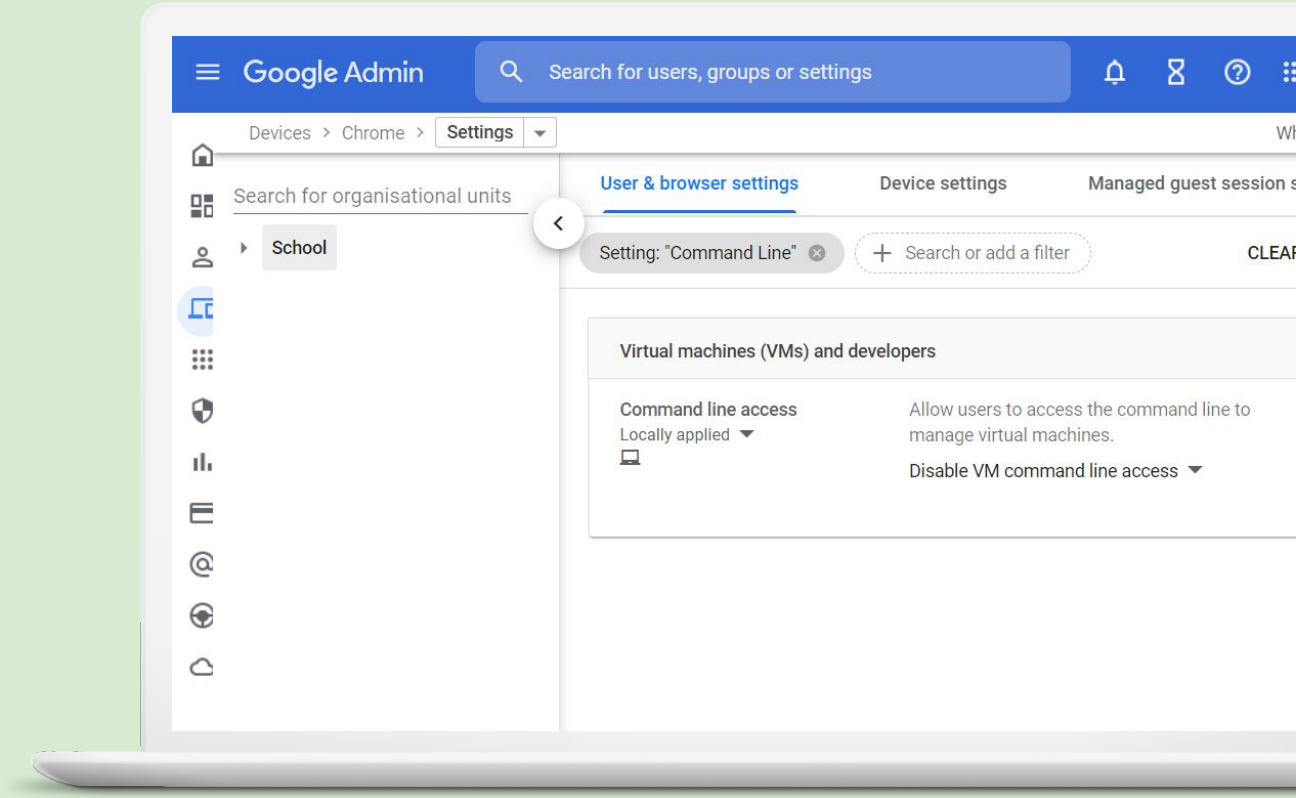


User settings

Command Line Access

Disable that users can access the command line (CLI) to manage virtual machines (VMs).

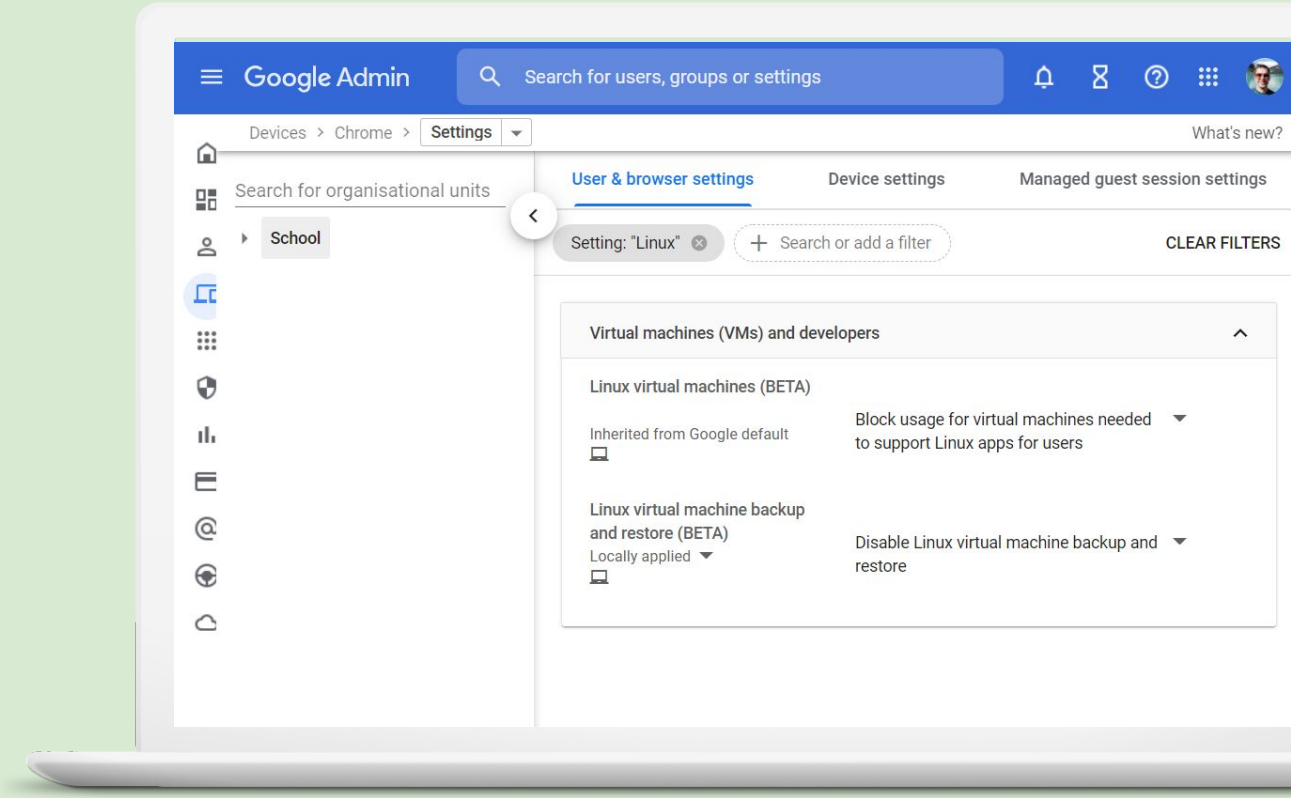
If the policy is enabled, the user can use virtual machine management CLI.



User settings

Linux Virtual Machines

Allows you to control whether users can use virtual machines to support Linux apps. The setting is applied to starting new Linux containers, not to those already running.



Device settings

Device Settings

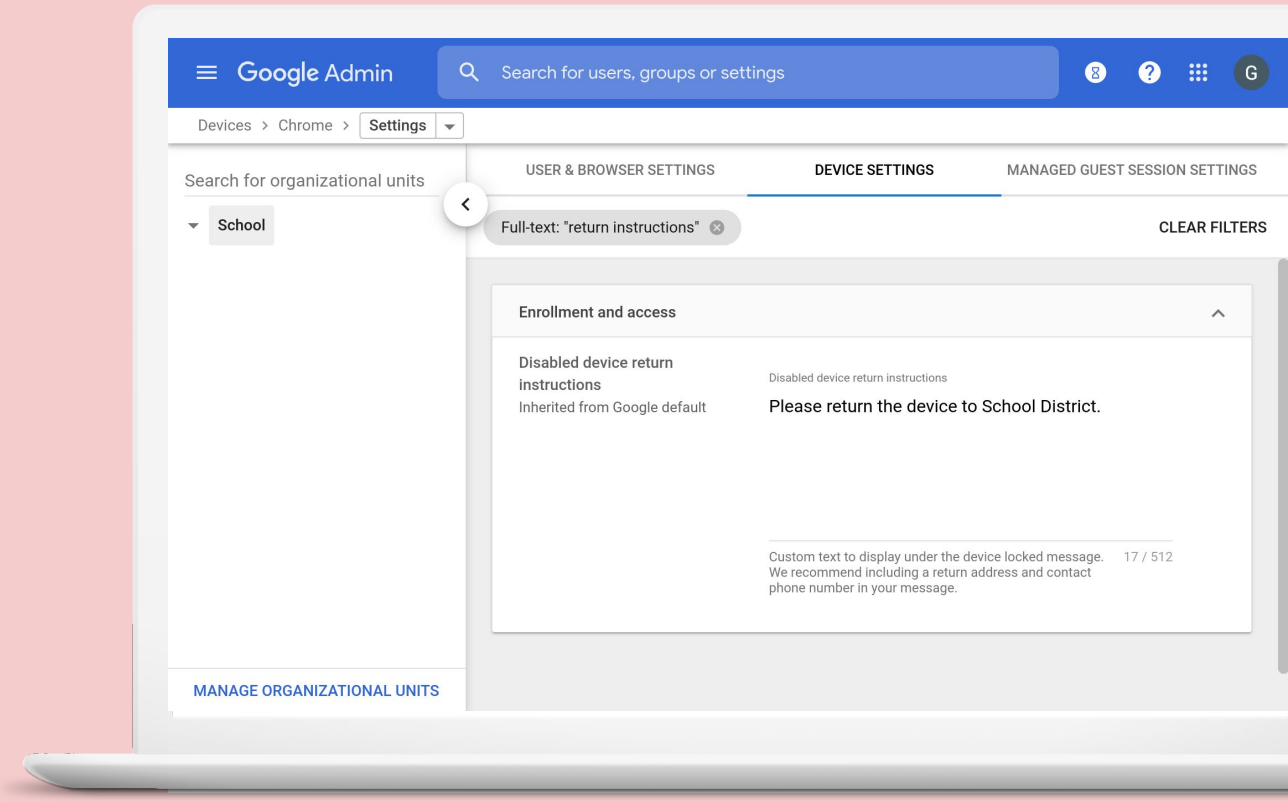
Create a custom, school-wide experience on each and every device, **no matter who signs in**.

Device settings help maintain control over **who can sign in** on your Chromebooks. For example, you can create a policy that only allows users within your domain to sign in.

Device settings

Disabled device return instructions

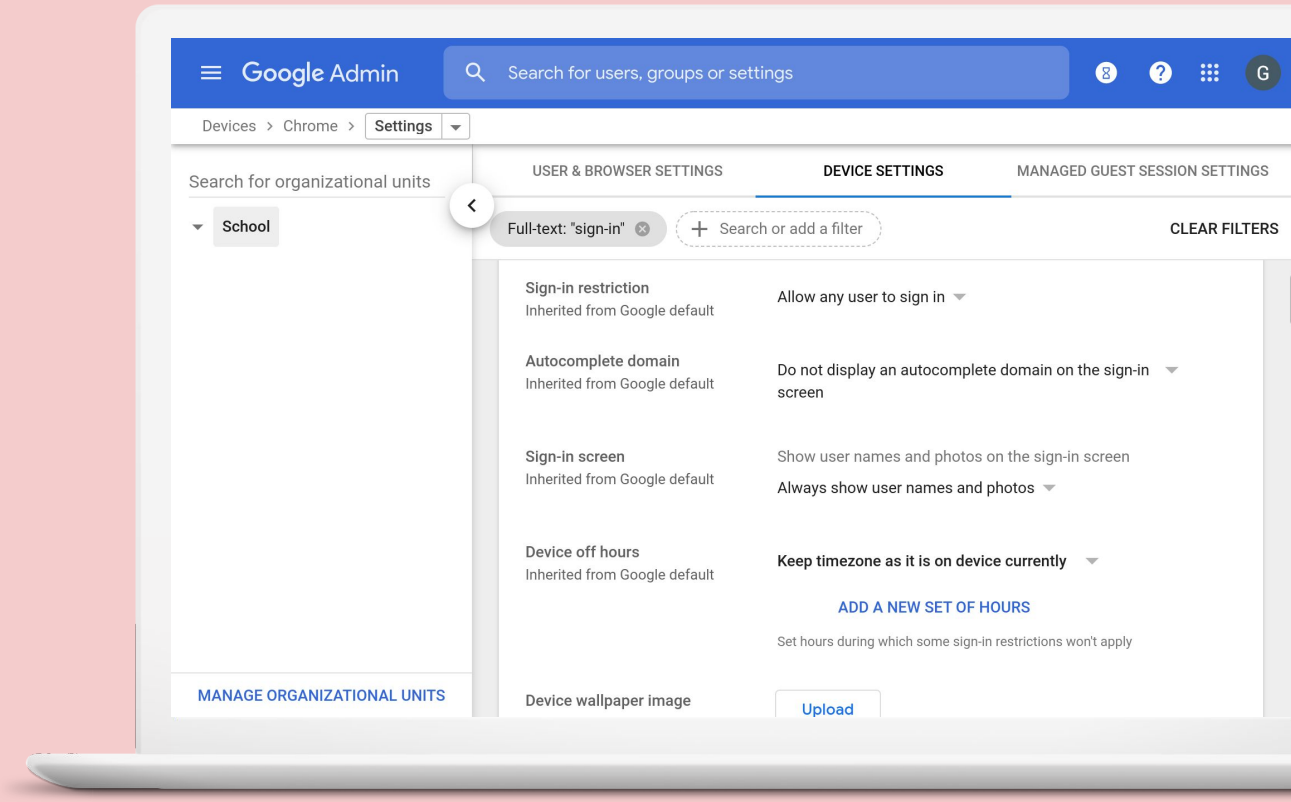
This setting controls the custom text on the disabled device screen. We recommend you include a return address and contact phone number in your message so that users who see this screen are able to return the device to your school.



Device settings

Specify who can sign in

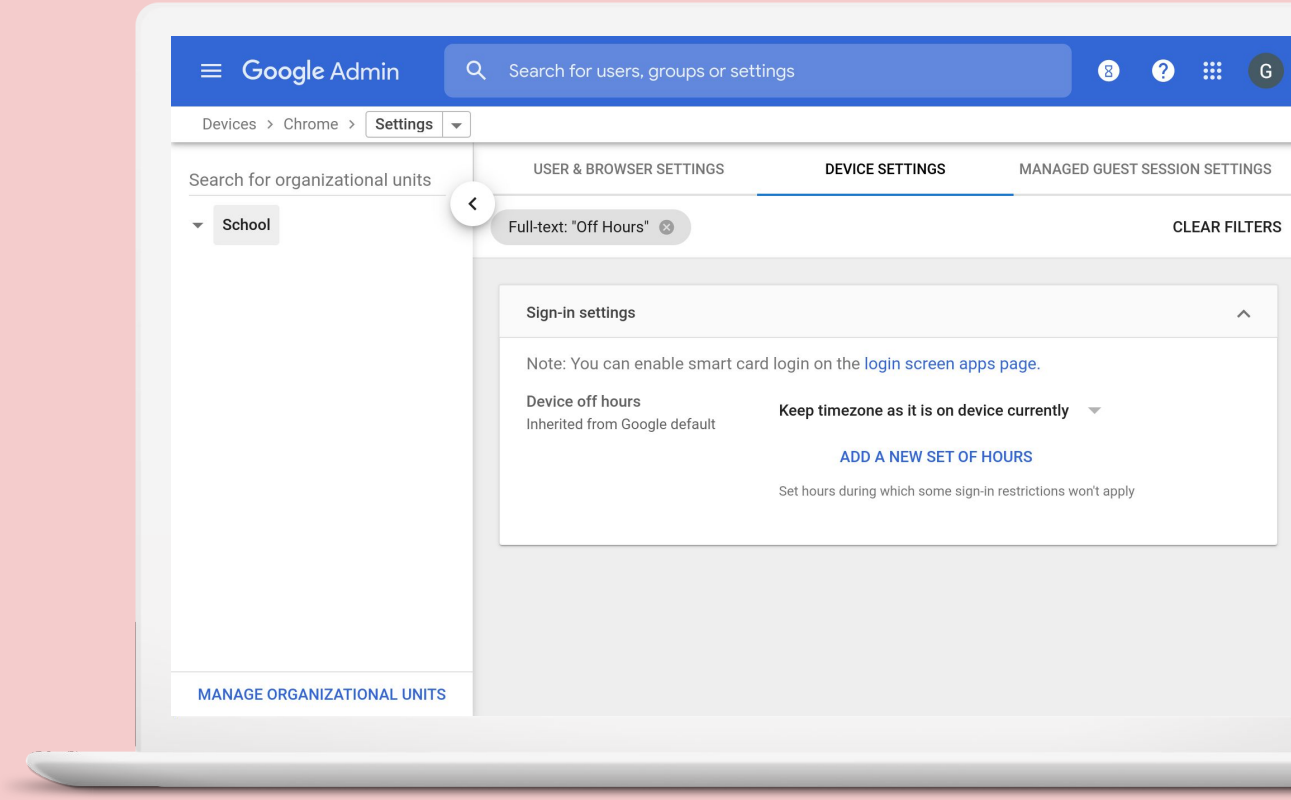
Ensure school-owned Chromebooks are only used for educational purposes by disabling guest mode and restricting sign in to your domain.



Device settings

Off Hours sign-in settings

Perfect for schools with BYOD programs, allows schools to block guest browsing or only allow users with a username ending in @domain.school.nz to sign in during school hours. Outside of school hours, users can browse in guest mode or sign in to their device using an account other than their @domain.school.nz account.

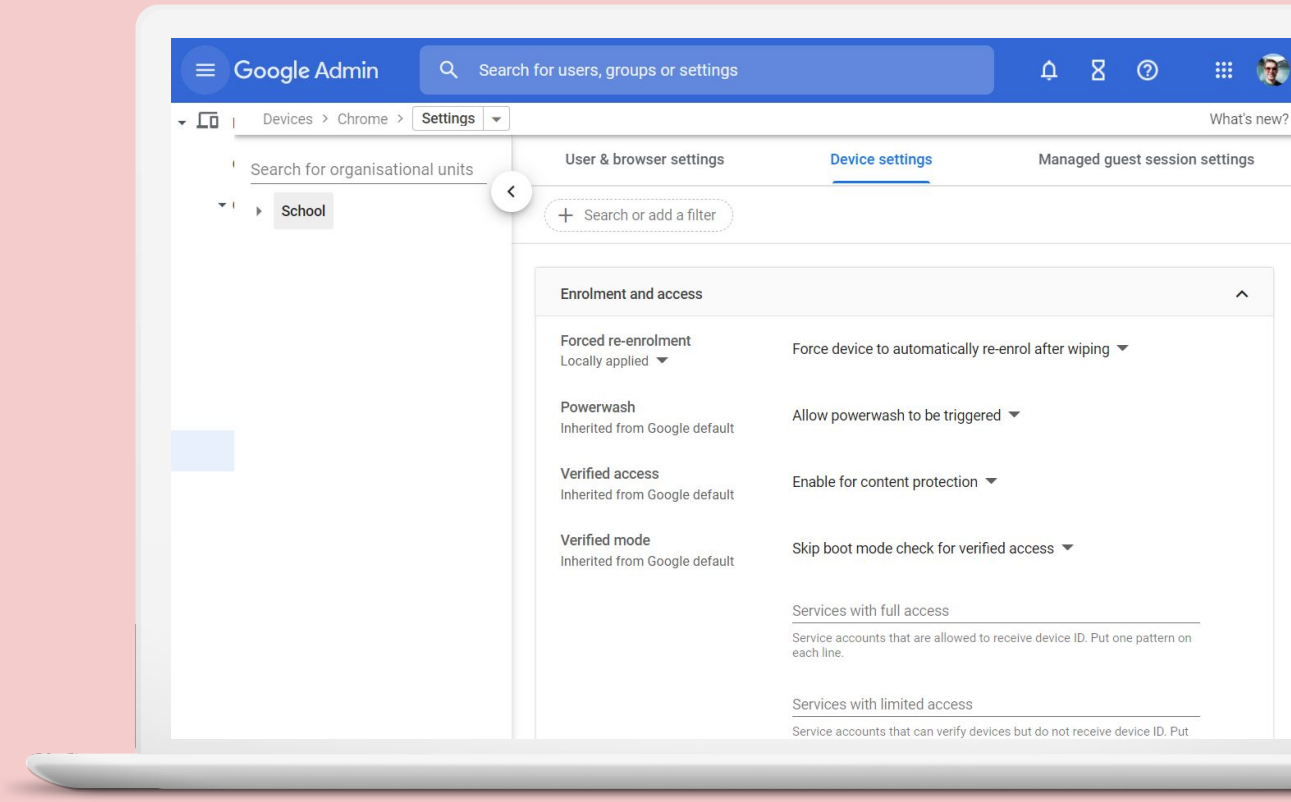


Device settings

Force Re-enrolment

Specifies whether Chrome OS devices are forced to re-enroll into your school after they've been wiped.

Avoid students wiping their devices and becoming unmanaged.

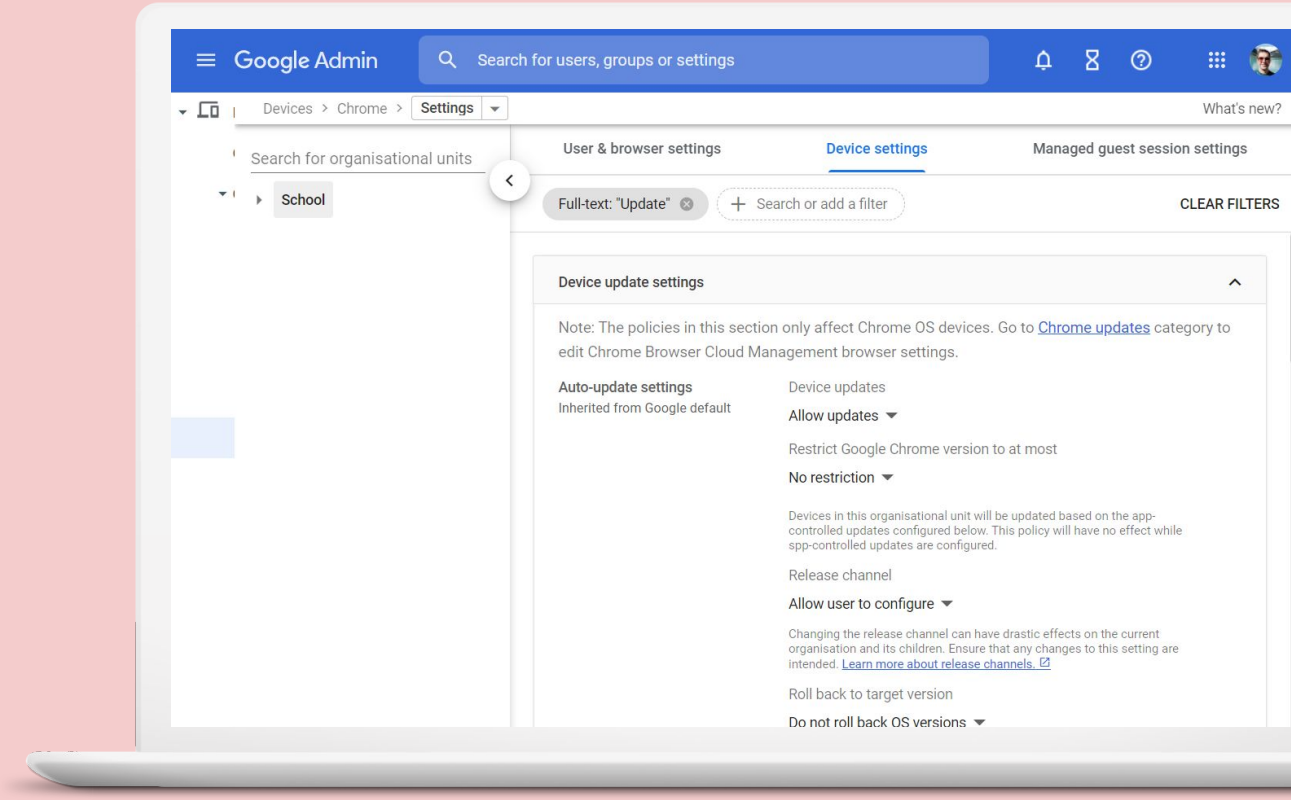


Device settings

Device Updates

You can allow Chrome OS devices to automatically update to new versions of Chrome OS as they're released and let users check for updates themselves. Allow updates is strongly recommended.

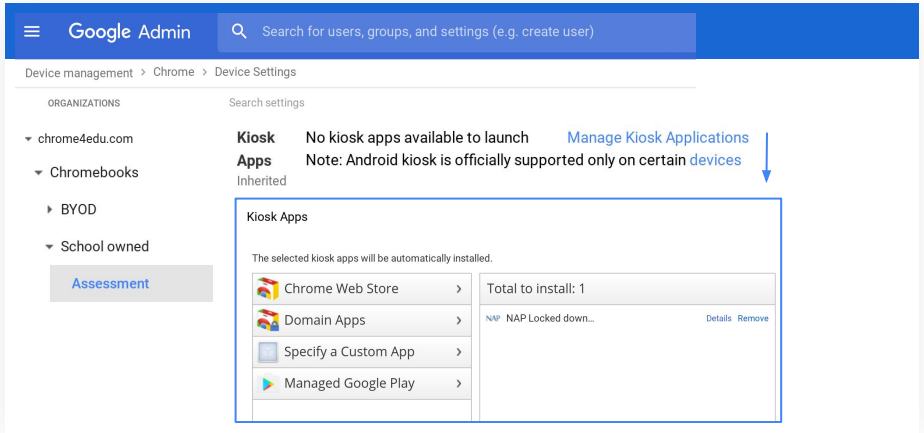
Optional: Control the Chrome OS version made available.



Assessments

Scenario 1: Kiosk mode: school sets up Chromebook to run as a Single App Kiosk running the exam app.

Note: You need to have the test available as a Chrome kiosk app.



Manage Kiosk Apps

1. Go to **Device management** > **Chrome management** > **Device settings** > **Kiosk Apps**. Click on **Manage Kiosk Applications**.
2. In the dialog box that appears, select the exam kiosk app you want to use. You can search for it on the **Chrome Web Store**, or manually install it if you have the app ID and URL by selecting **Specify a Custom App**.
3. On the same **Device settings** page, under **Kiosk Settings** > **Auto-Launch Kiosk App**, select the app.
4. Make sure the devices you want to administer the test with are under the organizational unit you select for the kiosk app.

Auto-Launch Setting for a Kiosk App

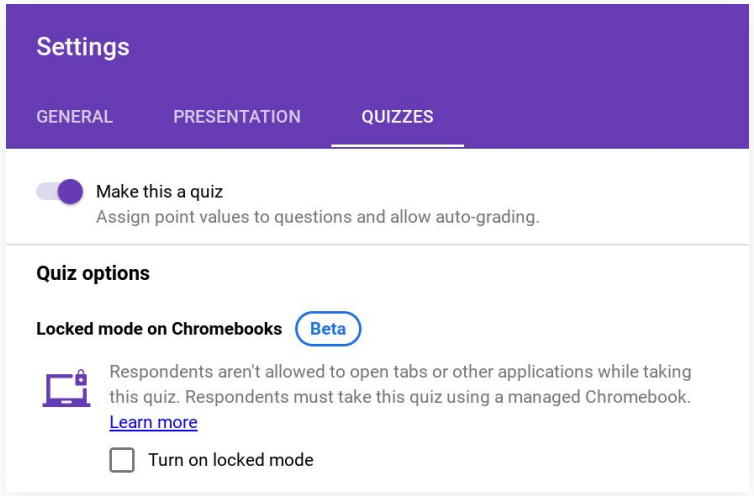
If Auto-Launch Kiosk App is not configured, then the student will see a menu of kiosk apps in the system tray on the login screen. The student needs to select the appropriate kiosk app to launch it in order to take the test. After the test is complete, the student can exit the kiosk app and log back into a user session.

If Auto-Launch Kiosk App is configured, when the device next boots, it will immediately load the kiosk app.

Assessments

Scenario 2: Locked mode: school sets up Google Forms quiz using locked mode feature

Note: Available only on managed Chromebooks, locked mode prevents students from navigating away from the Quiz in their Chrome browser until they submit their answers.



A new way to ensure students are distraction-free when taking Quizzes in Google Forms

For a lot of teachers, a day in the life might look like this: teach innovatively and creatively, quiz without distractions, grade efficiently, give thoughtful and constructive feedback, repeat.

Teachers assess knowledge and check for understanding every single day, and many use Quizzes in Google Forms to do just that.

But we've heard feedback from teachers that they want to ensure their students aren't navigating to other browser tabs while taking quizzes.

Now, teachers can enable locked mode with a simple checkbox in Google Forms, giving them full control over assessments.

To streamline the assignment process, we've also added the ability for all Classroom users to create a Quiz directly from Classroom. Instead of creating quizzes in a separate browser, you can create a quiz and assign it directly to your class, or multiple classes.

Additional resources

Click here

Click here

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Questions?

New Zealand Government

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Additional Webinars

[Did you know? Training Series](goo.gle/didyouknow) - goo.gle/didyouknow

In the "Did you know?" Training Series Google hosts Admin-centric training sessions covering Google Workspace for Education.

New Zealand Government

Contact details

Steve Smith
Program Manager
Google for Education NZ
nzsteve@google.com

Ministry of Education

Danielle Vandendungen
Strategic Advisor – Cyber Security in Schools
cyber.security@education.govt.nz

Mohan Parbhu
Commercial IT - Microsoft
mohan.parbhu@education.govt.nz

Mike Popata
Commercial IT - Google
mike.popata@education.govt.nz

We **shape** an **education** system that delivers
equitable and **excellent outcomes**

He mea **tārai** e mātou te **mātauranga**
kia **rangatira** ai, kia **mana taurite** ai ōna **huanga**

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

education.govt.nz

New Zealand Government