chrome enterprise

Bonnes pratiques de gestion cloud du navigateur Chrome

Sommaire

Introduction

Bienvenue dans la gestion cloud du navigateur Chrome ! Ce guide accompagne le Guide de gestion cloud du navigateur Chrome.

Vous y trouverez des explications détaillées pour :

- configurer votre console d'administration Google ;
- configurer une structure d'unités organisationnelles (UO) pour répartir vos machines ;
- comprendre comment enregistrer et gérer vos navigateurs sur différents systèmes d'exploitation, y compris en évaluant les limitations connues ;
- comprendre le fonctionnement des règles si une stratégie de groupe (GPO) est déjà en place ;
- activer le reporting sur vos appareils pour les extensions, et plus encore.

Étape 1

Accéder à la console d'administration (admin.google.com)

Les options sont les suivantes :

- Utiliser la console d'administration existante
- Créer une console depuis la page d'inscription

Étape 2

Configurer des UO (voir la procédure détaillée)

Étape 3

Configurer des comptes administrateur (voir la procédure détaillée)

Étape 4

Enregistrer des appareils

(voir la procédure détaillée et d'autres méthodes employées avec divers outils de déploiement)

Options pour accéder à la gestion cloud du navigateur Chrome

Pour bien vous lancer dans la configuration de la gestion cloud du navigateur Chrome, nous vous recommandons de suivre ce guide. Il aborde toutes les étapes de la configuration initiale. La gestion cloud du navigateur Chrome ne génère pas de frais supplémentaires. Il existe deux options pour accéder à la console d'administration :

1. Utiliser votre propre domaine (aucun service Google existant associé)
   - 10 comptes administrateur sont autorisés au total.
   - La gestion cloud du navigateur Chrome peut être associée directement au domaine de votre entreprise (une fois que vous avez validé votre domaine).
2. Utiliser votre propre domaine (services Google déjà associés)
   - La console d'administration est déjà configurée et validée.
   - Cette option ne génère pas de frais supplémentaires et n'utilise aucune de vos licences Google.
   - Le nombre de comptes administrateur autorisés dépendra du service Google associé.

La meilleure solution est d'utiliser la console d'administration Google existante de votre entreprise, le cas échéant. Si la console est configurée, la gestion cloud du navigateur Chrome est déjà présente. Il vous suffit d'accéder à la section correspondante dans la console et d'accepter les conditions d'utilisation.

Accéder à une console d'administration Google existante

Avant de créer un compte administrateur Google, vérifiez en interne si votre entreprise n'en possède pas déjà un. De nombreuses entreprises ont des comptes pour accéder à différents services Google comme Chrome OS, Google Workspace ou d'autres.

Le super-administrateur de votre entreprise doit configurer votre compte administrateur pour vous donner accès à la console où se trouve la gestion cloud du navigateur Chrome.

- Il doit également ajouter la licence de gestion cloud du navigateur Chrome à la console d'administration. Pour l'activer, il suffit d'accéder à la section "Gérer le navigateur" et de cliquer sur le bouton "Commencer" afin d'ajouter la licence sans frais à votre console d'administration Google.

La console permet de bénéficier d'une administration basée sur les rôles. Le super-administrateur peut donc vous fournir un accès limité à ce dont vous avez besoin pour gérer le navigateur Chrome.

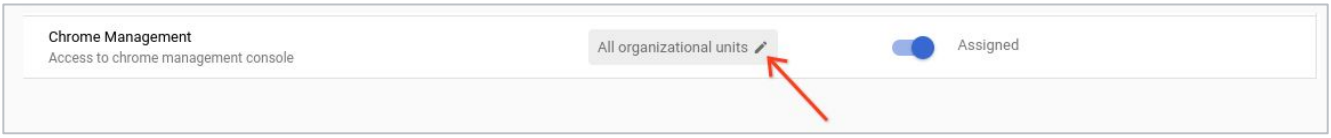
- Notez qu'un compte super-administrateur est requis pour générer d'autres comptes administrateur.
- Envisagez de demander un compte super-administrateur pour votre équipe afin de pouvoir générer le vôtre ultérieurement, si nécessaire.
- Si vous ne parvenez pas à retrouver le propriétaire d'origine en interne (par exemple, si la personne a quitté l'entreprise), cliquez sur ce lien pour en savoir plus sur la récupération de domaine.

Si votre entreprise possède déjà un compte dont vous n'êtes pas le super-administrateur, voici la procédure à suivre pour accéder à la gestion cloud du navigateur Chrome :

1. Demandez à un super-administrateur de se connecter sur la page admin.google.com et d'ajouter la licence de gestion cloud du navigateur Chrome à la console d'administration. Pour l'activer, il suffit d'accéder à la section "Gérer le navigateur" et de cliquer sur le bouton "Commencer" afin d'ajouter la licence sans frais à votre console d'administration Google.
2. Demandez au super-administrateur soit de créer un compte avec des droits de super-administrateur et de vous l'attribuer, soit d'accorder les droits suivants dans la console d'administration, s'il souhaite simplement vous donner accès à la gestion cloud du navigateur Chrome :
3. Sous **Compte > Rôles d'administrateur**, cliquez sur le bouton "Créer un rôle" et donnez-lui un nom, par exemple **Gestion du navigateur Chrome**.
4. Cochez l'option "Unités organisationnelles" pour accorder les droits suivants :
   - "Lire", "Créer", "Mettre à jour" et "Supprimer"
5. Sous "Gestion de Chrome", cochez "Paramètres" pour accorder tous les droits de gestion de Chrome.

Remarque : Si votre super-administrateur souhaite restreindre davantage les droits associés à ce compte administrateur, il peut créer une UO uniquement pour la gestion du navigateur Chrome et lui attribuer le rôle personnalisé.
Pour cela, il doit procéder comme suit :

1. Dans la console d'administration, accédez à **Annuaire > Utilisateurs** et sélectionnez le compte utilisateur auquel vous souhaitez attribuer le rôle de gestion du navigateur Chrome.
2. Faites défiler la page vers le bas et cliquez sur la section "Rôles et droits d'administrateur".
3. Sélectionnez le rôle personnalisé de gestion du navigateur Chrome créé lors des étapes précédentes, puis cliquez sur le bouton pour l'attribuer à l'utilisateur.
4. Une fois le rôle attribué, cliquez sur l'icône en forme de crayon sur le bouton **Toutes les unités organisationnelles** et sélectionnez la ou les UO auxquelles vous souhaitez donner à l'administrateur l'accès.



- Une fois connecté, l'administrateur ne verra aucune autre UO en dehors de celles auxquelles vous lui avez donné accès.

Cependant, il disposera de tous les droits pour gérer Chrome et créer des UO sous celle qui lui a été attribuée.

- Vous pouvez également afficher les modifications apportées dans la console à des fins d'audit. Consultez Journal d'audit de la console d'administration.

Utiliser votre propre domaine

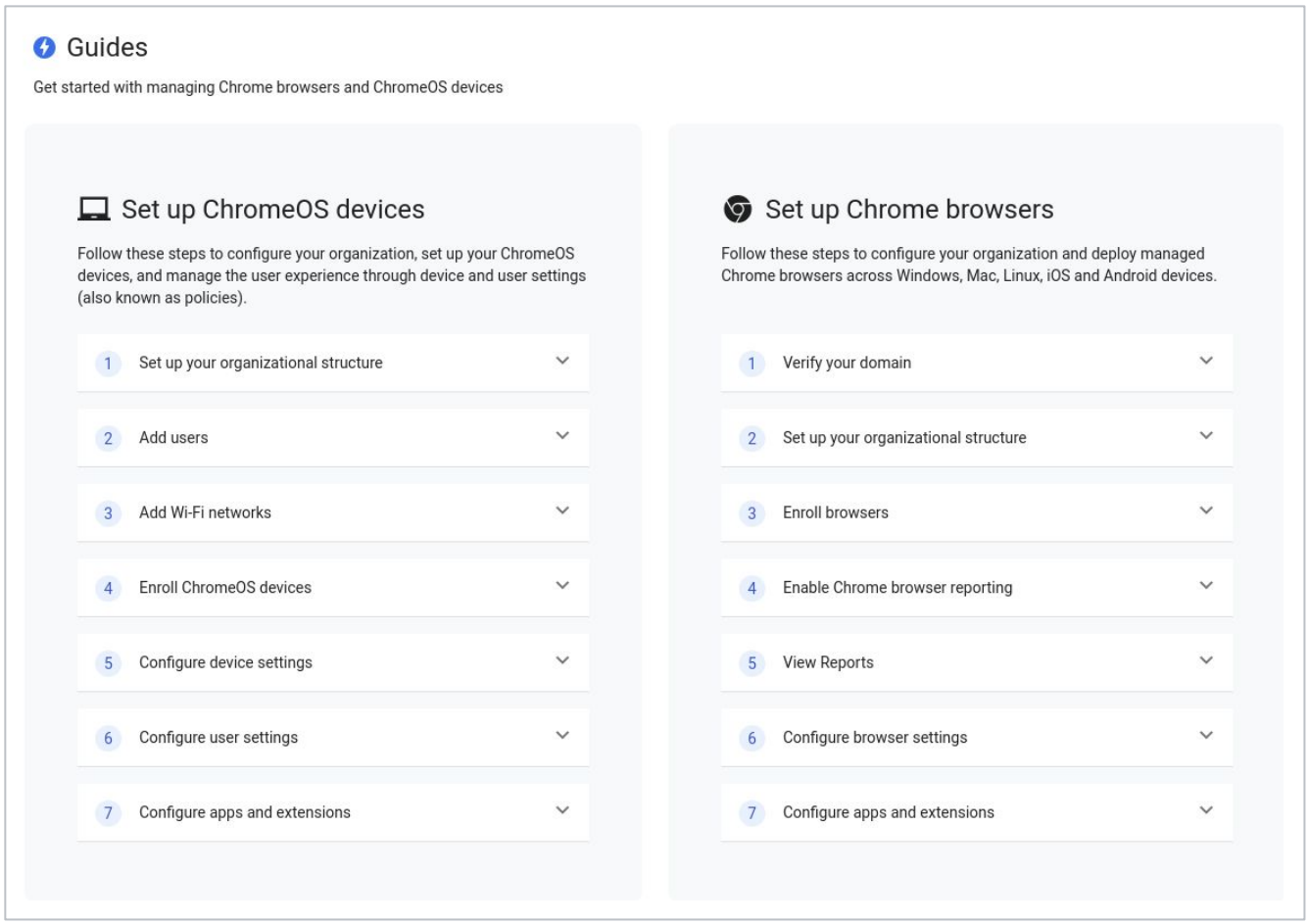
Si vous souhaitez utiliser le domaine de votre entreprise, mais que vous ne possédez pas encore de service Google, vous pouvez vous inscrire via ce lien. Google vous fournira une console d'administration sans frais supplémentaires.

- Lorsque la console d'administration est lancée pour la première fois, l'administrateur initial est considéré comme le super-administrateur et dispose ainsi de tous les droits d'administration de la console.
    - Vous avez également la possibilité d'inviter d'autres utilisateurs à devenir administrateurs (ils seront également super-administrateurs), mais vous ne pouvez pas créer de comptes pour eux tant que vous n'avez pas validé votre domaine. Pour savoir comment valider votre domaine, cliquez ici.
    - Nous vous recommandons vivement de valider votre domaine. Vous pourrez ainsi créer des rôles personnalisés pour appliquer le principe du moindre privilège et créer des comptes utilisateur.
- Pour en savoir plus, consultez cette page concernant les comptes dont l'adresse e-mail et le domaine ont été validés.

Guides

La gestion cloud du navigateur Chrome comporte une section très utile sous Appareils > Chrome > Guides. Elle couvre de nombreuses sections de ce guide, directement dans la console d'administration, et contient des liens vers les sections pertinentes de la console. Nous vous conseillons vivement de vous référer à ce guide dans la console, car il vous accompagnera à chaque étape que vous devrez suivre pour commencer.

Reportez-vous à la section ci-dessous concernant la gestion cloud du navigateur Chrome.



Configurer des unités organisationnelles

Une fois que vous avez accès à la console d'administration Google, vous devez configurer les UO dans lesquelles vos appareils seront gérés.

- Ces UO sont les "buckets" entre lesquels vous répartirez vos différents appareils enregistrés afin de définir des règles précises uniquement pour ces machines.
- Elles sont organisées dans une structure parent-enfant : toutes les configurations effectuées au niveau "parent" seront appliquées aux UO "enfants".
    - Notez que vous n'êtes pas obligé d'appliquer les règles définies au niveau parent aux UO enfants. Pour éviter tout travail supplémentaire, nous vous recommandons d'activer la règle de reporting cloud uniquement au niveau de l'UO racine.

Avant de créer une structure d'UO complexe, réfléchissez à la manière dont vous appliquez aujourd'hui les règles du navigateur Chrome. Les mêmes règles s'appliquent-elles pour la plupart de vos machines ?

- Si tel est le cas, nous vous recommandons de créer simplement une UO pour la production et une UO pour les tests. Si vous avez besoin de plus d'UO pour un ensemble de machines qui nécessitent des règles différentes de la norme, vous pouvez toujours créer une UO à ce stade.
- Pour en savoir plus sur la gestion des UO, cliquez ici.

Si vous utilisez déjà Workspace ou Chrome OS, nous vous recommandons de créer une structure d'UO distincte afin d'éviter tout conflit dans les règles appliquées.

- Le but est d'éviter que des règles initialement prévues pour les utilisateurs soient appliquées par inadvertance à des navigateurs récemment enregistrés et placés dans ces UO.

Configurer le contrôle des accès basé sur le rôle

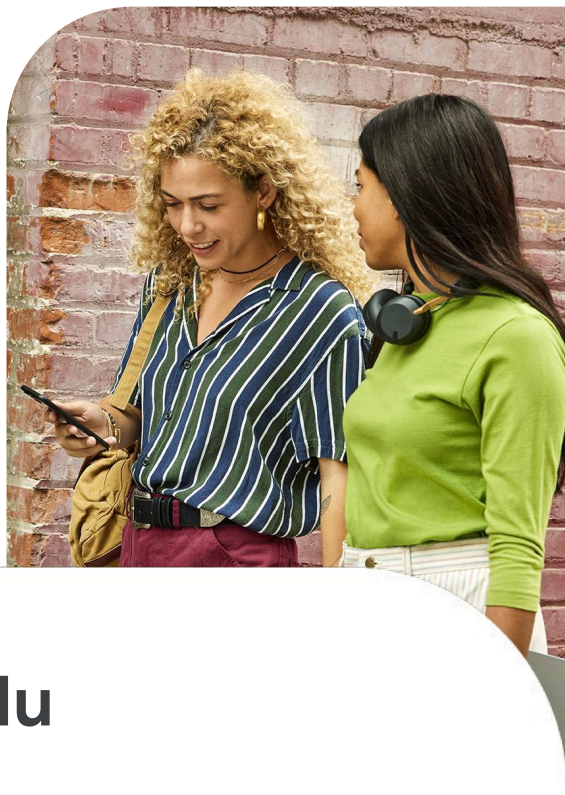
Une fois vos UO configurées, vous pouvez commencer à configurer des comptes pour vos administrateurs.

- De cette façon, vous pouvez déléguer aux administrateurs les accès dont ils ont besoin.
- Vous pouvez créer des comptes administrateur avec un accès limité à la gestion cloud du navigateur Chrome ou à des UO spécifiques, ou bénéficiant uniquement d'un accès en lecture seule.
  - Pour en savoir plus sur la création de différents comptes administrateur, cliquez ici.

Le rôle de gestion cloud du navigateur Chrome est un rôle personnalisé. Pour le créer, procédez comme suit :

1. Accédez à **Compte > Rôles d'administrateur**, puis cliquez sur le lien "Créer un rôle".
2. Donnez un nom au rôle personnalisé, tel que "Gestion cloud du navigateur Chrome".
3. Cochez chaque UO pour accorder tous les droits ("Lire", "Créer", "Mettre à jour", "Supprimer").
   - Vous pouvez accorder uniquement des droits en lecture, mais vous limiterez alors les capacités de gestion des administrateurs de votre navigateur.
4. Sous "Gestion de Chrome", cochez "Paramètres" pour accorder tous les droits sur l'ensemble des fonctionnalités de gestion cloud du navigateur Chrome.
   - Cette section propose une option d'affichage des rapports. Lorsqu'elle n'est associée qu'à l'accès en lecture seule aux UO (étape 3), le rôle d'administrateur en lecture seule est proposé.
     - Ce rôle est utile pour les administrateurs qui ont uniquement besoin de consulter des rapports, et non de définir des règles.
5. Appuyez sur le bouton "Continuer", puis sur le bouton "Créer un rôle" pour terminer.
6. Pour attribuer le rôle au compte utilisateur souhaité dans la console d'administration, accédez à Annuaire > Utilisateurs, sélectionnez l'utilisateur et faites défiler l'écran jusqu'à "Rôles et droits d'administrateur".
7. Attribuez le rôle que vous avez créé lors des étapes précédentes.
   - Si vous souhaitez limiter le champ d'application de ce rôle, sélectionnez l'icône en forme de crayon à côté de la colonne "Champ d'application du rôle" et limitez l'accès à une UO spécifique.
     - De cette façon, votre administrateur disposera uniquement des droits attribués ci-dessus sur les UO auxquelles vous lui donnez accès.
     - Cette option est particulièrement utile pour les environnements partagés, car elle vous permet d'appliquer le principe du moindre privilège aux autres UO auxquelles d'autres services Google peuvent être associés.

Configurer l'intégration avec un service SSO SAML tiers



Vous pouvez configurer l'authentification unique pour votre console d'administration Google. Pour en savoir plus, cliquez ici. Notez que les super-administrateurs sont les seuls comptes qui ne sont pas compatibles avec le langage SAML.

Déployer la gestion cloud du navigateur Chrome dans l'environnement de production

Pour en savoir plus sur l'enregistrement des navigateurs dans la console, cliquez ici. Vous y trouverez la procédure à suivre sous Windows, Mac et Linux, avec les différentes méthodes et les outils que vous pouvez utiliser pour déployer le jeton.

- Consultez cette ressource pour en savoir plus sur le déploiement du jeton d'enregistrement via d'autres outils tels que Jamf, Intune et bien d'autres.

Configurer la console en mode Reporting uniquement

De nombreux clients déploient le jeton d'enregistrement dans la console de façon progressive, en commençant par configurer le mode Reporting uniquement. La gestion cloud du navigateur Chrome propose des rapports pertinents sur les versions de Chrome et peut également fournir des informations détaillées sur les extensions, y compris sur leur emplacement d'installation et l'accès dont elles disposent aux sites Web que vos utilisateurs consultent et/ou aux appareils depuis lesquels ils utilisent le navigateur.

L'avantage, c'est que vous pouvez consulter ces rapports détaillés dans la console sans avoir à changer votre méthode de gestion actuelle. Il vous suffit de définir quelques règles pour que vos machines puissent importer des informations dans la console.

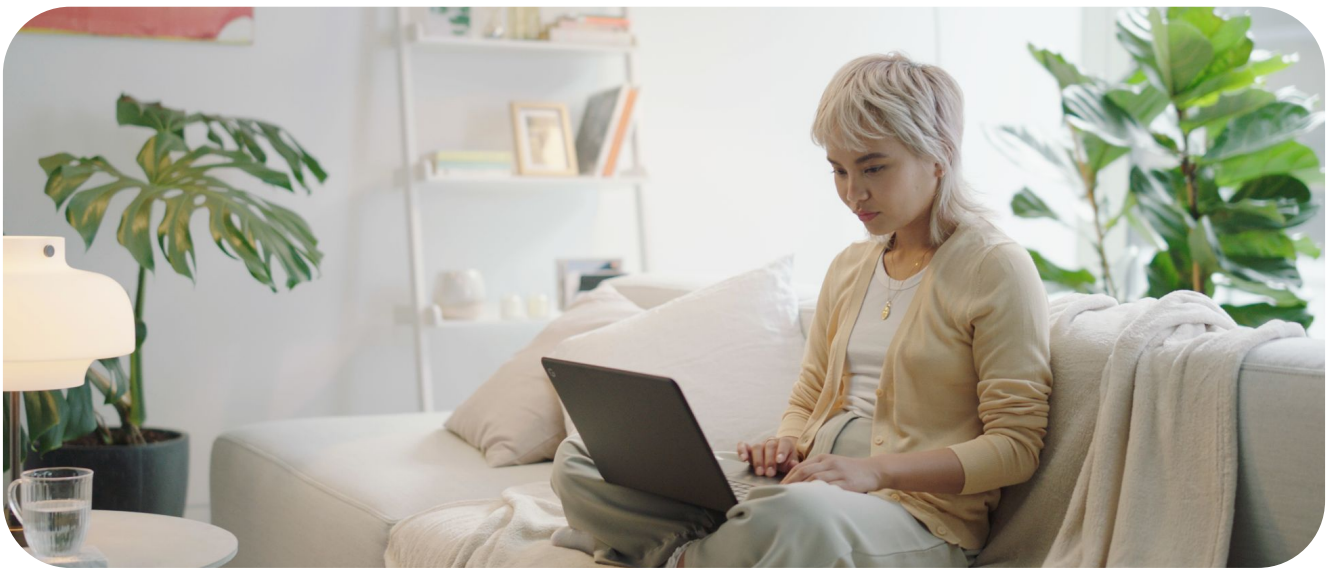
Les règles existantes que vous avez définies pour Chrome ne seront pas affectées. De cette façon, vous pouvez bénéficier des données de rapports en attendant de décider si vous souhaitez gérer toutes vos règles dans le cloud et/ou utiliser la console comme un outil de reporting.

Procédure à suivre :

1. Activez le reporting cloud en utilisant cette méthode.
2. Créez et configurez vos UO.
   - Il n'est pas nécessaire de créer une structure complexe si les règles de votre navigateur sont uniformes (c'est-à-dire que les mêmes règles s'appliquent pour la plupart des appareils).
   - Une ou deux UO suffisent généralement pour la plupart des environnements : une pour les tests et une pour la production.
3. Générez un jeton d'enregistrement à partir de l'UO dans laquelle vous souhaitez que les navigateurs soient enregistrés.
4. Déployez le jeton sur toutes les machines en production et utilisez la console comme outil de reporting pour les versions de Chrome et les extensions installées, jusqu'à ce que vous décidiez si vous souhaitez abandonner votre méthode de gestion actuelle pour configurer tout ce qui concerne Chrome dans le cloud.

Quelques points à noter sur le processus d'enregistrement :

- Pour que les règles soient appliquées depuis la console, vous devez lancer ou relancer Chrome.
  - Après l'enregistrement, l'affichage du navigateur dans la console peut prendre jusqu'à 24 heures.
- Modifier le jeton d'enregistrement directement dans le registre ne permet pas de déplacer le navigateur d'une UO à une autre. Le navigateur doit être déplacé directement dans la console pour que ce changement soit pris en compte, ou via l'API.
- Vous pouvez invalider ou supprimer des jetons d'appareil lorsque vous supprimez des navigateurs de la console d'administration, via la règle de gestion des jetons d'appareil située dans la section "Autres paramètres" de la console d'administration.
- Nous vous recommandons de remplacer l'option par défaut "Invalider le jeton" par "Supprimer le jeton". Ainsi, le jeton d'enregistrement sera toujours disponible et, si l'appareil a été supprimé par erreur, il sera réenregistré au prochain lancement de Chrome.



Compatibilité avec les machines virtuelles et physiques

VM non persistantes

La console d'administration n'accepte pas les VM non persistantes pour le moment. S'il est possible d'enregistrer une VM non persistante, celle-ci étant fréquemment recréée, elle sera associée à plusieurs entrées dans la console, ce qui entraînera des inexactitudes dans les rapports. En effet, chaque fois qu'une machine est recréée, son identifiant global unique (GUID) change. Les différents GUID générés correspondent en réalité à la même machine, et non à des machines différentes.

VM persistantes

La console accepte les VM persistantes à condition que chaque machine possède un identificateur de sécurité unique (GUID de la machine). Cet ID est habituellement généré en exécutant sysprep sur la machine au cours du processus de création d'image. Si vous utilisez un système (comme Citrix) qui déploie le même GUID sur toutes les machines, vous devrez exécuter un script (par exemple, un script RunOnce) pour modifier le GUID d'une machine. La machine apparaîtra alors comme une machine unique.

Voici un workflow type (Windows) :

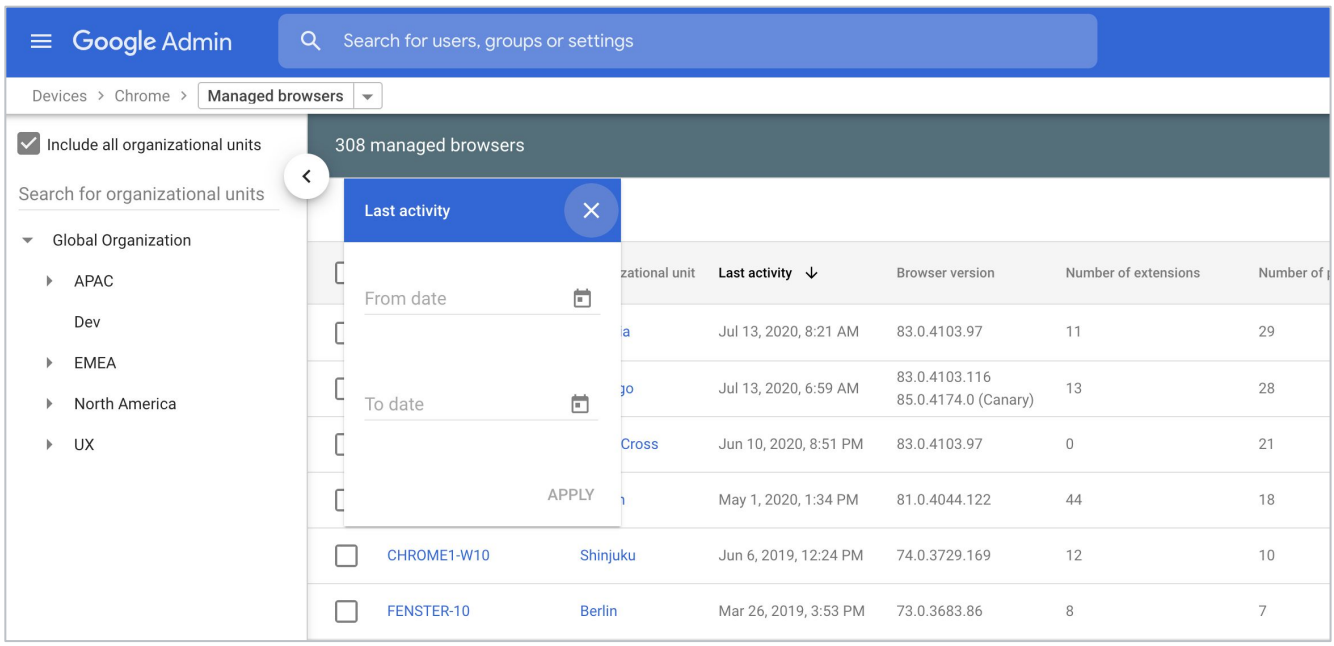
1. Fermez Chrome.
2. Supprimez le jeton d'appareil stocké ici :
   - **HKLM\Software\Google\Chrome\Enrollment**
     Nom de la valeur de chaîne : **dmtoken**
   - Vous pouvez laisser le jeton d'enregistrement là où il est, sauf si vous souhaitez déplacer l'appareil vers une nouvelle UO.
3. Supprimez le GUID de la machine. Le nouvel identifiant global unique de la machine sera généré lors de l'ajout automatique de la clé.
   - La clé se trouve généralement à cet emplacement : **HKLM\Software\Microsoft\Cryptography\MachineGuid**
4. Redémarrez Chrome.
5. Chrome lira le jeton d'enregistrement existant (ou le nouveau, si vous avez annulé l'existant) et activera un nouveau jeton d'appareil (DMtoke).

Compatibilité avec les machines physiques

La console est entièrement compatible avec les machines physiques. Toutefois, étant donné que le caractère unique de l'appareil tient à un identificateur de sécurité unique (GUID de la machine), si la machine est réinitialisée ou si son GUID change, elle sera enregistrée en tant que nouvelle machine dans la console.

Si une machine est réinitialisée, il est recommandé de la supprimer de la console, puis de l'enregistrer à nouveau à partir de sa nouvelle image pour ne pas avoir de machines en double. Pour éviter la présence de machines inactives dans votre console, vous pouvez utiliser la fonctionnalité de filtre dans la vue des appareils gérés. Vous pouvez filtrer les appareils directement dans la colonne "Dernière activité" ou cliquer sur le bouton "Rechercher ou ajouter un filtre" et sélectionner "Dernière activité".

Déterminez la durée pendant laquelle vous souhaitez que les machines inactives restent dans la console (par exemple, 90 jours, un an, etc.), et pensez à les supprimer. Vous pouvez également utiliser l'API pour supprimer ces machines après un certain délai. Reportez-vous à la section sur les API compatibles pour en savoir plus.



Consulter les rapports dans la gestion cloud du navigateur Chrome

Une fois les appareils enregistrés et présents dans la console, vous pouvez commencer à consulter les données provenant de ces appareils.

Avant de commencer à appliquer des règles (notamment pour les extensions), il est recommandé de faire d'abord un état des lieux de ce qui existe.

- Vous devez activer le reporting cloud pour que les données soient transmises à la console.
- Nous vous recommandons également de définir sur trois heures minimum la fréquence d'importation des rapports sur le navigateur géré, pour que les rapports soient importés plus souvent que la fréquence par défaut (24 heures).

Dans la section des navigateurs gérés, vous pouvez sélectionner l'un de vos appareils enregistrés, puis accéder à la section "Règles appliquées au navigateur" pour voir les règles déjà en vigueur.

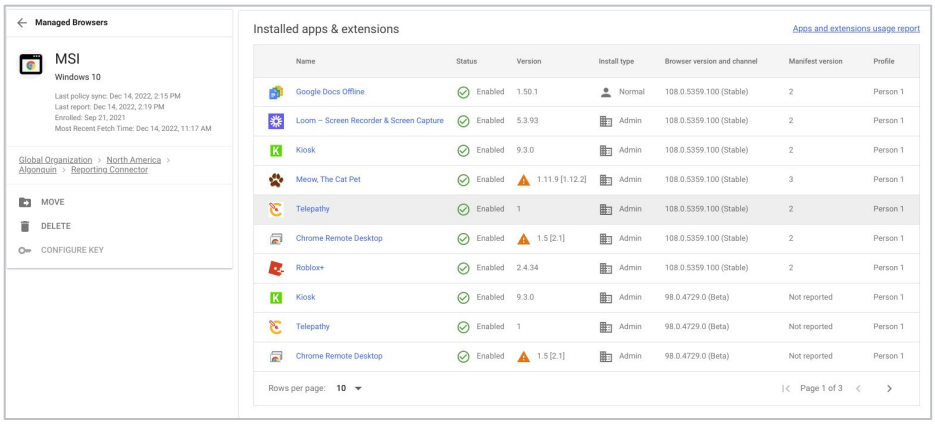
Applied browser policies

Machine policies

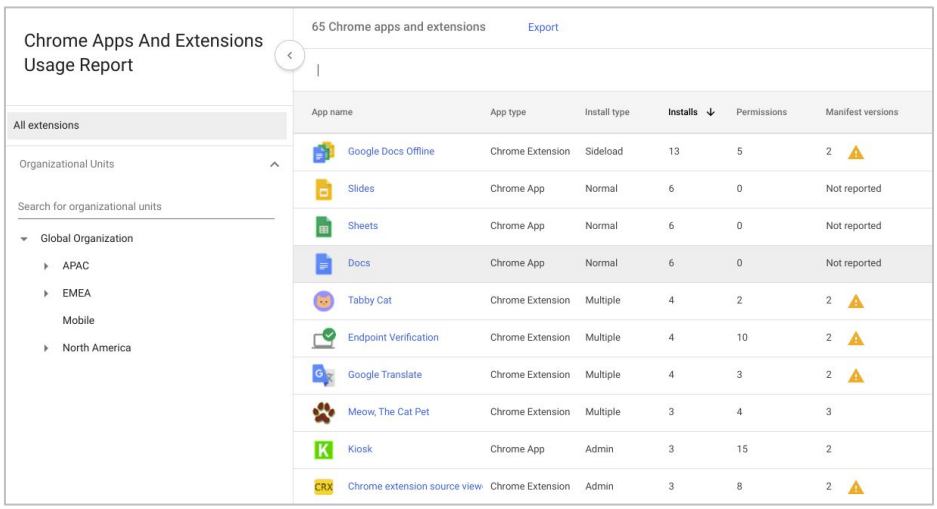
Name	Source	Status	Value
BrowserSignin	Cloud Machine Policy	Applied	1
BrowserSwitcherChromePath	Cloud Machine Policy	Applied	
BrowserSwitcherDelay	Cloud Machine Policy	Applied	3000
BrowserSwitcherEnabled	Cloud Machine Policy	Applied	true
BrowserSwitcherExternalSitelistUrl	Cloud Machine Policy	Applied	
BrowserSwitcherUrlList	Cloud Machine Policy	Applied	Show value
BrowserSwitcherUseIeSitelist	Cloud Machine Policy	Applied	false
CloudExtensionRequestEnabled	Cloud Machine Policy	Applied	true
CloudManagementEnrollmentToken	Local Machine Policy	Applied	5a3f21ed-3f4b-4c7e-ba38-de5cebfe8efc
CloudReportingEnabled	Cloud Machine Policy	Applied	true

Rows per page: 10 Page 1 of 3

Pour avoir un aperçu des extensions déjà installées sur la machine, consultez la section "Applications et extensions".



Pour un aperçu de toutes les extensions installées, cliquez sur le lien "Rapport sur l'utilisation des applications et des extensions".



Cette vue contient la liste de toutes les extensions présentes dans vos navigateurs enregistrés.

Appuyez sur le bouton "Exporter" pour exporter cette liste dans un fichier CSV.

Nous vous recommandons d'utiliser l'**API Extension Takeout** pour obtenir la liste complète des extensions et en savoir plus.

Vous pouvez consulter les instructions de configuration et regarder ce tutoriel vidéo.

Appliquer des règles

Une fois la communication de données effective entre vos appareils et la console, toutes les règles actuellement appliquées dans les règles de groupe fonctionnent avec celles appliquées depuis le cloud. En cas de conflit, les règles locales sont prioritaires sur les règles cloud par défaut.

- Si vous souhaitez ignorer cette fonctionnalité, dans la console d'administration, il existe une règle intitulée "Priorité des règles" vous permettant de modifier le processus d'application des règles en cas de conflit.
- Si vous souhaitez combiner des règles provenant de plusieurs sources (console d'administration et règles locales de la machine), vous pouvez utiliser la règle "Liste de règles fusionnées" : **Saisissez un astérisque (*) dans cette règle pour fusionner automatiquement toutes les règles prises en charge.**
- Cliquez ici pour en savoir plus sur la priorité et la fusion des règles.
- Si vous définissez une règle dans la console, celle-ci s'appliquera à la machine en temps quasi réel.
  - Notez que, par défaut, les rapports sont importés dans la console toutes les 24 heures :

    Vous pouvez définir la fréquence sur toutes les trois heures via la règle "Fréquence d'importation des rapports sur le navigateur géré".

API pour la gestion cloud du navigateur Chrome

Presque tous les paramètres de la console sont compatibles avec les API.
Pour une gestion à grande échelle (dans le cas du déplacement de machines et de modifications groupées, par exemple), nous vous recommandons de configurer l'API de façon à faciliter les choses
pour les administrateurs dans la console.

- Pour savoir comment configurer l'API dans la gestion cloud du navigateur Chrome, consultez ce guide.
- Chrome Enterprise dispose également d'un dépôt GitHub qui fournit de nombreux scripts différents ainsi que d'un framework C# appelé CBCM-CSharp que vous pouvez utiliser pour entraîner, créer, et résoudre des cas d'utilisation complexes grâce à l'automatisation et à l'intégration.
- Il contient des exemples d'optimisation qui permettent de déplacer les navigateurs, de supprimer les navigateurs inactifs, d'extraire des informations, etc.
- Vous y trouverez également des scripts PowerShell utiles pour activer le navigateur et forcer les mises à jour, et d'autres scripts pertinents liés à l'enregistrement pour la gestion cloud du navigateur Chrome.

Résoudre les problèmes liés à la gestion cloud du navigateur Chrome

Ma machine est présente dans la console d'administration, mais aucune information n'est renseignée (comme l'extension et la version).

- **Solution possible** : assurez-vous d'avoir activé le reporting cloud dans l'UO où l'appareil est enregistré.

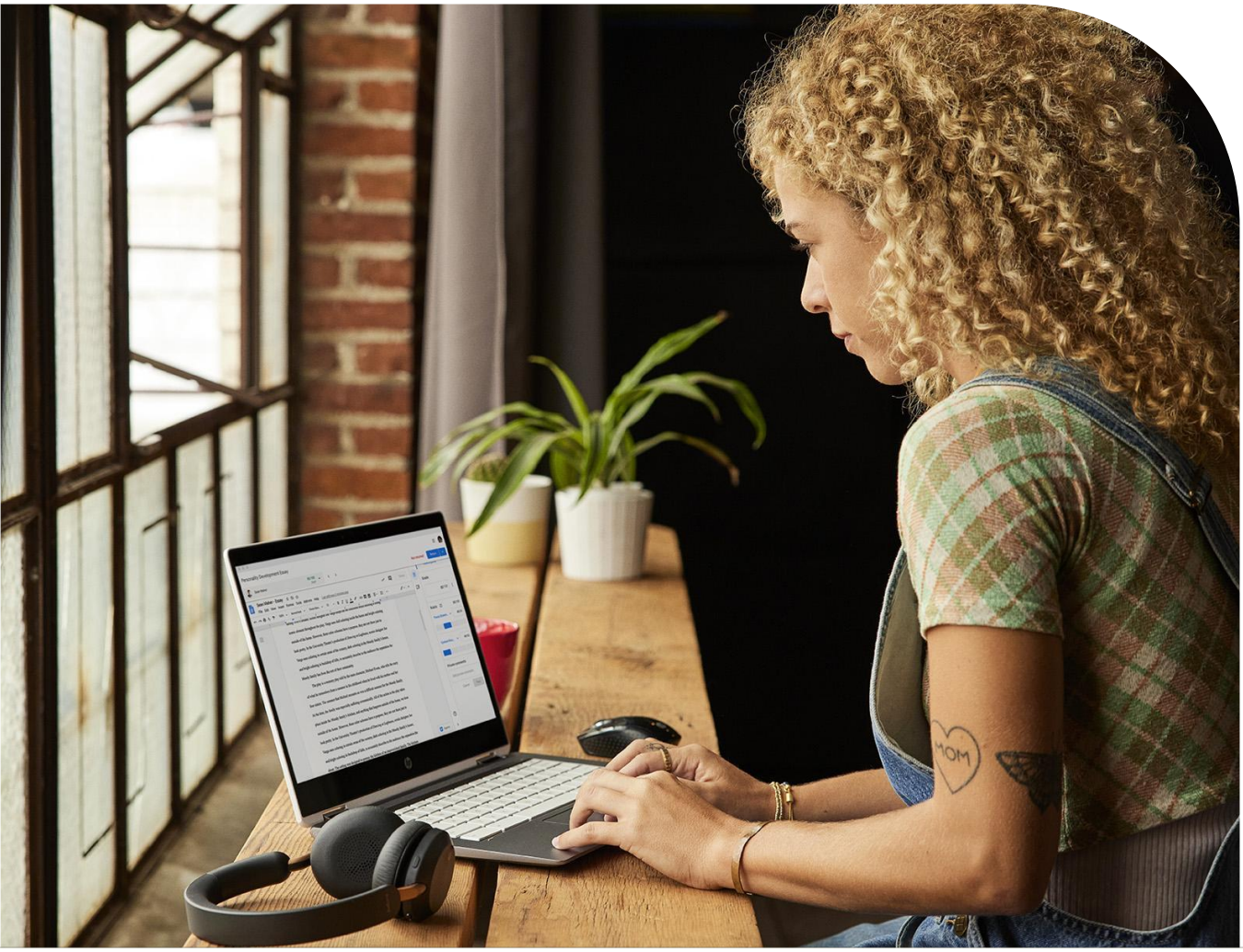
J'ai envoyé le jeton à mes machines, mais la plupart d'entre elles ne sont pas présentes dans la console.

- **Première solution possible** : Chrome doit redémarrer ou être lancé pour que l'enregistrement prenne effet dans la console. Cela prend généralement un peu de temps, mais si vous souhaitez accélérer les choses, vous pouvez utiliser ce script qui ajoutera le jeton d'enregistrement et lancera le navigateur dans un contexte système (les utilisateurs ne verront pas la fenêtre s'afficher). Attendez ensuite 15 secondes, le temps que l'enregistrement soit terminé, puis fermez Chrome.
- **Deuxième solution possible** : la mise à jour Google doit être disponible sur la machine pour que l'enregistrement soit effectué. Il n'est pas nécessaire que la mise à jour automatique soit activée. Assurez-vous que la mise à jour Google est disponible sur la machine et que les URL nécessaires à son fonctionnement ne sont pas bloquées. Pour obtenir la liste des URL, cliquez ici. Notez que l'URL la plus utilisée est la suivante : https://m.google.com/device management/data/api
- **Troisième solution possible** : la console marque les machines comme étant uniques en les identifiant à l'aide de leur GUID sous Windows et de leur numéro de série sur Mac. Si vous n'utilisez pas sys-prep sur vos images Windows, lorsqu'une machine s'enregistre avec un GUID associé à une autre machine, elle remplace celle qui est déjà présente dans la console.

Consultez la section sur la prise en charge des machines virtuelles persistantes dans ce guide pour savoir comment modifier le GUID de vos machines et ainsi éviter ce problème.

J'ai défini une règle dans la console et celle-ci s'est appliquée à la machine, mais elle n'apparaît pas dans la vue des appareils de la section des navigateurs gérés.

- **Solution possible** : Par défaut, les règles que vous configurez dans la console s'appliquent à la machine en quelques instants, mais la fréquence d'importation des rapports dans la console est définie sur 24 heures (vous pouvez réduire ce délai à toutes les trois heures via la règle).



Je vois plusieurs fois le même nom de machine dans la section des navigateurs gérés de la console.

- **Solution possible** : La console n'accepte pas les VM non persistantes. Si vous les enregistrez dans la console, elles figureront dans la section des navigateurs gérés, mais une fois recréées, elles recevront un nouveau GUID qui les fera apparaître en double, même si le nom de la machine est identique.

Une grande partie de mes machines sont inactives, car elles ont été remplacées ou réimagées.

- **Solution possible** : Utilisez la fonctionnalité de filtre dans la vue des appareils gérés. Vous pouvez filtrer les appareils directement dans la colonne "Dernière activité" ou cliquer sur le bouton "Rechercher ou ajouter un filtre" et sélectionner "Dernière activité", puis les supprimer.
  - Vous pouvez également configurer l'API et vous référer à la section de CBCM-Csharp concernant la suppression des navigateurs inactifs afin de l'automatiser.

Ressources

- Configurer la gestion cloud du navigateur Chrome
- Guide de gestion cloud du navigateur Chrome
- Liste des règles du navigateur Chrome
- Stratégies de gestion des mises à jour de Chrome
- Gérer les extensions dans votre entreprise
- Passer du shadow IT au navigateur Chrome géré