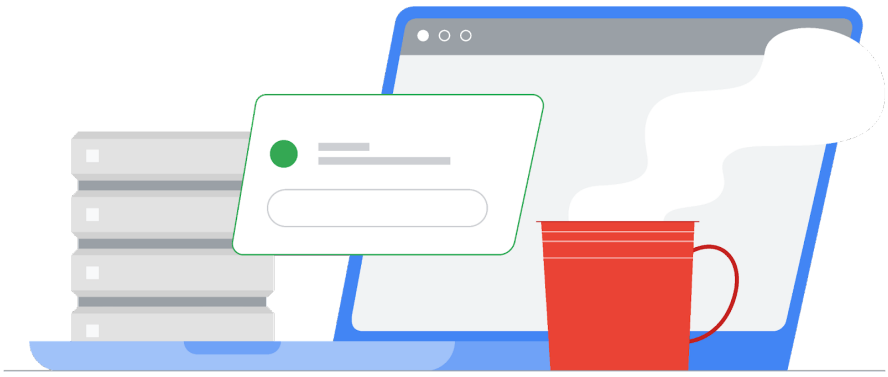
Google for Education

ChromeOS
Guía de prácticas recomendadas para monitorizar flotas

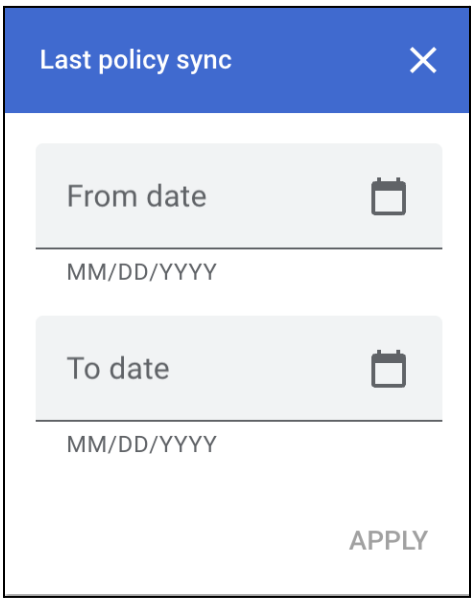
Febrero del 2023



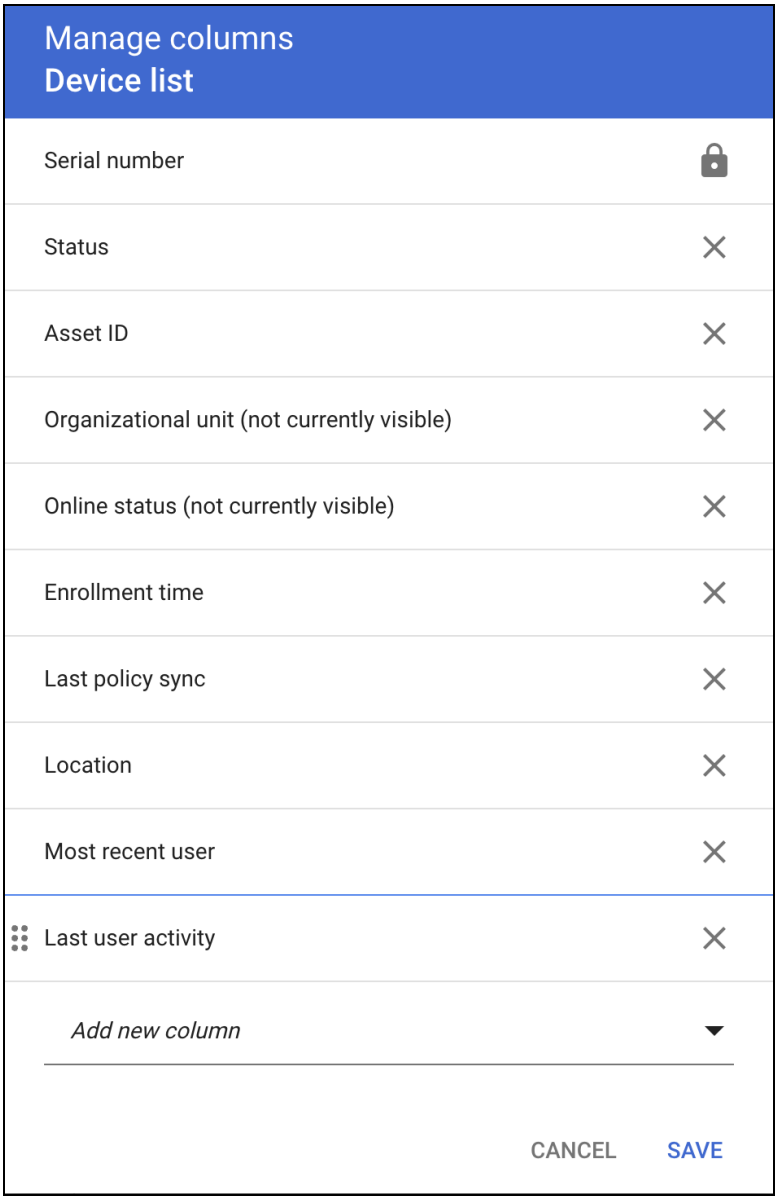
Índice

Buscar dispositivos en los que no se hayan sincronizado políticas recientemente

En la consola de administración, ve a Dispositivos > Chrome > Dispositivos para consultar un informe de todos los dispositivos, ordenados por la fecha de sincronización más reciente. Puedes añadir un filtro a la lista para que solo aparezcan los dispositivos que se hayan sincronizado en un periodo específico. Por ejemplo, los administradores pueden aplicar un filtro a "Última sincronización de políticas" con una fecha de inicio del 01/01/2022 y una fecha de finalización del 13/01/2023 para que solo se muestren los dispositivos que no tengan las políticas sincronizadas desde el 13 de enero del 2023 o principios de año.



Puedes editar las columnas de esta lista de dispositivos e incluir la columna "Usuario más reciente", que permite saber quién ha usado el dispositivo por última vez (el campo "Usuario" hace referencia al usuario que ha registrado el dispositivo, que no tiene por qué ser la persona que lo usa principalmente). Para editar las columnas, haz clic en el icono de la rueda dentada. En la parte inferior, haz clic en "*Añadir nueva columna*" y selecciona "Usuario más reciente". También puedes quitar columnas haciendo clic en la X. Cuando termines, haz clic en "GUARDAR".



De forma automática, los administradores también pueden recibir un informe de los dispositivos inactivos de la empresa que no se hayan sincronizado en los últimos 30 días.

Detectar si los usuarios registran sus dispositivos varias veces

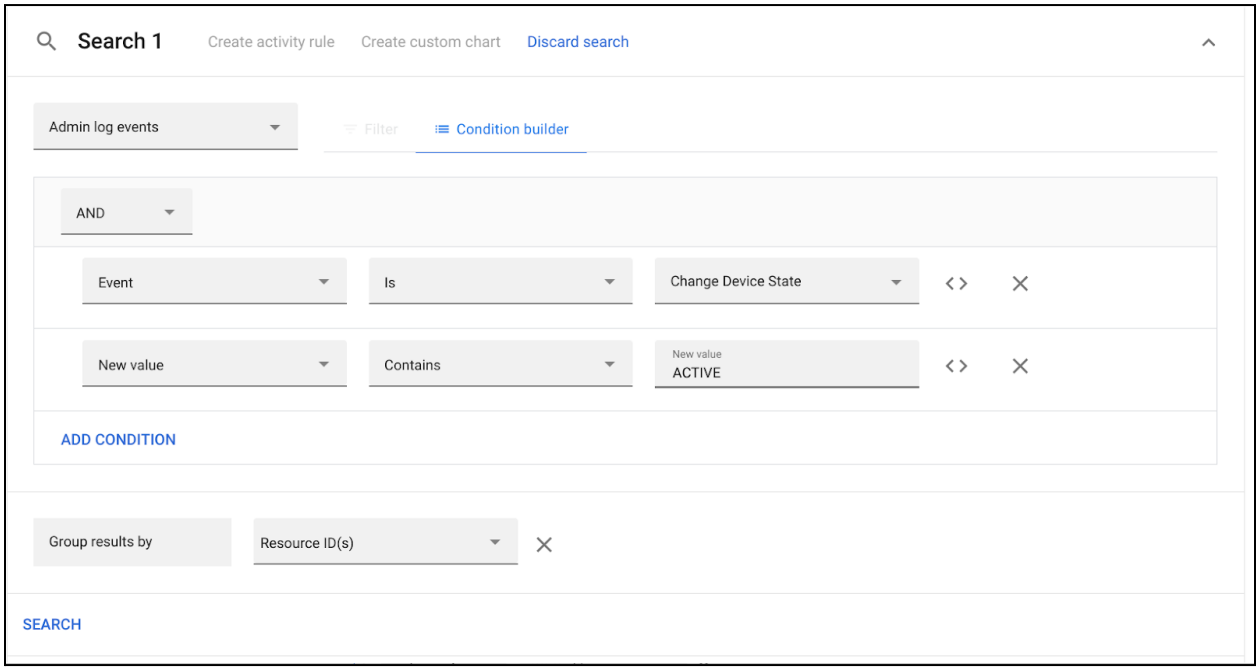
Si un usuario cancela reiteradamente el registro de su dispositivo para registrarlo de nuevo, esta información queda reflejada en los registros de auditoría para que los administradores estén al corriente. Con Google Workspace for Education Plus o Standard, este tipo de actividades pueden activar alertas automáticas o desencadenar acciones.

Si tienes Workspace for Education Plus o Standard

Investigar dispositivos

Puedes consultar más información sobre cómo usar la herramienta de investigación de seguridad.

- ➔ Ve a Informes → Investigación → Eventos de registro de administrador
- ➔ Haz clic en **Creador de condiciones**
- ➔ Añade la condición: "Evento" "Es" "Cambio de estado de dispositivo"
- ➔ Añade la condición: "Valor nuevo" "Contiene" "ACTIVE"
- ➔ Haz clic en **Agrupar resultados por** y selecciona "ID de recurso"



- ➔ Haz clic en **Buscar**

Si un usuario cancela frecuentemente el registro de un dispositivo específico para volverlo a registrar, es posible que esté actuando de forma deliberada.

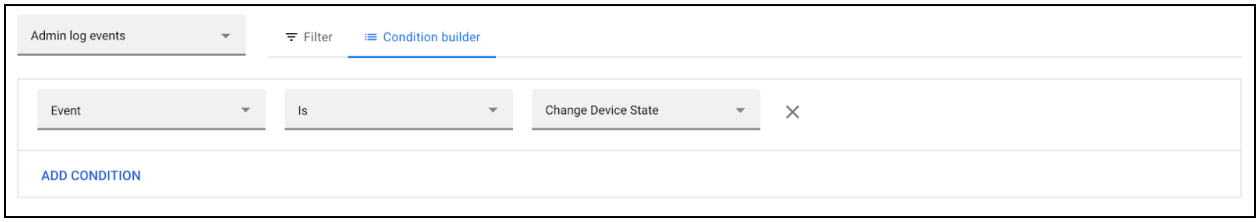
Crear una regla de actividad cuando se vuelva a registrar un dispositivo

Opcional: Arriba del todo, haz clic en "Crear regla de actividad" para guardar esta búsqueda como una regla y enviar notificaciones automáticas. Como puede haber falsos positivos, no te recomendamos que suspendas automáticamente a los usuarios que registren de nuevo sus dispositivos. Para obtener más información sobre cómo crear reglas de actividad, consulta Crear y gestionar reglas de actividad.

Si tienes Workspace for Education Fundamentals

Filtrar registros de auditoría

- ➔ Ve a Informes → Investigación → Eventos de registro de administrador
- ➔ Haz clic en **Creador de condiciones**
- ➔ Añade la condición: "Evento" "Es" "Cambio de estado de dispositivo"



- ➔ Haz clic en **Buscar**

Las columnas ID de recurso y Descripción siempre deben estar visibles de forma predeterminada.
Haz clic en **Exportar todo** para exportar los resultados a una hoja de cálculo de Google. Asigna un nombre al archivo de exportación y haz clic en **Exportar**.
Cuando el archivo haya terminado de exportarse, desplázate hasta "Resultados de la exportación" y haz clic en el nombre del archivo para abrir la hoja de cálculo de Google.
Para identificar qué dispositivos se han vuelto a registrar, añade una columna y prueba el texto "ACTIVE to ACTIVE" en la descripción. Abajo puedes ver una fórmula de ejemplo, donde "C" se corresponde con el campo "Descripción". Configura esta fórmula como la celda E1 de la hoja:

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

Inserta una tabla dinámica donde los encabezados de columna "ID de recurso" sean las filas, los encabezados de columna "Registrados de nuevo" sean las columnas y el cálculo de cualquier otro campo (como el encabezado de columna "Actor") sea el valor.

Impedir que los usuarios vuelvan a registrar dispositivos no autorizados

Algunas organizaciones permiten que los usuarios finales registren o vuelvan a registrar dispositivos. De esta forma, los usuarios pueden volver a registrar dispositivos mientras están en el trabajo o centro educativo y cancelar el registro mientras están desconectados de la red. Los administradores pueden inhabilitar este permiso para los usuarios si no quieren que puedan volver a registrar dispositivos fácilmente por su cuenta o, por el contrario, habilitarlo si prefieren que puedan hacerlo.

Para activar este ajuste en la consola de administración, ve a Dispositivos > Chrome > Configuración > Usuarios y navegadores. Selecciona la unidad organizativa (UO) correspondiente en la columna de la izquierda (por ejemplo, "Alumnos"). En "Permisos de registro", dentro de "Controles de registro", selecciona "No permitir que los usuarios de esta organización registren dispositivos nuevos o que ya hayan estado registrados anteriormente" para que los usuarios no puedan registrar dispositivos, o bien selecciona "Permitir que los usuarios de esta organización registren solo dispositivos que ya hayan estado registrados (es decir, no permitirles que registren dispositivos nuevos ni que se hayan dado de baja)" para que puedan volver a registrar dispositivos registrados previamente.

Monitorizar quién inicia sesión en dispositivos cuyo registro se ha cancelado

Los docentes o empleados pueden cambiar un ajuste de la política de dispositivos visual para detectar fácilmente los dispositivos no gestionados. Este cambio solo se aplicará a los dispositivos gestionados; no aparecerá en los dispositivos no gestionados.

Los administradores pueden elegir que los dispositivos siempre muestren información del sistema en la pantalla de inicio de sesión. En los dispositivos no gestionados no se mostrará la información "Gestionado por" o del sistema. Además, pueden cambiar el fondo de pantalla de inicio de sesión para que sea una imagen protegida.

En la consola de la lista de dispositivos, los administradores pueden monitorizar las sincronizaciones de políticas asociadas a usuarios recientes. Si comparan los datos de la lista de usuarios previstos con los de los usuarios con las políticas sincronizadas recientemente, pueden obtener una lista de los posibles usuarios con los dispositivos sin sincronizar. Pueden seguir monitorizando estos dispositivos para llevar a cabo una investigación física sobre el estado de su registro.

Detectar dispositivos que se han unido a una red gestionada mientras estaban sin gestionar

Puede sea posible determinar rápidamente qué Chromebooks deberían ser dispositivos gestionados cuando se unen a tu red Wi-Fi sin estar gestionados. Los administradores pueden usar la política DeviceHostnameTemplate para especificar un formato de nombre de host que puede incluir el número de serie o el ID de etiqueta de recurso. Este nombre de host se pueden consultar en las tablas de DHCP de la red. Si un dispositivo con una dirección MAC conocida se une a la red gestionada sin el nombre de host adecuado, lo más seguro es que se trate de un dispositivo cuyo registro se ha cancelado.

Por ejemplo: En la consola de administración, ve a Dispositivos > Chrome > Configuración > Dispositivo y desplázate hasta "Plantilla de nombre de host de red de dispositivo" en "Otros ajustes". Aplica una política de plantilla de nombre de host de red de "ManagedChromebook-${SERIAL_NUM}" a los Chromebooks gestionados. Estos dispositivos se mostrarán en el grupo de DHCP de la red del centro educativo con ese nombre de host configurado para identificarse fácilmente. Todas las demás concesiones en ese SSID o en esa red se mostrarán con un nombre de host genérico o sin definir. Si exportas las direcciones MAC de estos nombres de host genéricos o sin definir y las comparas con las direcciones MAC conocidas del cliente de Workspace de un archivo exportado, deberías poder identificar los dispositivos cuyo registro se ha cancelado.

Para exportar una lista de dispositivos con direcciones MAC de la red Wi-Fi, en la consola de administración, ve a Dispositivos > Chrome > Dispositivos, selecciona la UO en cuestión y haz clic en "Exportar" en la parte superior de la lista. El proceso de exportación aparecerá en la lista de tareas si haces clic en el icono del reloj de arena arriba a la derecha. Una vez completado, podrás descargar el CSV para ver los resultados. La columna "macAddress" incluye la dirección MAC de la red Wi-Fi (sin caracteres de dos puntos).

Aquí, los administradores pueden realizar distintas acciones con los dispositivos identificados, como rastrear esos dispositivos o usuarios, impedir que las direcciones MAC se unan a la red o segmentar esos dispositivos en una VLAN de acceso limitado. Con un filtro de contenido o un sistema de portal cautivo, los administradores de la red pueden redirigir esos dispositivos identificados a una página con instrucciones sobre cómo contactar con el equipo de TI en caso de necesitar asistencia o cómo volver a registrar sus dispositivos (si lo permite el administrador).

Ajustes recomendados

- ➔ Obligación de volver a realizar el registro: selecciona "Forzar la repetición automática del registro del dispositivo cuando se borren sus datos". Artículo del Centro de Ayuda sobre la obligación de volver a realizar el registro.
- ➔ Powerwash: selecciona "No permitir que se active la función Powerwash" solo para algunos usuarios, en vez de todos. Artículo del Centro de Ayuda sobre Powerwash.
- ➔ Modo verificado: selecciona "Requerir arranque en modo verificado para permitir el acceso verificado". Artículo del Centro de Ayuda sobre el modo verificado.
- ➔ Acceso verificado: selecciona "Habilitar la protección de contenido". Artículo del Centro de Ayuda sobre el acceso verificado.
- ➔ Permisos para volver a registrar dispositivos: selecciona las UOs específicas de los usuarios que tienen permiso.Artículo del Centro de Ayuda sobre los permisos de registro.
- ➔ Bloquea el acceso a las siguientes URLs internas:

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