GAT Labs
for education

Chromebook Management:

Best Practices for School Admins

Table of Contents

Chromebooks are reliable, affordable technical solutions for schools that blend traditional and online learning. Global shipments of ChromeOS devices are growing year after year. They are considered easy to use, secure, and durable.

However, giving each student a Chromebook doesn't guarantee its optimal usage. Schools must consider additional management tactics to ensure security and safety when using ChromeOS devices and the Chrome browser.

This comprehensive guide shares best practices for using the Google Admin Console and out-of-the-box solutions from GAT Labs to elevate Chromebook management and auditing at your school.

Why Schools Choose Chromebooks for Students?

Recently, Chromebooks have become increasingly common in the classrooms. They benefit educational institutions in many ways, including easy implementation and maintenance, which benefits them over iPads, Macs, and PCs.

- **Cost-efficient:** ChromeOS devices fit schools' tight budgets. They offer long battery life, are durable and lightweight, and are less costly to repair than traditional laptops.
- **Integrated with Google Workspace for Education:** Most drive data is cloud-based, which fosters collaboration, productivity, access to educational resources, and security in case of technical issues or a lost device.
- **Simple and user-friendly:** Chromebooks are based on web apps and cloud storage and offer a simple interface that doesn’t require advanced technical skills. Their straightforward operational system facilitates student learning and domain management in the case of small IT teams.
- **Secure:** ChromeOS devices offer strong security features. Built-in storage and automated backups decrease risks of data loss and malware and ensure learning continuity for students.

Chromebook Management Best Practices
for Ultimate Student Safety & Learning Experience

Before you start...

Chromebook Asset Management

This task may be the most time-consuming for school admins, but this effort lays the fundamentals for efficient Chromebook management.

An updated ChromeOS device inventory will streamline your daily operations, support security maintenance, and prevent device and data loss. Additionally, it allows you to categorize devices according to the school's needs, optimizing IT team efficiency and user experience.

The Chromebook inventory should include essential information about each device:

- Model
- Serial number
- Operating system
- Purchase date
- Warranty information
- Assigned user
- Allowed locations

GAT Labs for Education

GAT+ provides an overview of all your ChromeOS devices and optimizes their management with categorization and monitoring features. It allows you to sort devices by model and group and track their location in real time.

Additionally, GAT+ supports Chromebook data export to Asset Tiger, one of the leading free online asset management tools.

1. Device Management

Before auditing online safety and cybersecurity measures, ensure all your Chromebooks and users are in the right place. A well-structured device and user system can help you manage school-wide and group policies.

1. Chromebook Enrollment & Deprovision

You must first enroll each ChromeOS device to enforce school policies in the Google Admin Console. The steps and the features available depend on your Chrome Education license type.

Google Admin Console

Follow the instructions to enroll or deprovision each Chromebook individually. Note: Nobody can be signed in on the device to start enrollment; if an account is logged in, you need to deprovision or wipe the device first. When the enrollment process is complete, you can view all your enrolled devices in the Google Admin console and set device-level policies.

GAT Labs for Education

With GAT Labs' toolset, you can audit the number and type of enrolled ChromeOS devices in use to better organize them.

If you need to modify or remove a lot of Chromebooks, automated deprovision and transfer features will significantly speed up this massive task. With GAT Flow, you can build a workflow to disable, re-enable, or modify a Chromebook set assigned to any user or group in bulk. This functionality helps manage device transfers between different school units, groups, or users during offboarding or staff changes.

2. Organizational Units Management

When you enroll Chromebooks, they automatically go into the top-level organizational unit. To customize and apply device policies for different user types (student, teacher, or other school staff), you must move them to a relevant organizational unit.

Google Admin Console

The first option is moving each device to a previously created OU in your Google Admin console. You can see all the OUs and devices in each of the units. However, to streamline the process, you can configure a "Place Chrome device in user organization" setting to place a newly enrolled device in the OU of the enrolled user assigned to the device. This feature automatically applies the user's OU settings to the relocated device.

GAT Labs for Education

Speed up and simplify bulk student onboarding and Chromebook enrollment with GAT Flow. This tool allows you to create customized workflows to automatically import new students and assign them to relevant organizational units. Google admins can easily view, audit, and manage all OUs in one visual dashboard at any time.

2. Student Online Activity Monitoring

Creating a safe and secure educational environment is crucial for productive and enjoyable student learning. The following practices contribute to comprehensive online safety for each student using a Chromebook in the classroom.

1. Safe Chrome Browsing

1.1 Enabled Safe Search & Safe Browsing

Google Admin Console

These two settings are essential for ensuring a safe online experience in your school and CIPA compliance. Enable them on all students' Chromebooks in the Google Admin Console.

Safe Search filters online content that could be age-inappropriate for users under 18, such as explicit and violent images.

Safe Browsing protects students from potentially unsafe and harmful pages. From the three levels in the Google Admin Console, we recommend choosing the enhanced protection that safeguards your students from dangerous websites, downloads, and extensions.

Note: The Safe Browsing settings also work when a Chromebook is outside the school network because it's connected to the Google user account.

1.2 Disabled Incognito Mode & Guest Mode

Google Admin Console

These practices prevent IT-skilled students from bypassing online filtering settings enforced school-widely and, as a result, exposing themselves to harmful online content on their Chromebooks.

You can disallow Incognito Mode in the Security section and Guest Mode in the Chrome Management section in the Google Admin Console.

1.3 Disabled Developer Tools & Chrome Task Manager

Google Admin Console

Other ways to bypass filter solutions implemented by school admins are Developer Tools and the Chrome Task Manager. Students can use these to change network and app settings and disable Chrome extensions, among other things. This can lead to potential data exposure and other online threats to your Chromebooks.

Disable Developer Tools in the User Experience settings and the Chrome Task Manager in the Apps and Extensions settings.

1.4 User Browsing Monitoring

Google Admin Console

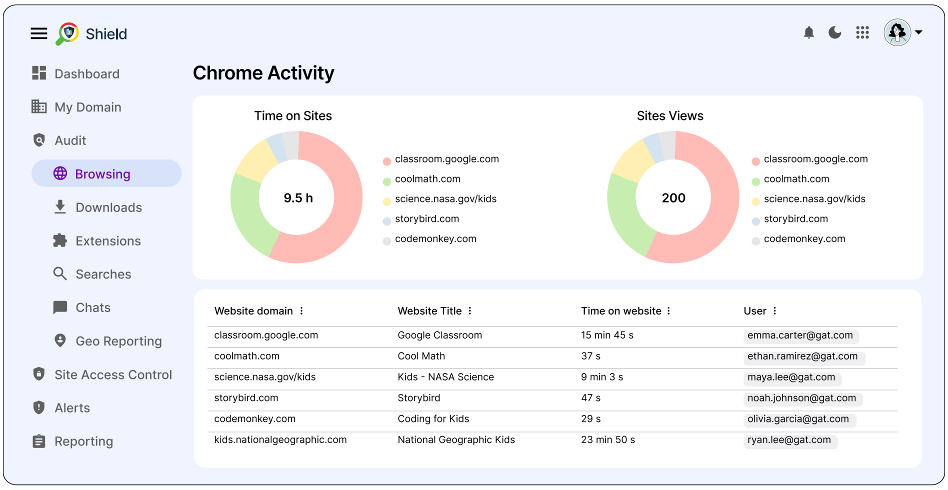
School admins should disable students to clear their browsing history to ensure complete visibility into student browsing activity and detect potential safety risks.

That's possible by turning on two options in the Security Settings in Google Admin Console: Always Save Browser History and Do not allow clearing history in the settings menu.

GAT Labs for Education

While the mentioned functionalities allow you to generally view what pages a student has visited in the past, you can take a more proactive approach to monitor student online activity in the Chrome browser.

GAT Shield allows you to track students' behavior and browsing activity in a given period and in real time. It shows time spent on each website by a student or a selected classroom and the top websites visited by students and used devices. These granular browsing insights help admins optimize student online experience and support teachers in keeping control of the classroom.



Website domain	Website Title	Time on website	User
classroom.google.com	Google Classroom	15 min 45 s	emma.carter@gat.com
coolmath.com	Cool Math	37 s	ethan.ramirez@gat.com
science.nasa.gov/kids	Kids - NASA Science	9 min 3 s	maya.lee@gat.com
storybird.com	Storybird	47 s	noah.johnson@gat.com
codemonkey.com	Coding for Kids	29 s	olivia.garcia@gat.com
kids.nationalgeographic.com	National Geographic Kids	23 min 50 s	ryan.lee@gat.com

1.5 Customized Start-up Pages

Google Admin Console

A tiny but valuable element that can improve browsing safety is displaying a personalized set of home pages on your Chromebooks. It can include the school's online safety policy to remind students how to behave when browsing on a school's device. You can add a startup page in the Chrome Settings in the Google Admin Console.

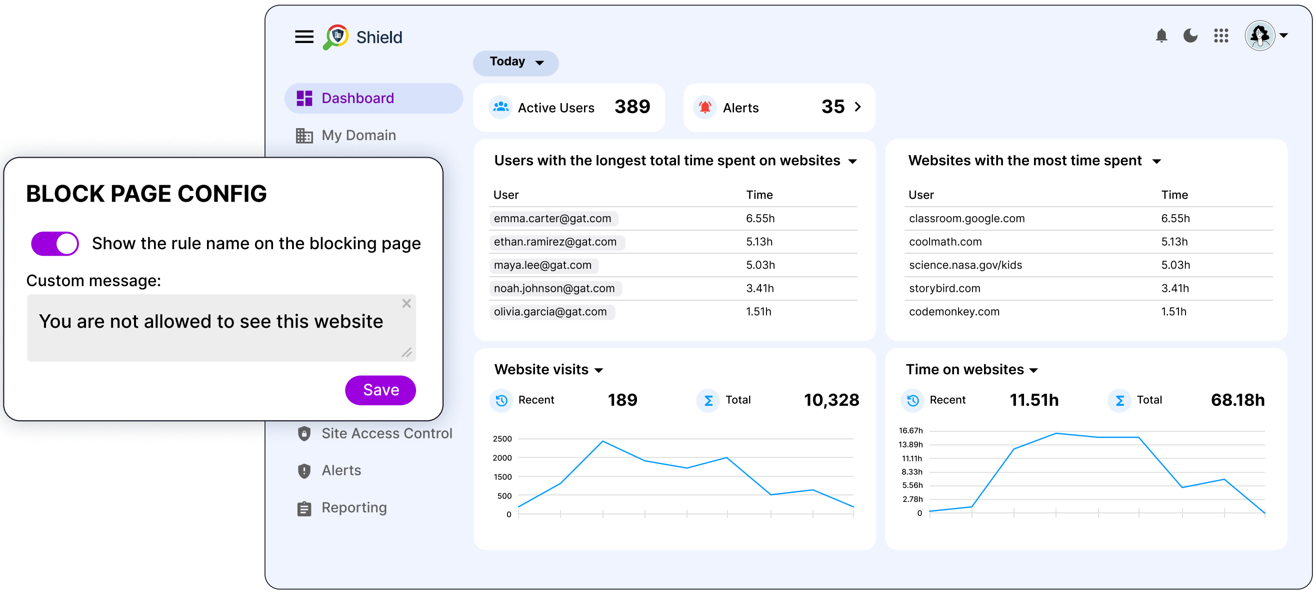
2. Web Filtering

2.1 Inappropriate Content Monitoring

GAT Labs for Education

As Chromebooks don't offer advanced web filtering, you need a third-party tool to filter and restrict online content. This contributes to your school's CIPA compliance and protects students' online well-being.

GAT Shield provides sophisticated features for controlling and adjusting internet access for each student, group, and classroom. Google admins can set filtering rules to comply with the school's security policies and ethical standards. Monitoring and alerting on customized keywords related to illegal and age-inappropriate activities, products, and other content help create a safe online environment for students.



BLOCK PAGE CONFIG

● Show the rule name on the blocking page

Custom message:

You are not allowed to see this website

Save

Users with the longest total time spent on websites

User	Time
emma.carter@gat.com	6.55h
ethan.ramirez@gat.com	5.13h
maya.lee@gat.com	5.03h
noah.johnson@gat.com	3.41h
olivia.garcia@gat.com	1.51h

Websites with the most time spent

User	Time
classroom.google.com	6.55h
coolmath.com	5.13h
science.nasa.gov/kids	5.03h
storybird.com	3.41h
codemonkey.com	1.51h

2.2 URL Filtering and Blocking

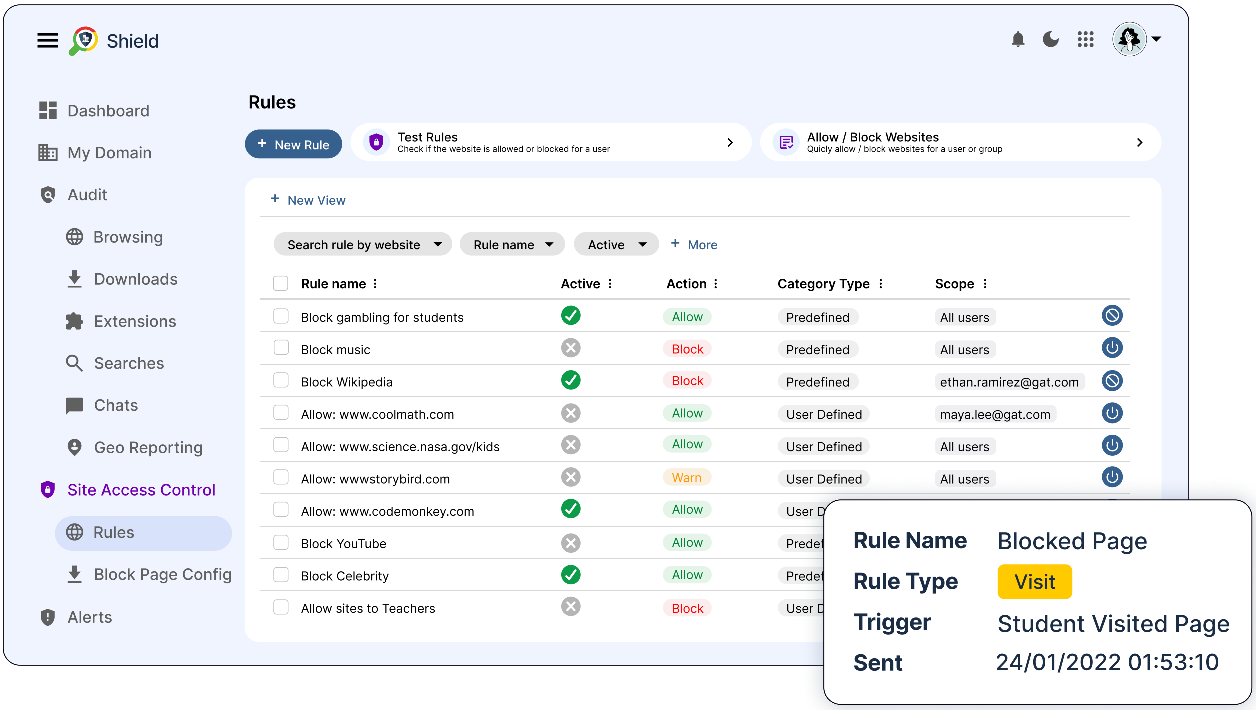
Google Admin Console

Although the Google Admin Console does not provide web filtering solutions, it allows you to block certain websites to avoid bypassing your filters by students. These can include, among others, chrome://extensions, chrome://certificate-manager, and chrome://settings/signOut. By disabling users from turning off or changing safety settings, you create an extra layer of protection against inappropriate online content.

GAT Labs for Education

Take the next step forward with advanced web filtering in the classroom using bulk website blacklisting and alert automation.

Site Access Control allows you to block specific URLs and entire websites and detect and block all pages found by the online search that contain a given keyword. You can set the blacklist for all users or a specific scope (set of users) or use predefined blocklists to speed up your work.



□	Rule name ⋮	Active ⋮	Action ⋮	Category Type ⋮	Scope ⋮
□	Block gambling for students	✓	Allow	Predefined	All users
□	Block music	✕	Block	Predefined	All users
□	Block Wikipedia	✓	Block	Predefined	ethan.ramirez@gat.com
□	Allow: www.coolmath.com	✕	Allow	User Defined	maya.lee@gat.com
□	Allow: www.science.nasa.gov/kids	✕	Allow	User Defined	All users
□	Allow: wwwstorybird.com	✕	Warn	User Defined	All users
□	Allow: www.codemonkey.com	✓	Allow	User D	
□	Block YouTube	✕	Allow	Predef	
□	Block Celebrity	✓	Allow	Predef	
□	Allow sites to Teachers	✕	Block	User D	

Rule Name	Blocked Page
Rule Type	Visit
Trigger	Student Visited Page
Sent	24/01/2022 01:53:10

Real-time alert rules notify admins when a student attempts to access a forbidden website. With this solution, the admin can take prompt action, such as redirecting to a specific URL, showing a warning, and taking screen capture to track further student behavior.

2.3 YouTube Restrictions

Google Admin Console

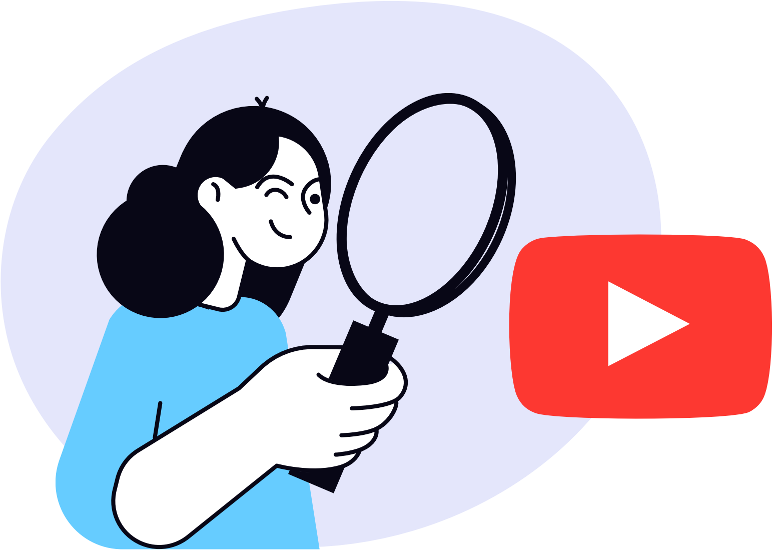
YouTube is one of the primary online resources for students in the classroom, so it deserves additional attention to make it a safe place for minor Chromebook users.

In the Google Admin Console, turn on one of two restricted YouTube access modes: Strict Restricted (which blocks many videos automatically) or Moderate Restricted (which allows more videos). These modes can be applied to specific OUs.

GAT Labs for Education

Enable real-time YouTube browsing monitoring for all your students in GAT Shield. This feature allows you not only to view browsing history (who, when, and how long spent watching a video) but also to see the content of a watched video live.

You can easily block specific videos (including embedded videos) and comments. If the video's owner is a user in your Google domain, you can change its status in GAT+.



3. Chromebook Cybersecurity Measures

This chapter discusses some good practices to strengthen Chromebook security in your school. They will decrease the risk of data loss or leakage, malware, and other risks affecting student data, accounts, devices, and the entire Google domain.

1. Access Management

Controlling device access is key to maintaining a secure learning environment for each student. A multifaceted approach will protect your school from unauthorized access to Google accounts, sensible school data, and significant cybersecurity threats.

1.1 Sign-in Restrictions: Password & 2FA

Google Admin Console

Enforce strong password requirements for all Chromebook users (choosing the "top-level organizational unit" setting). In the reporting section of the Google Admin Console, you can check the strength of each student's current password. We also recommend turning on obligatory 2-step Verification for all students to create an extra layer of ChromeOS device security.

Additionally, you can protect student data by preventing users from reusing their passwords on dangerous or unauthorized websites. With active password detection, students will be forced to use a different password on a disallowed website.

GAT Labs for Education

Optimize the implementation of the school's password policy for your Chromebook users and assign this security task to an external automation tool. With GAT Flow, you can generate strong passwords when onboarding or modifying students in bulk and change their passwords anytime. The same tool enables you to automate 2FA management with a workflow triggered when a student tries to disable this login method.

1.2 Managed Guest Sessions

Google Admin Console

This mode allows multiple users to share the same Chromebook without signing in to their Google accounts. If your students need to share or loan a device with full and secure browser functionality, follow these steps.

GAT Labs for Education

The GAT Shield extension is also available for managed guest sessions, so you can still monitor student activity to secure the device and user privacy.

1.3 Drive Permissions

Google Drive is a fundamental part of a successful Chromebook experience in the classroom. It fosters collaboration between students and teachers and offers incomparable storage and sharing features.

Google Admin Console

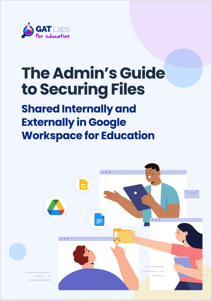
Review shared files in your domain with the Drive log events audit. You can search for files shared outside your domain using the audit and investigation page and the security investigation tool.

GAT Labs for Education

Keep all content stored in your school’s Drives under control with domain-wide visibility and file share audit automation.

Monitor, manage, or reduce user permissions for each file, folder, and Drive to minimize access levels with GAT+. Identify and change folder ownership for only specific users in bulk.

View and audit internal and external shares of files and detect high-risk shares in and outside the school domain. As the only tool in the market, GAT+ reports external files shared into your domain, which is crucial for ensuring Google Workspace cybersecurity.



GAT Labs for education

The Admin’s Guide to Securing Files

Shared Internally and Externally in Google Workspace for Education

Discover file share audits with GAT Labs.

Download our Guide to Managing Files Shared in and Externally in Google Drive.

Download Guide

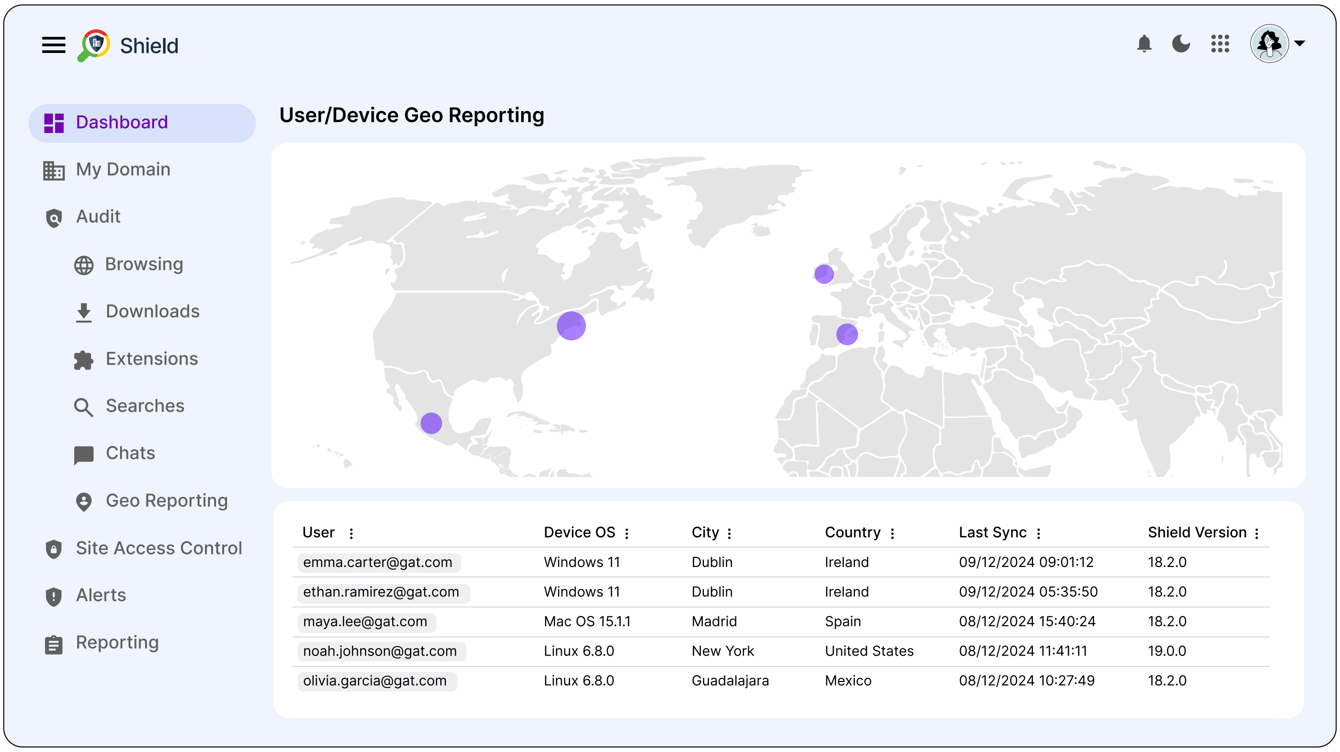
2. Geolocation for DLP & Anti-Theft Prevention

GAT Labs for Education

Protect all your ChromeOS devices, school data, and user privacy in case of device theft or loss. Real-time geolocation allows you to track every device and react quickly when it's found outside the default location.

While unusual login detection isn't available in the Admin Console, you can geolocate your Chromebooks in GAT Shield anytime. You can also see real-time reports on them and other login events (i.e., a failed login attempt) in the GAT+ visual dashboard.

Additionally, create an alert rule to monitor Chromebook user logins from unexpected locations. You will be notified when a student logs in on the school's device outside the selected area. Then, you can remotely disable potentially lost or stolen Chromebooks. Detailed real-time login auditing can detect cybersecurity issues promptly and protect your school data from breaches.



User/Device Geo Reporting

User	Device OS	City	Country	Last Sync	Shield Version
emma.carter@gat.com	Windows 11	Dublin	Ireland	09/12/2024 09:01:12	18.2.0
ethan.ramirez@gat.com	Windows 11	Dublin	Ireland	09/12/2024 05:35:50	18.2.0
maya.lee@gat.com	Mac OS 15.1.1	Madrid	Spain	08/12/2024 15:40:24	18.2.0
noah.johnson@gat.com	Linux 6.8.0	New York	United States	08/12/2024 11:41:11	19.0.0
olivia.garcia@gat.com	Linux 6.8.0	Guadalajara	Mexico	08/12/2024 10:27:49	18.2.0

3. Third-Party App Management

3.1 Apps and Extensions Blocking

Google Admin Console

Blocking Chromebook applications and extensions stops students from downloading non-educational and potentially distracting content. As a result, it strengthens your cybersecurity protection and focuses attention in the classroom. Select the Block all other apps and extensions option in the Apps and Extensions settings to prevent new app installations.

GAT Labs for Education

With GAT+, you can proactively create policies for applications installed in the domain. It allows you to ban specific apps for individual users or OUs and trust other apps that may be necessary in the classroom. A user can still install a banned app, but GAT+ detects this action in real-time, notifies you, and removes user permissions required by the app.

3.2 Third-Party App Auditing

Google Admin Console

First, you audit all configured apps, accessed apps, and apps pending review in App access control. Working for an education institution, you may want to restrict access to specific apps; they can get a Trusted, Limited, Specific Google data, or Blocked status. Different settings can apply to users under and above 18 years old. In the case of unconfigured apps, if a user tries to sign in, the Google admin can choose a specific action to be performed.

GAT Labs for Education

In GAT+, conduct an applications risk assessment to identify high-risk apps and maintain your Chromebooks' security. From this audit, you will find out what apps have been granted the widest privileges (High scope risk score) and judge whether they are trustworthy or should be removed. Some risky privileges given to third-party apps are:

- “https://mail.google.com”
- “https://www.googleapis.com/auth/gmail”
- “https://docs.google.com/feeds”
- “https://www.googleapis.com/auth/drive”
- “https://www.googleapis.com/auth/admin”
- “https://www.googleapis.com/auth/apps”

Learn more on third-party apps auditing in Google Workspace for Education on our blog.

Read our Blog

3.3 Chrome Extension Auditing

Google Admin Console

Start reviewing each extension's usage and other information on the Apps & Extension usage page. Extension details include, among others, app name and type, the number of permissions requested by the app, and how many browsers have this extension installed.

In the Google Admin Console, you can also block or force the installation of an extension, search for a given app, and export full apps and extensions usage report data for a specific OU.

GAT Labs for Education

GAT Shield provides an extensions risk assessment for extensions installed on your Chromebooks. It shows the type of access level required from the school domain by an extension (permission score: low/medium/high). Pay attention to high-score extensions as they may require enough resources to potentially damage the Chrome browser or device.

Additionally, you can track extension activation and usage through the Browsing live reports.

4. Downloads Management

Since downloaded files, whether from Gmail, Drive, or a website, are one of the most common “means of transport” for malware, tracking them is essential for school cybersecurity and data protection.

Google Admin Console

In Drive Log Events, you can preview most downloads, including shared files. However, you won’t see who downloaded the file, and you won't receive a notification when this happens.

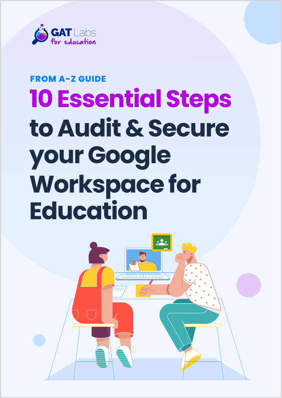
GAT Labs for Education

Start monitoring all downloads through the Chrome browser across your Google domain with GAT Shield real-time audit. It shows the admin the file's original location and destination, size, format, download date and time, and the user who downloaded it. With customized filters, you can search for information on a specific Chromebook and geolocation where the download event occurred.

4. Chromebook Fleet Review

1. Scheduled Audits

Conduct recurrent audits to ensure ongoing compliance, cybersecurity, and online safety for your ChromeOS devices and students using them. Depending on your institution's size, schedule reviews on a regular basis, at least once a year. Automate reports in GAT+ to stay on top of your Chromebook health effortlessly.



GAT Labs for education

FROM A-Z GUIDE

10 Essential Steps to Audit & Secure your Google Workspace for Education

Explore GAT Labs' Comprehensive Guide to Audit and Secure your Google Workspace for Education in 10 Steps.

Download Guide

2. Regular Training

You're not alone, Google admin. Ensuring school Chromebook safety is a team effort. End-users are usually the weakest links, so they need to understand what's in play. To raise cybersecurity awareness and share good practices for the entire school, provide training and workshops for students and teachers using Chromebooks in the classroom.

GAT Labs
for education

Dive Deeper Into GAT Labs

Schedule a Demo

15-Day Free Trial