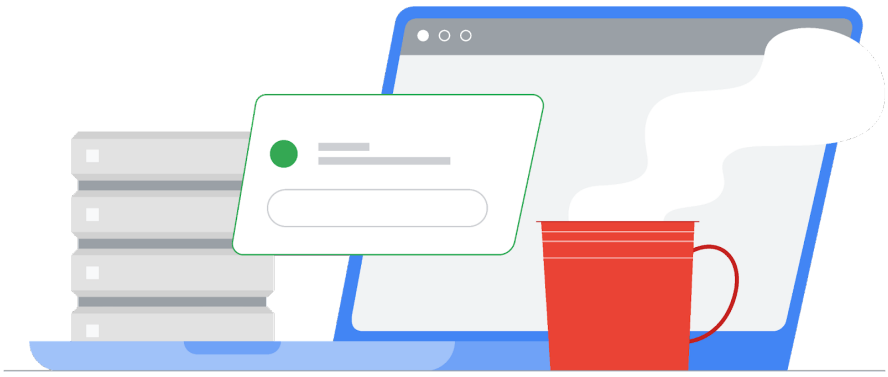
Google for Education

ChromeOS
Guide des bonnes pratiques de surveillance du parc

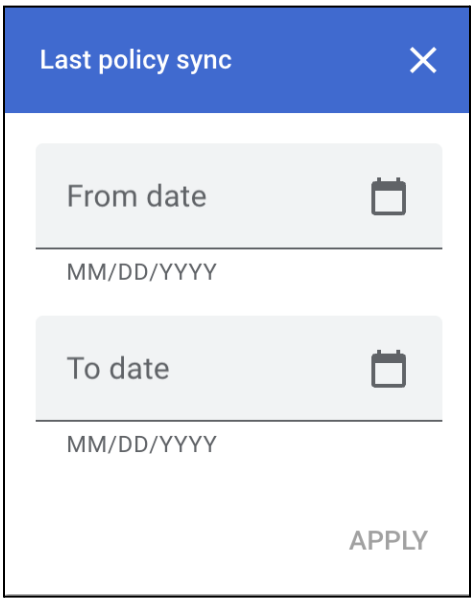
Février 2023



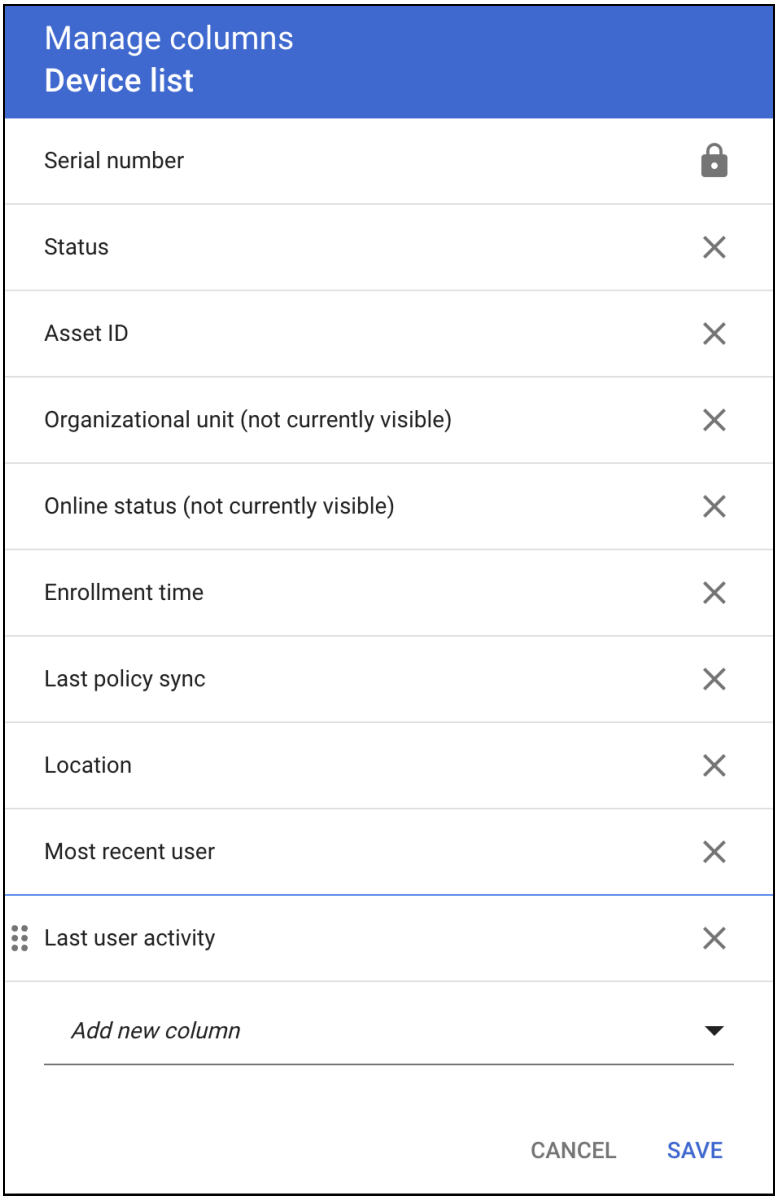
Sommaire

Trouver les appareils n'ayant pas synchronisé les règles récemment

Dans la console d'administration, accédez à Appareils > Chrome > Appareils pour consulter un rapport sur l'ensemble des appareils triés par date de la dernière synchronisation. Vous pouvez ajouter un filtre pour afficher les appareils qui ont effectué la synchronisation au cours d'une période spécifique. Par exemple, un administrateur peut ajouter le filtre "Dernière synchronisation des règles", et définir "01/01/2022" dans le champ "Du" et "13/01/2023" dans le champ "Au". Ainsi, seuls les appareils qui ont synchronisé les règles entre ces dates s'afficheront.



Les colonnes de cette liste des appareils peuvent être modifiées pour inclure la valeur "Dernier utilisateur", qui correspond au dernier utilisateur de l'appareil (le champ "Utilisateur" correspond à l'utilisateur ayant enregistré l'appareil, qui n'est pas forcément son utilisateur principal). Pour modifier les colonnes affichées, cliquez sur l'icône en forme de roue dentée. Ensuite, en bas de la page, cliquez sur *Ajouter une colonne* et sélectionnez "Dernier utilisateur". Vous pouvez également supprimer des colonnes en cliquant sur l'icône X. Lorsque vous avez terminé, cliquez sur ENREGISTRER.



Les administrateurs peuvent également choisir de recevoir automatiquement un rapport sur les appareils inactifs de l'entreprise qui n'ont pas effectué de synchronisation au cours des 30 derniers jours.

Identifier les utilisateurs qui réenregistrent leur appareil de manière répétée

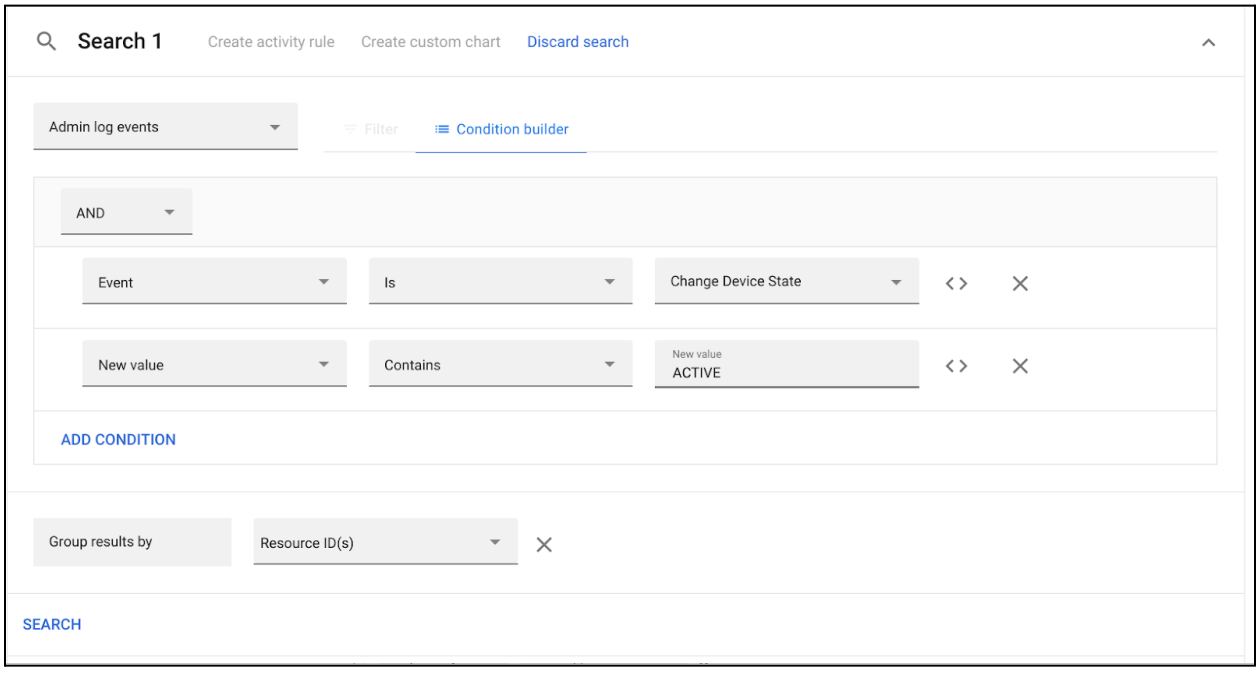
Si un utilisateur annule l'enregistrement de son appareil et le réenregistre de manière répétée, les journaux d'audit peuvent afficher cette information pour en informer les administrateurs. Avec Google Workspace for Education Plus ou Standard, ces réenregistrements peuvent déclencher des alertes ou actions automatiques.

Si vous disposez de Workspace for Education Plus ou Standard

Enquêter sur les appareils

Pour découvrir comment utiliser l'outil d'investigation, accédez à la page Outil d'investigation de sécurité.

➔ Accédez à Reporting → Investigation → Événements du journal d'administration.
➔ Cliquez sur **Générateur de conditions**.
➔ Ajoutez une condition où "Événement" "Est" "Modification de l'état d'un appareil".
➔ Ajoutez une deuxième condition où "Nouvelle valeur" "Contient" "ACTIF".
➔ Cliquez sur **Grouper les résultats par** et sélectionnez "ID des ressources".



➔ Cliquez sur **Rechercher**.

Si des appareils spécifiques sont fréquemment réenregistrés, cela peut signifier que les utilisateurs annulent l'enregistrement de leur appareil et le réenregistrent volontairement.

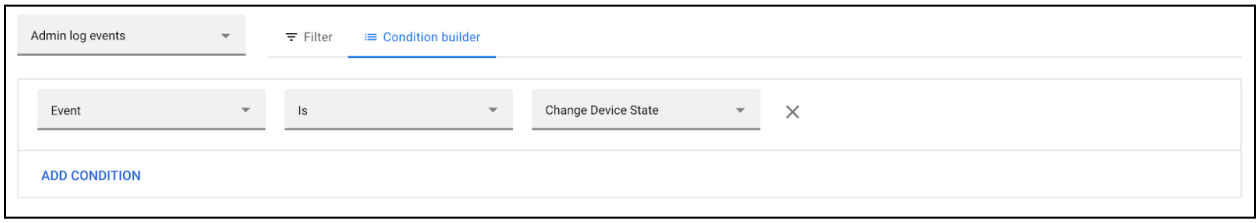
Créer une règle d'activité pour les réenregistrements

Facultatif : Cliquez sur "Créer une règle d'activité" en haut pour enregistrer cette recherche en tant que règle et activer l'envoi automatique de notifications. Pour le moment, nous déconseillons de suspendre automatiquement les comptes des utilisateurs qui réenregistrent leur appareil en raison de faux positifs potentiels. Pour en savoir plus sur la création de règles d'activité, consultez Créer et gérer des règles d'activité.

Si vous disposez de Workspace for Education Fundamentals

Filtrer les journaux d'audit

- ➔ Accédez à Reporting → Investigation → Événements du journal d'administration.
- ➔ Cliquez sur **Générateur de conditions**.
- ➔ Ajoutez une condition où "Événement" "Est" "Modification de l'état d'un appareil".



- ➔ Cliquez sur **Rechercher**.

Les colonnes "ID des ressources" et "Description" doivent s'afficher par défaut.
Cliquez sur **Tout exporter** pour exporter vos résultats de recherche dans une feuille de calcul Google Sheets. Nommez l'exportation et cliquez sur **Exporter**.
Une fois l'exportation terminée, faites défiler la page jusqu'à "Exporter les résultats de l'action" et cliquez sur le nom de l'exportation pour ouvrir la feuille de calcul Google Sheets.
Identifiez les appareils réenregistrés en ajoutant une colonne et en testant le texte "ACTIVE to ACTIVE" dans la description. Dans la formule d'exemple ci-dessous, "C" correspond au champ "Description". Insérez-la dans la cellule E1 de la feuille :

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

Insérez un tableau croisé dynamique en utilisant l'en-tête de colonne "ID des ressources" pour les lignes, l'en-tête de colonne "Réenregistré" pour les colonnes et les autres champs, comme l'en-tête de colonne "Acteur", pour les valeurs.

Empêcher les utilisateurs d'enregistrer des appareils non autorisés

Certaines organisations autorisent les utilisateurs finaux à enregistrer ou réenregistrer des appareils. Dans ce cas, les utilisateurs peuvent réenregistrer des appareils lorsqu'ils se trouvent à l'école ou au travail, puis annuler leur enregistrement en dehors du réseau. Les administrateurs peuvent désactiver cette autorisation s'ils ne souhaitent pas que les utilisateurs puissent facilement réenregistrer leurs appareils eux-mêmes, ou l'activer dans le cas contraire.

Pour activer ou désactiver ce paramètre dans la console d'administration, accédez à Appareils > Chrome > Paramètres > Utilisateurs et navigateurs. Sélectionnez l'UO pertinente dans la colonne de gauche ("Élèves", par exemple). Dans "Autorisations d'enregistrement" sous "Paramètres d'enregistrement", sélectionnez "Ne pas autoriser les utilisateurs de cette organisation à enregistrer ou à réenregistrer des appareils" pour empêcher les utilisateurs d'enregistrer des appareils, ou "Autoriser les utilisateurs de cette organisation uniquement à réenregistrer des appareils (interdiction d'enregistrer de nouveaux appareils ou des appareils déprovisionnés)" pour les autoriser à réenregistrer des appareils existants.

Surveiller les connexions des utilisateurs sur des appareils dont l'enregistrement a été annulé

Pour que les enseignants ou les employés puissent identifier les appareils non gérés plus facilement, il est possible de modifier le paramètre visuel des règles relatives aux appareils. Cette modification ne sera appliquée qu'aux appareils gérés à ce moment, et non aux appareils non gérés.

Les administrateurs peuvent définir les appareils sur Toujours afficher les informations système sur l'écran de connexion. Les appareils non gérés n'afficheront pas "Géré par" ni les informations système. De plus, le fond d'écran de connexion peut être remplacé par une image protégée.

Les administrateurs peuvent surveiller la liste des appareils dans la console pour identifier les synchronisations des règles associées aux utilisateurs récents. Comparer

la liste des utilisateurs attendus à celle des utilisateurs ayant récemment synchronisé les règles permet d'identifier les utilisateurs d'appareils n'ayant pas effectué de synchronisation. Il est alors possible d'intervenir physiquement sur ces appareils pour confirmer leur état d'enregistrement.

Identifier les appareils qui ont rejoint un réseau géré en étant non gérés

Il est possible d'identifier rapidement les Chromebooks devant être gérés lorsqu'ils rejoignent votre réseau Wi-Fi en étant non gérés. Les administrateurs peuvent utiliser la règle DeviceHostnameTemplate pour spécifier un format de nom d'hôte pouvant inclure un numéro de série et/ou un identifiant d'appareil. Ce nom d'hôte est visible dans les tables DHCP du réseau. Si un appareil avec une adresse MAC rejoint le réseau géré sans le nom d'hôte correct, il s'agit probablement d'un appareil dont l'enregistrement a été annulé.

Exemple : Dans la console d'administration, accédez à Appareils > Chrome > Paramètres > Appareil et faites défiler la page jusqu'à "Modèle de nom d'hôte du réseau de l'appareil", sous "Autres paramètres". Appliquez un modèle de règle de nom d'hôte du réseau de type "ManagedChromebook-${SERIAL_NUM}" aux Chromebooks gérés. Ce modèle apparaît alors dans le groupe DHCP du réseau d'une école avec un nom d'hôte configuré facilement identifiable. Tous les autres baux de ce SSID/réseau apparaîtront avec un nom d'hôte générique ou non défini. Exporter les adresses MAC de ces noms d'hôte et les comparer à l'exportation des adresses MAC connues d'un locataire Workspace devrait vous aider à identifier les appareils dont l'enregistrement a été annulé.

Pour exporter la liste des appareils avec une adresse MAC de Wi-Fi, accédez à Appareils > Chrome > Appareils dans la console d'administration, puis sélectionnez l'UO de votre choix et cliquez sur "Exporter" au-dessus de la liste. Le processus d'exportation apparaîtra dans la liste des tâches si vous cliquez sur l'icône en forme de sablier en haut à droite. Une fois l'exportation terminée, vous pouvez télécharger le fichier CSV pour consulter les résultats. La colonne "macAddress" inclut l'adresse MAC du Wi-Fi (sans deux-points).

L'administrateur peut ensuite effectuer plusieurs actions concernant les appareils identifiés, y compris retrouver ces appareils et leurs utilisateurs, empêcher complètement les adresses MAC de rejoindre le réseau ou isoler les appareils dans un VLAN à accès limité. En utilisant un filtre de contenu ou un système de portail captif, les administrateurs réseau peuvent rediriger les appareils identifiés vers une page

contenant des instructions sur la façon de contacter l'assistance informatique ou de réenregistrer leur appareil (si l'administrateur le permet).

Paramètres recommandés

- ➔ Réenregistrement forcé : défini sur "Forcer le réenregistrement automatique de l'appareil après un effacement de données" (article du Centre d'aide)
- ➔ Powerwash : défini sur "Ne pas autoriser le déclenchement de Powerwash" pour tous les utilisateurs, sauf ceux sélectionnés (article du Centre d'aide)
- ➔ Mode validé : défini sur "Exiger le démarrage en mode validé pour l'accès validé" (article du Centre d'aide)
- ➔ Accès validé : défini sur "Activer la protection du contenu" (article du Centre d'aide)
- ➔ Autorisations de réenregistrement des appareils : sélectionnez les UO d'utilisateurs autorisés (article du Centre d'aide)
- ➔ Bloquez l'accès aux URL internes suivantes :

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