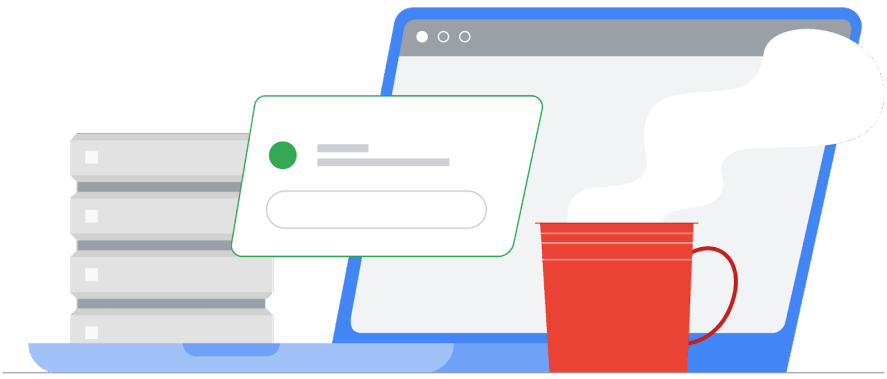
Google for Education

Guida alle best practice per il monitoraggio del parco risorse ChromeOS

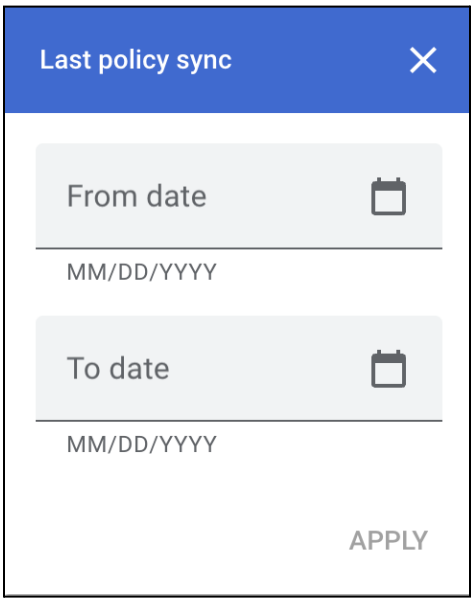
Febbraio 2023



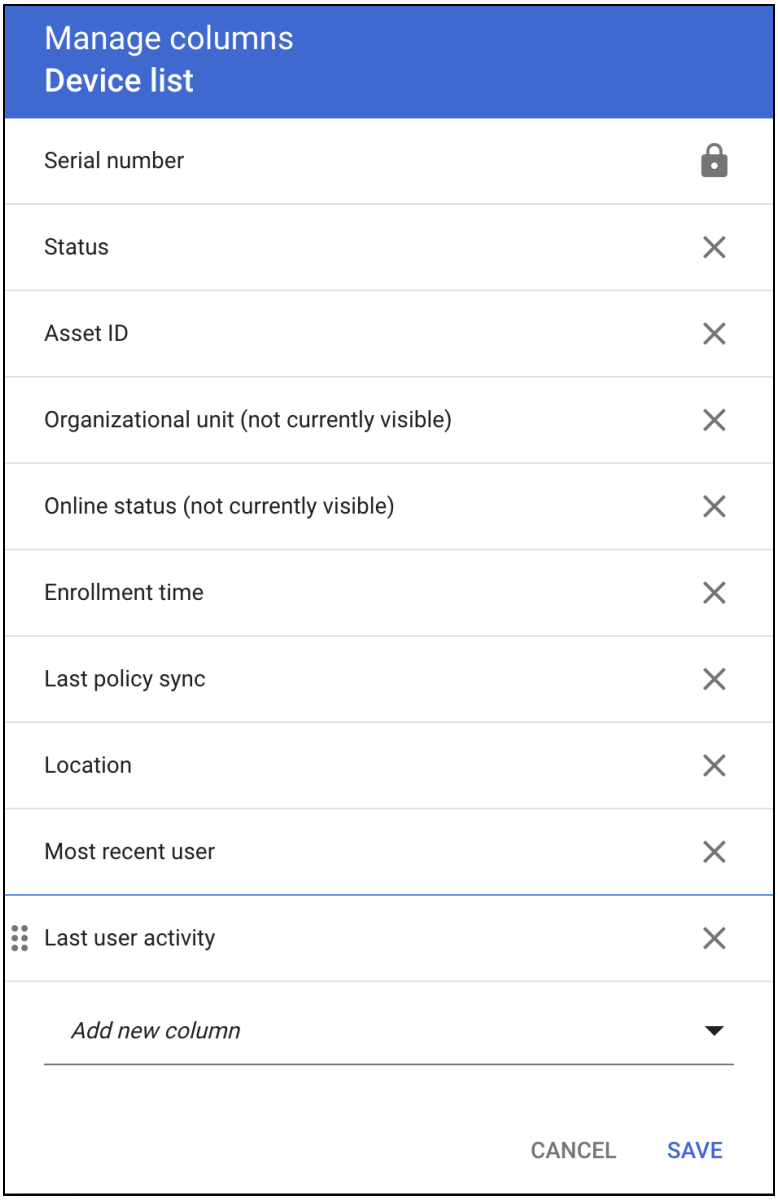
Sommario

Trovare i dispositivi che non hanno sincronizzato il criterio di recente

Nella Console di amministrazione, vai a Dispositivi > Chrome > Dispositivi per visualizzare un report di tutti i dispositivi, elencati in base all'ora dell'ultima sincronizzazione. È possibile aggiungere un filtro all'elenco per visualizzare i dispositivi sincronizzati in un determinato periodo di tempo. Ad esempio, un amministratore può impostare un filtro per "Ultima sincronizzazione criteri" con 01/01/2022 come "Data di inizio" e 13/01/2023 come "Data di fine" per mostrare solo i dispositivi che non hanno sincronizzato il criterio dal 13 gennaio 2023 o all'inizio dell'anno.



Le colonne per questo elenco di dispositivi possono essere modificate in modo che includano "Utente più recente", ossia l'ultimo utente che ha utilizzato il dispositivo (il campo "Utente" corrisponde all'utente che ha registrato il dispositivo, che potrebbe non essere l'utente principale del dispositivo). Per modificare le colonne visualizzate, fai clic sull'icona a forma di ingranaggio, in basso fai clic su "*Aggiungi nuova colonna*" e seleziona "Utente più recente". Puoi anche rimuovere le colonne facendo clic sulla X. Al termine, fai clic su "SALVA".



Inoltre, gli amministratori possono ricevere automaticamente un report sui dispositivi aziendali inattivi che non hanno effettuato la sincronizzazione negli ultimi 30 giorni.

Rilevare se gli utenti registrano ripetutamente i dispositivi

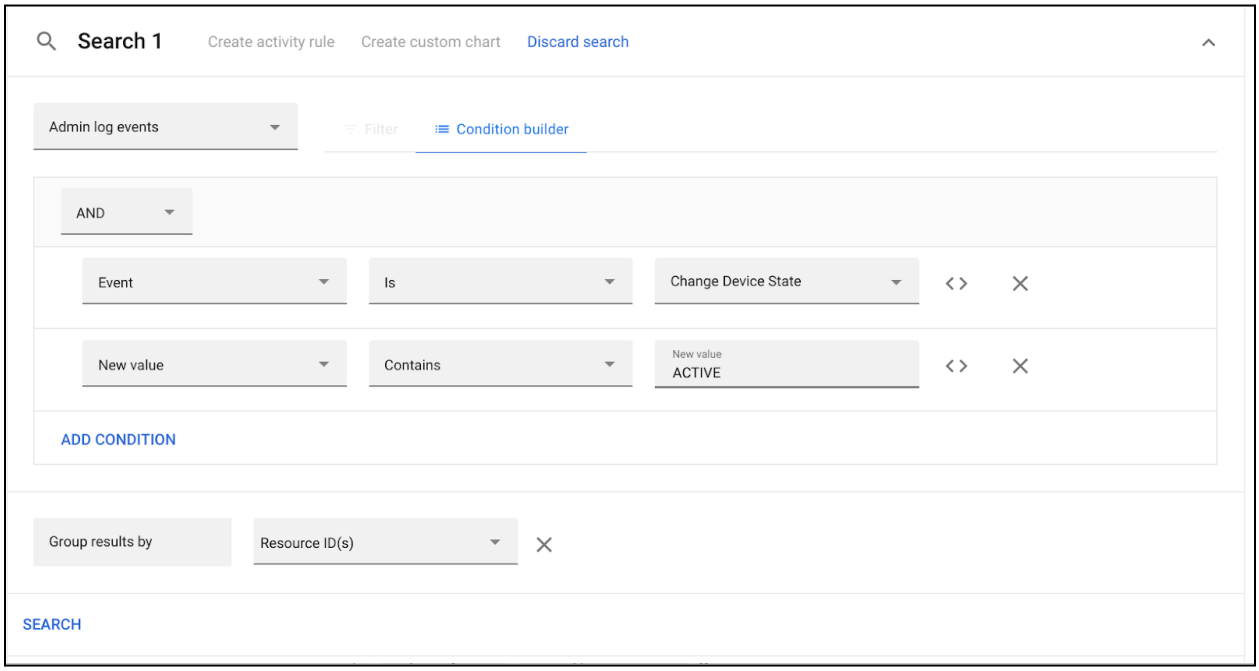
Se un utente annulla la registrazione del dispositivo e poi lo registra di nuovo ripetutamente, i log di controllo possono acquisire queste informazioni e rivelarle agli amministratori. Con Google Workspace for Education Plus o Standard, queste registrazioni ripetute dei dispositivi possono attivare azioni o avvisi automatici.

Se hai Workspace for Education Plus o Standard

Esamina i dispositivi

Per saperne di più su come utilizzare lo strumento di indagine, vedi Strumento di indagine sulla sicurezza.

➔ Vai a Reporting → Indagine → Eventi dei log amministrativi
➔ Fai clic su **Generatore di condizioni**
➔ Aggiungi una condizione in cui "Evento" "È" "Modifica stato dispositivo"
➔ Aggiungi una condizione in cui "Nuovo valore" "Contiene" "ATTIVO"
➔ Fai clic su **Raggruppa risultati per** e seleziona "Raggruppa per ID risorsa"



➔ Fai clic su **Cerca**

Le occorrenze frequenti di dispositivi specifici che vengono registrati nuovamente potrebbero indicare che gli utenti stanno annullando la registrazione e registrando nuovamente i dispositivi in modo intenzionale.

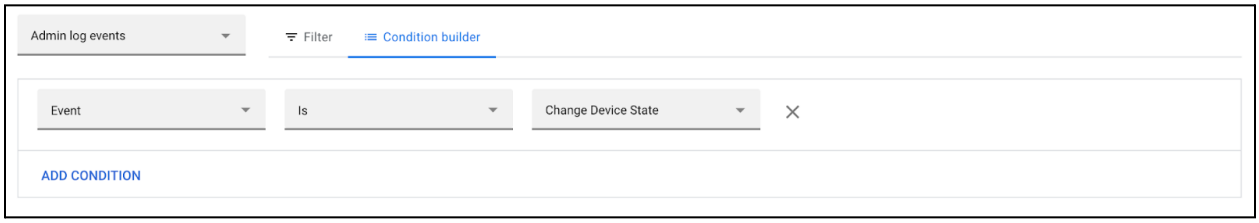
Crea una regola di attività per le nuove registrazioni

(Facoltativo) Fai clic su "Crea regola attività" in alto per salvare questa ricerca come regola e inviare notifiche automatiche. La sospensione automatica degli utenti che registrano nuovamente i dispositivi non è consigliata al momento a causa della possibilità di falsi positivi. Per maggiori informazioni sulla creazione di regole di attività, consulta Creare e gestire le regole di attività.

Se hai Workspace for Education Fundamentals

Filtra log di controllo

- ➔ Vai a Reporting → Indagine → Eventi dei log amministrativi
- ➔ Fai clic su **Generatore di condizioni**
- ➔ Aggiungi una condizione in cui "Evento" "È" "Modifica stato dispositivo"



- ➔ Fai clic su **Cerca**

Le colonne relative a ID risorsa e descrizione dovrebbero essere visibili per impostazione predefinita.
Fai clic su **Esporta tutto** per esportare i risultati in un foglio Google. Fornisci un nome per l'esportazione e fai clic su **Esporta**.
Quando l'esportazione è terminata, scorri verso il basso fino a "Esporta risultati azione" e fai clic sul nome dell'esportazione per aprire il foglio Google.
Identifica i dispositivi di cui è in corso una nuova registrazione aggiungendo una colonna e testando il testo "da ATTIVO ad ATTIVO" nella descrizione. Vedi una formula di esempio di seguito in cui C è il campo Descrizione. Imposta questa formula come cella E1 del foglio:

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

Inserisci una tabella pivot utilizzano le intestazioni di colonna "ID risorsa" come righe, l'intestazione di colonna "Registrati nuovamente" come colonne e il conteggio di eventuali altri campi, ad esempio l'intestazione di colonna "Attore", come valore.

Impedire agli utenti di registrare dispositivi non autorizzati

Alcune organizzazioni consentono agli utenti finali di registrare o registrare nuovamente i dispositivi. Questa autorizzazione consentirebbe agli utenti di registrare nuovamente dispositivi mentre sono a scuola o al lavoro e annullarne la registrazione quando si trovano al di fuori della rete. Gli amministratori possono valutare la possibilità di disabilitare questa autorizzazione per gli utenti se non vogliono che questi siano in grado di registrare nuovamente i dispositivi in modo autonomo o abilitarla se vogliono che gli utenti abbiano questa possibilità.

Per attivare/disattivare questa impostazione nella Console di amministrazione, vai a Dispositivi > Chrome > Impostazioni > Utenti e browser. Seleziona la UO pertinente nella colonna a sinistra (ad esempio, "Studenti"). Per "Autorizzazioni di registrazione" in "Controlli di registrazione" seleziona "Non consentire agli utenti di questa organizzazione di registrare dispositivi nuovi o di registrare nuovamente dispositivi esistenti" per impedire agli utenti di registrare dispositivi o "Consenti agli utenti di questa organizzazione di registrare di nuovo soltanto dispositivi esistenti (non consentire la registrazione di dispositivi nuovi o di cui è stato eseguito il deprovisioning)" per consentire agli utenti di registrare nuovamente i dispositivi esistenti.

Monitorare l'accesso degli utenti sui dispositivi di cui è stata annullata la registrazione

Per consentire a insegnanti e dipendenti di individuare più facilmente i dispositivi non gestiti, è possibile modificare un'impostazione di visualizzazione dei criteri relativi ai dispositivi. Questa modifica si applica solo ai dispositivi gestiti attualmente. I dispositivi non gestiti non mostreranno la modifica.

Gli amministratori possono configurare i dispositivi affinché mostrino sempre le informazioni sul sistema nella schermata di accesso. I dispositivi non gestiti non mostreranno le informazioni sul sistema o l'informazione "Gestito da". Inoltre, lo sfondo di accesso può essere modificato con un'immagine protetta.

Gli amministratori possono monitorare l'elenco di dispositivi nella Console per verificare le sincronizzazioni dei criteri associate agli utenti recenti. Il controllo incrociato tra l'elenco di utenti previsto e gli utenti con criteri sincronizzati di recente può restituire un elenco di potenziali utenti con dispositivi che non sono stati sincronizzati. Questi dispositivi rimanenti possono essere ulteriormente monitorati per un'eventuale indagine fisica sul relativo stato di registrazione.

Individuare i dispositivi che sono entrati in una rete gestita mentre erano in stato non gestito

Puoi determinare rapidamente i Chromebook che dovrebbero essere gestiti quando accedono alla tua rete Wi-Fi in stato non gestito. Gli amministratori possono utilizzare il criterio DeviceHostnameTemplate per specificare il formato di un nome host che può includere numero di serie e/o ID etichetta asset. Questo nome host è visibile nelle tabelle DHCP di rete. Se un dispositivo con un indirizzo MAC noto entra nella rete gestita senza il nome host appropriato, si tratterà probabilmente di un dispositivo di cui è stata annullata la registrazione.

Ad esempio: Nella Console di amministrazione vai a Dispositivi > Chrome > Impostazioni > Dispositivo e scorri verso il basso fino a "Modello del nome host della rete del dispositivo" in "Altre impostazioni". Applica un criterio per modello del nome host della rete di "ManagedChromebook-${SERIAL_NUM}" ai Chromebook gestiti. Verrà visualizzato nel pool DHCP della rete di una scuola con quel nome host configurato facilmente identificabile. Tutti gli altri lease su questa rete/SSID verranno visualizzati con un nome host generico o non definito. L'esportazione degli indirizzi MAC di questi nomi host generici o non definiti e il confronto con un'esportazione degli indirizzi MAC noti di un tenant di Workspace dovrebbero contribuire a identificare il dispositivo di cui è stata annullata la registrazione.

Per esportare un elenco di dispositivi con indirizzi MAC Wi-Fi, nella Console di amministrazione vai a Dispositivi > Chrome > Dispositivi, seleziona l'UO che ti interessa, quindi fai clic su "Esporta" sull'elenco. Il processo di esportazione verrà visualizzato nell'elenco delle attività facendo clic sull'icona della clessidra in alto a destra. Al termine, puoi scaricare il file CSV per vedere i risultati. La colonna "macAddress" comprende gli indirizzi MAC WiFi (senza i caratteri dei due punti).

Da qui, l'amministratore può intraprendere diverse azioni con i dispositivi identificati, tra cui individuare questi dispositivi e utenti, impedire che gli indirizzi MAC entrino completamente nella rete o segmentare questi dispositivi in una VLAN ad accesso limitato. Utilizzando un sistema di filtro dei contenuti o di captive portal, gli

amministratori di rete possono reindirizzare questi dispositivi identificati a una pagina con le istruzioni su come contattare il team IT per l'assistenza o su come registrare nuovamente i dispositivi (se consentito dall'amministratore).

Impostazioni consigliate

- ➔ Nuova registrazione forzata: imposta su "Forza la nuova registrazione automatica del dispositivo in seguito alla cancellazione dei dati" Articolo del Centro assistenza sulla Nuova registrazione forzata
- ➔ Powerwash: imposta su "Non consentire l'attivazione di Powerwash" per tutti tranne per utenti selezionati Articolo del Centro assistenza su Powerwash
- ➔ Modalità verificata: imposta su "Richiedi l'avvio in modalità verificata per l'Accesso verificato" Articolo del Centro assistenza sulla Modalità verificata
- ➔ Accesso verificato: imposta su "Abilita per la protezione dei contenuti" Articolo del Centro assistenza sull'Accesso verificato
- ➔ Autorizzazioni per la nuova registrazione del dispositivo: seleziona OrgUnits specifiche di utenti autorizzati. Articolo del Centro assistenza sulle autorizzazioni di registrazione
- ➔ Blocca l'accesso ai seguenti URL interni:

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