Google for Education

ChromeOS Fleet Monitoring Best Practices Guide

May 2023

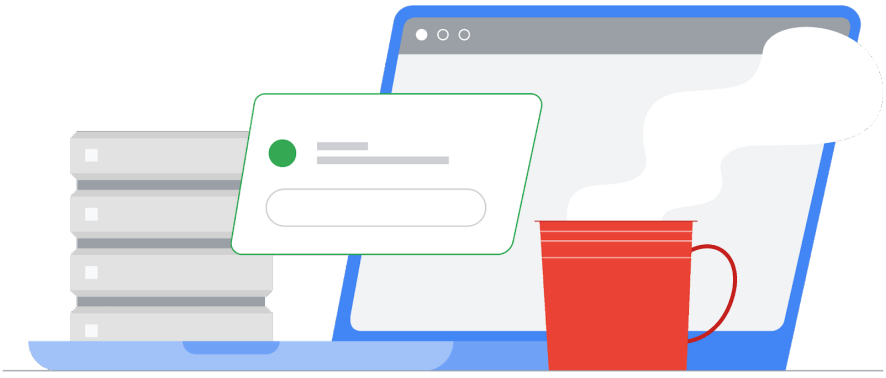


Table of contents

Find devices that have not synced policy recently 2

Detect if users repeatedly re-enroll their devices 4

If you have Workspace for Education Plus or Standard 4

Investigate Devices 4

Create an Activity Rule for Re-enrollments 5

If you have Workspace for Education Fundamentals 5

Filter Audit Logs 5

Prevent users from enrolling unauthorized devices 6

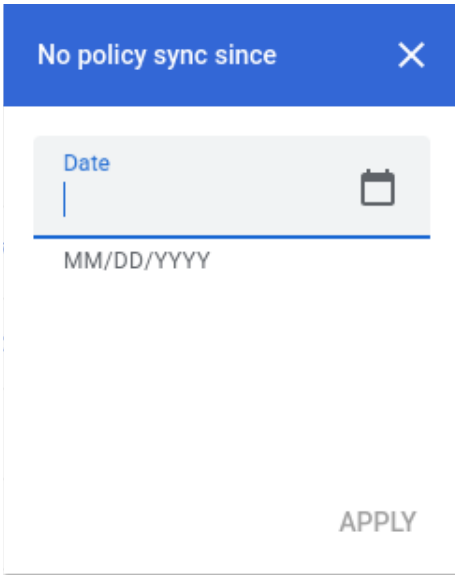
Monitor users logging in on unenrolled devices 6

Detect devices that have joined a managed network while unmanaged 7

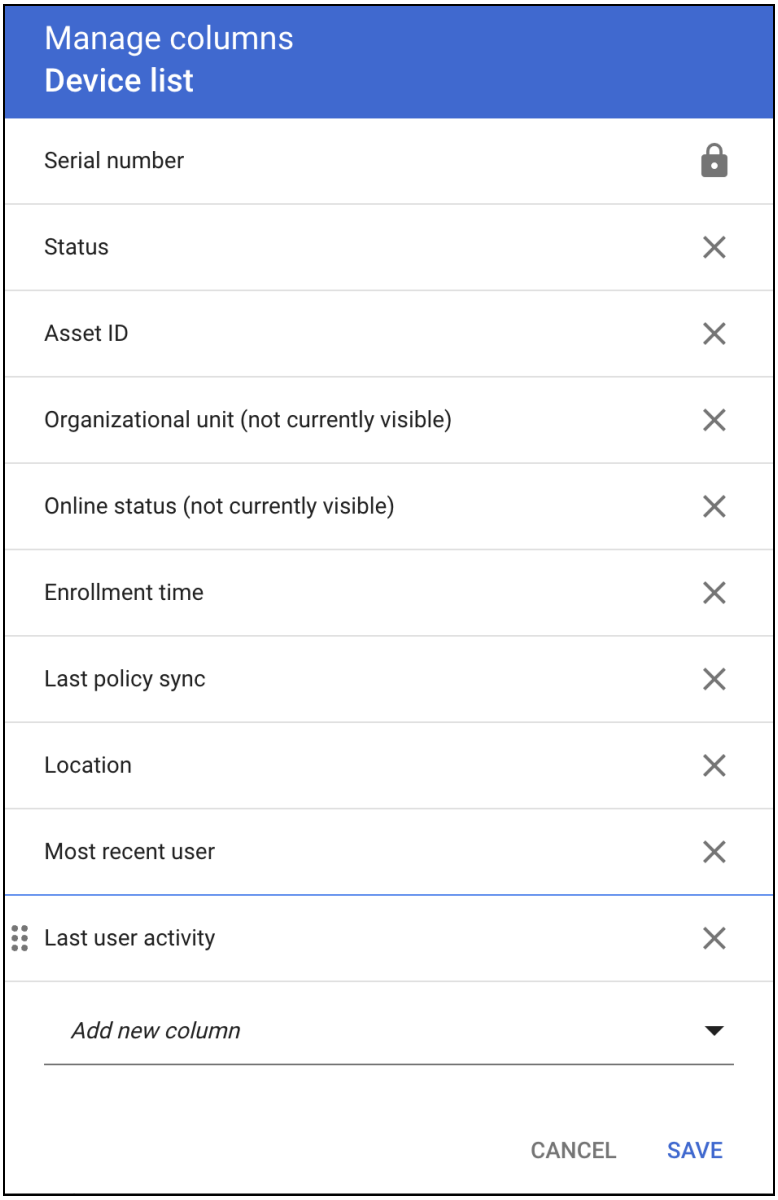
Recommended Settings 8

Find devices that have not synced policy recently

In the Admin console, go to Devices > Chrome > Devices to view a report of all devices, sorted by last sync time. A filter can be added to the list to show devices that have not synced a specific date. For example, an administrator can set a filter for “No Policy sync since” with “ Date” of 01/13/2023 and to only show devices that haven’t synced policy since January 13, 2023 or earlier this year.



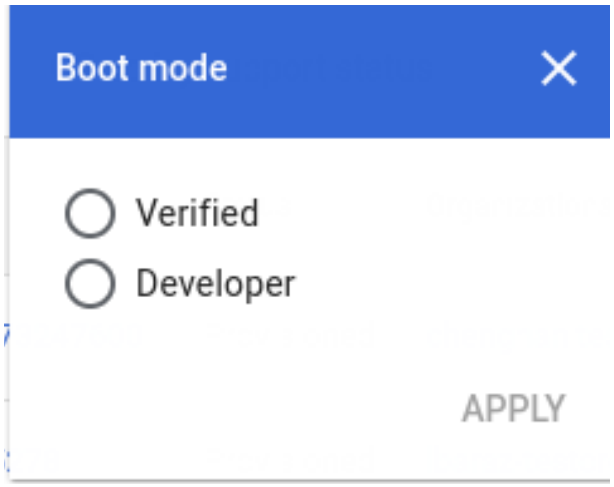
The columns for this list of devices can be edited to include “Most recent user” which is the last user to use the device (the “User” field is the user that enrolled the device, which may not be the primary user of the device). To edit the columns shown click the gear icon, and at the bottom click “*Add new column*” and select “Most recent user”. You can also remove columns by clicking the X. Click “SAVE” when done.



Admins can also automatically [receive a report of inactive company devices] that haven't synced within the last 30 days.

Find Devices in Developer Mode

In the Admin console, go to Devices > Chrome > Devices to view a report of all devices filtered by Boot Mode. This will enable administrators to find devices in Developer Mode versus Verified Boot mode.



Detect if users repeatedly re-enroll their devices

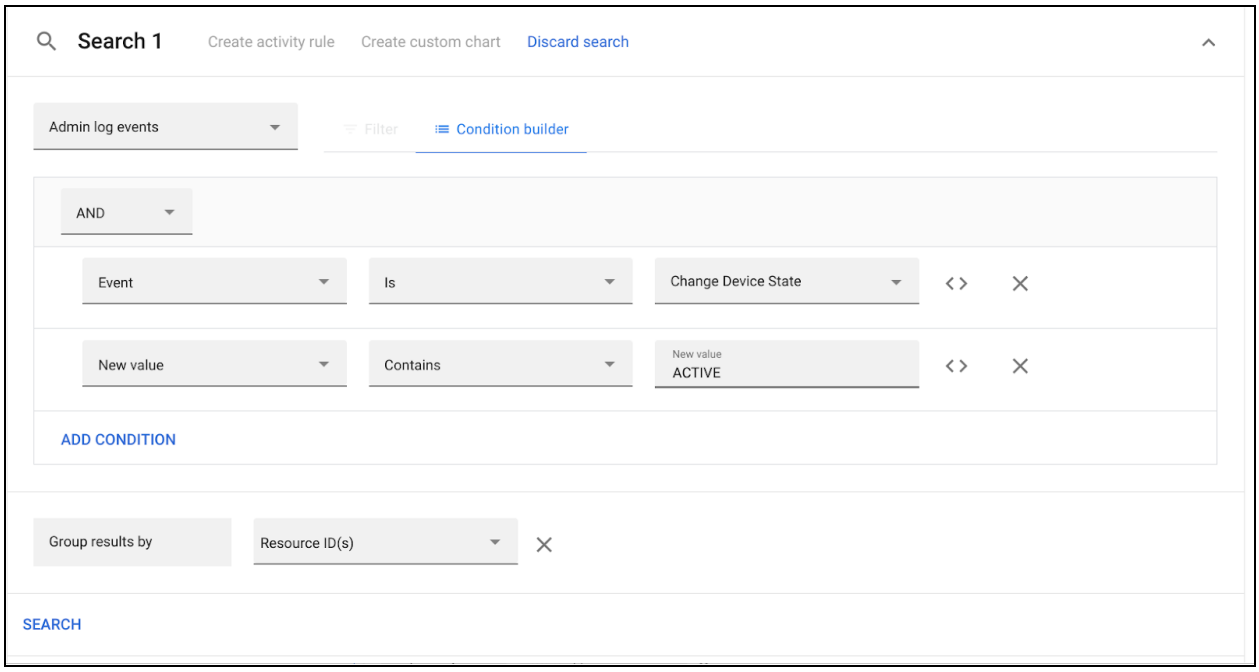
If a user repeatedly un-enrolls and re-enrolls their device, audit logs can capture this information and surface it to admins. With Google Workspace for Education Plus or Standard these device re-enrollments can trigger automatic alerts or actions.

If you have Workspace for Education Plus or Standard

Investigate Devices

For more information on how to use the Investigation Tool, see Security Investigation Tool.

- ➔ Go to Reporting → Investigation → Admin log events
- ➔ Click **Condition builder**
- ➔ Add a condition where “Event” “Is” “Change Device State”
- ➔ Add a condition where “New value” “Contains” “ACTIVE”
- ➔ Click **Group results by** and select “Group By Resource ID(s)”



➔ Click **Search**

Frequent occurrences of specific devices being re-enrolled could indicate users that are intentionally un-enrolling and re-enrolling devices.

Create an Activity Rule for Re-enrollments

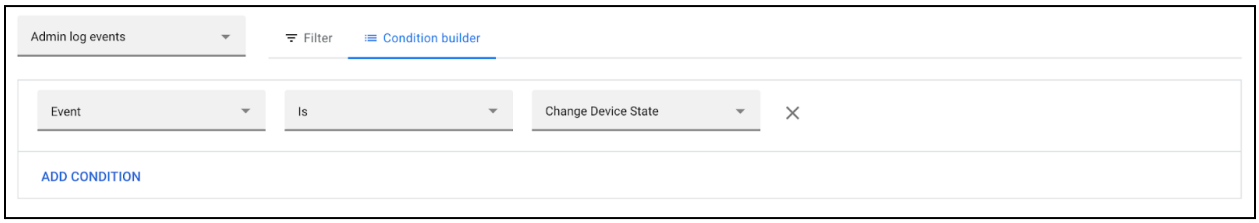
Optional: Click “Create activity rule” at the top to save this search as a rule and send automatic notifications. Automatically suspending users that re-enroll devices is not currently recommended due the possibility of false positives. For more information on creating activity rules, see Create and manage activity rules.

If you have Workspace for Education Fundamentals

Filter Audit Logs

➔ Go to Reporting → Investigation → Admin log events
➔ Click **Condition builder**

➔ Add a condition where “Event” “Is” “Change Device State”



➔ Click **Search**.

The Resource IDs and Description columns should be visible by default.
Click **Export all** to export the results to a Google Sheet. Provide a name for the export and click **Export**.
When the export is completed, scroll down to “Export action results” and click the name of the export to open the Google Sheet.
Identify devices re-enrolling by adding a column and testing for the text “ACTIVE to ACTIVE” in the description. See an example formula below where C is the Description field. Set this formula as cell E1 of the sheet:

```
=Arrayformula(if(row(C:C)=1,"Reenrolled",REGEXMATCH(C:C,
"ACTIVE to ACTIVE")))
```

Insert a pivot table using the column headers “Resource IDs” as the Rows, the column header “Reenrolled” as the columns and the counting of any other field, such as the column header “Actor”, as the value.

Prevent users from enrolling unauthorized devices

Some organizations allow end users to enroll or re-enroll devices. This permission would allow users to re-enroll devices while at school/work and un-enroll them while off-network. Admins can consider disabling this permission for users if they do not want them to be able to easily re-enroll devices on their own, or enable it if they do want users to have this ability.

To toggle this setting in the Admin console go to Devices > Chrome > Settings > Users & browser. Select the relevant OU on the left hand column (such as “Students”). For “Enrollment permissions” under “Enrollment controls” select “Do not allow users in this

organization to enroll new or re-enroll existing devices" to prevent users from enrolling devices or "Only allow users in this organization to re-enroll existing devices (cannot enroll new or deprovisioned devices)" to allow users to re-enroll existing devices.

Monitor users logging in on unenrolled devices

To make it easier for teachers or employees to spot unmanaged devices, a visual device policy setting can be changed. This change would only apply to currently managed devices. Unmanaged devices will not display the change.

Admins can set devices to always display system information on the login screen. Unmanaged devices would not display the Managed By or the system information. Further, the login wallpaper can be changed to a protected image.

Admins can monitor on the Device list console for policy syncs in association to recent users. Cross referencing the expected user list against users with recently synced policies can return a list of potential users with devices that have not synced. These remaining devices can be further monitored for possible physical investigation on their enrollment state.

Detect devices that have joined a managed network while unmanaged

It may be possible to quickly determine Chromebooks that should be managed when they join your Wi-Fi network in an unmanaged state. Admins can use the DeviceHostnameTemplate policy to specify a hostname format that can include serial number and/or asset tag ID. This host name is visible in network DHCP tables. If a device with a known MAC address joins the managed network without the proper hostname it is likely an unenrolled device.

For example: In the Admin console go to Devices > Chrome > Settings > Device and scroll down to "Device network hostname template" under "Other settings". Apply a network hostname template policy of "ManagedChromebook-${SERIAL_NUM}" to managed Chromebooks. These will show up in the DHCP pool of a school's network with that easily identifiable configured hostname. All other leases on that SSID/network will show up with a generic or undefined hostname. Exporting those generic or

undefined hostnames' MAC addresses and comparing them against an export of a Workspace tenant's known MAC addresses should help to identify which device is unenrolled.

To export a list of devices with Wi-Fi MAC addresses, in the Admin console go to Devices > Chrome > Devices, select the desired OU, then click "Export" above the list. The export process will appear in the tasks list by clicking the hourglass icon at the top right. When complete you can download the CSV to see the results. The "macAddress" column includes the WiFi MAC address (without colon characters).

From here, the Admin can take several actions with the identified devices including track down those devices/users, block the MAC addresses from joining the network entirely, or segment those devices into a limited access VLAN. Using a content filter or captive portal system, network administrators could redirect those identified devices to a page with instructions on how to contact IT for support or how to re-enroll their devices (if allowed by the administrator).

Recommended Settings

- ➔ Forced Re-enrollment - Set to "Force device to automatically re-enroll after wiping" Forced Re-enrollment Support Article
- ➔ Powerwash - Set to "Do not allow Powerwash to be triggered" for all but select users Powerwash Support Article
- ➔ Verified Mode - Set to "Require verified mode boot for verified access" Verified Mode Support Article
- ➔ Verified Access - Set to "Enable for content protection" Verified Access Support Article
- ➔ Device re-enrollment permissions - Select specific organizational units of users allowed to. Enrollment Permissions Support Article
- ➔ Block access to the following internal URLs:

```
chrome://policy
chrome://net-export
chrome://prefs-internals
chrome://version
chrome://kill
chrome://hang
```