

Google for Education

# Panduan Praktik Terbaik Pemantauan Perangkat ChromeOS

Februari 2023



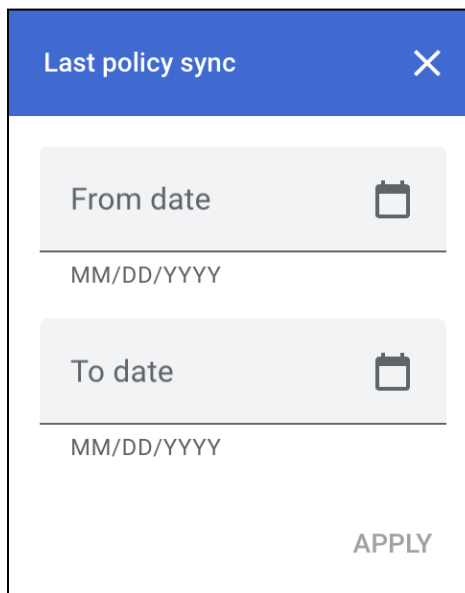
## Daftar isi


---


<b>Menemukan perangkat yang baru-baru ini belum menyinkronkan kebijakan</b>	<b>2</b>
<b>Mendeteksi apakah pengguna mendaftarkan ulang perangkat berulang kali</b>	<b>4</b>
Jika Anda menggunakan Workspace for Education Plus atau Standard	4
Investigasi Perangkat	4
Buat Aturan Aktivitas untuk Pendaftaran Ulang	5
Jika Anda menggunakan Workspace for Education Fundamentals	5
Filter Log Audit	5
<b>Mencegah pengguna mendaftarkan perangkat tanpa izin</b>	<b>6</b>
<b>Memantau pengguna yang login di perangkat yang dibatalkan pendaftarannya</b>	<b>7</b>
<b>Mendeteksi perangkat yang telah bergabung ke jaringan terkelola dalam keadaan tidak terkelola</b>	<b>7</b>
<b>Setelan yang Direkomendasikan</b>	<b>8</b>

## Menemukan perangkat yang baru-baru ini belum menyinkronkan kebijakan

Di konsol Admin, buka Perangkat > Chrome > Perangkat untuk melihat [laporan semua perangkat](#) yang diurutkan berdasarkan waktu sinkronisasi terakhir. Filter dapat ditambahkan ke daftar untuk menampilkan perangkat yang telah disinkronkan selama durasi tertentu. Misalnya, administrator dapat menyetel filter untuk “Sinkronisasi kebijakan terakhir” dengan “Dari tanggal” 01/01/2022 dan “Hingga tanggal” 13/01/2023 untuk hanya menampilkan perangkat yang belum menyinkronkan kebijakan sejak 13 Januari 2023, atau awal tahun ini.















From date   
MM/DD/YYYY

To date   
MM/DD/YYYY

APPLY

Kolom daftar perangkat ini dapat diedit untuk menyertakan “Pengguna terbaru”. Pengguna ini adalah pengguna terakhir yang menggunakan perangkat (kolom “Pengguna” berisi pengguna yang mendaftarkan perangkat. Dia mungkin bukan pengguna utama perangkat tersebut). Untuk mengedit kolom yang ditampilkan, klik ikon roda gigi, lalu di bagian bawah, klik “*Tambahkan kolom baru*” dan pilih “Pengguna terbaru”. Anda juga dapat menghapus kolom dengan mengklik tanda X. Klik “SIMPAN” setelah selesai.

Manage columns	
Device list	
Serial number	
Status	
Asset ID	
Organizational unit (not currently visible)	
Online status (not currently visible)	
Enrollment time	
Last policy sync	
Location	
Most recent user	
 Last user activity	
<i>Add new column</i>	
<hr/>	
CANCEL    SAVE	

Admin juga dapat otomatis [menerima laporan tentang perangkat perusahaan yang tidak aktif](#) yang belum disinkronkan dalam 30 hari terakhir.

## Mendeteksi apakah pengguna mendaftarkan ulang perangkat berulang kali

Jika pengguna berulang kali membatalkan pendaftaran dan mendaftarkan ulang perangkatnya, log audit dapat mengambil informasi ini dan memberitahunya kepada admin. Dengan Google Workspace for Education Plus atau Standard, pendaftaran ulang perangkat ini dapat memicu tindakan atau pemberitahuan otomatis.

### Jika Anda menggunakan Workspace for Education Plus atau Standard

#### Investigasi Perangkat

Untuk mengetahui informasi lebih lanjut terkait cara menggunakan Alat Investigasi, lihat [Alat Investigasi Keamanan](#).

- Buka Pelaporan → Investigasi → Peristiwa log Admin
- Klik **Pembuat kondisi**
- Tambahkan kondisi dengan "Acara" "Sedang" "Status Perangkat Diubah"
- Tambahkan kondisi dengan "Nilai baru" "Berisi" "AKTIF"
- Klik **Group results by**, lalu pilih "Group By Resource ID(s)"

Search 1 Create activity rule Create custom chart Discard search

Admin log events Filter Condition builder

AND

Event Is Change Device State <> X

New value Contains New value ACTIVE <> X

ADD CONDITION

Group results by Resource ID(s) X

SEARCH

- Klik **Telusuri**

Sering terjadinya pendaftaran ulang untuk perangkat tertentu dapat mengindikasikan adanya pengguna yang secara sengaja membatalkan pendaftaran perangkat dan mendaftarkannya kembali.

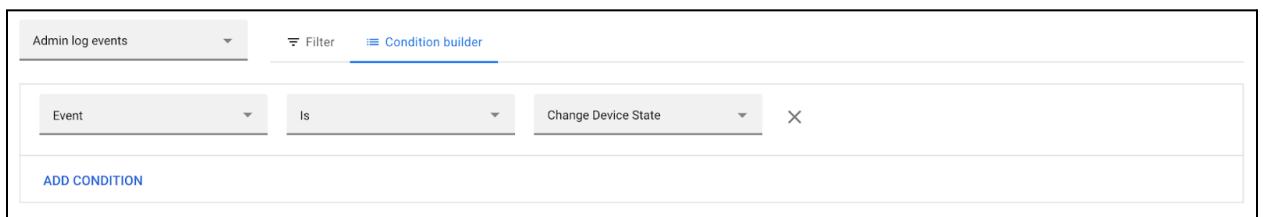
## Buat Aturan Aktivitas untuk Pendaftaran Ulang

Opsional: Klik “Buat aturan aktivitas” di bagian atas untuk menyimpan penelusuran ini sebagai aturan dan mengirimkan notifikasi otomatis. Saat ini, otomatis menanggukkan pengguna yang mendaftarkan ulang perangkat tidak direkomendasikan karena adanya kemungkinan positif palsu (PP). Untuk mengetahui informasi selengkapnya mengenai aturan aktivitas, lihat [Membuat dan mengelola aturan aktivitas](#).

## Jika Anda menggunakan Workspace for Education Fundamentals

### Filter Log Audit

- Buka Pelaporan → Investigasi → [Peristiwa log Admin](#)
- Klik **Pembuat kondisi**
- Tambahkan kondisi dengan "Acara" "Sedang" "Status Perangkat Diubah"



- Klik **Telusuri**.

Secara default, kolom Deskripsi dan ID Resource harus terlihat.

Klik **Ekspor semua** untuk mengekspor hasil ke Spreadsheet Google. Beri nama untuk ekspor tersebut, lalu klik **Ekspor**.

Setelah ekspor selesai, scroll ke bawah ke “Ekspor hasil tindakan”, lalu klik nama ekspor untuk membuka Spreadsheet Google.

Identifikasi pendaftaran ulang perangkat dengan menambahkan kolom dan menguji teks “ACTIVE to ACTIVE” (“AKTIF untuk AKTIF”) di deskripsi. Lihat formula contoh di bawah dengan C sebagai kolom Deskripsi. Tetapkan formula ini sebagai sel E1 pada sheet:

```
=Arrayformula(if(baris(C:C)=1,"Didaftarkan ulang",REGEXMATCH(C:C,"AKTIF untuk AKTIF")))
```

[Sisipkan tabel pivot](#) menggunakan header kolom “ID Resource” sebagai Baris, header kolom “Didaftarkan ulang” sebagai kolom, dan penghitungan kolom lainnya, seperti header kolom “Pelaku”, sebagai nilai.

## Mencegah pengguna mendaftarkan perangkat tanpa izin

Beberapa organisasi mengizinkan pengguna akhir untuk mendaftarkan atau mendaftarkan ulang perangkat. Izin ini akan memungkinkan pengguna untuk mendaftarkan ulang perangkat saat di sekolah/kantor dan membatalkan pendaftarannya ketika berada di luar jaringan tersebut. Admin dapat mempertimbangkan untuk menonaktifkan izin ini bagi pengguna jika tidak ingin mereka mendaftarkan ulang perangkat sendiri dengan mudah, atau mengaktifkan setelan ini jika admin ingin pengguna mampu melakukan tindakan tersebut.

Untuk mengaktifkan atau menonaktifkan setelan ini di konsol Admin, buka Perangkat > Chrome > Setelan > [Pengguna & browser](#). Pilih OU yang relevan di kolom sebelah kiri (misalnya “Siswa”). Untuk “Izin pendaftaran” di bagian “Kontrol pendaftaran”, pilih “Jangan izinkan pengguna dalam organisasi ini untuk mendaftarkan perangkat baru atau mendaftarkan perangkat yang ada” guna mencegah pengguna mendaftarkan perangkat. Atau, pilih “Hanya izinkan pengguna di organisasi ini mendaftarkan ulang perangkat yang ada (tidak dapat mendaftarkan perangkat baru atau yang telah dicabut aksesnya)” untuk mengizinkan pengguna mendaftarkan ulang perangkat yang ada.

## Memantau pengguna yang login di perangkat yang dibatalkan pendaftarannya

Untuk memudahkan pengajar atau karyawan menemukan perangkat tidak terkelola, visual setelan kebijakan perangkat dapat diubah. Perubahan ini hanya akan berlaku untuk perangkat yang saat ini terkelola. Perangkat tidak terkelola tidak akan menampilkan perubahan ini.

Admin dapat menyetel perangkat untuk [selalu menampilkan informasi sistem](#) di layar login. Perangkat tidak terkelola tidak akan menampilkan Dikelola Oleh atau informasi sistem. Selain itu, [wallpaper login](#) dapat diubah menjadi gambar yang dilindungi.

Admin dapat memantau [konsol Daftar perangkat](#) untuk menyinkronkan kebijakan yang berkaitan dengan pengguna terbaru. Melakukan referensi silang atas daftar pengguna yang telah diketahui terhadap pengguna yang baru disinkronkan kebijakannya dapat

menampilkan daftar calon pengguna dengan perangkat yang belum disinkronkan. Perangkat yang belum disinkronkan tersebut dapat dipantau lebih lanjut untuk kemungkinan dilakukannya investigasi fisik terkait status pendaftarannya.

## Mendeteksi perangkat yang telah bergabung ke jaringan terkelola dalam keadaan tidak terkelola

Anda dapat menentukan dengan cepat Chromebook yang harus dikelola ketika perangkat bergabung ke jaringan Wi-Fi dalam keadaan tidak terkelola. Admin bisa menggunakan kebijakan [DeviceHostnameTemplate](#) untuk menentukan format nama host yang dapat mencakup nomor seri dan/atau ID tag aset. Nama host ini dapat dilihat di tabel DHCP jaringan. Jika perangkat dengan alamat MAC yang diketahui bergabung ke jaringan terkelola tanpa nama host yang tepat, perangkat tersebut mungkin merupakan perangkat yang dibatalkan pendaftarannya.

Contoh: Di konsol Admin, buka Perangkat > Chrome > Setelan > Perangkat, lalu scroll ke bawah ke “Template nama host jaringan perangkat” di bagian “Setelan lainnya”.

Terapkan kebijakan template nama host jaringan

“ManagedChromebook-`${SERIAL_NUM}`” untuk Chromebook terkelola. Template ini akan muncul dalam kumpulan DHCP jaringan sekolah dengan nama host yang dikonfigurasi dan mudah dikenali. Seluruh lease lainnya di jaringan/SSID tersebut akan muncul dengan nama host umum atau yang tidak ditentukan. Mengekspor alamat MAC nama host umum atau yang tidak ditentukan tersebut dan membandingkannya dengan ekspor alamat MAC tenant Workspace yang diketahui akan membantu mengidentifikasi perangkat mana yang dibatalkan pendaftarannya.

Untuk mengekspor daftar perangkat dengan alamat MAC Wi-Fi, di konsol Admin buka Perangkat > Chrome > Perangkat, pilih OU yang diinginkan, lalu klik “Ekspor” di atas daftar. Proses ekspor akan muncul di daftar tugas dengan mengklik ikon jam pasir di kanan atas. Setelah proses selesai, Anda dapat mendownload file CSV untuk melihat hasilnya. Kolom “macAddress” mencakup alamat MAC WiFi (tanpa karakter titik dua).

Dari sini, Admin dapat melakukan beberapa tindakan dengan perangkat teridentifikasi termasuk melacak perangkat/pengguna tersebut, memblokir alamat MAC agar sama sekali tidak dapat bergabung ke jaringan, atau mengelompokkan perangkat tersebut ke dalam VLAN dengan akses terbatas. Dengan menggunakan sistem captive portal atau filter konten, administrator jaringan dapat mengalihkan perangkat teridentifikasi tersebut ke halaman dengan instruksi terkait cara menghubungi IT untuk mendapatkan dukungan atau cara mendaftarkan ulang perangkat (jika diizinkan oleh administrator).



## Setelan yang Direkomendasikan

- [Pendaftaran Ulang Paksa](#) - Setel ke “Paksa perangkat mendaftar ulang secara otomatis setelah dihapus total” [Artikel Dukungan Pendaftaran Ulang Paksa](#)
- [Powerwash](#) - Setel ke “Jangan izinkan powerwash dipicu” untuk semua pengguna, kecuali pengguna tertentu [Artikel Dukungan Powerwash](#)
- [Mode Terverifikasi](#) - Setel ke “Wajibkan booting mode terverifikasi untuk akses terverifikasi” [Artikel Dukungan Mode Terverifikasi](#)
- [Akses Terverifikasi](#) - Setel ke “Aktifkan untuk perlindungan konten” [Artikel Dukungan Akses Terverifikasi](#)
- [Izin pendaftaran ulang perangkat](#) - Pilih Unit Organisasi tertentu untuk pengguna yang diizinkan menggunakan setelan ini. [Artikel Dukungan Izin Pendaftaran](#)
- [Blokir akses](#) untuk URL internal berikut:

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