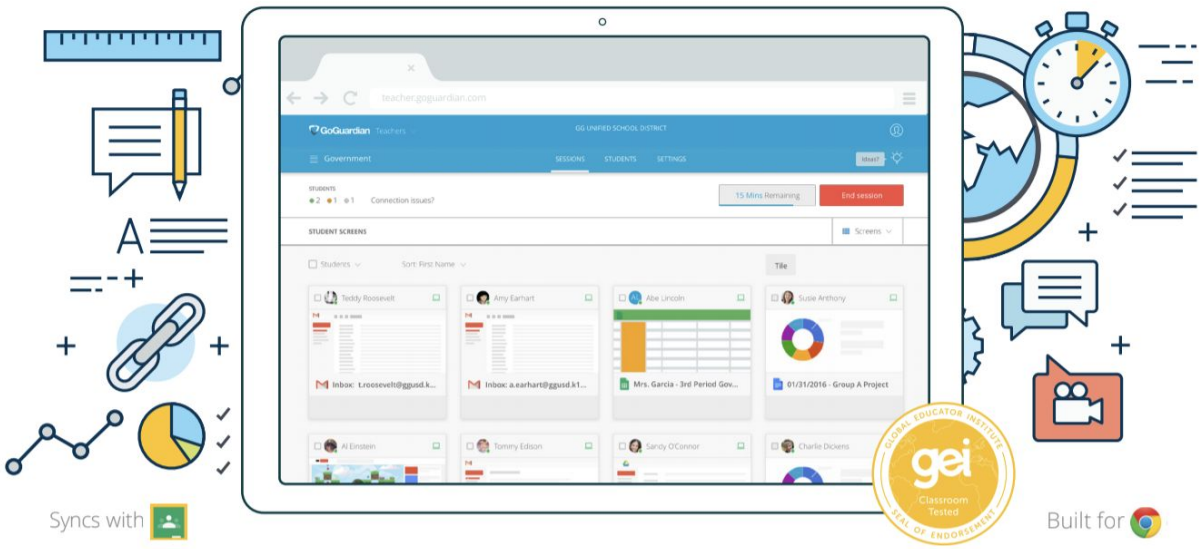
GoGuardian Admin

Training Guide



Welcome to **GoGuardian Admin**!

We're excited to get you started using GoGuardian Admin in your organization!

After completing the setup using this guide, you will be able to do the following:

- View student browsing history
- Use **Policies** to regulate which websites students can and cannot access
- Set up **Smart Alerts** to stay on top of attempts at undesirable student browsing
- Place additional restrictions on students attempting to abuse browsing privileges using the **Penalty Box**
- **Export PDFs and CSVs** of student individual browsing activity
- Keep track of the most used apps and most visited sites for your organization
- Locate and make use of many of GoGuardian Admin's most helpful features

We hope you enjoy using GoGuardian Admin and find it helps you maximize learning and minimize distractions in your school.

Sincerely,

The GoGuardian Team

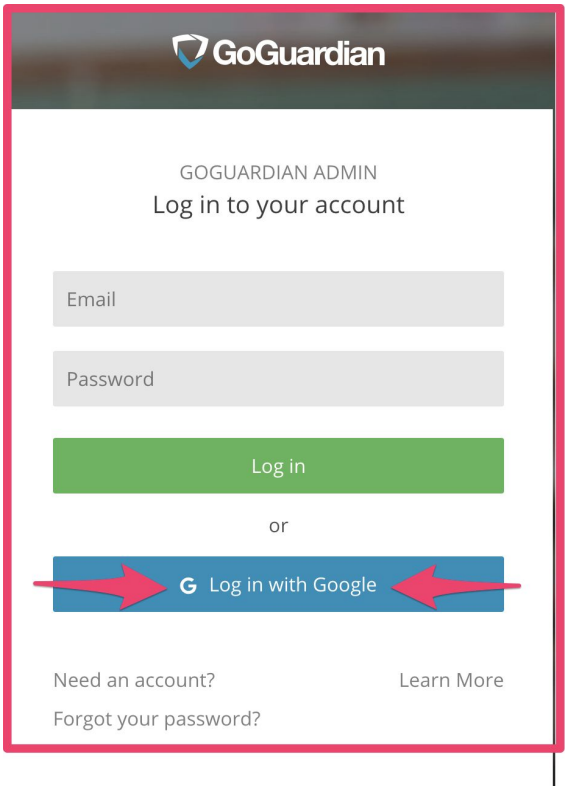
Table of Contents

Getting Started

Once your administrator has created your account, navigate to **admin.goguardian.com** and select **Log in with Google**

You can also create a password following the steps here.

Protip: We recommend using Log in with Google to avoid any extra steps.



QUICK GLOSSARY GUIDE

GAC stands for the Google Admin Console. This is where you can add OUs (and add user accounts to those OUs) or move user accounts around. This is also where GoGuardian's extensions will be force-installed so that you can filter and monitor student browsing. The Google Admin Console can be found at admin.google.com.

OU stands for Organization Unit. Think of these like folders that house any number of users or devices within your Google Admin Console. These are also shown when clicking the Configuration button in GoGuardian Admin. Because OUs function similarly to folders, they can also be nested under one another in much the same way you would create a master folder and then add multiple subfolders under it.

Policies are how you set allowances and restrictions on user browsing enforced by GoGuardian Admin. Policies can be created by clicking the Configuration button in GoGuardian Admin. To edit a Policy, you can click Configuration, then click My Policies, then click the pencil icon on whichever Policy you would like to edit. Each Policy consists of a Website URLs portion, a Website Categories portion, a YouTube portion, and an Apps & Extensions portion.

Dashboard provides a bird's eye view of your organization's activity as a whole (including the number of students currently online, top 50 most visited websites, top 50 most viewed videos, top 50 most viewed Google Docs, top 50 apps, top 10 most flagged students, and an activity timeline with the number of sites visited, blocked attempts, flagged activity, and YouTube views).

All Students provides a log of all users in your organization (including student emails accidentally entered or misspelled in GoGuardian Teacher, so please take care to double-check user email addresses before entering them, as incorrectly entered emails and names cannot be removed).

Theft Recovery allows you to track stolen devices (the device must be in use to be tracked).

Configuration is where you can set restrictions and additional settings that will apply to your entire organization. This includes Web Proxy settings, At School and Out of School settings, Customized Block Page settings and settings like Safe Translator, SafeSearch, blocking direct IP access, and filtering iFrame content.

Penalty Box is where you can add misbehaving students to restrict access to all sites except those you explicitly allow.

Activity Log allows you to see which administrative changes were made to Policies and at what date and time. You can also access Blocked Attempts from this menu; allowing you to see which users were recently blocked from a site and the category responsible for the block.

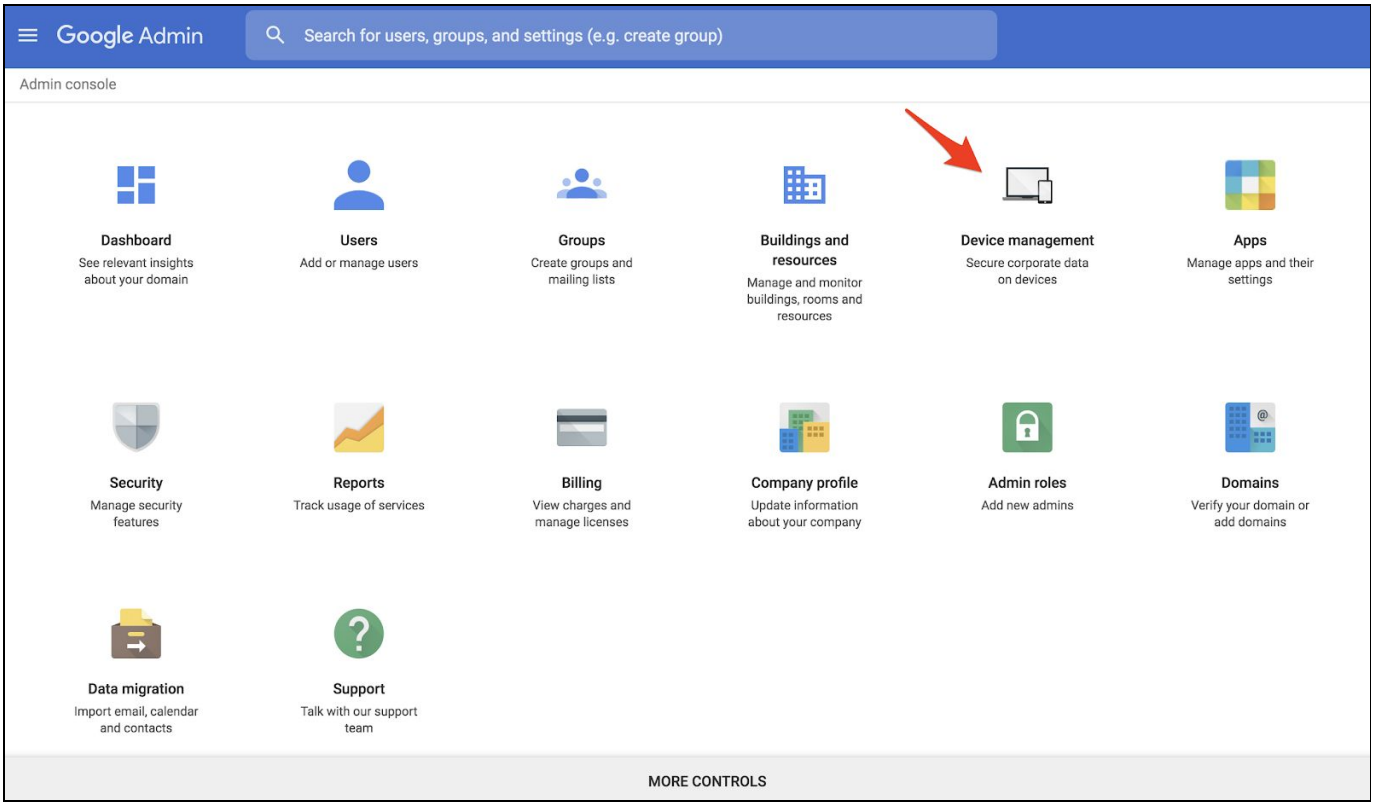
Simulator is a tool that allows you to test Policy changes to see how they will apply to users within a designated OU.

Smart Alerts are where you can set triggers that help monitor, restrict, and alert administrators of unwanted student browsing activity. At this time, Smart Alerts can only be set to detect explicit student browsing activity.

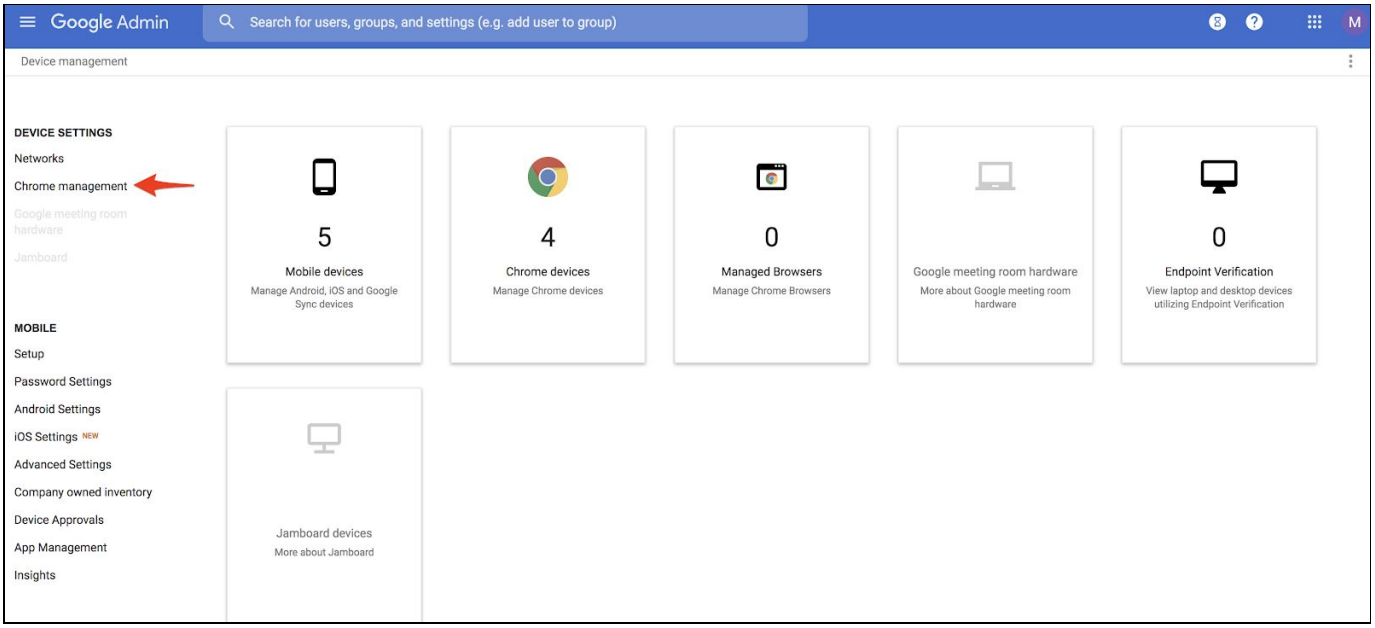
Setup

***Note: The GoGuardian extensions cannot be installed on an OU for Chromebooks. The extensions are user account-based, not device based. So, the extensions must be force-installed on an OU that has user accounts in it.**

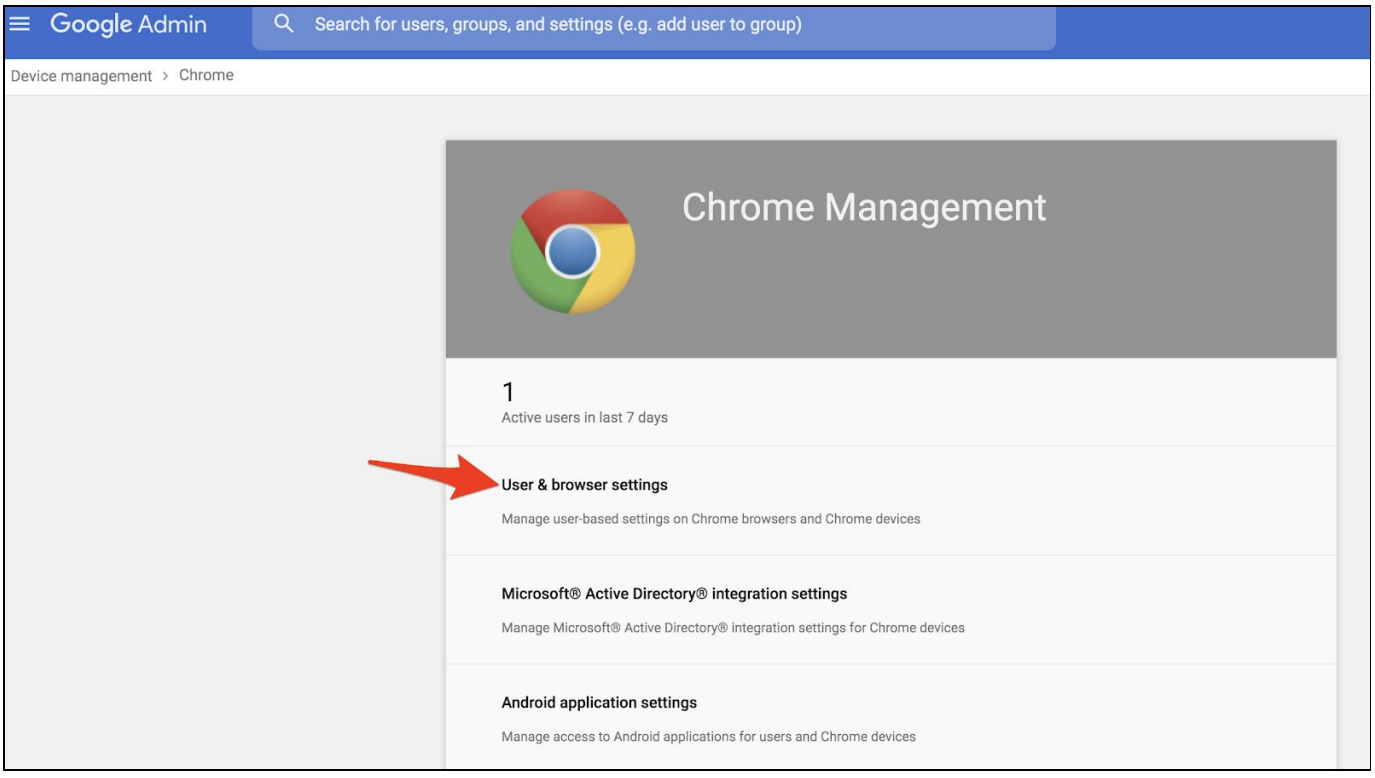
Setup begins by adding your GoGuardian extensions into Google Admin Console at admin.google.com. From your Google Admin Console homepage, click on **Device Management**:



Then, **Chrome Management** on the left:



Finally, click **User & browser settings**:



From the **User Settings** page, locate the **Organization** column on the left, and select the OU that you would like to install the GoGuardian extensions to. This OU should contain user accounts of the users you wish to filter and monitor in GoGuardian (ie., “Students” OU).

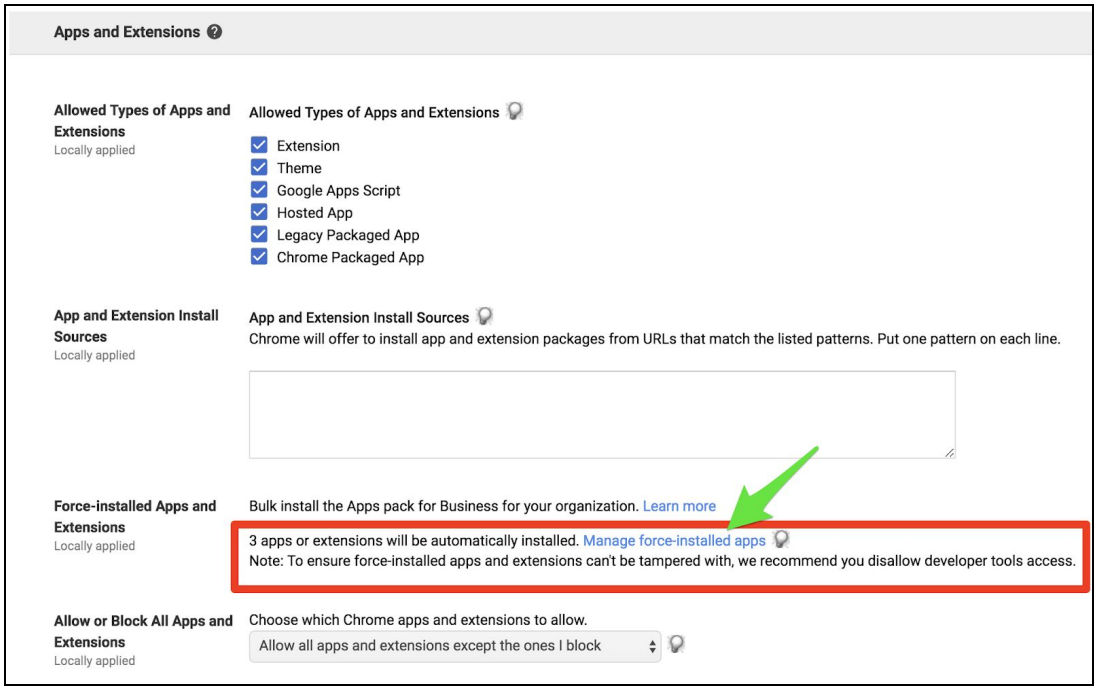
If you wish to monitor all users in the organization, including teachers and staff, you can highlight the domain-level (top-level) OU for your organization, to install the GoGuardian extensions to all users.

Keep in mind that installing the GoGuardian extensions on teachers' and staff accounts is unrelated to their access to GoGuardian products. To manage users' product access, visit manage.goguardian.com and log in with your Super User account.

***NOTE**: If you need assistance with creating additional OUs to house your student accounts, this Google article may prove useful: Create Additional OUs

The Google Admin Console has recently made a few changes to their look and layout, so both the older and newer look will be referenced below.

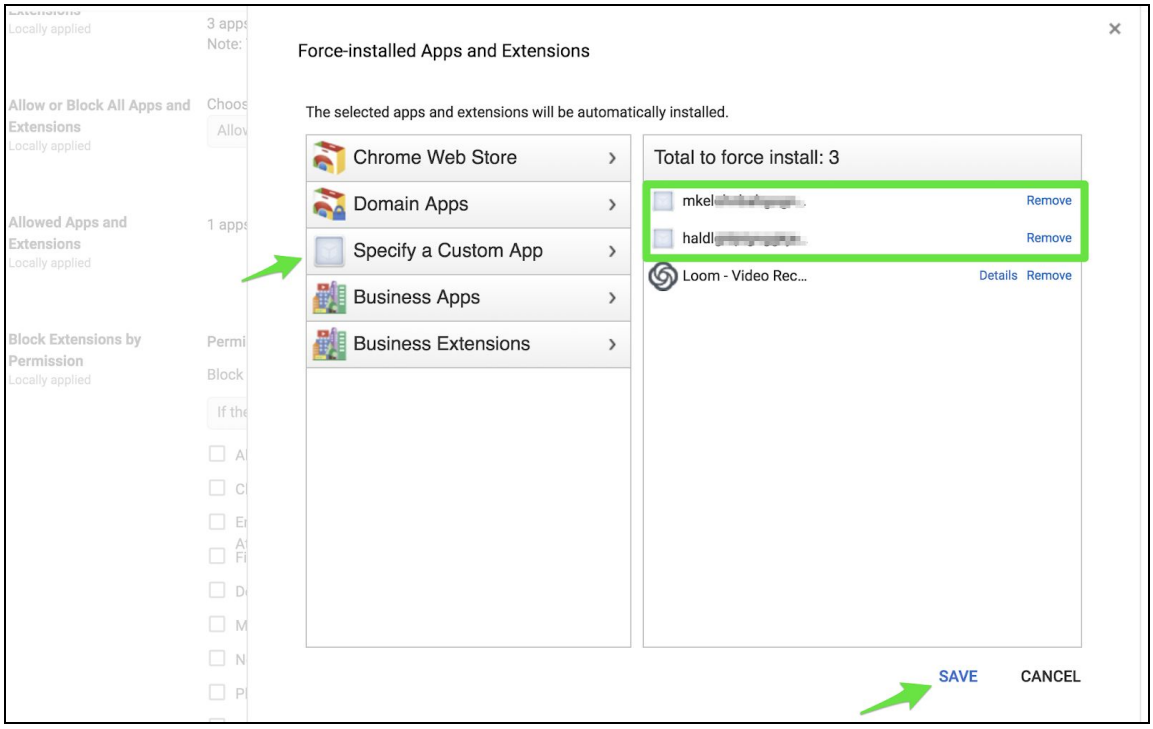
Installing Admin Extensions (**Legacy Google Admin Console UI**)



By clicking **Manage force-installed apps,** you can apply your organization's GoGuardian extensions. Your GoGuardian extensions can be copied and pasted from this page:

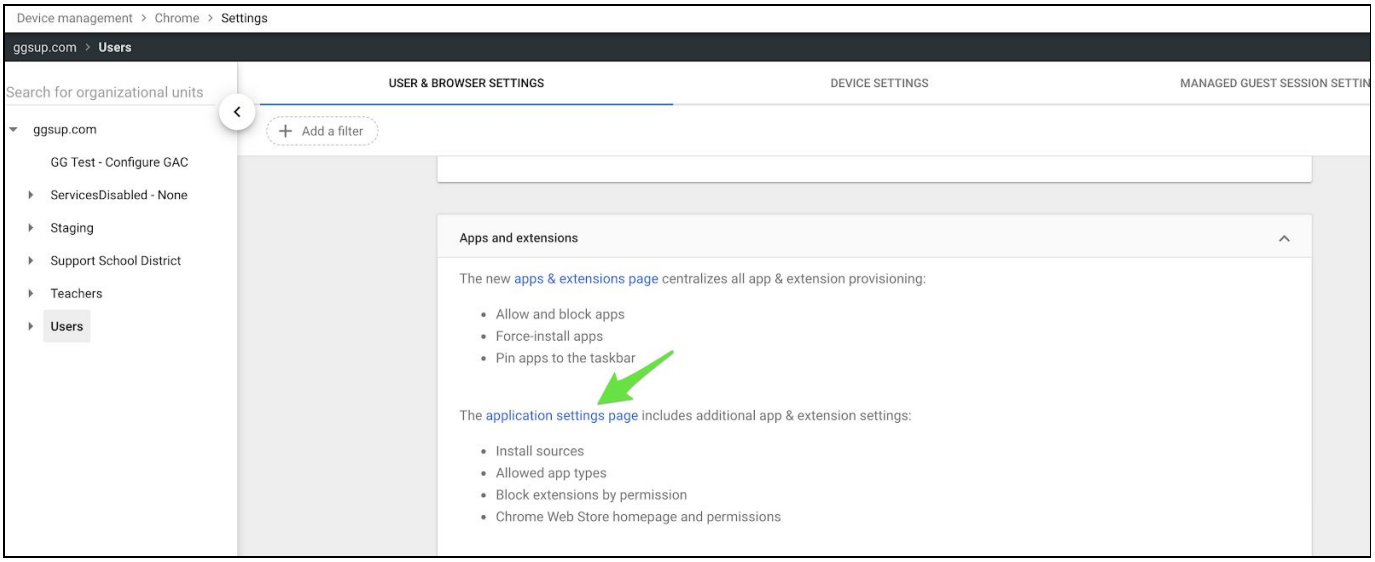
https://account.goguardian.com/#/getting-started/deploy

After copying and pasting your GoGuardian extension IDs and URLs, click the “Save” button at the bottom right of the pop-up window.

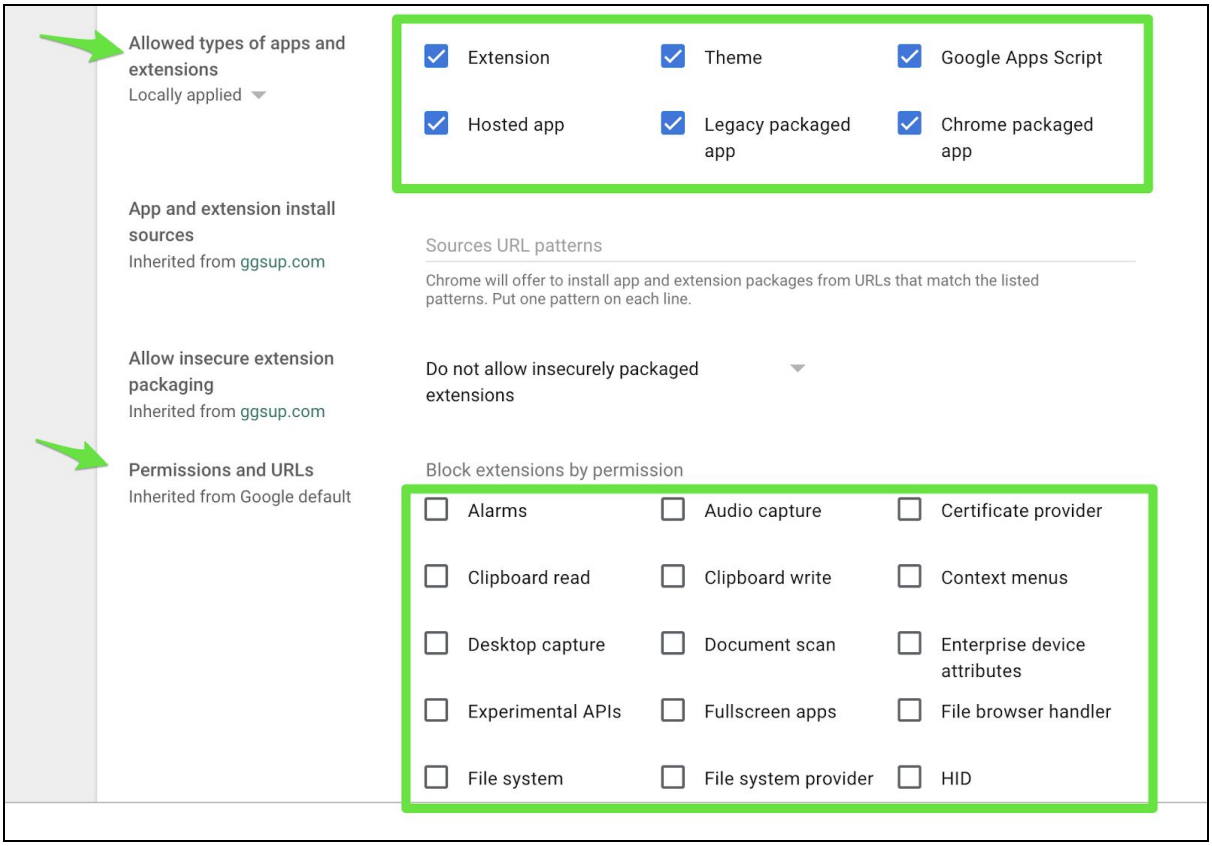


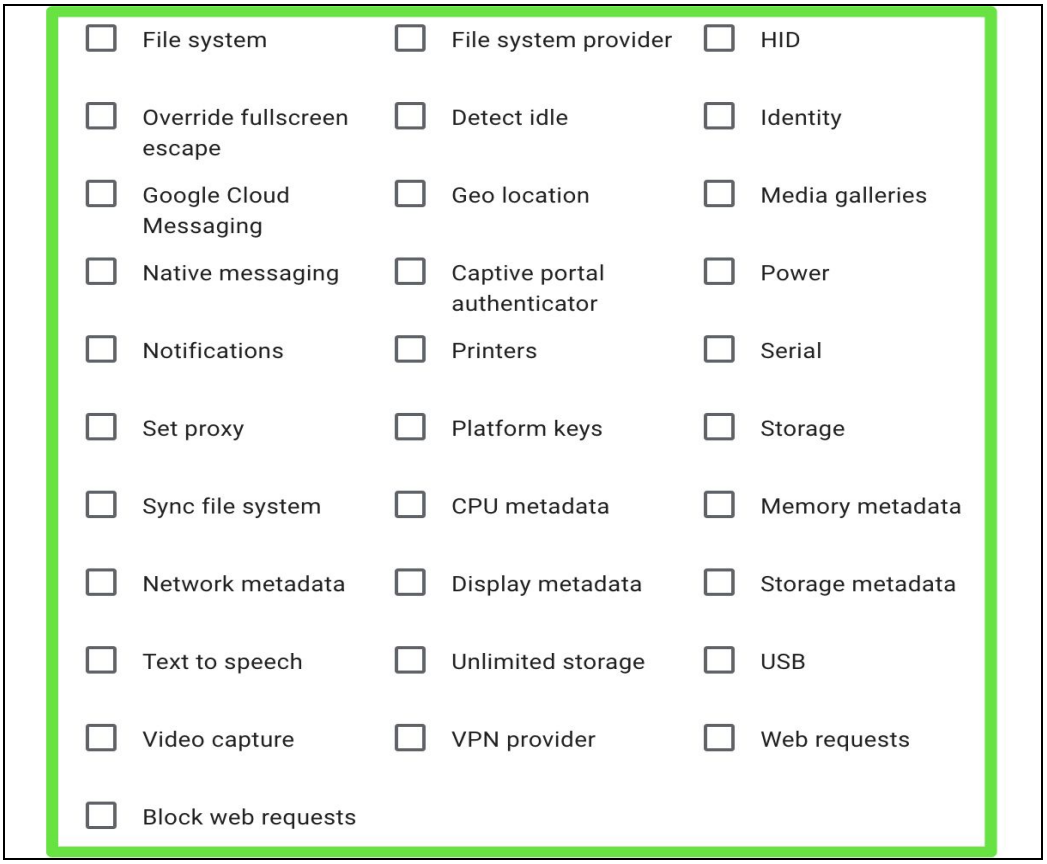
Installing Admin Extensions (**New Google Admin Console UI**)

Before installing extensions (or if extensions were installed and both aren’t deploying as expected), it would be highly recommended to check your Application Settings Page.



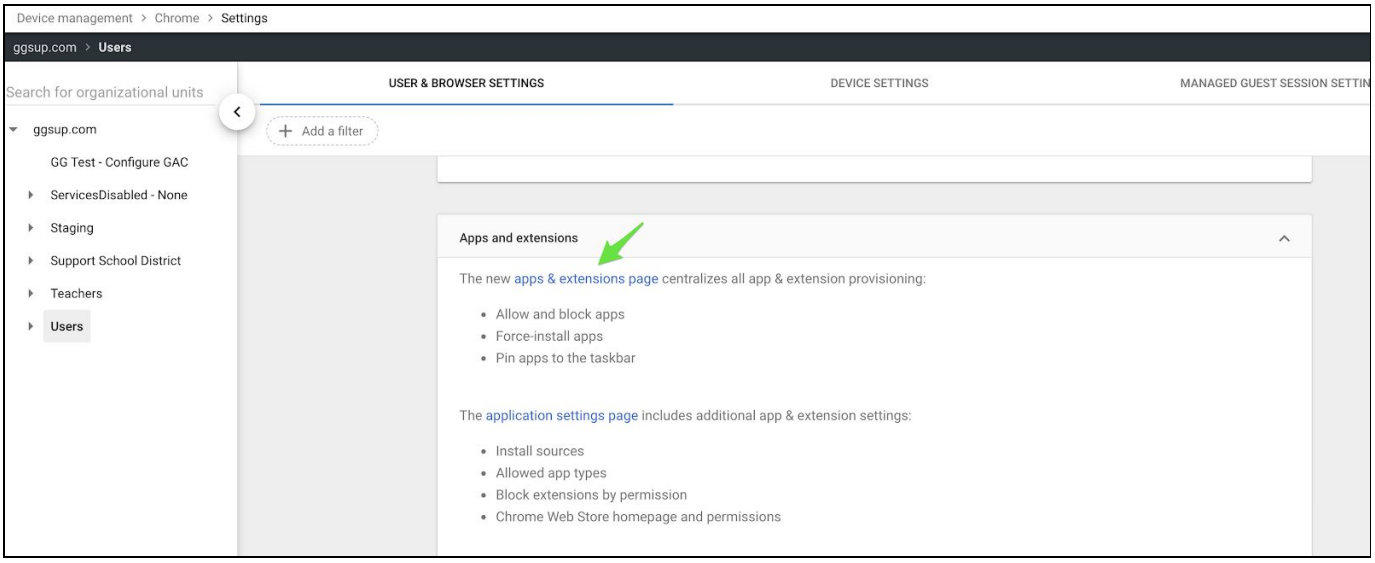
All types of apps and extensions should be allowed, and it would be recommended to leave all Permissions and URLs unchecked if possible (Note: If multiple checkboxes are checked for your Permissions and URLs, you may need to remove them and save changes one at a time in order for your changes to update as desired).

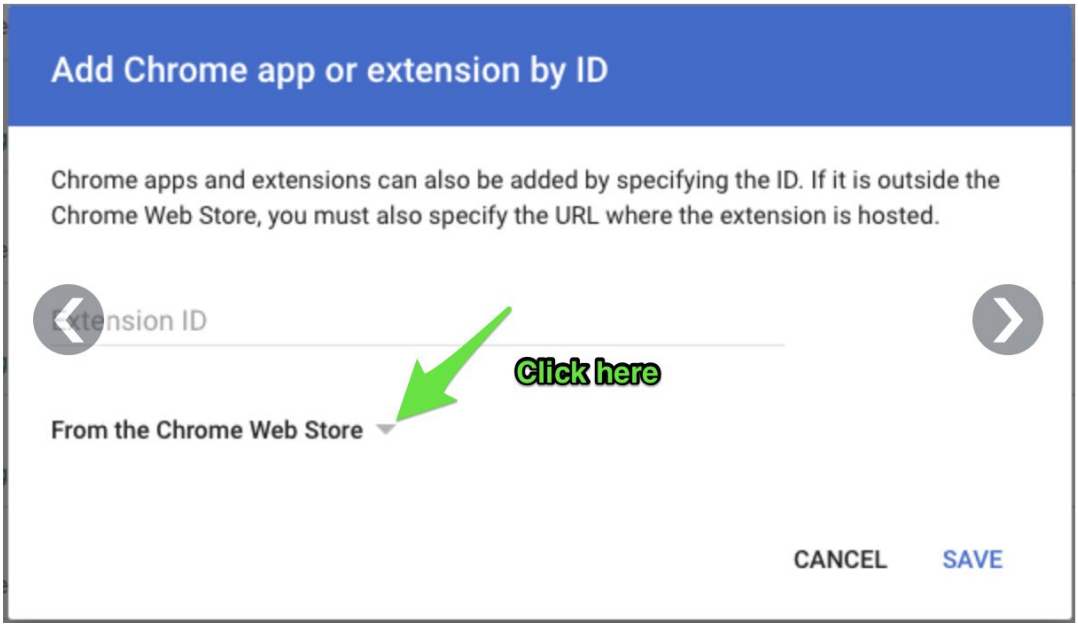


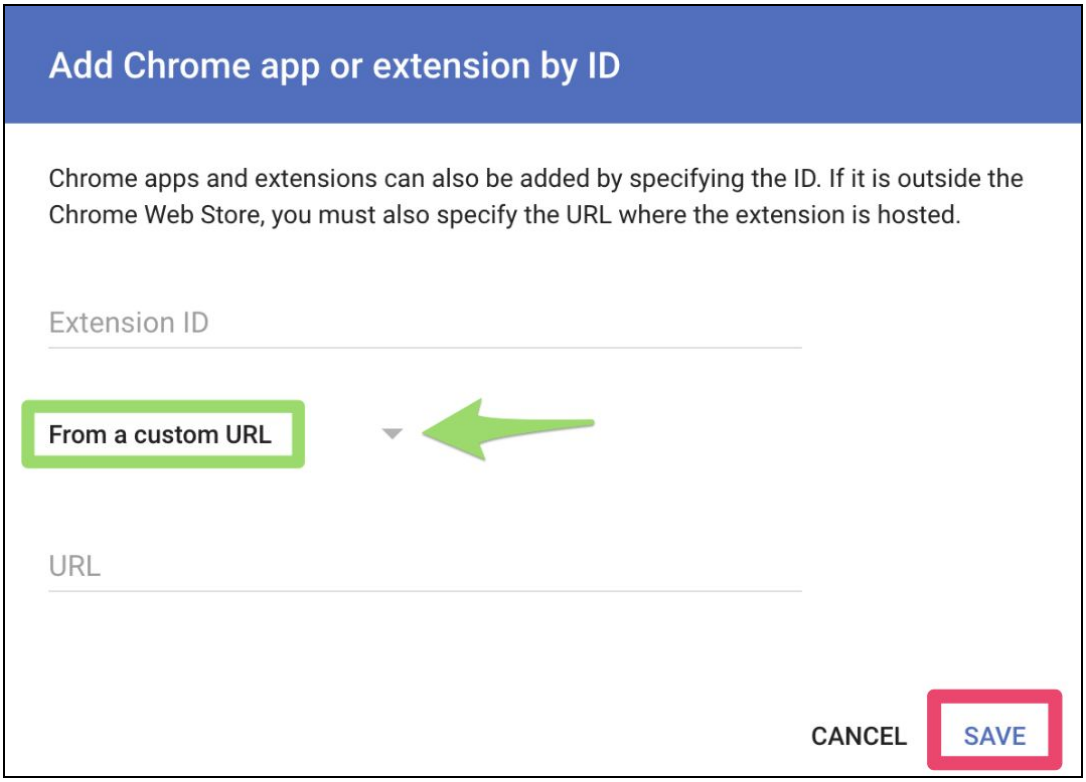


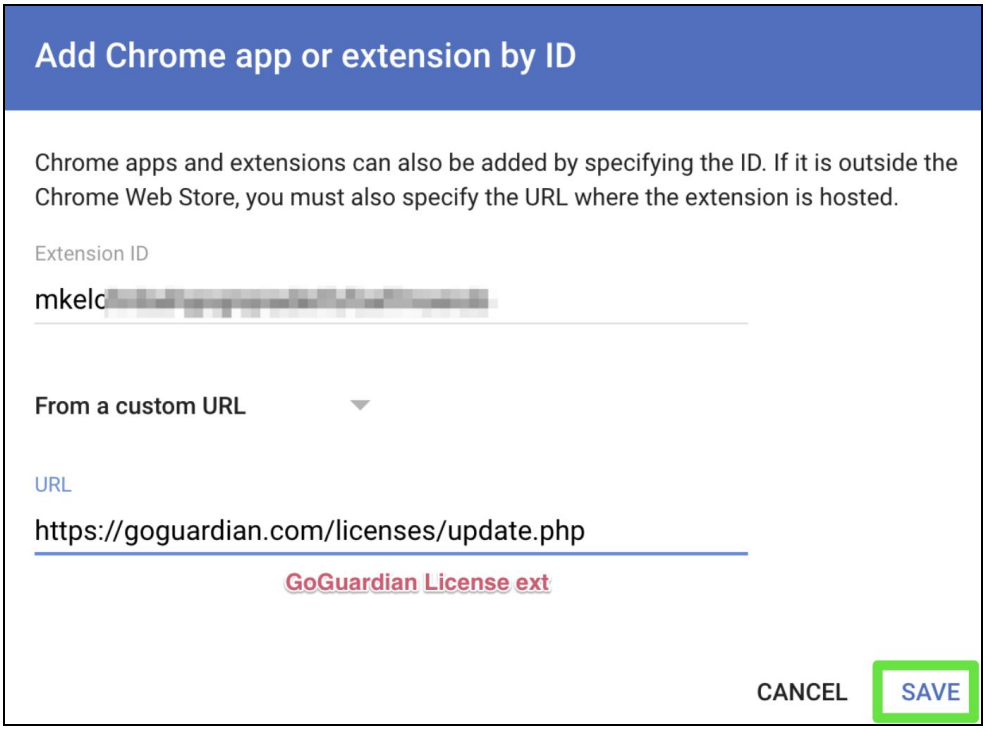
Once your application settings are configured, you can navigate back to your apps & extensions page and select the OU that you would like the GoGuardian extensions to apply to.

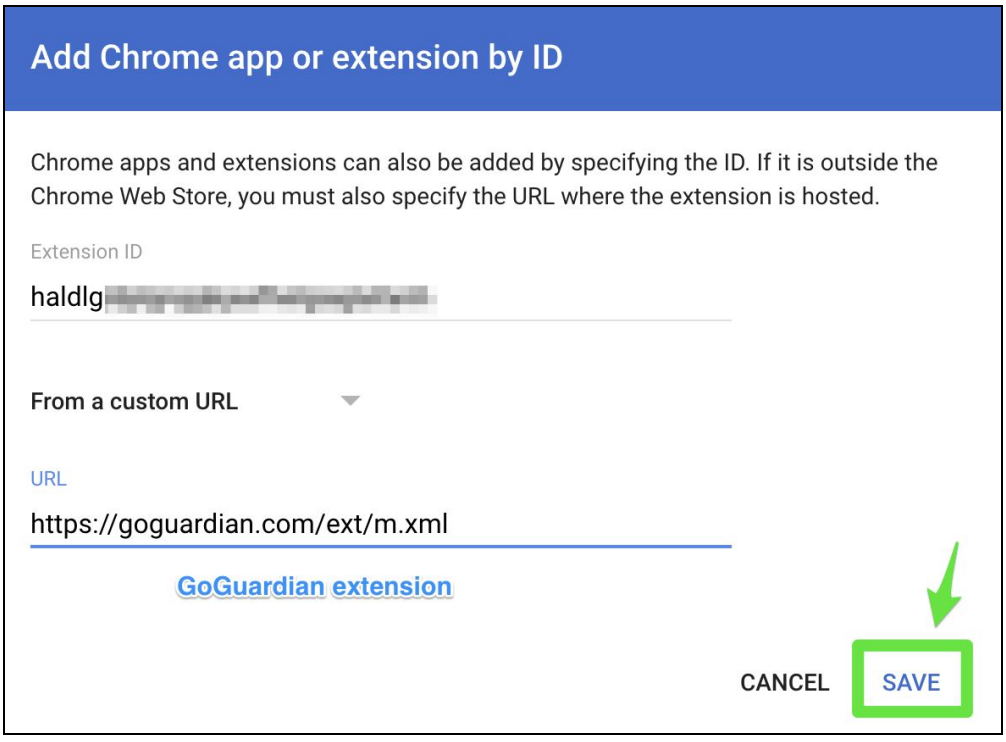
Note: If GoGuardian's extensions are not meant to apply to all staff and students, it is highly recommended that another OU be created for the student accounts. Then, that OU can be selected for the GoGuardian extension force-installation.




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
Click here
From the Chrome Web Store
CANCEL
SAVE

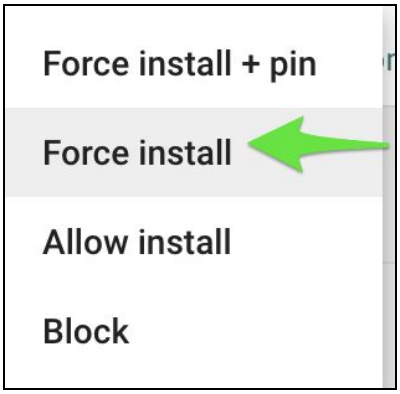

Add Chrome app or extension by ID
Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.
Extension ID
From a custom URL
URL
CANCEL
SAVE



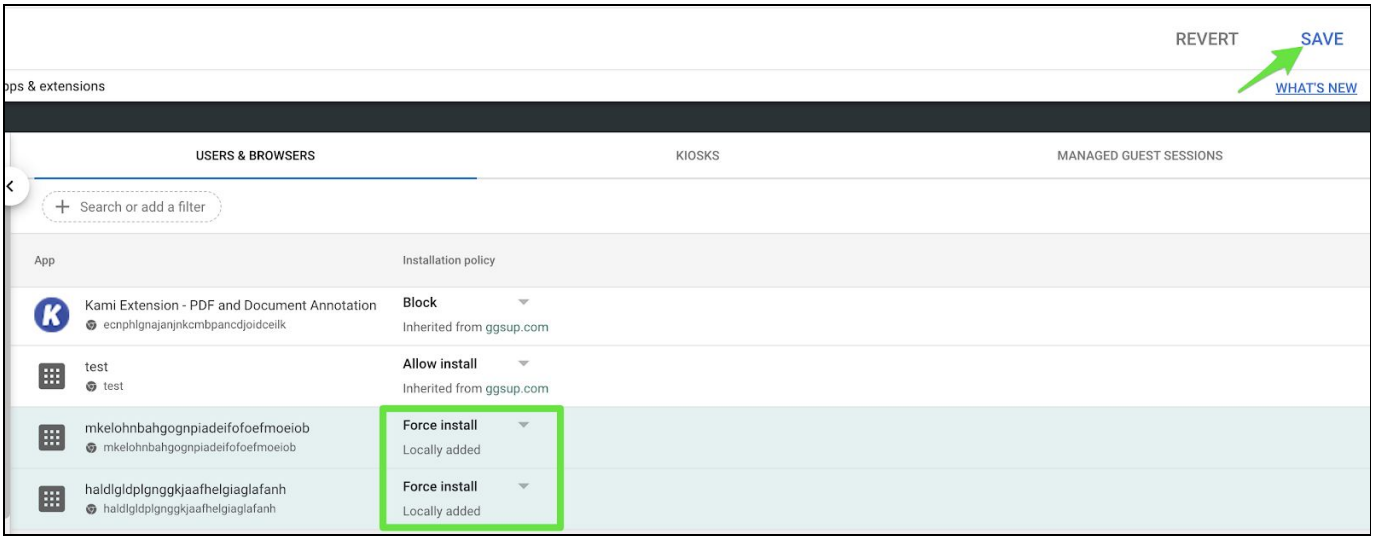


After adding the first extension ID and URL, click the save button in the bottom-right of the pop-up window to save this extension to your OU. After saving, you can add the second extension ID and URL, and save.

Once your GoGuardian extensions have been added and saved, click the dropdown arrow next to first extension and choose ‘Force install’. Then, do the same for the second one.



After selecting **Force install** for both, don't forget to save this change by clicking **Save** at the top-right of the screen.

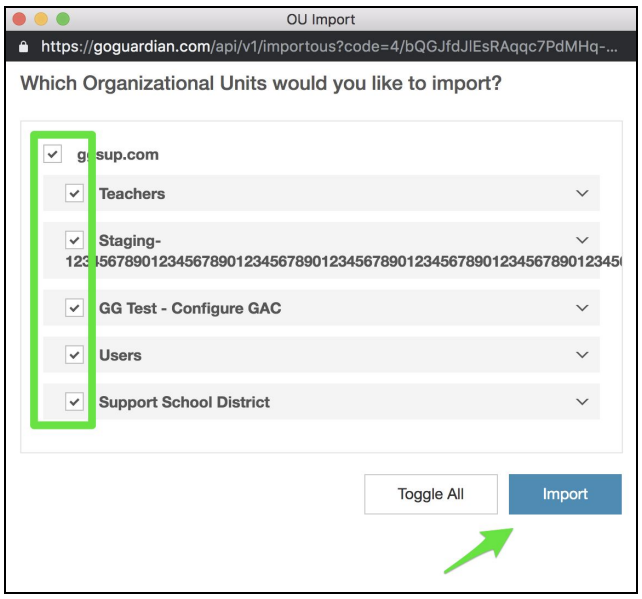


If you would like additional step-by-step recommendations on configuring your User and Device Settings in the Google Admin Console please refer to the links below before moving on:

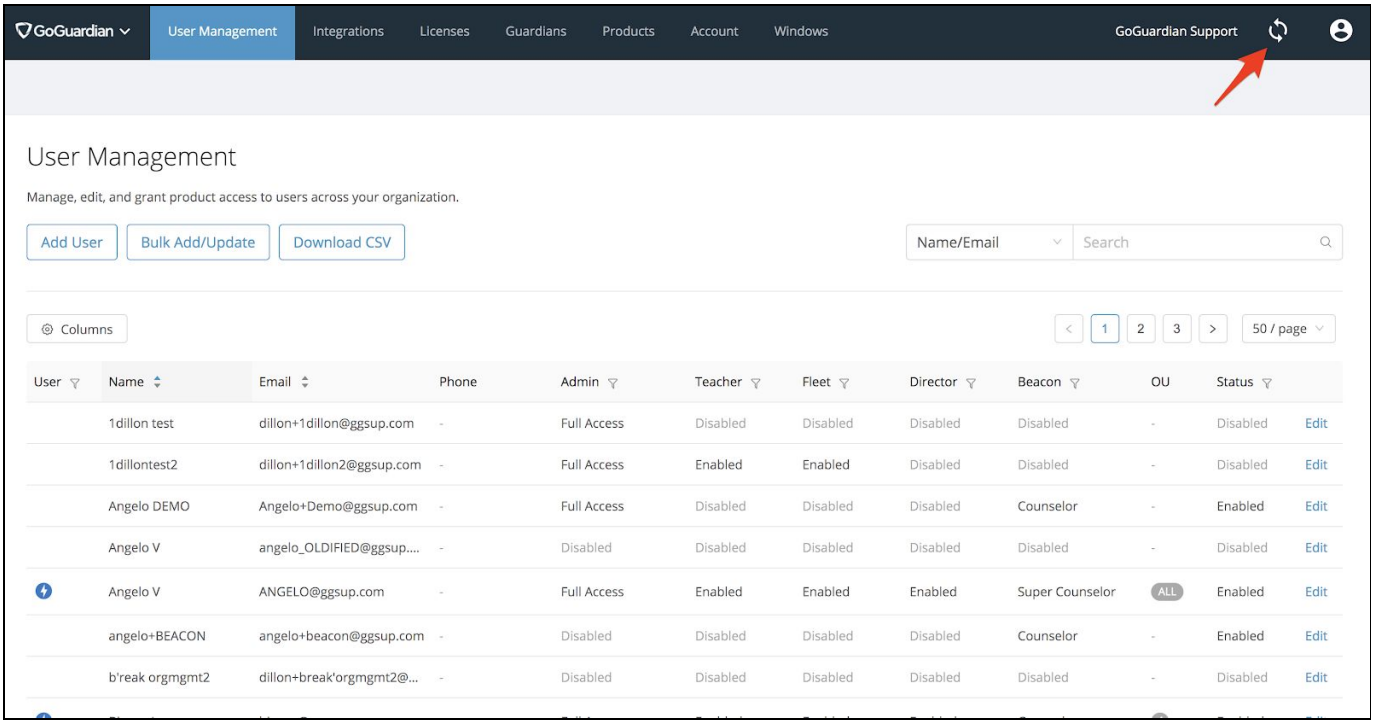
- Installing GoGuardian Admin
- Google Admin Console Best Practices

Your next step will be to manually import your OUs into GoGuardian. You can import OUs in the GoGuardian Admin Classic View (also known as Admin 1.0) by clicking here:

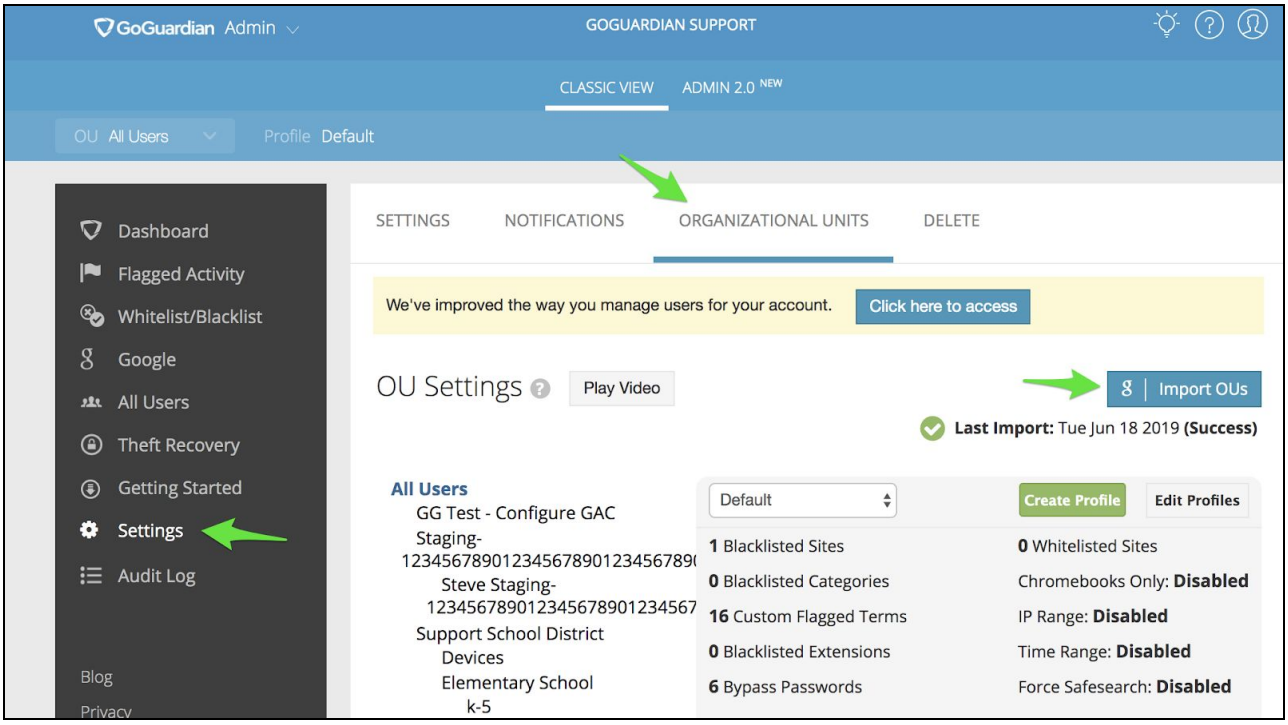
(***Note**: this step is how GoGuardian Admin is able to mirror the OU structure from your Google Admin Console. Whichever OUs you would like for GoGuardian to index your users into nightly will need to be selected when importing).



You can manually import your OUs in Org Management at **manage.goguardian.com**, by clicking the circular arrow icon in the top right.

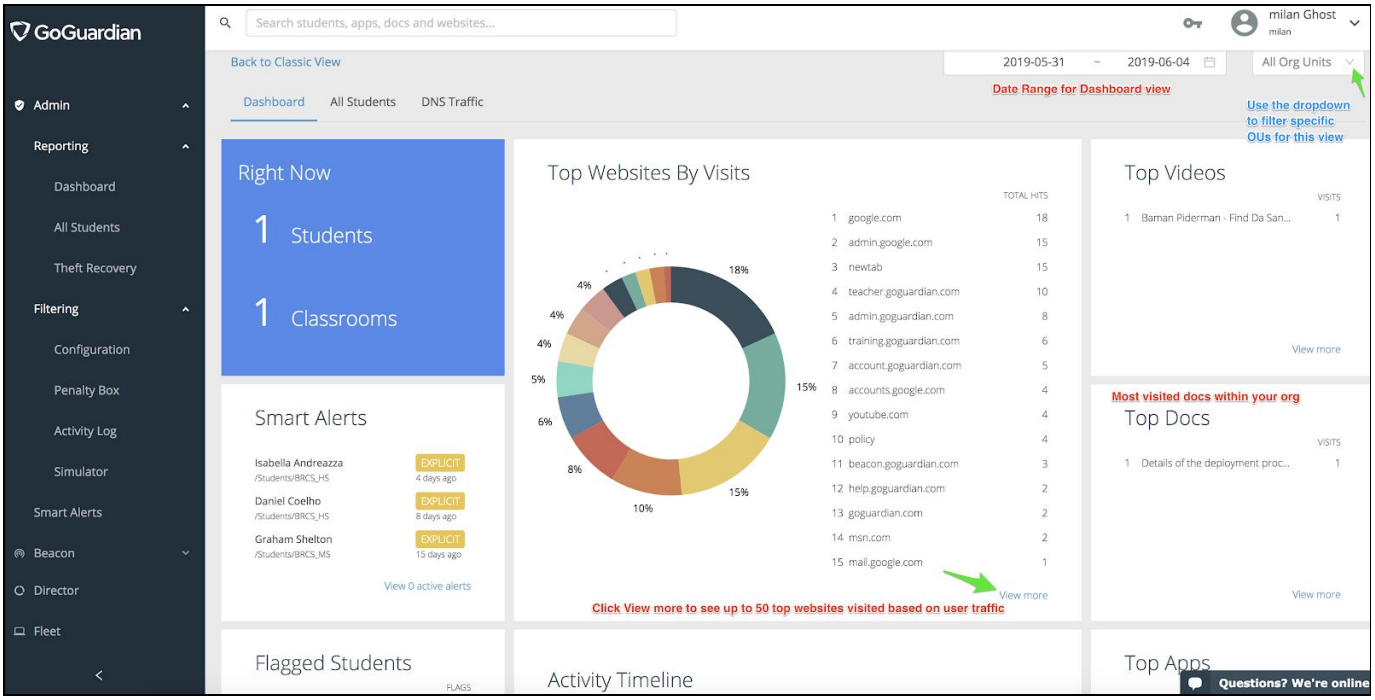


You can also import OUs manually from the Admin Classic View page at:
https://goguardian.com/account/settings/OU



***Note:** Although the nightly automatic sync will pull information on all OUs that GoGuardian is currently aware of, it will not pull data for newer OUs that have not been imported from the Google Admin Console. Therefore, if any significant changes are made (such as changing the name of a pre-existing OU or creating a brand new OU), another manual OU import is required to pull the updated data from your Google Admin Console into GoGuardian.

Dashboard



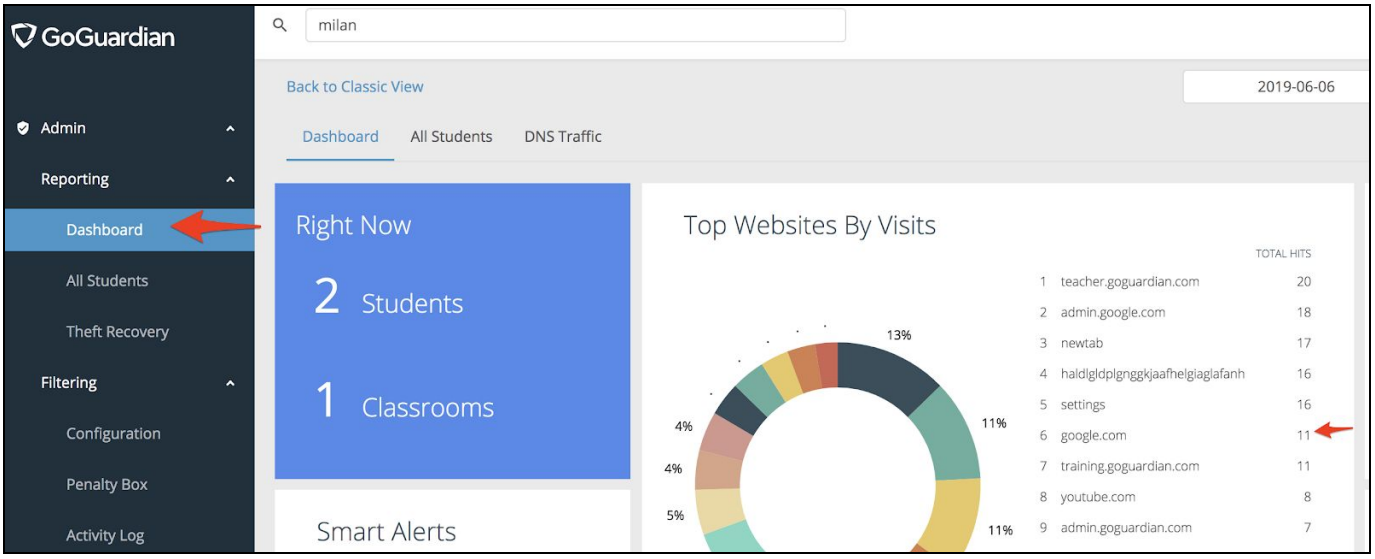
From the **Dashboard**, you can see a bird's-eye view of your organization's activity (which can also be filtered down to a single organization unit or **OU**). You can also view the top 50 most visited websites for your organization, the top 50 Google docs, a quick glance of recent Smart Alerts, Most Flagged Students, an overall Flagged Activity Timeline, the top 50 apps used by your org, and the number of students and classrooms currently online.

***Note**: If you're using the newer Admin 2.0, and would like to access Admin 1.0 for any reason, you can do so from this view by clicking the Back to Classic View link (just under the Global search bar at the top left corner of the dashboard).

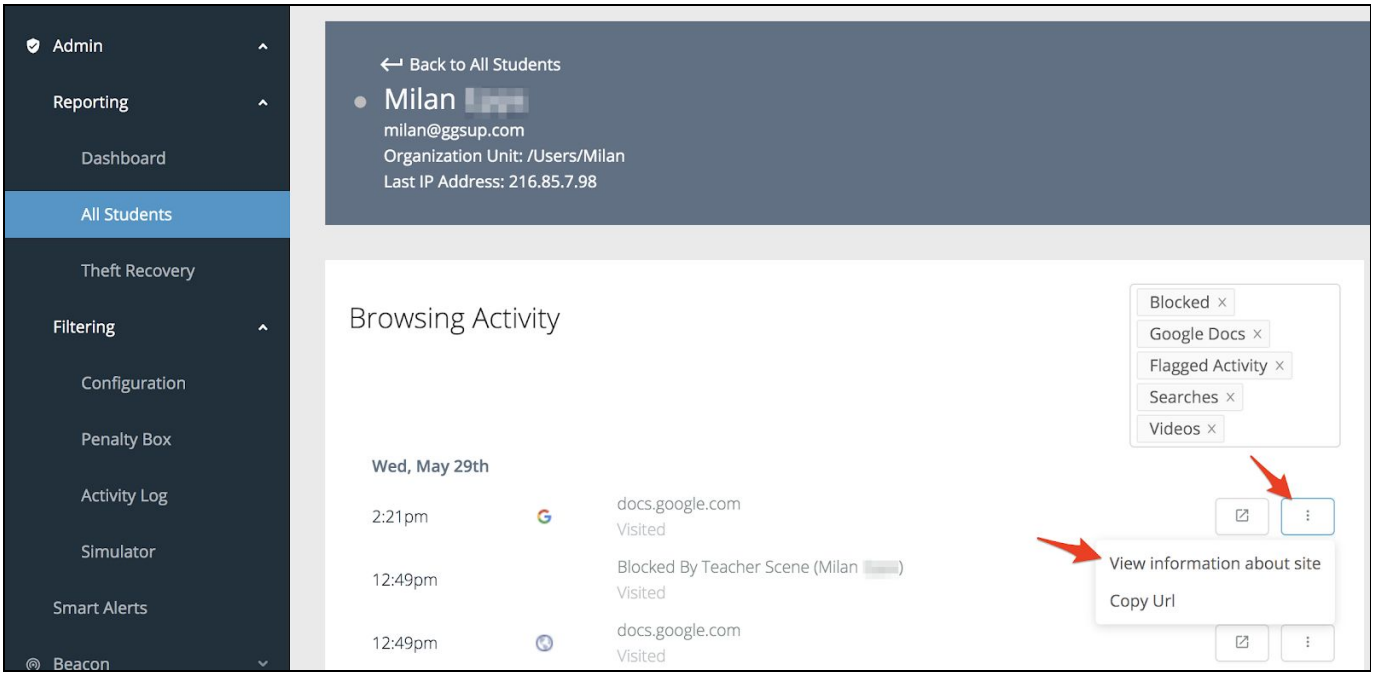
Site Information

There are two ways to see additional information about sites that users are visiting.
NOTE: *Admin currently offers domain-level reporting, not specific page-level reporting.*

1. **Dashboard View**: From this view, you can click directly on a site to see additional information about it (including the URL, the number of visits, top users, and recent activity) across a specified date range.



2. **Student Browsing Activity**: When looking at an individual user's browsing activity, you can access the View information about site option to view this page as well.



Configuration

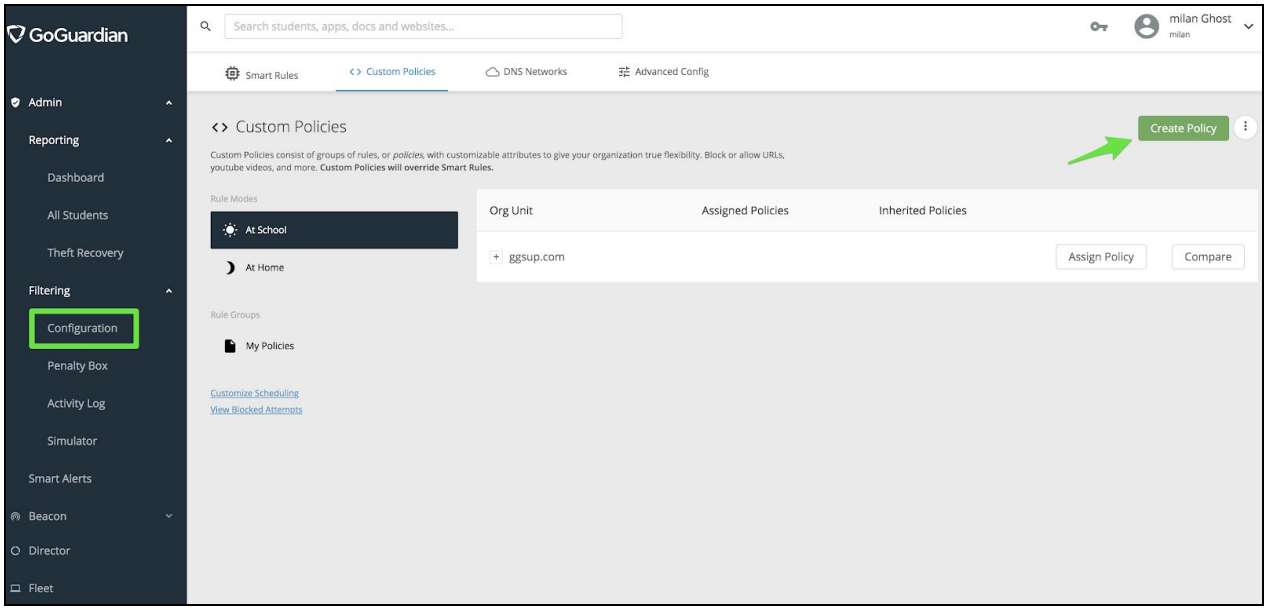
Creating a Policy

Policies can be created in one of two ways:

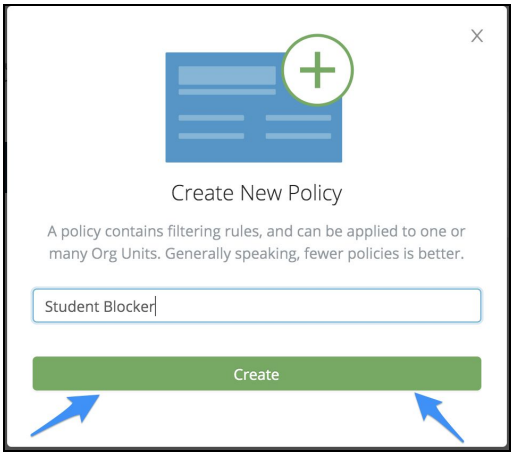
- **Creating a brand new Policy from scratch**
- **Duplicating a pre-existing Policy and renaming it**

Creating a New Policy

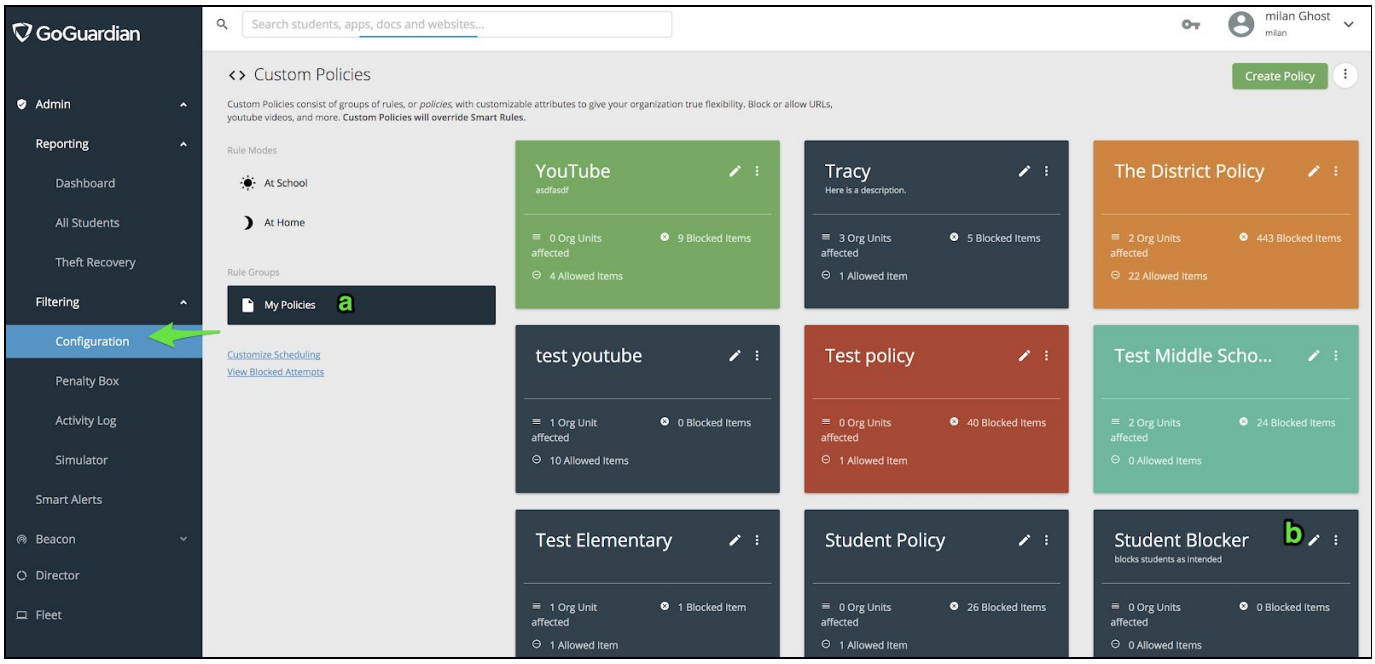
1. Click the **Configuration** link in the left navigation bar
2. Click Create Policy at the top right corner of the screen.



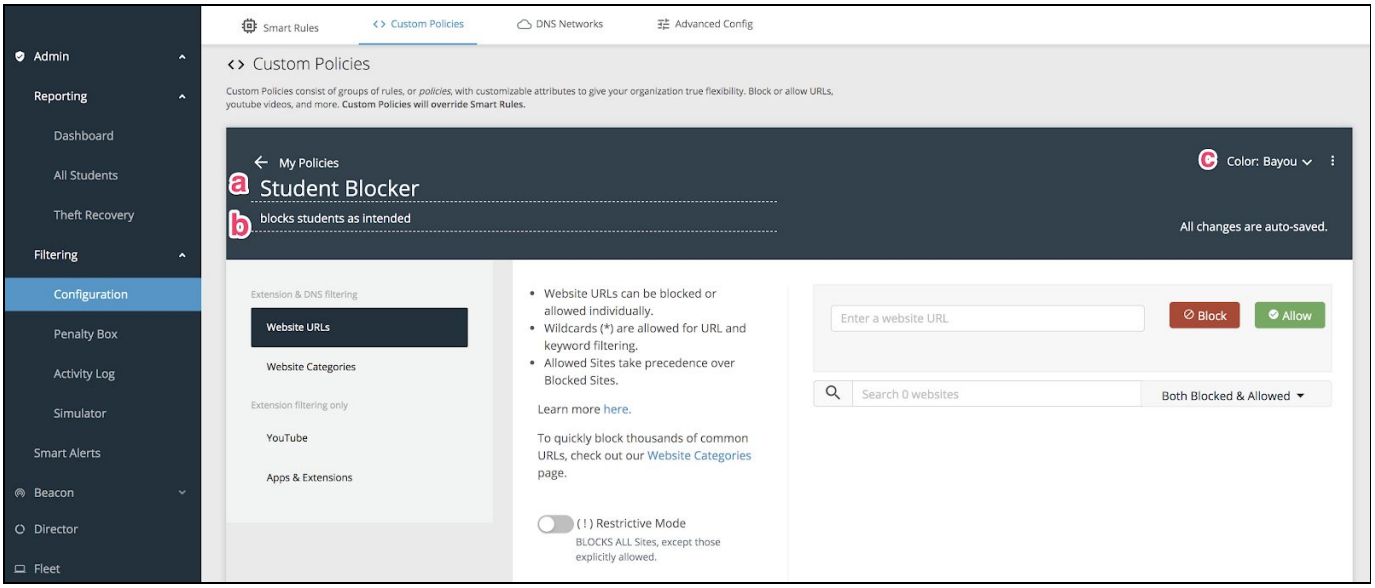
3. Enter a name for the Policy and click the **Create** button.



4. Click **My Policies** and find your Policy.
5. Click the pencil icon on the upper right corner of the card to edit the Policy.



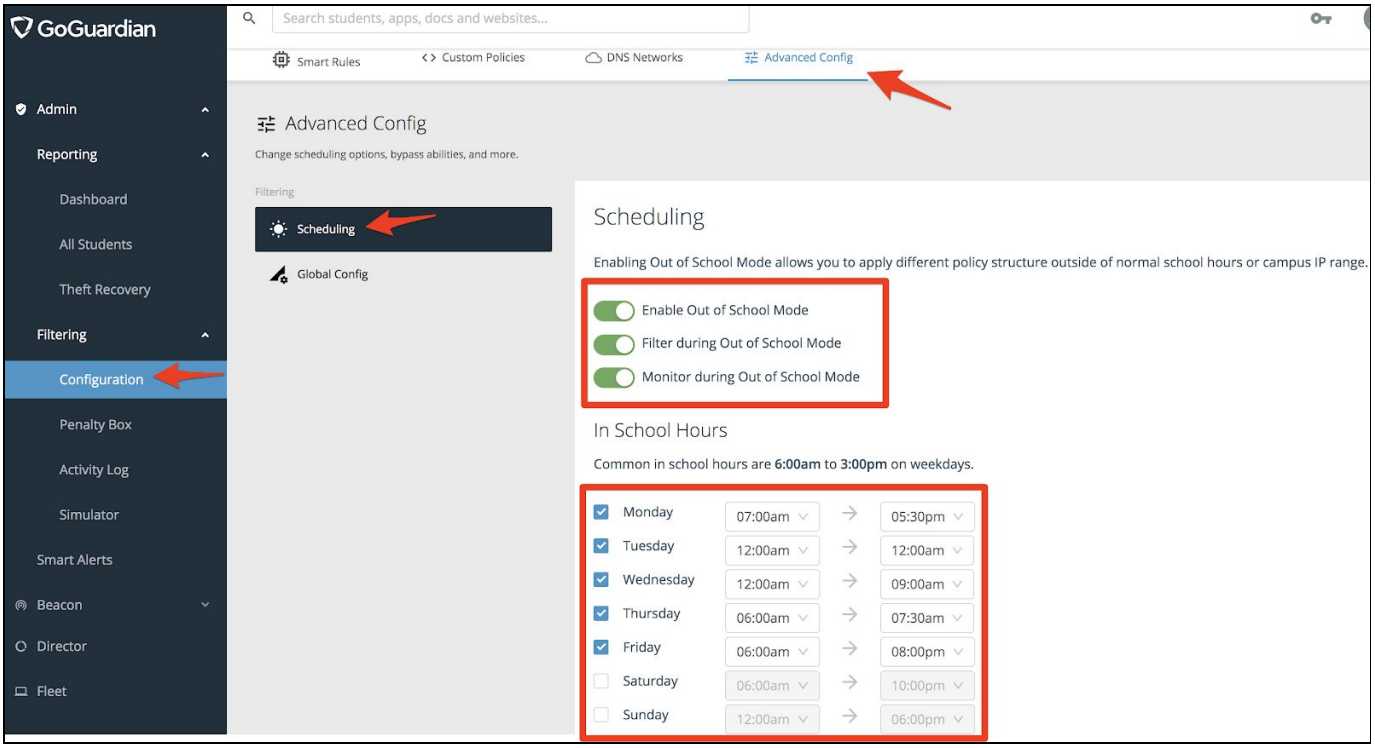
6. Edit the appearance of the Policy *(optional)*
   a. The **name** can be edited here by clicking into the name of your Policy and typing.
   b. A **description** can be added just below the Policy name if desired.
   c. The **color** of the Policy can also be changed by clicking the dropdown arrow next to the word Color.



7. Add preferred Blocked or Allowed Sites for your Policy (Note: Although, you can add as many site URLs as you'd like, if you plan to add an extensive number of blocked websites, it may be easier to set your Policy to "Restrictive Mode" and only add the websites that users should be allowed to access).

**Any changes made to a Policy may take up to 20 minutes to propagate across all user accounts. If a new site is allowed or blocked in a Policy, you may not see it take effect immediately.*

Out of School Mode



With Out of School Mode, you can set filtering and monitoring for your organization based on time and location.

Filter/Monitor by Time

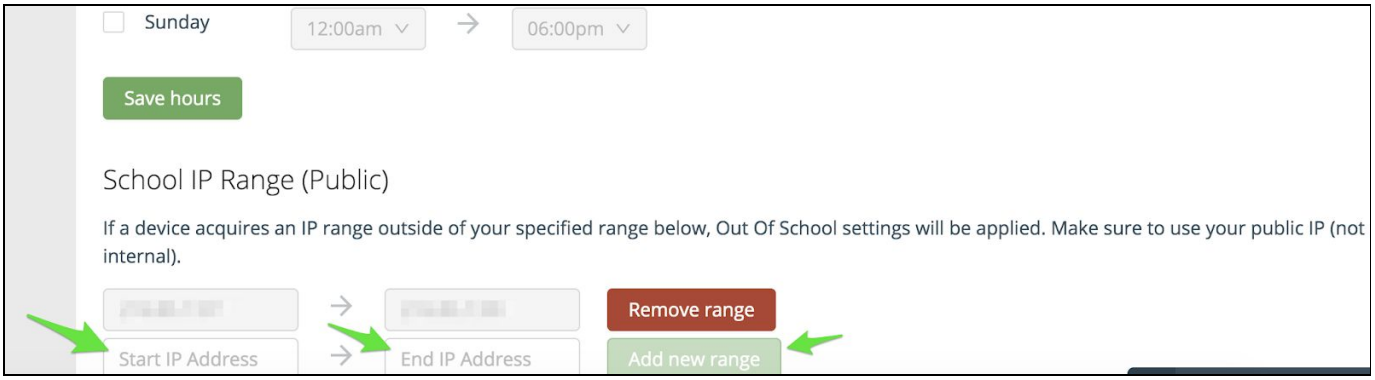
To set filtering and monitoring by time, the Enable Out of School Mode option must be toggled on (green). Once that is done, you have the option of either only filtering (necessary for controlling which sites students can access), only monitoring (necessary to see browsing history), or continuing to both filter and monitor. Then, set the hours and days for your normal filtering/monitoring to apply under *In School Hours.*

***Note:** If Filtering is enabled, but Monitoring is disabled, Smart Alerts will still block sites that trigger the alert, but screenshots will not be taken for what triggered the Smart Alert block.

Filter/Monitor by Location

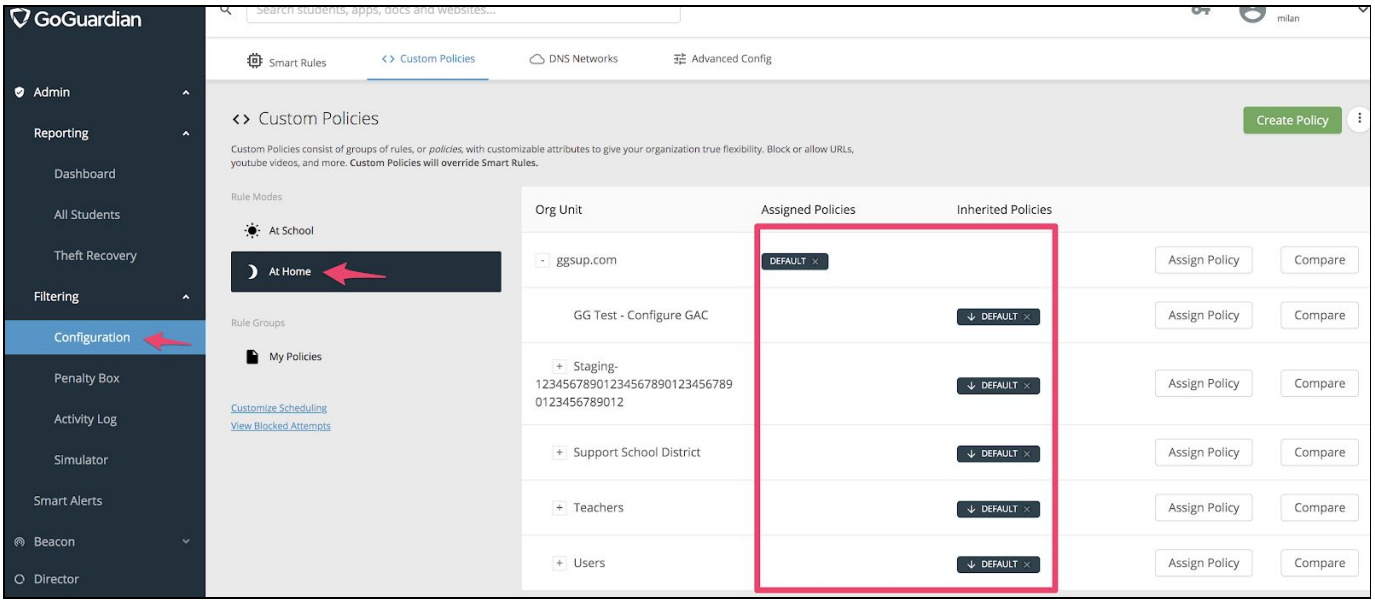
To filter/monitor users based on location, you can set the public IP range of your school. Anyone outside of this IP range will be subject to your organization's Out of School settings.

***Note:** School hours must be entered to enforce Out of School Mode based on IP Range. If times are not specified, the entire day will be in Out of School mode.



***Note:** If you do not need to use Out of School Mode based on location, we would recommend not setting an IP Range here.

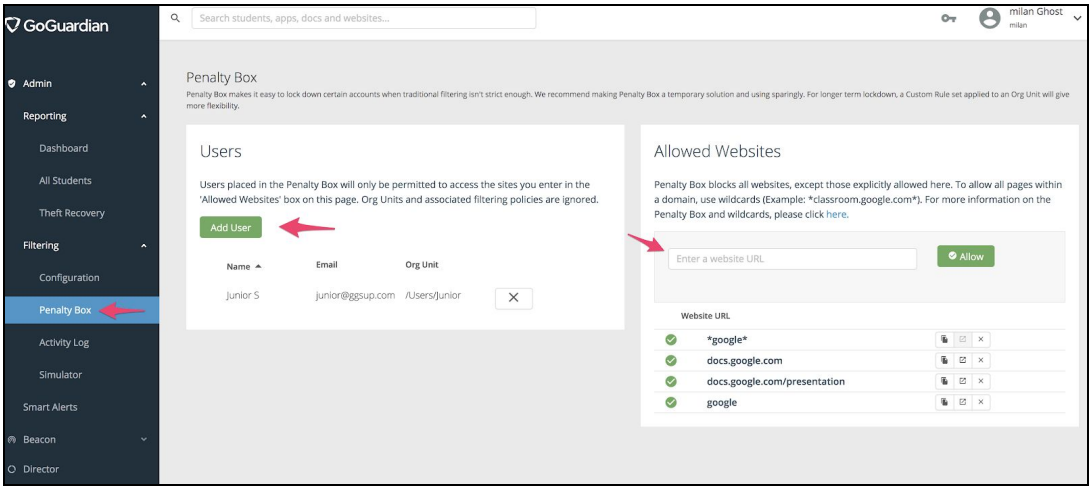
After configuring your settings for Out of School Mode, you can navigate back to *Configuration* > *At Home* (or you can click *here*), and assign Policies that will apply the desired restrictions/allowances to your OUs when Out of School Mode is activated for a user.



For more information on Out of School Mode, please click *here.*

Penalty Box

The Penalty Box allows an administrator to restrict an individual student's browsing. By clicking the Add User button and entering either the student's name or email, a student can be entered into the Penalty Box; where all sites except for the Allowed Websites will be inaccessible to that student.

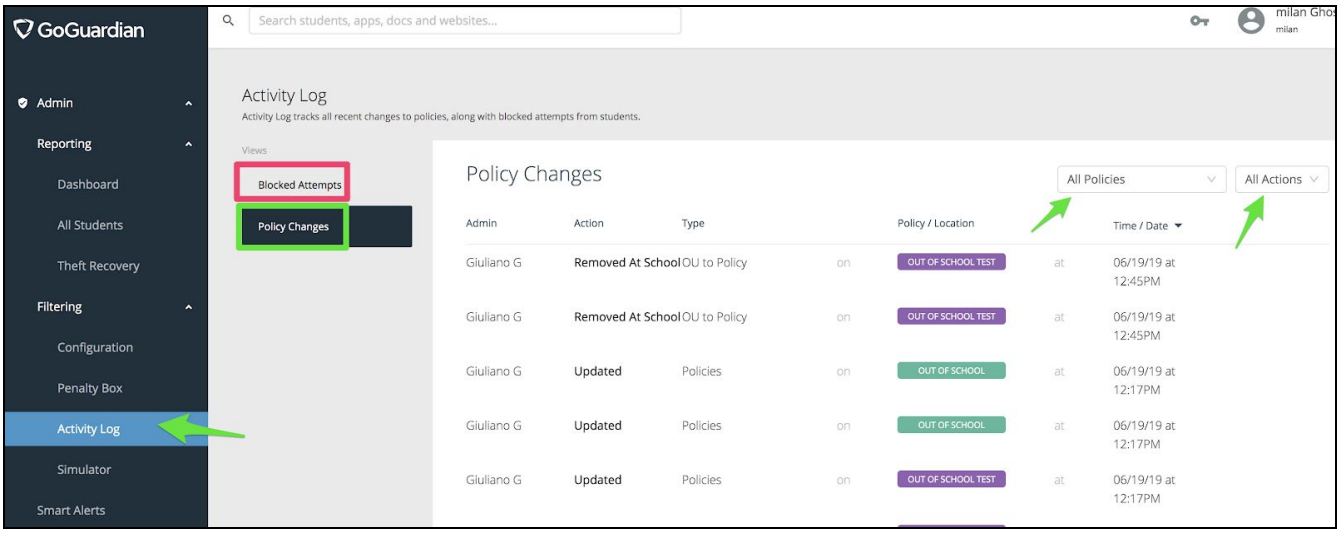


*Note: Although other sites can be entered as allowances for the Penalty Box, access to YouTube is not possible for users entered into the Penalty Box.

For more information on the Penalty Box, please click *here*.

Activity Log

The Activity Log allows you to view any recent changes to Policies or Blocked Attempts for your organization.



Policy Changes

By Default, this is set to All Policies (allowing you to see the most recent changes to all of your Policies). You can filter which Policy you would like to view recent changes from by clicking the dropdown arrow in the upper-right corner of the screen and changing the setting from 'All Policies' to whichever Policy you would like to view changes for.

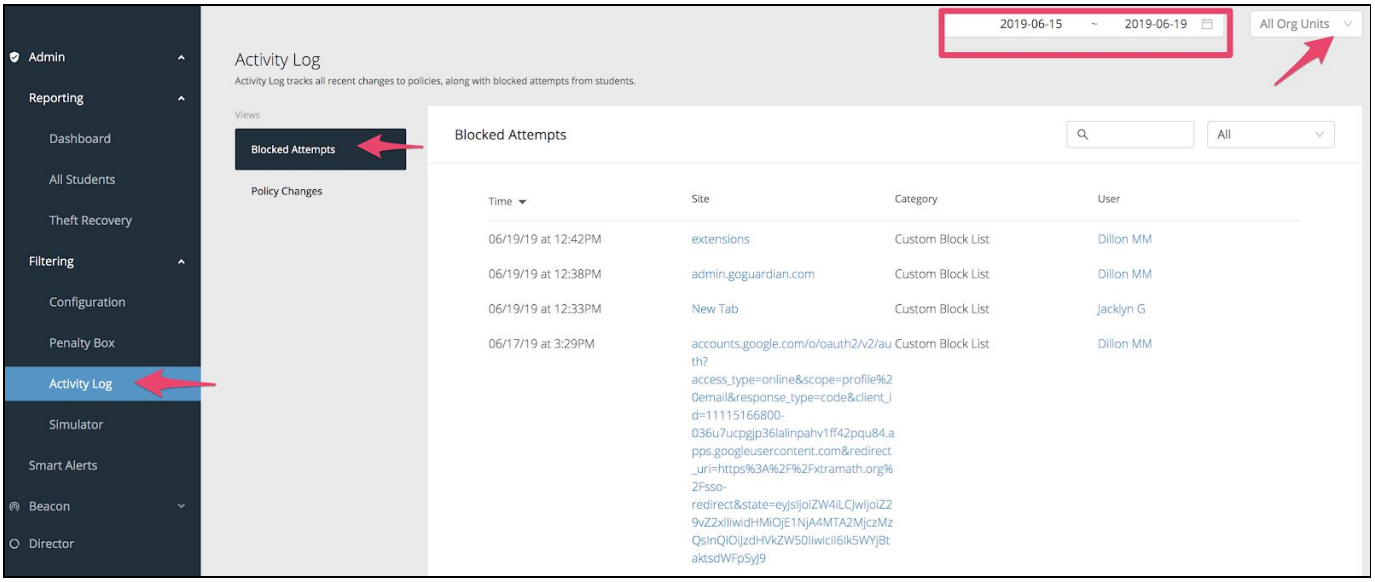
The setting to the far upper-right is set to All Actions by default. But this can also be changed to only show Added, Removed, Updated, Enabled, Disabled, Duplicated, or Bulk Added changes to Policies.

Blocked Attempts

Blocked attempts will show the most recent blocks users have experienced. The following information can be found in the corresponding fields:

- **Time**: When the block occurred
- **Site**: The exact URL responsible for the block
- **Category**:The category of the block

  **Note: Custom Block List generally points to a Policy block. To gain additional information, click on the user's name in the User field and look through the user's browsing history*

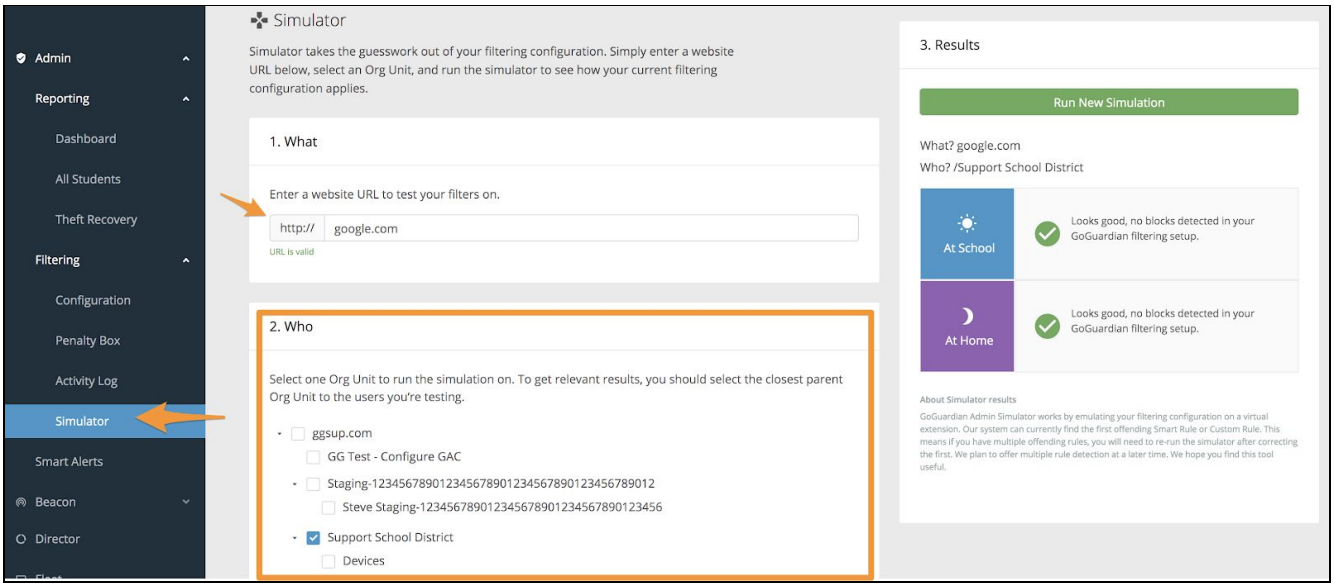


At the top corner of the screen, you'll find the date range for blocked attempts. This field can be adjusted to date back as far as ***six months ago*** (if your organization has used GoGuardian Admin for at least that long) and to show up to ***30 days of history at a time***.

In the far upper-right, you'll find that **All Org Units** is the default setting. However, this can also be adjusted to filter blocked attempt history for a specific OU by clicking the dropdown arrow.

Simulator

The simulator allows you to test how a Policy will apply to your OUs. You can enter a site URL that has been added to your Policy and test to see if it can be accessed.



***Note:** You may need to clear your device cache after adding a new URL to a Policy to see the result accurately reflected in the Simulator.

****Note**: Even if a site block or allowance is properly reflected in the Simulator, it can still take up to 20 minutes to take the desired effect on all user accounts.

For more information on the Simulator, please click *here.*

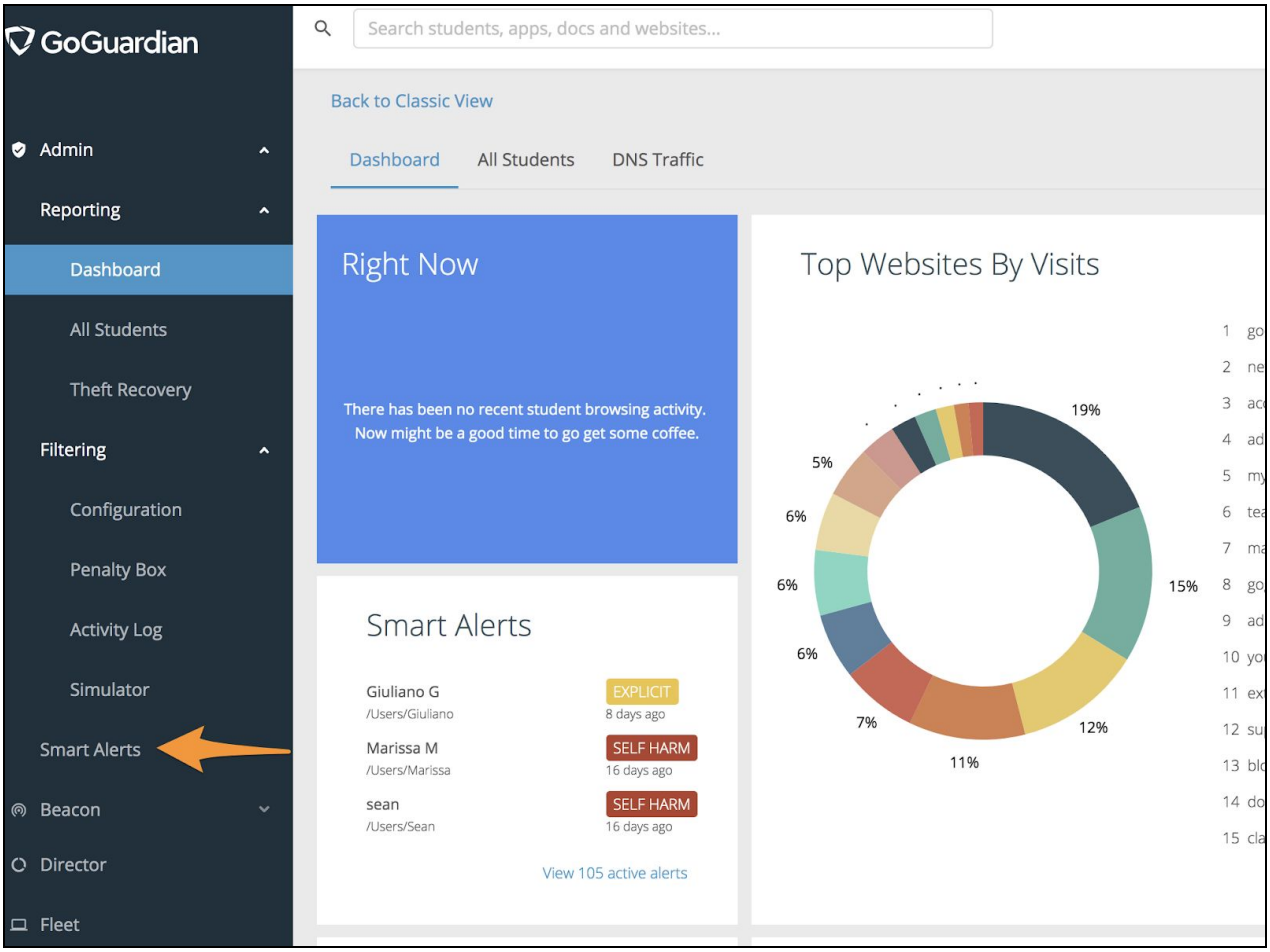
Smart Alerts

Smart Alerts are created when GoGuardian's proprietary algorithm determines that a page has explicit content based on the page's text content.

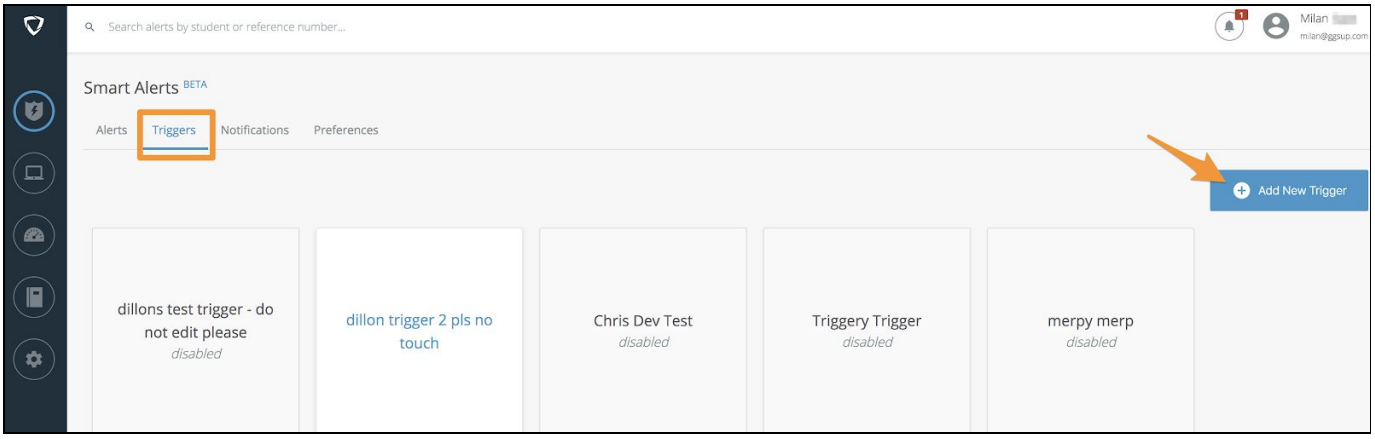
If you would like to take advantage of the features of GoGuardian Smart Alerts for your organization (notifying specific administrators of student activity, blocking access to explicit sites, or messaging students attempting to access undesirable sites) you can create a new **Trigger** and configure its settings from the **Triggers** tab.

Creating a Smart Alert Trigger

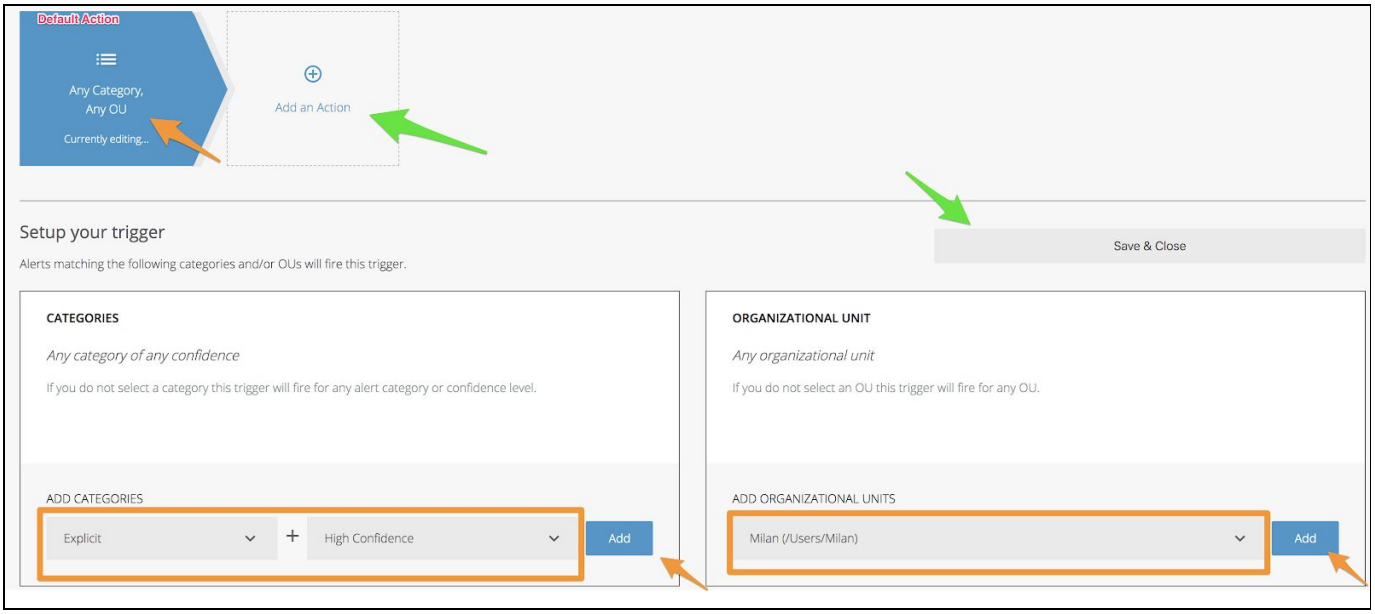
To create a Smart Alert Trigger, you can navigate to your Smart Alerts by clicking the Smart Alerts button in the left column.



Then, click the Triggers tab and the Add New Trigger button at the top left.



From here you can name your Trigger.

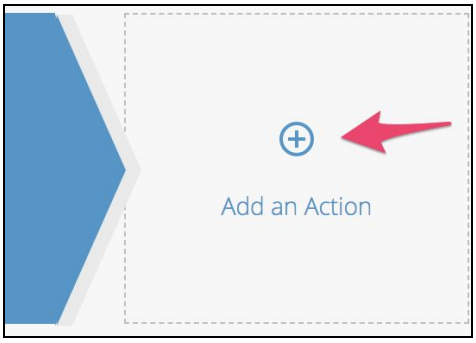


With the Default Action tile selected, you can select the Category and the Confidence level for your Smart Alert Trigger.

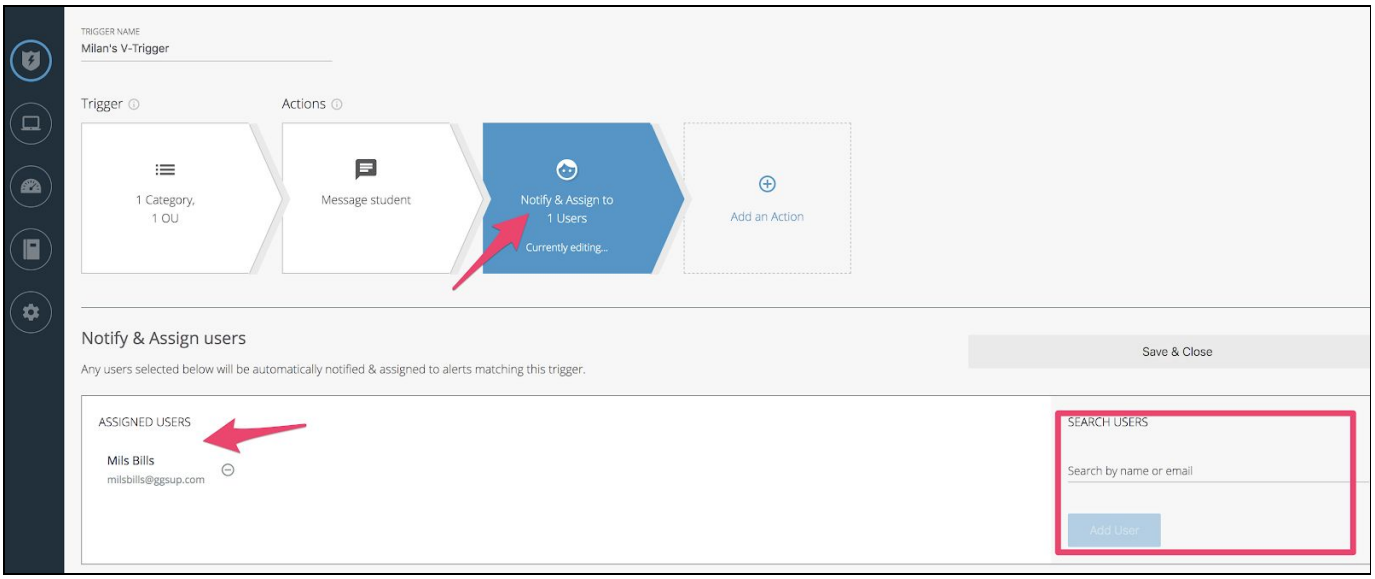
Note: ***The higher the Confidence Level, the more certain GoGuardian's AI will need to be before triggering a Smart Alert for users accessing potentially unwanted content. Setting the Confidence Level lower will ensure that Smart Alerts are triggered more often, but can also create more false positive alerts.***

After adding the Category and Confidence Level, you can select a specific OU for your Smart Alert Trigger to apply to (*Note: Not selecting a specific OU or Confidence level means that the trigger will fire for all OUs and Confidence levels respectively*).

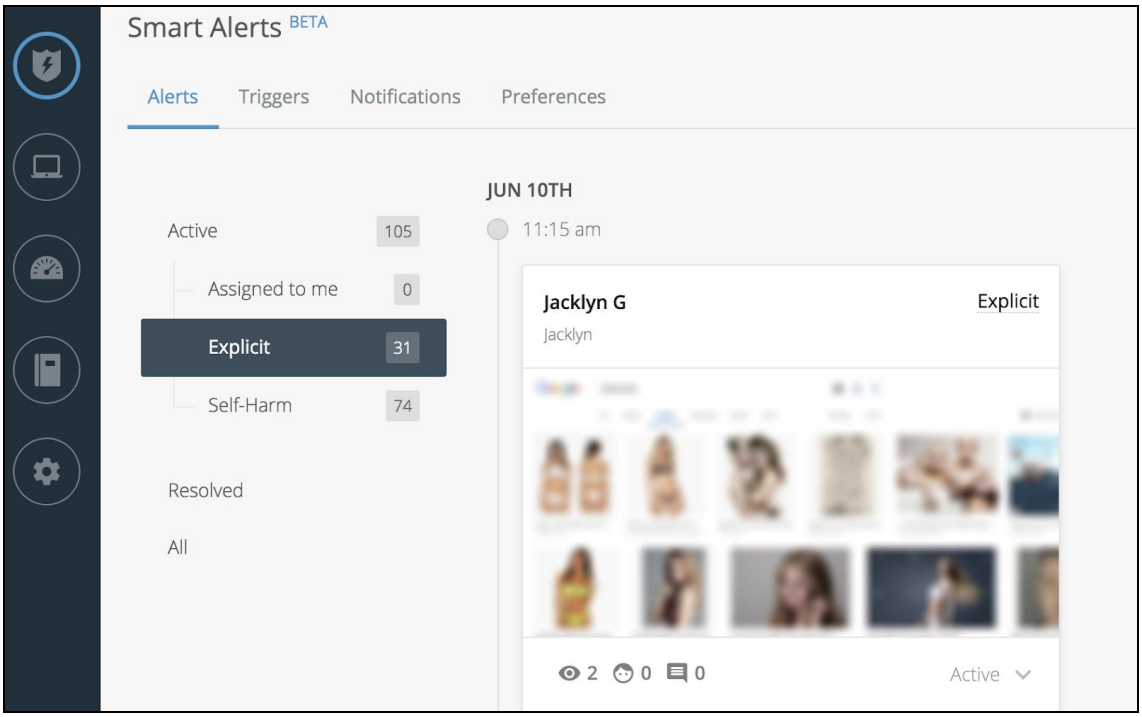
To add additional actions (such as Assigning Users, Messaging the student, and Blocking content), click the Add an Action button just to the right of the previous action.

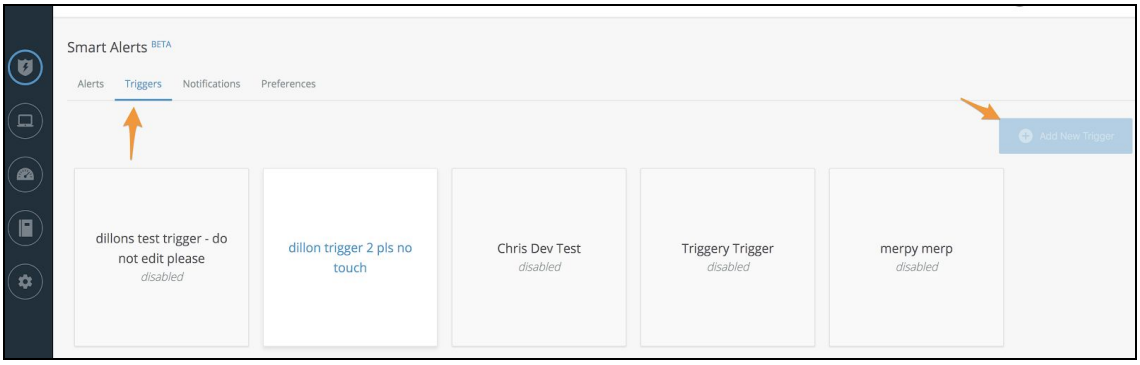


To assign specific users to receive alert notifications when someone triggers an alert, you can add the action for it and assign the users by either name or email.



***Note:** To assign a user, they must have access to the OU that Smart Alert applies to. OU acces can be configured in the Manage Organization portal by editing that specific user's sub-org access. Please click [Here] for additional details.





***Note:** Smart Alerts for the "Self-Harm" category is no longer available for new customers. For more information, please reach out to your sales representative.

For more information about Smart Alerts, please click *here.*

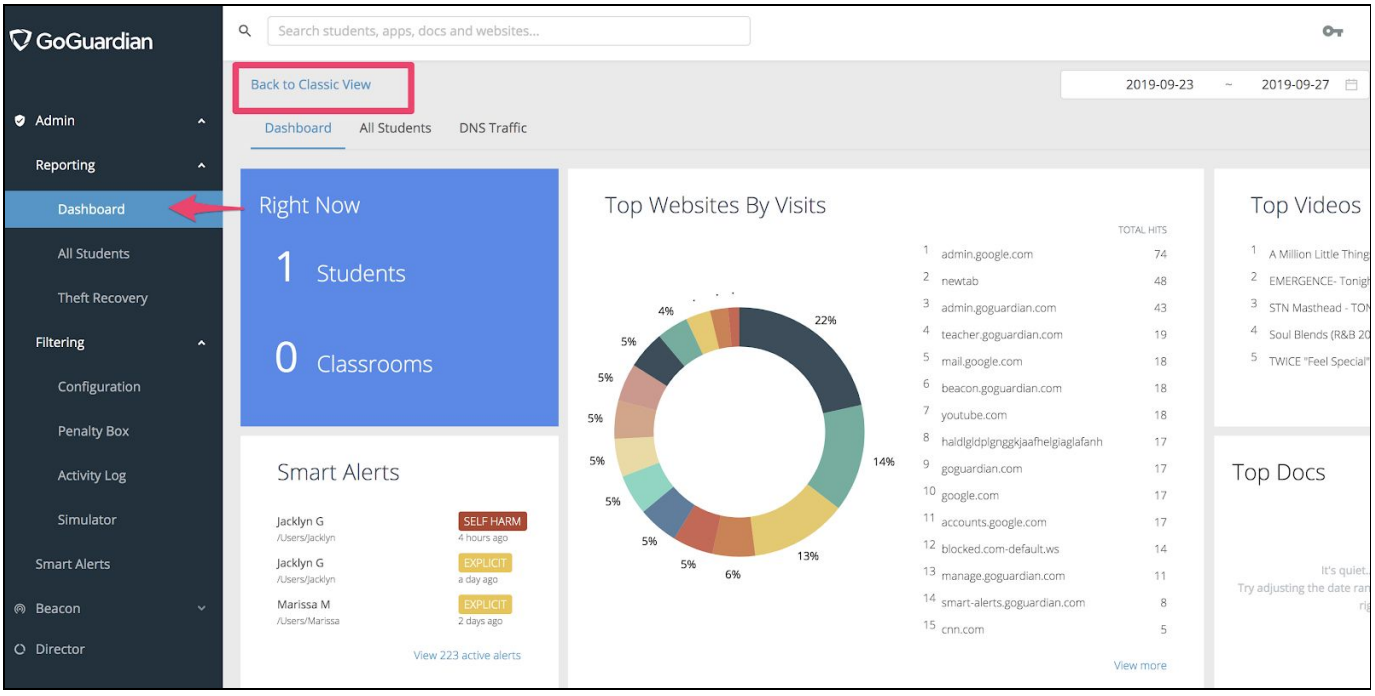
Smart Alert Quick Facts

- Smart Alerts are currently only configured for Explicit material
- Smart Alerts can only be viewed by an admin that has access to that same OU within Org Management. This can be edited by a Super User at manage.goguardian.com.
- Smart Alerts cannot be adjusted to catch specific terms or sites based on a school's preferences. GoGuardian's proprietary algorithm determines whether or not a site should trigger an alert.

FAQs / Troubleshooting

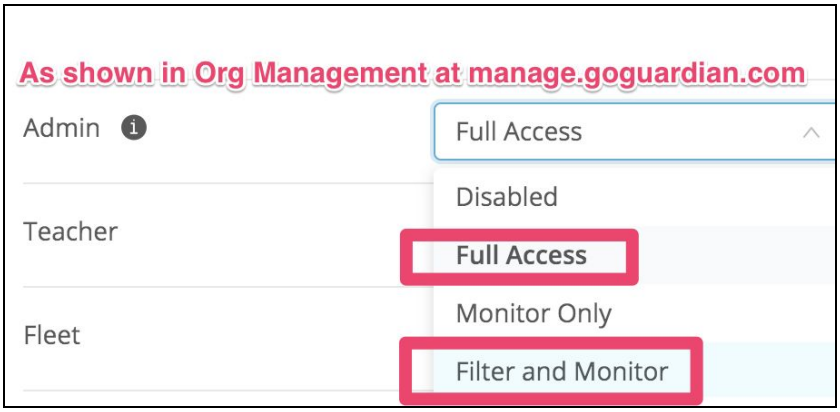
Admin 1.0 (Classic View) FAQs

Note: If you are using Admin 2.0, you can reach Admin 1.0, by clicking Dashboard > Back to Classic View

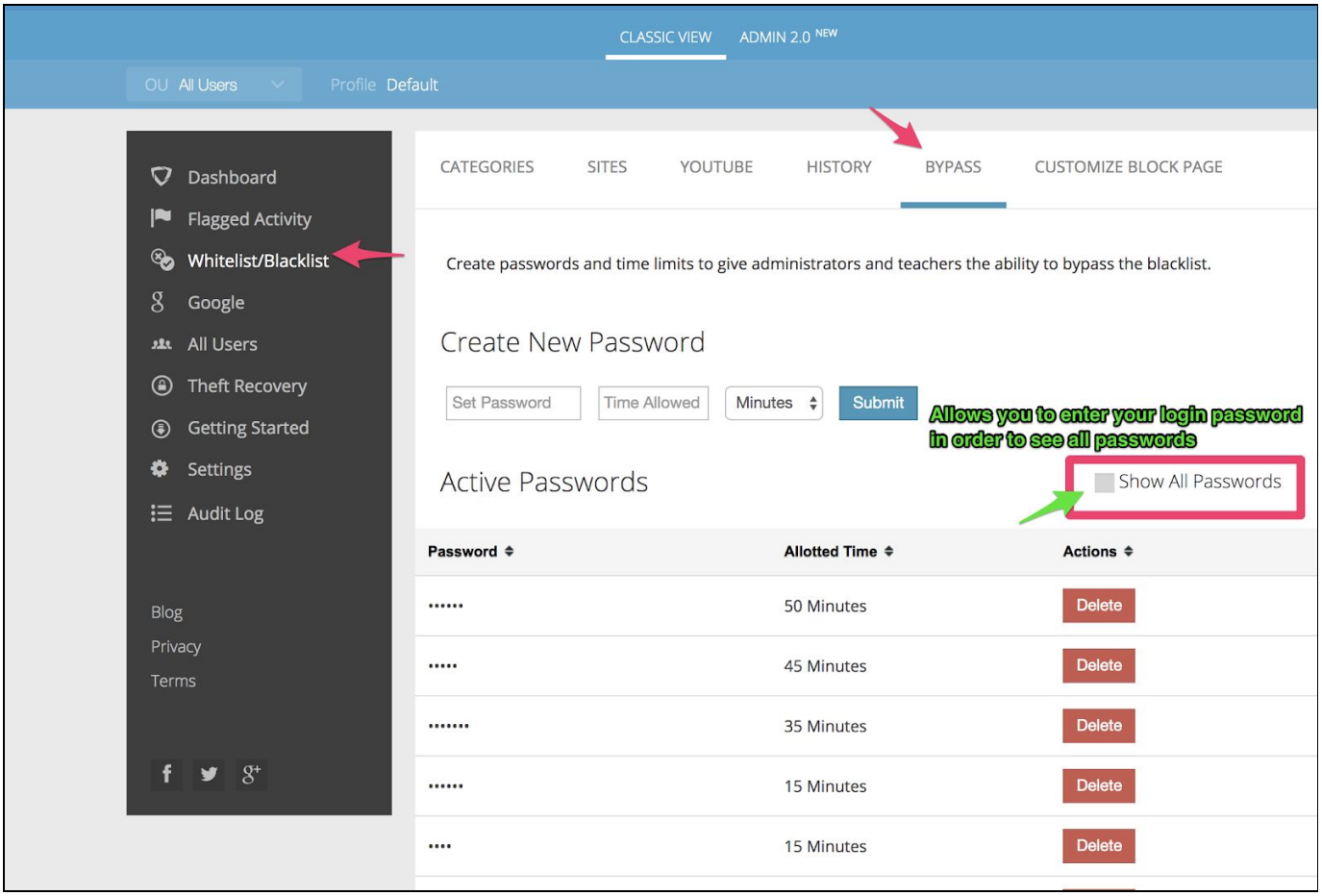


Bypass Passwords

Bypass passwords can be used to bypass a Blacklisted or Policy-restricted site. When creating a password, you will also need to specify how long the bypass will work on a restricted site. If that time expires, the bypass can be re-entered to reset the time allowance. To set a bypass password, an admin must have either Filter and Monitor access or Full Access.



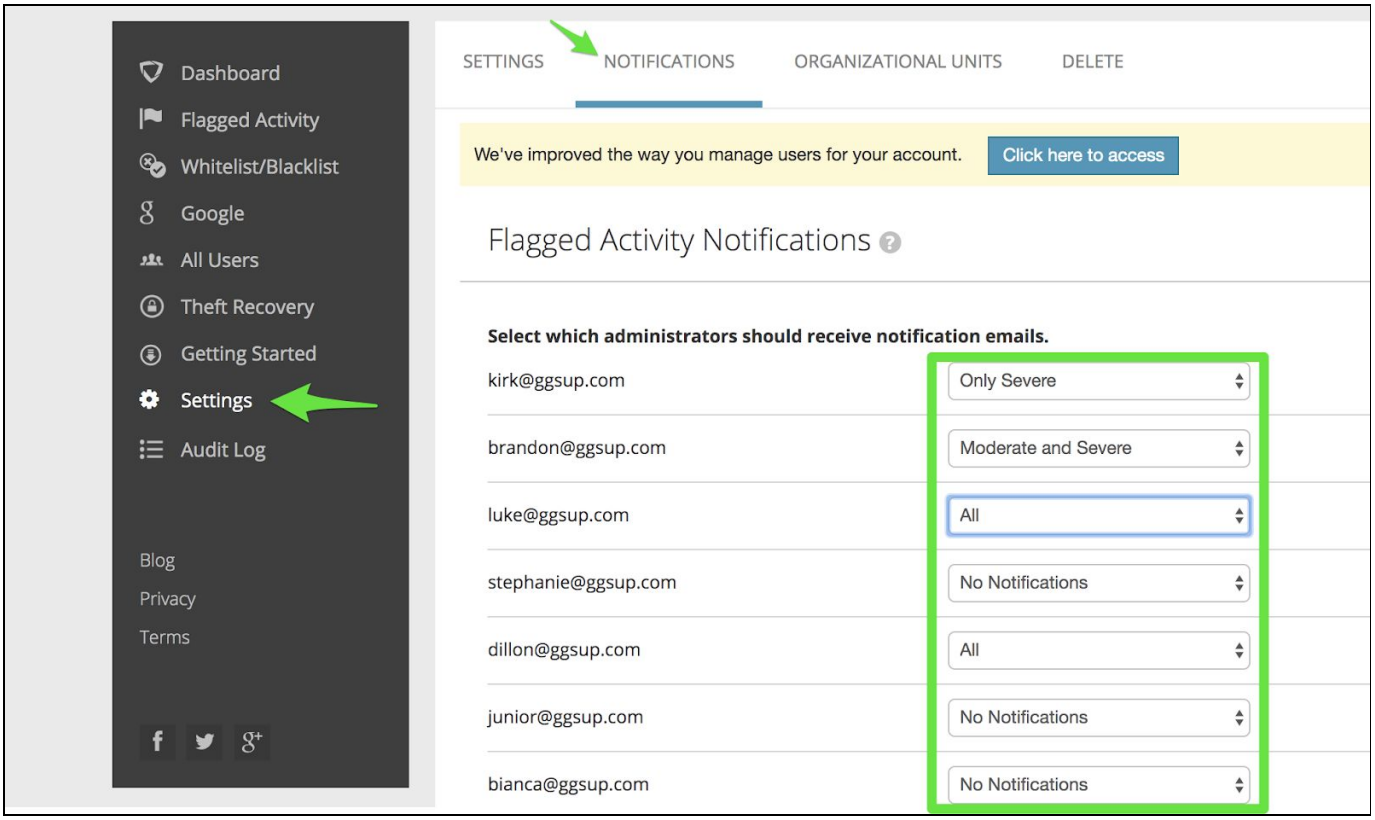
Note: Using a bypass password will allow access to any site that is otherwise restricted by a Policy (in Admin 2.0) or that is found in the Blacklisted sites (in Admin 1.0). If a block page is reached while trying to navigate to a different restricted site, the user will need to re-enter the bypass password each time.



You can view all Bypass Passwords by clicking the Show All Passwords checkbox.

Notifications

Notification settings allow an admin to be emailed when a Flagged Activity alert arises. Notifications can be set by clicking Settings > Notifications. From here any admin can set their notifications to All, Only Severe, Moderate and Severe, or None.



Notifications apply specifically to Flagged Activity, and Flagged Activity is based on Flagged Terms settings.

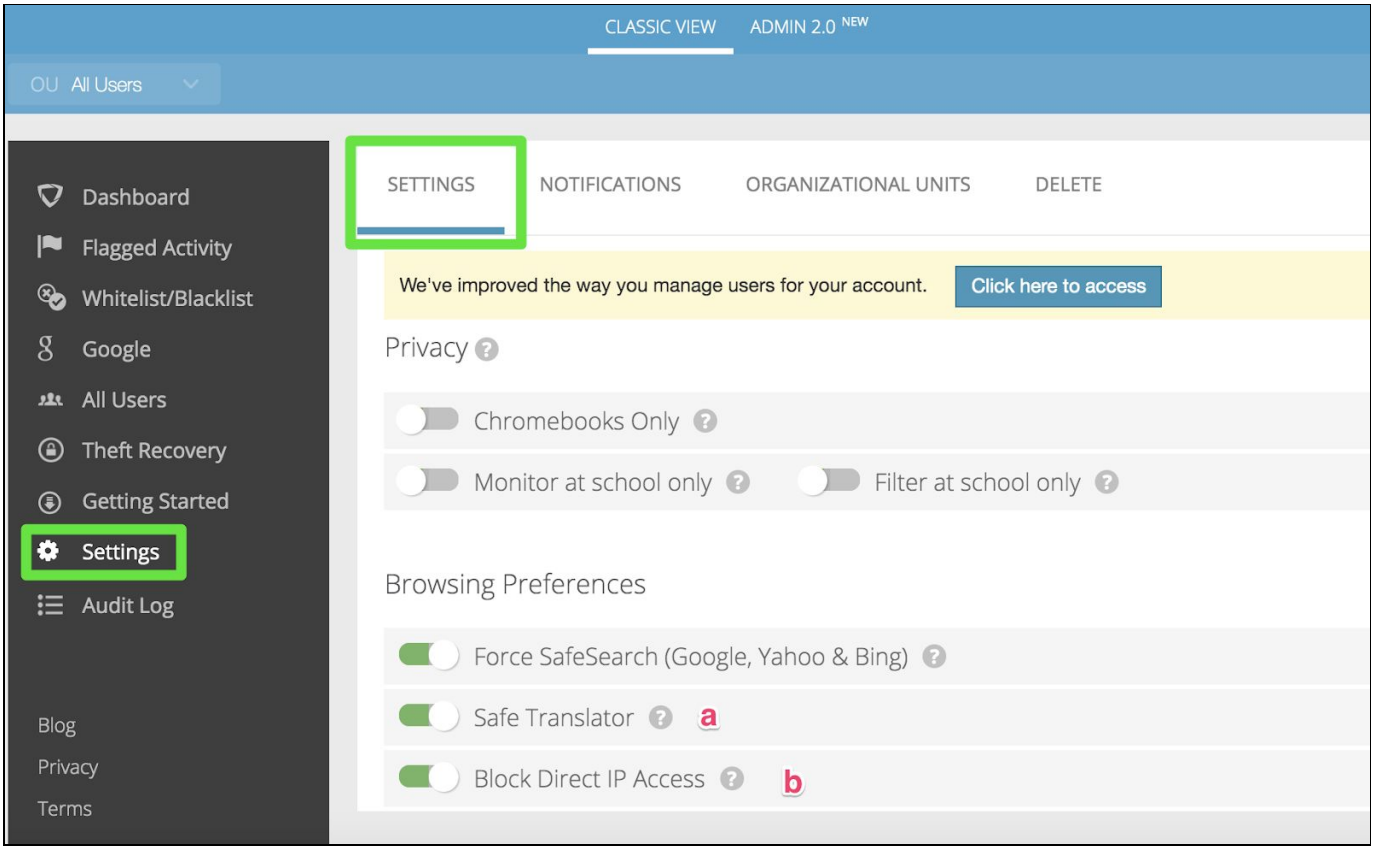
Flagged Terms

Flagged Terms are the exact terms that GoGuardian is looking for within a webpage. If the terms on your flagged terms page match the words found anywhere on a website (even if it's a comment on the page from another user or if the word is somewhere within the metadata of that page) it will trigger a flagged activity alert.

Your Flagged Terms can be set or reset in GoGuardian Admin 1.0 under Flagged Activity > Flagged Terms. If you do not see a Flagged Term that you would like to look for, or if you would like to reset a term to a higher or lower severity (based on your notification settings), you can add a new term (or delete an existing term and add it back) and you will see the option to set the severity of that term to either Low, Moderate, or Severe.

This is similar to a number scale where Low would fall somewhere between 1 and 3, Moderate would fall somewhere between 4 and 7, and Severe would fall somewhere between 8 and 10.

Settings



The Settings page allows you to enable things like Safe Translator (a) and Block Direct IP Access (b).

a. Safe Translator will prevent translation sites from being accessed (this may prove useful if students are attempting to access foreign sites that aren't specifically blocked by your settings).
    i. Note: Sites like wordreference.com are categorized as translator sites. If you would like for students to access this site, you can do so by adding a Wildcard to your Whitelist (an example Wildcard for wordreference would be *wordreference.com*).
b. Block Direct IP Access will prevent direct IPs from being used to access sites. This works similarly to the Safe Translator (preventing students from using a Direct IP in lieu of a site URL to gain access to an otherwise restricted site).
    i. If there is a direct IP that users need to access, it would be recommended to create a Wildcard for that as well (an example of a direct IP Wildcard would be *74.125.224.72*).

*To view the Admin 2.0 version of the settings page click here.

Audit Log

The Audit Log can be used to keep track of which changes were made by which Admin. An example of a change would be importing OUs or creating a new Bypass Password.

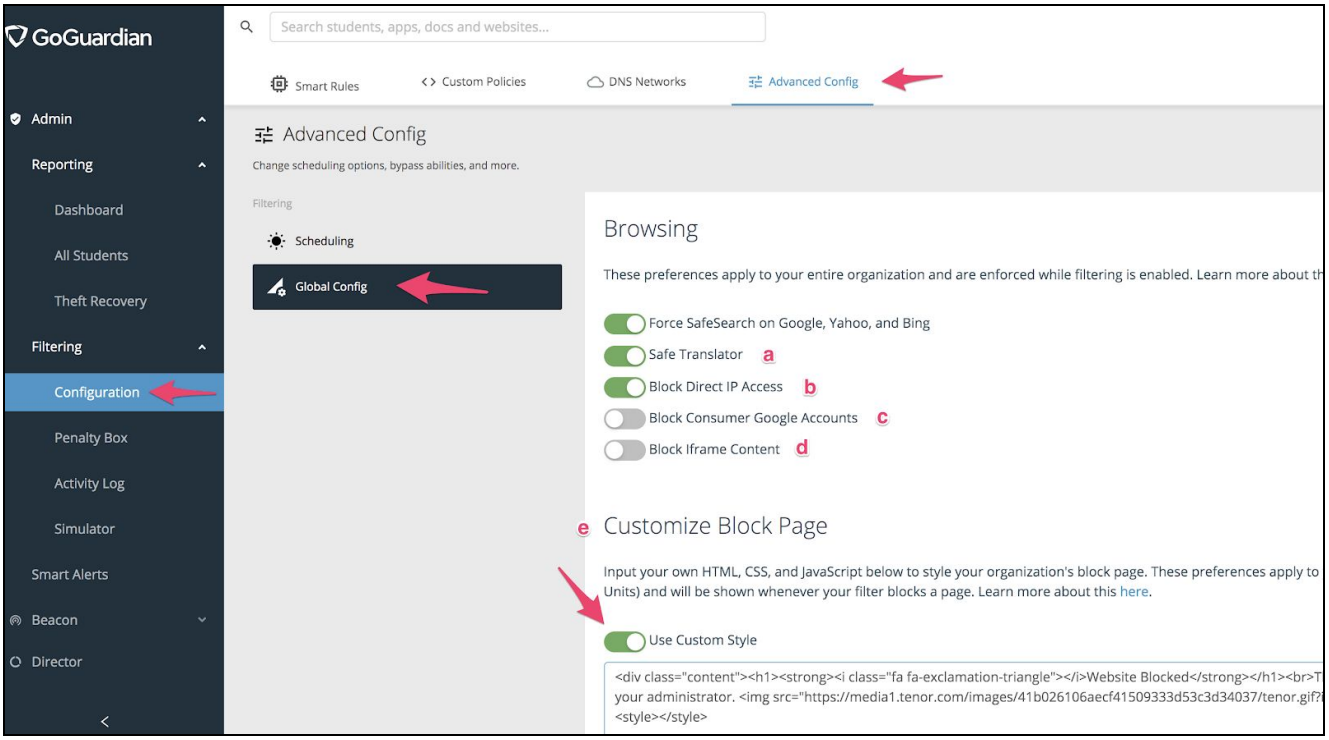
The Audit Log only applies to changes made in Classic View. So, any changes made in Admin 2.0 will not reflect in the 1.0 Audit Log.

You can access the Audit Log directly in the left panel within GoGuardian Admin Classic View.

Admin 2.0 FAQ

Global Config

You can reach Global Config by clicking Configuration > Advanced Config > Global Config.



The Global Config page allows you to enable things like Safe Translator (a), Block Direct IP Access (b), Block Consumer Google Accounts (c), and Block iframe Content (d).

a. **Safe Translator** will prevent translation sites from being accessed (this may prove useful if students are attempting to access foreign sites that aren't specifically blocked by your settings).
    ii. Note: Sites like wordreference.com are categorized as translator sites. If you would like for students to access this site, you can do so by adding a Wildcard to your Policy (an example Wildcard for wordreference would be *wordreference.com*).

b. **Block Direct IP Access** will prevent direct IPs from being used to access sites. This works similarly to the Safe Translator (preventing students from using a Direct IP in lieu of a site URL to gain access to an otherwise restricted site).

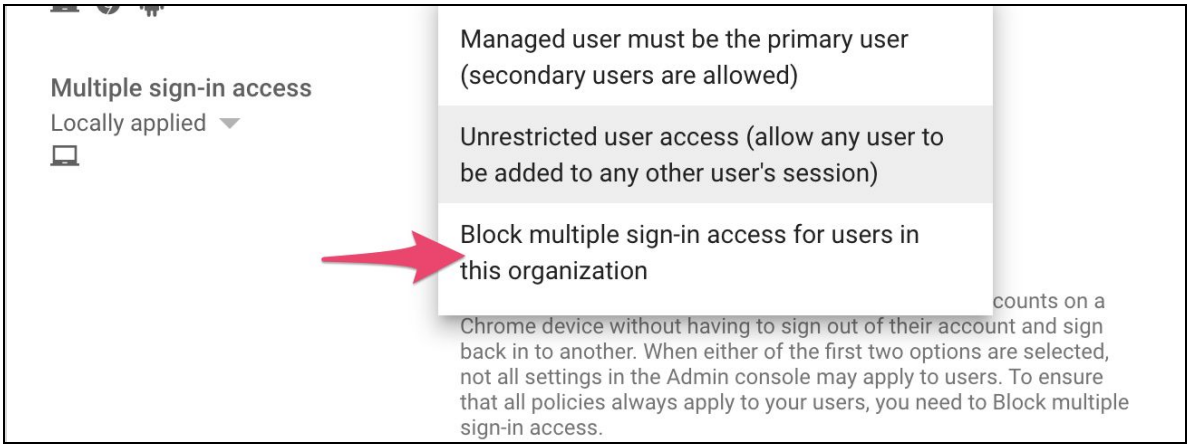
iii. If there is a direct IP that users need to access, it would be recommended to add a Wildcard for that to your Policy as well (an example of a direct IP Wildcard would be *74.125.224.72*).

c. **Block Consumer Google Accounts**

i. The Block Consumer setting is a global setting that prevents users from accessing other Google accounts. You cannot bypass this setting by allowing URLs it blocks in policies.

If you think you will want to allow a particular group of users to access other Google accounts, you can use the Google Admin Console setting at admin.google.com which can be applied to specific OUs rather than all OUs.

ii. Block consumer accounts allows you to prevent students from using their personal gmail accounts. This setting has also been added to the Google Admin Console under User & browser settings.



*Note for additional Google Admin Console setting recommendations, we suggested taking a look at our Google Admin Console Best Practices article. You can click here to view it.

d. Block iframe Content

i. Block iframe Content allows you to apply the same Policy settings to embedded content as you do to other websites (ex. If YouTube videos are blocked on your Default Policy, but Google Docs are allowed, a student could embed a YouTube video in a Google Doc. But Block iframe content prevents the blocked YouTube video from showing on the Google Doc).

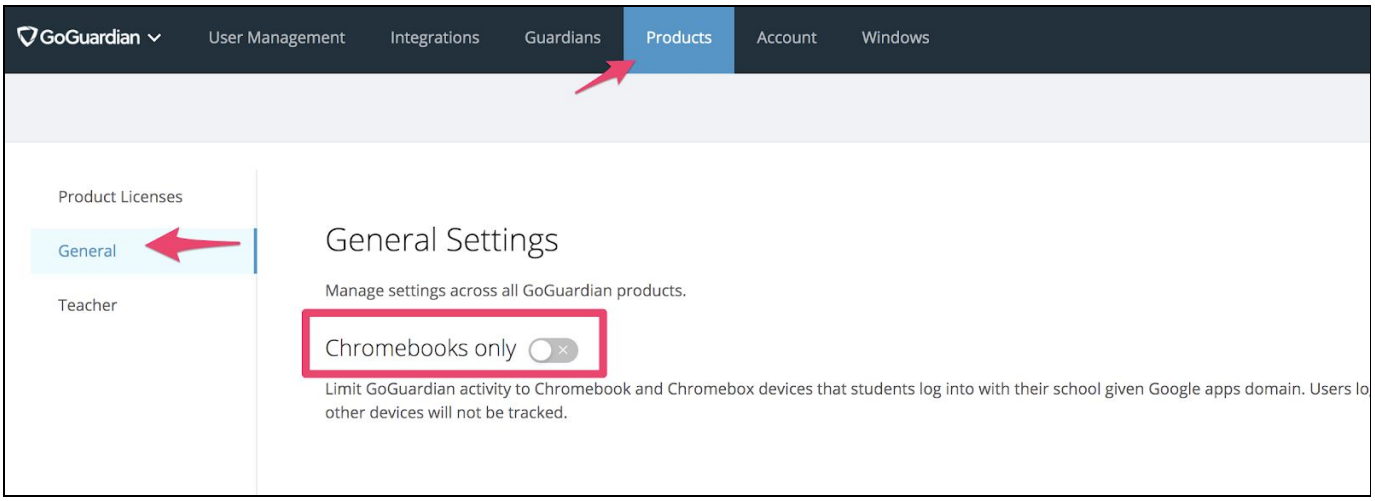
e. Customize Block Page

i. Customize Block page allows you to add the desired HTML to a block page that students reach when trying to access a restricted site. The block page will show in place of the standard GoGuardian Admin block page.

General Settings (for Super Users only)

If you do wish to allow students to be monitored on non-Chromebooks, Super Users can disable the Chromebooks only setting in Org Management at under Products > General. Or to access this setting directly, you can click here.

*Note: If all devices are Windows devices, or if you need to lock down student browsing on your Windows devices, we recommend going through the Windows setup, which cane be found by navigating to the Windows tab in Org Management, or by clicking here.



I'm not seeing any changes after importing/syncing OUs!

For all scenarios below, please try clearing cache first on your device:
CTRL+Shift+R (on Mac devices: CMD+Shift+R)

What's the difference between Smart Alerts and Flagged Activity?

- **Flagged Activity** refers to any preset Flagged Terms that are found on a webpage (whether or not a student typed the term(s) in on that page. This could point to comments or metadata on that page from other users).
    - Flagged Terms are the terms that GoGuardian Admin searches for when users are browsing online. If one of these 'flagged terms' is found on a webpage (even if not entered by the student) that will trigger a flagged activity alert. You can access your flagged terms here.
- **Smart Alerts** refers to alerts that were triggered based on what is found on a webpage that a student was on (specifically content of an explicit nature (or related self-harm for organizations that were with GoGuardian when self-harm alerts were offered). This could be determined by page content or what is typed in a search.

For more information about the difference between Flagged Activity and Smart Alerts, please click *here.*

Contact FAQs

I have an idea on a feature that would be great to add to GoGuardian! Where can I submit it?

Make a feature request recommendation or upvote ideas at ideas.goguardian.com!

I would like to send GoGuardian some feedback via social media! Where can I submit it?

Twitter: @GoGuardian *Facebook: https://www.facebook.com/goguardian*

Where do I go if I have more questions?

Check out our GoGuardian Admin Help Center for more resources or to contact us.

Welcome to GoGuardian! If you have any additional questions, please feel free to look through our Help Center at help.goguardian.com. Or you can email or chat with tech support during our normal business hours (M-F 6am - 5pm PST)

help.goguardian.com