Gérer les extensions dans votre entreprise

Gérer les extensions Chrome en toute sécurité et à grande échelle

Sommaire

Objet de ce guide

Il existe de nombreuses extensions utiles pour le navigateur Chrome. Un grand nombre d'entre elles sont peut-être présentes sur les ordinateurs de vos utilisateurs. Les contrôler et les surveiller peut donc s'avérer difficile pour les administrateurs informatiques.

Ceux-ci trouveront expliquées dans ce guide les meilleures méthodes de gestion des extensions. Ils y découvriront la procédure à suivre pour gérer les extensions à l'aide de la gestion cloud du navigateur Chrome et des stratégies de groupe Windows.

Ce guide décrit les différentes méthodes de gestion des extensions. Vous pouvez effectuer les actions suivantes :

1. Bloquer les extensions en fonction de leurs autorisations
2. Gérer l'accès des extensions de sites Web
3. Autoriser ou bloquer les extensions dans la gestion cloud du navigateur Chrome ou par stratégie de groupe Windows
4. Auto-héberger vos propres extensions sur site

Sujets abordés	Instructions et recommandations de gestion des extensions pour le navigateur Chrome dans votre entreprise
Public principal	Administrateurs de Microsoft® Windows® et de la gestion cloud du navigateur Chrome (pour Windows, Mac et Linux)
Enseignements	Bonnes pratiques de gestion des extensions avec le navigateur Chrome

Dernière mise à jour : *29 octobre 2021*

Emplacement de publication : *https://support.google.com/chrome/a/answer/9296680*

Introduction

Les entreprises ont la volonté de protéger les données de leurs utilisateurs. Elles souhaitent pouvoir s'assurer facilement de la sécurité et de la pertinence des extensions qui leur sont destinées. Les administrateurs informatiques doivent pouvoir :

1. empêcher l'installation d'extensions malveillantes ;
2. conserver les extensions dont les utilisateurs ont besoin ;
3. fournir un accès limité aux données des utilisateurs et de l'entreprise.

Ce guide a pour but de vous montrer comment gérer facilement les extensions à l'aide de différentes méthodes. Il présente les différentes options qui s'offrent à vous et vous aide à choisir la plus adaptée.

Points à prendre en compte pour la gestion des extensions Chrome

Vos utilisateurs ont besoin d'accéder à certains sites, applications et extensions pour réaliser leur travail. En tant qu'administrateur informatique, votre rôle est de protéger les données des utilisateurs et de l'entreprise. Vous devez mettre en place une stratégie pour choisir comment vous allez gérer les extensions.

Les questions à vous poser :

- Quels sont les règlements et les mesures de conformité que je dois suivre ?
- Quels types d'appareils ou accès aux sites Web pourraient aller à l'encontre des règles de sécurité de mon entreprise ?
- Quel volume de données utilisateur ou entreprise est stocké sur les machines des utilisateurs ?

À mesure que vous répondrez à ces questions, sachez que Google propose des règles qui vous permettent :

- de bloquer ou d'autoriser les extensions en fonction de vos règles de protection des données ;
- d'installer d'office les extensions nécessaires sur les machines de vos utilisateurs ;
- de gérer les extensions en leur attribuant le minimum de droits requis pour qu'elles fonctionnent correctement.

La méthode classique de gestion consiste à autoriser ou bloquer des extensions au cas par cas, mais il existe un moyen plus simple de procéder. Vous pouvez gérer les extensions en fonction des autorisations dont elles ont besoin. Pour cela, recherchez les autorisations que vous souhaitez accorder. Ensuite, appliquez les règles qui autorisent ou bloquent les extensions répondant à vos critères.

Que sont les autorisations d'extension ?

Les extensions requièrent des droits pour apporter des modifications à une machine ou à une page Web afin de fonctionner correctement. On appelle ces droits des "autorisations". Les développeurs doivent lister les droits et accès requis par leurs extensions. Il existe deux grandes catégories d'autorisations, bien que de nombreuses extensions fassent appel aux deux :

- Les autorisations des sites donnent accès aux sites Web que vos utilisateurs consultent.
  Par exemple : modifier une page Web, accéder aux cookies, modifier des onglets.
- Les autorisations des appareils peuvent donner accès à la machine lorsque le navigateur est en cours d'utilisation.
  Par exemple : accès au port USB, à l'espace de stockage, à l'écran.

Comment les extensions sont-elles mises à jour ?

Les mises à jour des extensions ont lieu uniquement lorsque Chrome est en cours d'exécution. Elles se produisent dans les quelques minutes qui suivent le lancement de Chrome, puis à nouveau toutes les 5 heures.

- Elles s'effectuent selon le processus suivant :
  a. Chrome envoie une requête contenant la liste des extensions et versions installées à un serveur Google.
  b. Nos serveurs répondent par un ensemble d'instructions précisant les extensions devant être mises à jour.
  c. Chrome demande ensuite les fichiers CRX pour chacune des extensions obsolètes et applique la mise à jour localement.
- Comment les extensions peuvent-elles devenir obsolètes ?
  a. La mise à jour peut ne pas s'effectuer au cours d'une session utilisateur courte si la taille du téléchargement de la mise à jour est volumineuse ou si les utilisateurs ont installé de nombreuses extensions.
  b. Chrome n'a pas été lancé.
  c. Les développeurs des extensions ont choisi de limiter le nombre de clients pour lesquels ils déploient une mise à jour.
  d. Si une entreprise héberge elle-même une extension, celle-ci peut devenir obsolète du fait d'un problème d'accès ou d'une erreur de configuration.
  e. D'autres problèmes dus à des erreurs de développement d'extension peuvent expliquer ce phénomène.

Pour dépanner des extensions obsolètes, vous pouvez les désinstaller, puis les réinstaller, ou bien forcer manuellement leur mise à jour avec chrome://extension>enable developer mode> et en appuyant sur le bouton de mise à jour.

Gérer les extensions

Il est recommandé à la plupart des organisations de gérer leurs extensions en fonction de leurs autorisations et des sites Web auxquelles elles ont accès. Cette méthode est plus sûre, plus facile à gérer et adaptable.

Elle vous fait gagner du temps puisque vous devez configurer les règles une seule fois. Les longues listes d'autorisations et de blocages à gérer sont révolues, même si vous pouvez toujours inclure une petite liste de blocage d'extensions ne devant pas être installées. De plus, grâce au règlement sur les hôtes à l'exécution, vos sites les plus importants seront protégés. Pour gérer les extensions de votre organisation avec cette méthode :

1. Recherchez les extensions qui sont installées sur les ordinateurs de vos utilisateurs.
    - **Méthode 1 (recommandée) :** utilisez la gestion cloud du navigateur Chrome. Cette fonctionnalité est proposée sans coût supplémentaire pour vos utilisateurs. Vous pourrez voir :
        - la version installée et le nombre d'installations de l'extension, et si c'est l'utilisateur ou l'administrateur qui a procédé à l'installation ;
        - les autorisations requises pour l'extension ;
        - l'état de l'extension (activée ou désactivée).
    - La procédure à suivre pour configurer la gestion cloud du navigateur Chrome se trouve ici.
    - Une fois que vous avez configuré la console, enregistré vos machines et activé l'importation d'informations cloud, vous pouvez afficher toutes les extensions installées sous **Appareils > Chrome > Rapport sur l'utilisation des applications et des extensions**.
        - En cliquant sur une extension, vous accédez à des détails supplémentaires sur les autorisations qu'elle requiert et des exemples d'emplacements où elle est installée.
            - Bientôt (fin 2021/début 2022), une nouvelle page d'informations (affichée ci-dessous) s'ouvrira lorsque vous cliquerez sur une extension.
            - Ces détails sur l'extension concernent les autorisations requises et des informations provenant directement de la fiche du Chrome Web Store.
            - Pour plus d'informations sur la gestion des extensions dans la gestion cloud du navigateur Chrome, regardez cette vidéo YouTube.
        - Vous pouvez aussi exporter toutes les données sur une extension depuis les navigateurs enregistrés vers un fichier CSV à l'aide de l'API Takeout de la gestion cloud du navigateur Chrome.
            - Pour en savoir plus, consultez les ressources suivantes : Guide par étapes | Article du blog | Démonstration Vidéo
    - **Méthode 2 : Enquête : demandez à vos collègues et à leurs responsables quelles extensions ils utilisent régulièrement. Élaborez une liste des extensions dont les utilisateurs ont besoin.

2. Sélectionnez les sites qui doivent être sûrs :
    - Déterminez les sites Web ou domaines sensibles pour lesquels vous voulez empêcher les extensions d'apporter des modifications ou de lire les données.
        - Vous empêcherez l'accès à ces sites en bloquant les appels d'API lorsque l'extension est en cours d'exécution. Cela implique de bloquer les requêtes Web, l'accès en lecture des cookies, l'injection de JavaScript, XHR, etc.

3. Identifiez les autorisations qui pourraient présenter un risque pour vos utilisateurs :
    - Examinez la liste des extensions que vous avez élaborée à l'étape 1. Examinez les extensions qui sont installées et les autorisations dont elles ont besoin.
        - **Conseil :** Les autorisations utilisées par les extensions ne sont pas toujours très claires. Contactez le fournisseur pour obtenir plus d'informations sur les extensions dont vous avez obligatoirement besoin. Il devrait pouvoir vous expliquer les modifications que l'extension pourrait apporter aux machines et aux sites Web.
    - Consultez la liste Declare Permissions (Déclarer les autorisations). Elle présente toutes les autorisations qu'une extension peut utiliser. Décidez ensuite des autorisations que vous voulez accorder dans votre organisation.

        - Pour plus d'informations sur les risques liés à des autorisations d'extensions spécifiques, consultez ce document.
4. Dressez la liste des données que vous avez collectées, à savoir :
    - **Extensions requises :** vous pouvez décomposer cette liste par département, emplacement de bureau ou toute autre information pertinente.
    - **Liste d'autorisation :** les extensions requises qui seraient normalement bloquées étant donné leurs autorisations, mais qui doivent pouvoir s'exécuter, par exemple :
        - les extensions dont vos utilisateurs ont besoin ;
        - les extensions définies comme ne présentant aucun risque après conversation avec le fournisseur.
    - **Liste de blocage :**

        - les extensions qui ne peuvent pas être installées.

            - Cette liste indique les autorisations qui ne sont pas autorisées à s'exécuter.

        - La liste de blocage présente les sites Web et les domaines qui doivent rester sûrs et auxquels les extensions n'auront pas accès.

            - Comparez cette liste de blocage aux autres dont vous disposez. Vous vous apercevrez peut-être que vous pouvez assouplir vos règles de liste de blocage actuelles.

5. Soumettez votre liste aux personnes concernées et à l'équipe informatique pour qu'elles l'approuvent.
6. Mettez vos nouvelles règles à l'épreuve dans un environnement de test ou avec un petit groupe pilote d'utilisateurs,
7. puis déployez ces nouvelles règles par phases auprès des collaborateurs.
8. Soyez à l'écoute des commentaires de vos utilisateurs.
9. Répétez et ajustez le processus une fois par mois, par trimestre ou par an.

Vous disposerez ainsi d'une base d'autorisations que vous accordez, tandis que d'autres seront bloquées. Les sites Web sensibles seront protégés. La sécurité de votre navigateur sera améliorée, et vos utilisateurs bénéficieront d'une meilleure expérience. Il se peut que vos collaborateurs aient accès à des extensions qu'ils ne pouvaient pas installer auparavant, mais ils ne pourront pas les exécuter sur vos sites sensibles, sauf si vous les y autorisez. Pour savoir comment configurer cette méthode, consultez ces sections dans le guide :

- Gérer les extensions par le biais des autorisations/blocages
- Hôtes bloqués pendant l'exécution (protéger les sites Web sensibles)
- Installer d'office les extensions pour les utilisateurs
- Autoriser/bloquer (si nécessaire) des extensions

Pour découvrir la gestion des extensions dans la gestion cloud du navigateur Chrome, consultez cette vidéo YouTube.

Présentation des différentes règles de gestion des extensions

Bon nombre de ces règles seront détaillées dans les autres sections du document, mais voici une présentation de quelques options qui s'offrent actuellement à vous pour gérer les extensions (certaines s'appliquent également aux applications) via la stratégie de groupe Windows ou les fichiers .plist sur Mac :

- ExtensionInstallAllowlist : les extensions dont vous avez approuvé l'installation dans votre environnement.
- ExtensionInstallBlockList : les extensions dont vous n'autorisez pas l'installation. Si elles sont déjà installées, elles seront désinstallées. Si un utilisateur tente de les installer, il en sera empêché. De plus, une nouvelle fonctionnalité apparaît dans le Chrome Web Store : le bouton "Ajouter à Chrome" devient rouge et prévient l'utilisateur que l'extension ne peut pas être installée.
- ExtensionInstallForceList : l'extension fera l'objet d'une installation silencieuse sur la machine de l'utilisateur. Celui-ci ne peut ni désactiver, ni désinstaller l'extension. Ce paramètre ignore la règle "ExtensionInstallBlockList".
- BlockExternalExtensions : ce paramètre bloque l'installation des extensions provenant de sources externes. Par exemple, si une application installée ajoute une extension à Chrome par l'intermédiaire du registre, ce paramètre bloque le chargement de l'extension.
- ExtensionAllowedTypes : vous pouvez créer ici une liste des types d'extensions et d'applications dont vous autorisez l'installation. Les extensions, thèmes, scripts utilisateur, applications hébergées, anciennes applications empaquetées et applications de plateformes sont les valeurs compatibles.
    - Notez bien que tous les éléments que vous voulez autoriser doivent être inclus dans la liste. Tous ceux laissés en dehors de cette liste ne seront pas installés.
    - Pour plus d'informations sur les différents types, voici un lien sur les extensions et applications dans le Chrome Web Store.
- ExtensionInstallSources : auparavant, les utilisateurs pouvaient cliquer sur un lien qui renvoyait vers un fichier .crx, et Chrome leur proposait d'installer l'extension après quelques avertissements. Cette fonctionnalité a été supprimée pour raisons de sécurité après la version 21 de Chrome.
    - Cette règle vous permet d'obtenir cette ancienne fonctionnalité d'installation pour des URL spécifiques que vous indiquez dans la règle. Voici un lien vers les formats de correspondance d'URL qui peuvent être utilisés dans cette règle.

- ExtensionsSettings : cette règle offre plusieurs fonctionnalités ; sa création nécessite un script JSON, et elle doit être formatée dans une chaîne de ligne unique.
    - Ce paramètre peut être complexe et fera l'objet d'une présentation plus complète dans plusieurs sections de ce document.
        - Nous vous recommandons d'utiliser la gestion cloud du navigateur Chrome, car la quasi-totalité des fonctionnalités est incluse sans qu'il y ait besoin de script JSON, et il est possible d'auditer les extensions installées.

Remarque concernant l'engagement de Google en faveur de conventions d'attribution de noms inclusives : les règles suivantes sont maintenant obsolètes et seront supprimées de Chrome 97, assurez-vous donc d'adopter la nouvelle règle d'ici là.

- ExtensionInstallWhitelist est remplacé par ExtensionInstallAllowlist
- ExtensionInstallBlacklist est remplacé par ExtensionInstallBlocklist

Bloquer les extensions en fonction de leurs autorisations

Vous pouvez contrôler les extensions que vos utilisateurs peuvent installer à l'aide de leurs autorisations. Une extension installée, mais dont les autorisations sont bloquées, sera désactivée. Si un utilisateur essaie d'installer une extension avec une autorisation bloquée, l'installation sera impossible.

Gérer les extensions en fonction de leurs autorisations dans la gestion cloud du navigateur Chrome

(Windows, Mac et Linux)

Vous pouvez bloquer les extensions qui ont besoin d'autorisations non accordées. Par exemple, vous pouvez empêcher les extensions de se connecter à des appareils USB ou empêcher l'accès aux cookies.

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.
2. Sélectionnez l'unité organisationnelle comportant les utilisateurs pour lesquels vous souhaitez autoriser des extensions.
3. Cliquez sur l'icône en forme de roue dentée pour afficher les paramètres supplémentaires .

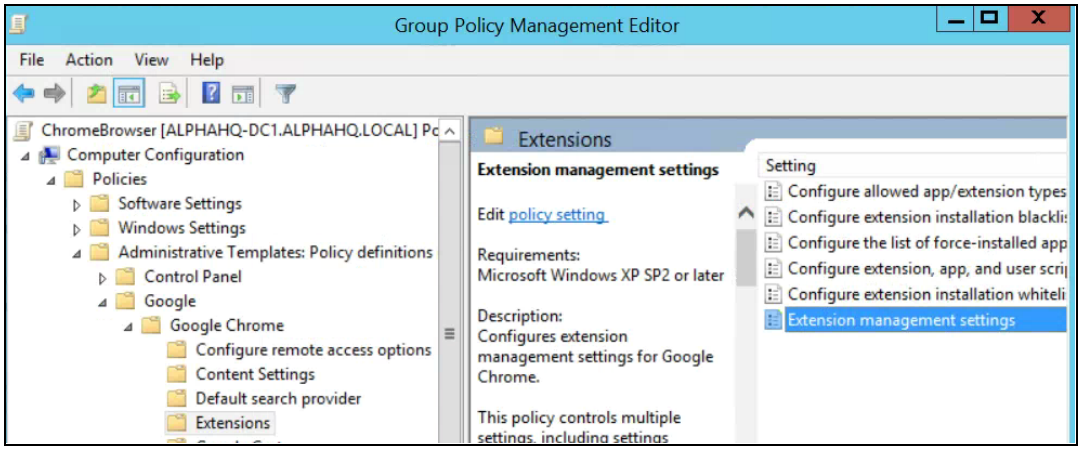
4. Cochez chaque autorisation à bloquer ou à accorder dans la **section Autorisations et URL**.

   a. Vous pouvez aussi cliquer sur une extension individuelle dans l'onglet "Utilisateurs et navigateurs" et la gérer via les autorisations sous Autorisations et accès par URL > Personnaliser les autorisations pour cette application ou cette extension.
      i. Remarque : Cette opération remplacera toute règle globale s'appliquant déjà à l'extension en question.
      ii. Pour en savoir plus sur chaque autorisation, consultez cette liste d'autorisations.
5. Cliquez sur **Enregistrer**.

Gérer les extensions en fonction de leurs autorisations dans la stratégie de groupe

(Windows uniquement)

1. Accédez à l'objet de stratégie de groupe dans la console de gestion Microsoft.
2. Effectuez un clic droit > cliquez sur **Modifier**.
3. Dans l'éditeur de gestion des stratégies de groupe, accédez à **Stratégies > Modèles d'administration > Google Chrome > Extensions > Paramètres de gestion des extensions**.



Chemin d'accès de la configuration des paramètres de gestion des extensions

4. Activez la règle, puis saisissez les autorisations que vous voulez accorder ou bloquer, en les compressant en une chaîne JSON unique.

Format conforme à cet exemple de données JSON (Dans cet exemple, toutes les extensions ayant besoin d'un appareil USB sont bloquées.)

```
{
	"*": {
		"blocked_permissions": ["usb"]
	}
}
```

Données au format JSON sous forme compacte :

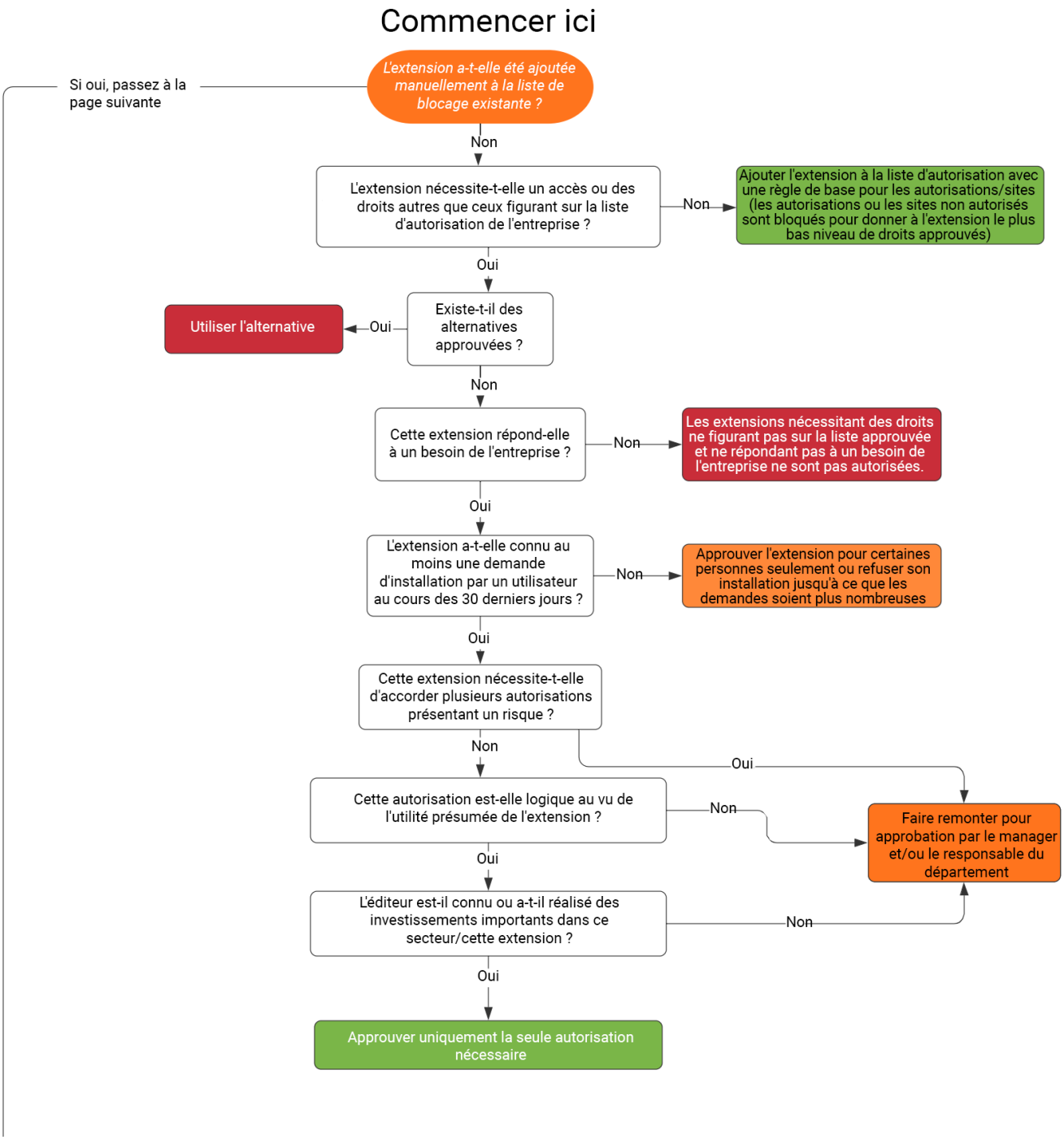
```
{"*":{"blocked_permissions":["usb"]}}
```

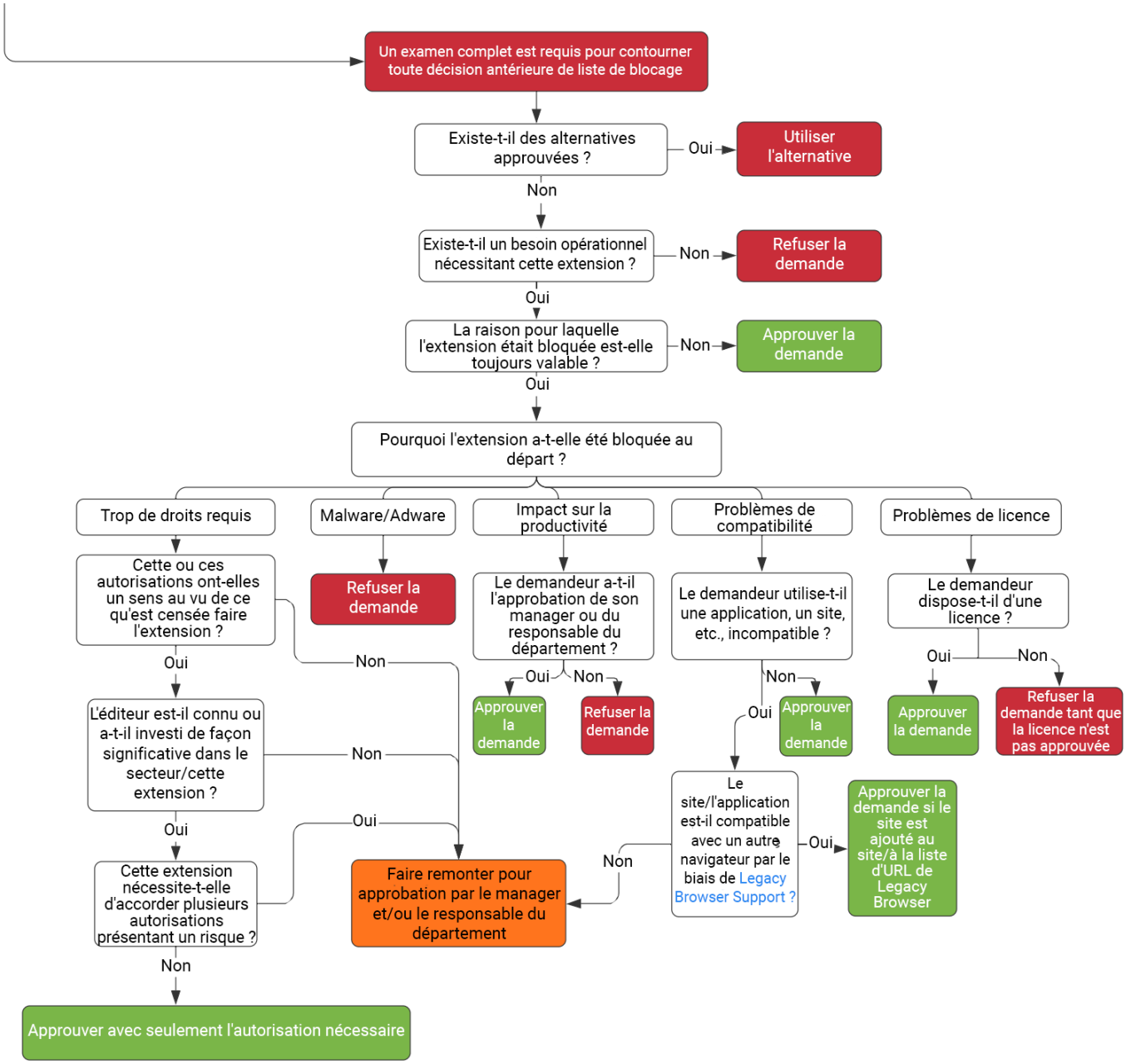
Conseil :

- Pour bloquer toutes les extensions qui utilisent cette autorisation, utilisez un astérisque (comme illustré ci-dessus) en guide d'ID d'extension.
- Si vous voulez bloquer plusieurs autorisations via JSON, voici un exemple de blocage d'alimentation, de printerProvider, série et USB pour toutes les extensions :
    - {"*":{"blocked_permissions":["power","printerProvider","serial","usb"]}}
- Si vous indiquez une ID d'extension, la règle s'appliquera uniquement à cette extension. Dans l'exemple ci-dessus, remplacez le * par l'ID d'extension. Vous pouvez bloquer plusieurs éléments, mais ils doivent être séparés dans leurs propres entrées dans la chaîne JSON.
    - Pour savoir comment trouver l'ID d'extension, consultez l'étape 3 de cet article d'aide.

Créer un processus d'exception pour les extensions qui nécessitent des autorisations risquées

Parfois, vous pouvez avoir besoin d'extensions qui requièrent des autorisations que vous avez jugées comme étant trop risquées pour pouvoir s'exécuter dans votre environnement. Pour vous donner une idée de ce à quoi peut ressembler un workflow d'exception, voici un exemple de workflow pour une extension obligatoire actuellement bloquée.





- Notez que ce flux est fourni à titre d'exemple uniquement, chaque entreprise disposant de ses propres workflow ou processus de gestion du changement.

Gérer les extensions avec la règle de paramètres des extensions

Windows offre plusieurs manières de gérer les extensions. L'une d'entre elles, courante, consiste à configurer plusieurs règles dans une chaîne JSON ou dans le registre Windows à l'aide de la règle de paramètres des extensions.
Conseil : Cette règle est compatible avec Mac, Chrome OS et Linux. La page de la règle propose des exemples de valeurs pour ces autres plateformes.

Cette règle peut agir sur des paramètres comme l'URL de mise à jour, depuis laquelle l'extension est téléchargée pour l'installation de départ, et les autorisations bloquées, qui ne sont pas autorisées à s'exécuter. Pour plus d'informations, consultez la description complète des paramètres des extensions.Vous trouverez également d'autres informations dans ces articles d'aide : Configurer la règle ExtensionSettings et Règles relatives aux applications et aux extensions.

Vous avez le choix de définir tous les paramètres de gestion des extensions par l'intermédiaire de cette règle ou via des règles individuelles.

- Le paramètre d'hôtes autorisés/bloqués pendant l'exécution (blocage d'extensions sur des sites Web spécifiques) peut seulement être défini via GPO dans la règle des paramètres des extensions.
    - Il peut aussi être défini via la gestion cloud du navigateur Chrome.
- Notez que la règle des paramètres des extensions peut remplacer d'autres règles que vous avez ailleurs dans la stratégie de groupe, par exemple :
    - ExtensionAllowedTypes
    - ExtensionInstallAllowlist
    - ExtensionInstallForcelist
    - ExtensionInstallSources
    - ExtensionInstallBlocklist

La règle des paramètres des extensions est définie par le biais d'une des deux méthodes suivantes :

- Registre Windows
- Chaîne JSON dans l'éditeur des stratégies de groupe Windows

Conseils :

- Il peut être difficile de mettre correctement en forme une chaîne JSON. Utilisez une vérification JSON avant de mettre en place la règle.
- Si vous avez des difficultés à mettre correctement en forme la chaîne JSON, vous pouvez utiliser la méthode par clé de registre, et Chrome la convertira en JSON dans chrome://policy dans le navigateur de la machine cible.
    - Copiez simplement cette chaîne JSON et vous pouvez l'appliquer via GPO via la règle des paramètres des extensions.
    - Vous pouvez aussi utiliser cette méthode en configurant les paramètres des extensions via la gestion cloud du navigateur Chrome et en copiant la sortie JSON.

Configurer la règle des extensions à l'aide du registre Windows

La règle ExtensionSettings doit être écrite dans le registre sous :
`HKLM\Software\Policies\Google\Chrome\ExtensionSettings\`

- Il est possible d'utiliser HKCU au lieu de HKLM. Le chemin d'accès équivalent peut être configuré avec GPO.
- Les clés peuvent être créées à l'aide de la méthode de votre choix sur la machine de l'utilisateur.

Pour Chrome, tous les paramètres commenceront avec cette clé :
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\`

La clé que vous créerez ensuite concerne le champ d'application de la règle. Nommez la clé selon l'ID d'extension pour l'appliquer à une seule extension. Nommez la clé avec un astérisque pour l'appliquer à toutes les extensions. Par exemple, utilisez l'emplacement suivant pour les paramètres qui s'appliquent uniquement à l'extension Google Hangouts :
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd`

Pour les paramètres qui s'appliquent à toutes les extensions, utilisez cet emplacement :
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*`

Différents paramètres nécessiteront différents formats, selon qu'ils correspondent à une chaîne ou un tableau de chaînes. Les valeurs de tableau nécessitent le terme **`[ " value " ]`**. Les valeurs de chaîne peuvent être saisies sans [“ ”]. Voici la liste des paramètres qui correspondent à des tableaux de chaînes :

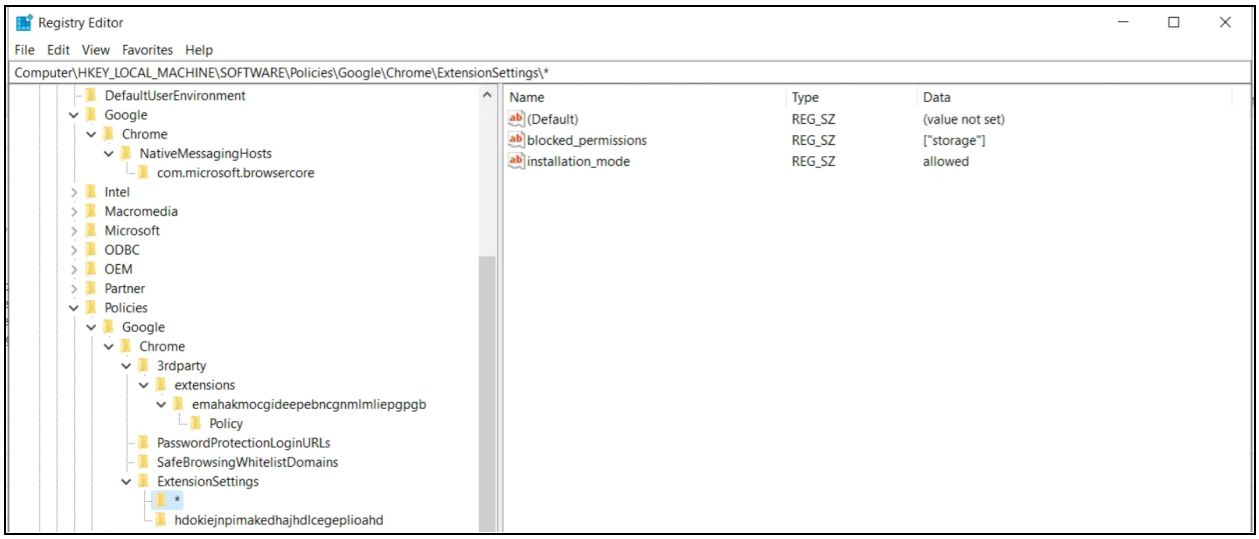
- Installation_mode = chaîne
- update_url = chaîne
- blocked_permissions = tableau de chaînes
- allowed_permissions = tableau de chaînes
- minimum_version_required = chaîne
- runtime_blocked_hosts = tableau de chaînes
- runtime_allowed_hosts = tableau de chaînes
- blocked_install_message = chaîne

Si vous voulez définir plusieurs valeurs dans une seule chaîne (comme des autorisations bloquées), voici un exemple de cette syntaxe :

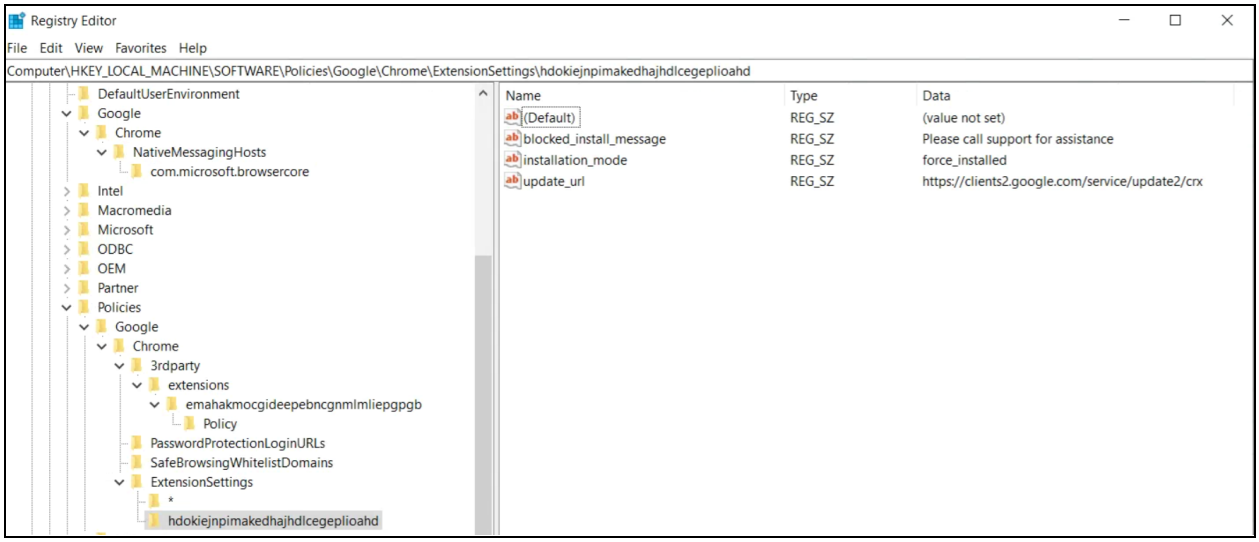
- [“power”,”printerProvider”,”serial”,”usb”]

Name	Type	Data
(Default)	REG_SZ	(value not set)
blocked_permissions	REG_SZ	["power", "printerProvider", "serial", "usb"]

Voici des exemples d'affichage des clés dans le registre :



La clé de champ d'application (*) par défaut et ses valeurs



Un champ d'application individuel et ses valeurs

Ici, les clés définies dans le registre sont converties en JSON avec la règle de chrome://policy dans le navigateur :

Chrome policies

S'applique à	Niveau	Source	Nom de la règle
Machine	Obligatoire	Plate-forme	DefaultBrowserSetting Enabled
Machine	Obligatoire	Plate-forme	ExtensionSettings


```
{
  "*": {
  "blocked-permissions": [ "storage" ],
  "installationjnode": "allowed"
  },
  "hdokiejnpimakedhajhdlcegeplioahd": {
  "blocked_install_message": "Please call support for assistance",
   "installation_mode": "force_installed",
  "update_url": "https://clients2.google.com/service/update2/crx"
   }
}
```


Configurer à l'aide d'une chaîne JSON dans l'éditeur des stratégies de groupe Windows

La procédure d'utilisation de la règle des paramètres des extensions à l'aide de GPO implique que vous ayez déjà importé les modèles ADM/ADMX pour les règles Chrome.

Pour les autres plates-formes d'OS, cliquez sur les liens suivants : Mac | Linux | Chrome OS

1. Dans l'éditeur de gestion GPO, accédez à **Google Chrome > Extensions > Extensions management setting policy** (Règle des paramètres de gestion des extensions).
2. Activez la règle. Dans la zone de texte, saisissez les données correspondantes de manière compacte au format JSON (JavaScript Object Notation) sous la forme d'une ligne unique, sans sauts de ligne.
   Pour valider les règles et les compacter sur une seule et même ligne (voir l'exemple de données au format JSON ci-dessous), utilisez cet outil de compression JSON tiers.

Mettre correctement en forme JSON pour la règle des paramètres des extensions :
Pour utiliser cette méthode, vous devez comprendre les deux parties de cette règle, le champ d'application **par défaut** et le champ d'application **individuel**. Le champ d'application par défaut s'applique à toutes les extensions. Le champ d'application individuel s'applique uniquement à l'extension spécifiée.

Le champ d'application par défaut est identifié par l'astérisque (*). Cet exemple montre un champ d'application par défaut et un champ d'application d'extension individuel :

```
{
   "*": {},
   "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

Les paramètres d'une extension sont définis à partir d'un seul champ d'application. S'il existe un champ d'application individuel pour cette extension, les paramètres correspondants s'appliquent. Si aucun champ d'application d'extension individuel n'existe, le champ d'application par défaut est utilisé.

Voici un exemple de script JSON qui empêche toute extension de s'exécuter sur .example.com et bloque toute extension qui nécessite l'autorisation "USB" :

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

Données au format JSON sous forme compacte :

```
{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}
```

Exemples de références avec exemples de valeurs pour la gestion des extensions à l'installation :

- "allowed" (par défaut)
  L'utilisateur peut installer l'extension à partir du Chrome Web Store
  Exemple de code JSON :
  `{ "*": {"installation_mode": "allowed" }}`

- "blocked"
  L'utilisateur ne peut pas installer l'extension à partir du Chrome Web Store
  Exemple de code JSON :
  `{ "*": {"installation_mode": "blocked" }}`

- "blocked_install_message"
  Vous pouvez ici spécifier un message personnalisé à afficher lorsque l'installation est bloquée.
  Exemple de code JSON - blocked_install_message :
  `{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}`

- "force_installed"
  - L'extension est installée automatiquement sans interaction de l'utilisateur.
  - Celui-ci ne peut ni la désactiver, ni la supprimer.

  `{ "*": {"installation_mode": "force_installed" }}`

- "normal_installed"
  L'extension est installée automatiquement sans interaction de l'utilisateur, qui ne peut pas la désactiver.
  `{ "*": {"installation_mode": "normal_installed" }}`

- "removed"
  (Chrome 75 ou version ultérieure) Les utilisateurs ne peuvent pas installer l'extension. Si les utilisateurs ont déjà installé l'extension, le navigateur Chrome la supprime.
  `{ "*": {"installation_mode": "removed" }}`

- `"toolbar_pin"`

  Détermine si l'icône de l'extension est épinglée dans la barre d'outils. Vous pouvez choisir l'une des options suivantes :
  force_pinned : l'icône de l'extension est épinglée dans la barre d'outils et visible à tout moment. L'utilisateur ne peut pas la masquer dans le menu des extensions.
  default_unpinned : par défaut, l'extension est masquée dans le menu des extensions, mais l'utilisateur peut l'épingler dans la barre d'outils.
  Si vous ne configurez pas ce champ, il est défini par défaut sur le comportement default_unpinned.
  `{ "*": {"toolbar_pin": "forced_pinned" }}`

Si une extension utilise la fonctionnalité installation_mode, alors un autre champ "update_url" doit aussi être défini, et pointer vers l'emplacement depuis lequel l'extension peut être installée.

- Si l'extension que vous téléchargez est hébergée sur le Chrome Web Store, utilisez "https://clients2.google.com/service/update2/crx".

- Si vous hébergez l'extension sur votre propre serveur, saisissez l'URL à laquelle Chrome doit accéder pour télécharger l'extension empaquetée (fichier .crx).
  Exemple de code JSON - force_installed extension with update_url :
  `{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url": "https://clients2.google.com/service/update2/crx"}}`
- Depuis Chrome 89, vous pouvez aussi utiliser le paramètre override_update_url pour spécifier l'utilisation par Chrome de l'URL dans le champ update_url field ou l'URL de mise à jour indiquée dans la règle ExtensionInstallForcelist pour les mises à jour d'extension ultérieures.
  - Si cette règle n'est pas configurée ou si elle est définie sur "False", Chrome utilise l'URL spécifiée dans le fichier manifeste de l'extension pour les mises à jour.

Empêcher les extensions d'altérer les pages Web

Ce paramètre empêche les extensions de modifier et de lire les données de vos sites Web les plus sensibles.
Cette règle empêche les extensions :
- d'injecter des scripts dans vos sites Web ;
- de consulter les cookies ;
- d'apporter des modifications de type requête Web.

Ce paramètre n'interdit pas l'installation ou la suppression d'extensions par l'utilisateur. Il empêche seulement les extensions d'altérer les sites Web que vous spécifiez.

Vous pouvez utiliser deux paramètres pour cette fonctionnalité.
- **runtime_blocked_hosts** : les extensions ne peuvent pas interagir avec ces hôtes.

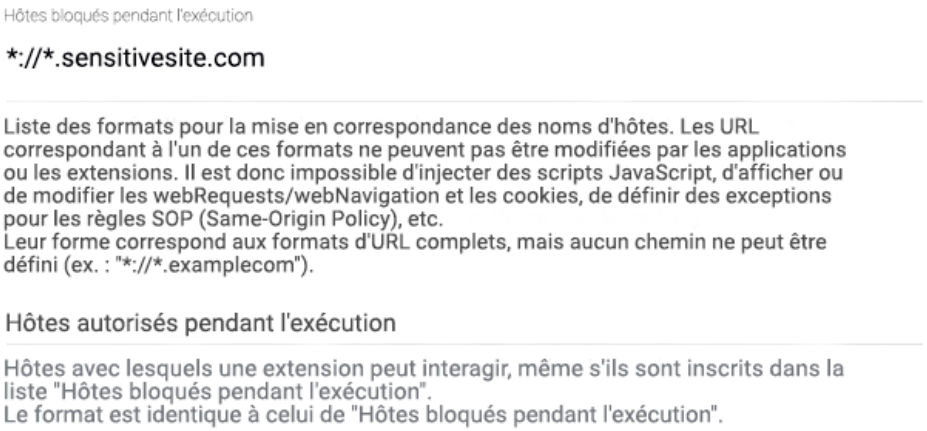
- **runtime_allowed_hosts** : les extensions peuvent interagir avec les hôtes de cette liste même s'ils sont définis dans runtime_blocked_hosts.

Conseil : Chaque instance de runtime_blocked_hosts et de runtime_allowed_hosts peut avoir 100 formats d'hôte au maximum. Si vous en définissez plus, votre règle sera invalide.

Gestion cloud du navigateur Chrome
Le blocage par hôte pendant l'exécution est plus facile dans la gestion cloud du navigateur Chrome que dans GPO. Aucun code JSON n'est requis, et il vous suffit de saisir l'URL que vous voulez bloquer dans les paramètres des extensions. Pour ce faire, vous devez enregistrer les appareils utilisant les navigateurs dans la gestion cloud du navigateur Chrome. La fonctionnalité est proposée sans coût supplémentaire. La procédure d'enregistrement se trouve ici.

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.
2. Sélectionnez l'unité organisationnelle comportant les utilisateurs pour lesquels vous souhaitez autoriser des extensions.
3. Cliquez sur l'icône en forme de roue dentée permettant d'accéder aux paramètres supplémentaires  .
4. Saisissez l'URL des sites Web sur lesquels les extensions ne doivent pas s'exécuter dans la section "Hôtes bloqués pendant l'exécution". Pour en savoir plus sur la syntaxe, consultez Syntaxe des URL bloquées et des URL autorisées.
    a. Vous pouvez saisir plusieurs URL en appuyant sur "Entrée" après chaque saisie d'URL pour saisir une nouvelle entrée.
    b. Vous pouvez aussi cliquer sur une extension individuelle et définir les hôtes autorisés et les hôtes bloqués dans la section sur les autorisations et l'accès par URL.
        i. Remarque : cette opération remplacera toute règle globale s'appliquant déjà à l'extension en question.
        ii. Il existe également une section allowed_hosts pour les exceptions des URL qui sont listées dans la section des hôtes de blocage à l'exécution.

5. Cliquez sur **Enregistrer**.



Section "Hôtes bloqués pendant l'exécution" dans Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs > Paramètres supplémentaires.

GPO
Ces instructions indiquent comment gérer ce GPO sur les machines Windows. Pour les autres plateformes, cliquez sur les liens suivants : Mac | Linux

Dans la règle des paramètres des extensions, vous pouvez définir les paramètres suivants pour bloquer (ou autoriser) l'altération des sites Web ou des domaines :

- Runtime_blocked_hosts
  Ce paramètre empêche les extensions d'apporter des modifications ou de lire les données des sites Web que vous choisissez.

- Runtime_allowed_hosts
  Ce paramètre autorise les extensions à apporter des modifications aux sites Web ou à en lire les données.

Le format servant à spécifier votre ou vos sites dans la chaîne JSON dans l'une ou l'autre des règles est le suivant :

```
[http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
```

Remarque : Les sections [hostname|*] et [eTLD|*] sont obligatoires, tandis que la section [subdomain|*] est facultative.

Exemples de formats d'hôte valides et de formats correspondants :

Formats d'hôtes valides	**Correspondance établie**	**Adresses ne correspondant pas au format**
://.example.*	http://example.com https://test.example.co.uk	https://example.google.com http://example.google.co.uk
http://example.*	http://example.com http://example.ly	https://example.com http://test.example.com
http://example.com	http://example.com	https://example.com http://test.example.co.uk
://	Toutes les URL	

Voici un exemple de chaîne JSON qui bloque l'accès à une seule extension. Cette chaîne empêche une seule extension de modifier un site spécifique :

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Données au format JSON sous forme compacte :

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

Voici un exemple de blocage de plusieurs sites pour toutes les extensions :

```
{
   "*": {"runtime_blocked_hosts": [ "*://*.importantwebsite.com",
"*://*.importantwebsite2.com" ]
   }
```

Données au format JSON sous forme compacte :

```
{"*":{"runtime_blocked_hosts":["*://*.importantwebsite.com","*://*.importantweb
site2.com"]}}
```

Dans le cas de plusieurs extensions, séparez-les chacune dans leur propre entrée, pour chaque ID d'application que vous souhaitez bloquer. Voici un exemple de la marche à suivre pour empêcher deux extensions de s'exécuter sur le même domaine :

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      },
      "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Données au format JSON sous forme compacte :

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn":
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

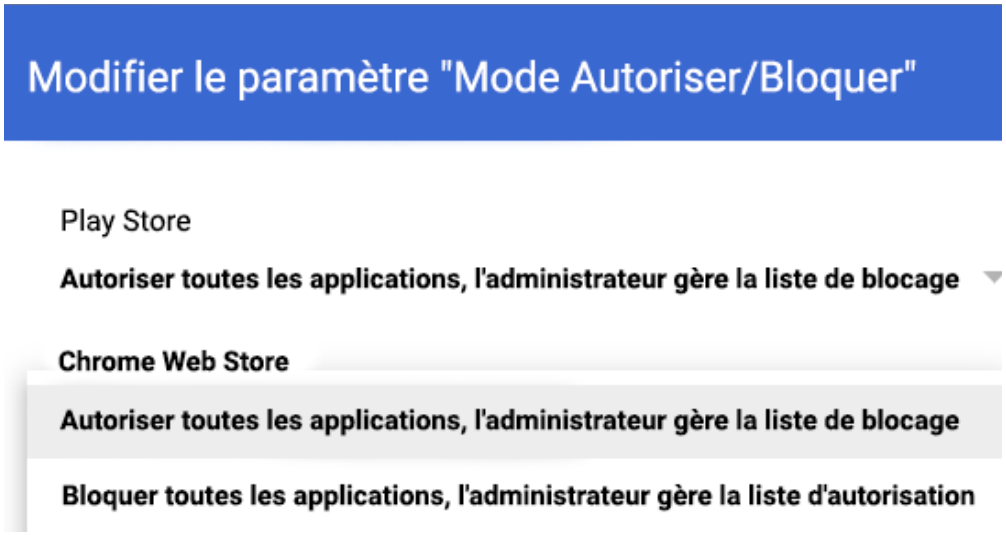
Autoriser ou bloquer des extensions dans la console d'administration Google

Les administrateurs peuvent contrôler les extensions que les utilisateurs sont autorisés à installer en créant des listes d'autorisation et de blocage. Vous pouvez autoriser les utilisateurs à installer toute application ou extension. Vous pouvez définir des règles pour bloquer ou autoriser des applications pour tous les utilisateurs ou seulement une partie des collaborateurs.

La procédure suivante part du principe que vous savez comment modifier les paramètres dans la console d'administration.

Autoriser toutes les extensions à l'exception de celles que vous souhaitez bloquer

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs > Paramètres supplémentaires**.
2. Sélectionnez sur la gauche l'unité organisationnelle pour laquelle vous souhaitez autoriser les extensions.
3. Faites défiler la page jusqu'à la section "Mode Autoriser/Bloquer" pour le Chrome Web Store, cliquez sur "Modifier" et sélectionnez l'option **Autoriser toutes les applications, l'administrateur gère la liste de blocage**.



Paramètre "Mode Autoriser/Bloquer"

4. Cliquez sur **Enregistrer**.
5. Cliquez sur l'onglet "Utilisateurs et navigateurs" pour revenir à la page précédente.
6. Ajoutez chaque extension que vous voulez bloquer en cliquant sur le bouton jaune "Plus" en bas à droite.
7. Choisissez votre méthode d'ajout à la console ("Ajouter à partir du Chrome Web Store", "Ajouter une application ou une extension Chrome à l'aide de son ID", "Ajouter par URL").

8. Sélectionnez la liste déroulante d'une extension et choisissez **Bloquer**.
9. Cliquez sur **Enregistrer**.

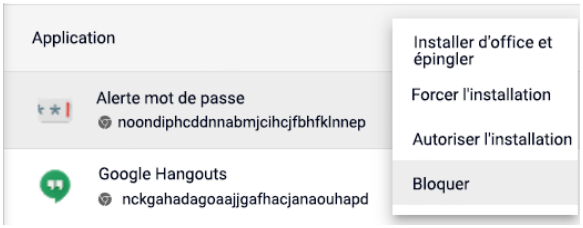
Bloquer toutes les extensions à l'exception de celles que vous souhaitez autoriser

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs > Paramètres supplémentaires**.
2. Sélectionnez sur la gauche l'unité organisationnelle pour laquelle vous souhaitez bloquer les extensions.
3. Faites défiler la page jusqu'à la section "Mode Autoriser/Bloquer" pour le Chrome Web Store et sélectionnez l'option **Bloquer toutes les applications, l'administrateur gère la liste d'autorisation**.

4. Cliquez sur **Enregistrer**.
5. Cliquez sur l'onglet "Utilisateurs et navigateurs" pour revenir à la page précédente.
6. Ajoutez chaque extension que vous voulez autoriser en cliquant sur le bouton jaune "Plus" en bas à droite.
7. Choisissez votre méthode d'ajout à la console ("Ajouter à partir du Chrome Web Store", "Ajouter une application ou une extension Chrome à l'aide de son ID", "Ajouter par URL").
8. Sélectionnez la liste déroulante d'une extension et choisissez **Autoriser l'installation**.
   a. Vous pouvez aussi installer d'office l'extension sur vos machines utilisateur en sélectionnant "Forcer l'installation".
9. Cliquez sur **Enregistrer**.

Bloquer ou autoriser une extension

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.
2. Sélectionnez l'unité organisationnelle pour laquelle vous voulez autoriser ou bloquer l'extension.
   - Notez que l'unité organisationnelle héritera des paramètres de l'unité organisationnelle parente, mais que vous pouvez ignorer cette règle en utilisant des sous-unités.
3. Sélectionnez l'extension que vous voulez bloquer ou autoriser, ou ajoutez-la (voir les étapes 6 et 7 de la section précédente).
4. Dans la colonne "Règles d'installation", sélectionnez "Bloquer", "Forcer l'installation" ou "Autoriser l'installation".



5. Cliquez sur **Enregistrer**.

Installer d'office des extensions

Si vous savez que l'utilisateur a besoin d'une extension, vous pouvez la lui installer. Si vous installez d'office une extension, toutes les autorisations dont elle a besoin pour fonctionner lui sont accordées. L'utilisateur ne pourra pas la supprimer et elle sera installée de façon autonome. Si vous supprimez une extension de la liste des extensions installées d'office, elle sera supprimée de la machine de l'utilisateur.

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.
2. Sélectionnez l'unité organisationnelle pour laquelle vous voulez installer d'office des extensions.
3. Sélectionnez la ou les extensions existantes que vous voulez installer d'office ou ajoutez-les.
   a. Pour ajouter la ou les extensions que vous voulez installer, cliquez sur l'icône "Plus" jaune en bas à droite.
   b. Choisissez votre méthode d'ajout à la console ("Ajouter à partir du Chrome Web Store", "Ajouter une application ou une extension Chrome à l'aide de son ID", "Ajouter par URL").
4. Sélectionnez la ou les extensions que vous voulez installer d'office et, dans la colonne "Règles d'installation", sélectionnez **Forcer l'installation** dans le menu déroulant.

5. Cliquez sur **Enregistrer**.

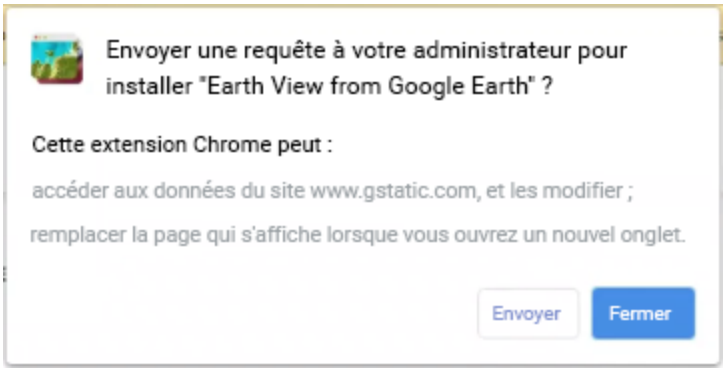
Notez que vous pouvez créer une collection Chrome Web Store personnalisée d'extensions sélectionnées par l'administrateur pouvant être consultée par vos utilisateurs. Ce paramètre nécessite que les utilisateurs soient connectés à Google avec leurs identifiants d'entreprise.

- Ce paramètre se trouve dans la console d'administration dans Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs > Paramètres supplémentaires > Page d'accueil du Chrome Web Store > Utiliser la collection du Chrome Web Store.

- Ensuite, vous pouvez afficher toutes vos extensions sur cette page, ou bien vous pouvez cliquer sur des extensions individuelles dans la section "Utilisateurs et navigateurs" et activer le bouton "Inclure dans la collection du Chrome Web Store".

Autoriser les utilisateurs à demander des extensions : workflows des extensions

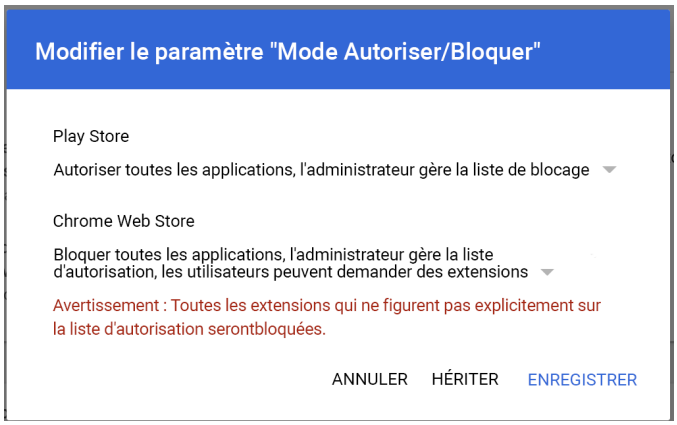
La console d'administration Google vous permet, en tant qu'administrateur, d'autoriser les utilisateurs à demander les extensions dont ils ont besoin dans le Chrome Web Store. Vous pouvez ensuite autoriser, bloquer ou installer automatiquement les extensions demandées par les utilisateurs.



Exemple de boîte de dialogue de demande du Chrome Web Store

Notez que cette fonctionnalité est semblables aux listes d'autorisation/de blocage. Lorsque la fonctionnalité est activée, **toutes** les extensions sont bloquées par défaut. Pour prévenir tout problème, il est recommandé de suivre ce processus :

1. Examinez les extensions dont se servent actuellement vos utilisateurs à l'aide du rapport Takeout sur les extensions dans la gestion cloud du navigateur Chrome.
    - Pour plus d'informations, consultez cette vidéo YouTube sur la configuration de l'API Takeout.
2. Élaborez la liste des extensions essentielles (GPO ou console d'administration) en fonction des données recueillies à l'étape 1.
3. Activez la fonctionnalité de workflow des extensions sous **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs > Paramètres supplémentaires > Mode Autoriser/Bloquer** et appuyez sur le bouton "Modifier".
4. Sous Chrome Web Store, sélectionnez **Bloquer toutes les applications, l'administrateur gère la liste d'autorisation, les utilisateurs peuvent demander des extensions** dans le menu déroulant.



Activer les workflows des extensions dans la console d'administration

- Nous vous recommandons de commencer par appliquer les paramètres à un petit nombre d'utilisateurs et d'appareils dans une unité organisationnelle de test pour prévenir tout problème pour les utilisateurs finaux et recueillir des retours. Une fois que vous êtes prêt, vous pouvez les appliquer à toute votre organisation.

5. Les demandes d'approbation et de refus sont gérées sous **Appareils > Chrome > Applications et extensions > Demandes**.
6. Cliquez sur la ligne de la demande d'extension que vous voulez examiner.
7. Vous pouvez y consulter les informations sur l'extension et sélectionner la règle d'installation dans le menu déroulant :
   - Forcer l'installation : installe l'extension de façon autonome, celle-ci ne peut pas être supprimée.
   - Autoriser l'installation : permet aux utilisateurs d'installer l'extension.
   - Bloquer : empêche les utilisateurs d'installer l'extension. Cela supprime également l'extension pour les utilisateurs qui l'ont installée.

Pour plus d'informations sur cette fonctionnalité, consultez l'article du centre d'aide sur les workflows des extensions ou cette vidéo YouTube sur les workflows des extensions.

Autoriser ou bloquer les extensions dans la stratégie de groupe

Avant de commencer : Pour la procédure suivante, vous devez déjà gérer Chrome pour vos utilisateurs. Pour plus d'informations sur la manière de déployer Chrome sur Windows, reportez-vous au guide de déploiement du navigateur Chrome (Windows). Pour le déploiement et la gestion des règles sur Mac®, consultez Installer le navigateur Chrome sous Mac.

Sous Windows, il existe deux types de modèles de règles : le modèle ADM et le modèle ADMX. Vérifiez bien le type que vous utilisez sur votre réseau. Les modèles précisent quelles sont les clés de registre à définir pour configurer Chrome, ainsi que les valeurs possibles de ces clés. Ce sont les valeurs définies dans ces clés de registre qui déterminent le comportement de Chrome.

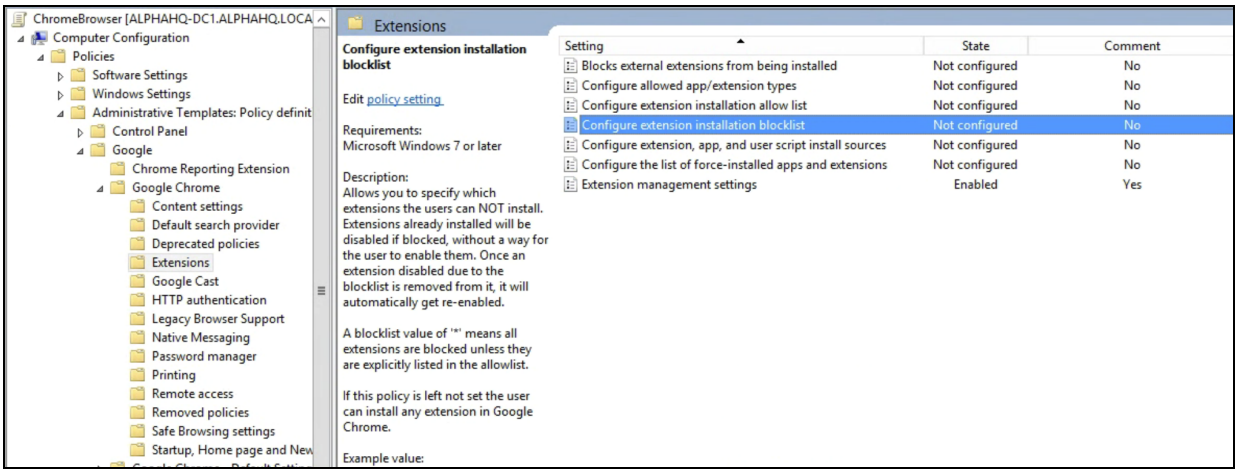
1. Téléchargez les modèles de règles Chrome.
   Les modèles Windows, ainsi que la documentation sur les règles courantes pour tous les systèmes d'exploitation, sont disponibles en cliquant sur ce lien.
2. Ouvrez le modèle ADM ou ADMX que vous avez téléchargé :
   a. Accédez à **Démarrer > Exécuter : gpedit.msc**.
   b. Accédez à **Stratégie Ordinateur local > Configuration ordinateur > Modèles d'administration**.
   c. Effectuez un clic droit sur **Modèles d'administration**, puis sélectionnez **Ajout/Suppression de modèles**.
   d. Ajoutez le modèle chrome.adm via la boîte de dialogue qui s'affiche.

Ensuite, si ce n'est pas déjà le cas, un dossier Google ou Google Chrome s'affichera sous les modèles d'administration.

- Si vous ajoutez le modèle ADM sous Windows 7 ou 10, il apparaît dans le dossier "Modèles d'administration classiques/Google/Google Chrome".

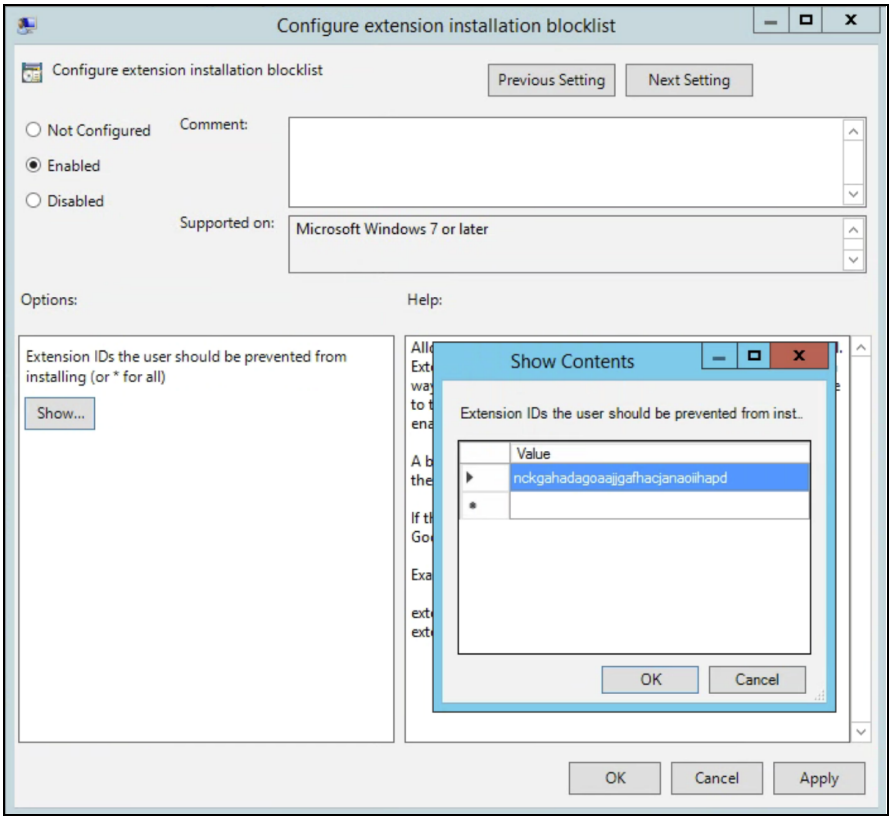
Autoriser toutes les extensions à l'exception de celles que vous souhaitez bloquer

1. Dans l'éditeur de stratégie de groupe, ouvrez le modèle que vous avez ajouté.
2. Accédez à **Google > Google Chrome > Extensions > Configurer la liste de blocage concernant l'installation des extensions**.



Chemin d'accès vers les règles de gestion des extensions

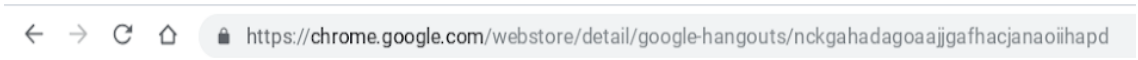
3. Dans le paramètre, sélectionnez **Activé**.
4. Cliquez sur **Afficher**.
5. Saisissez l'ID d'application des extensions que vous voulez bloquer.



Configurer la liste de blocage concernant l'installation des extensions

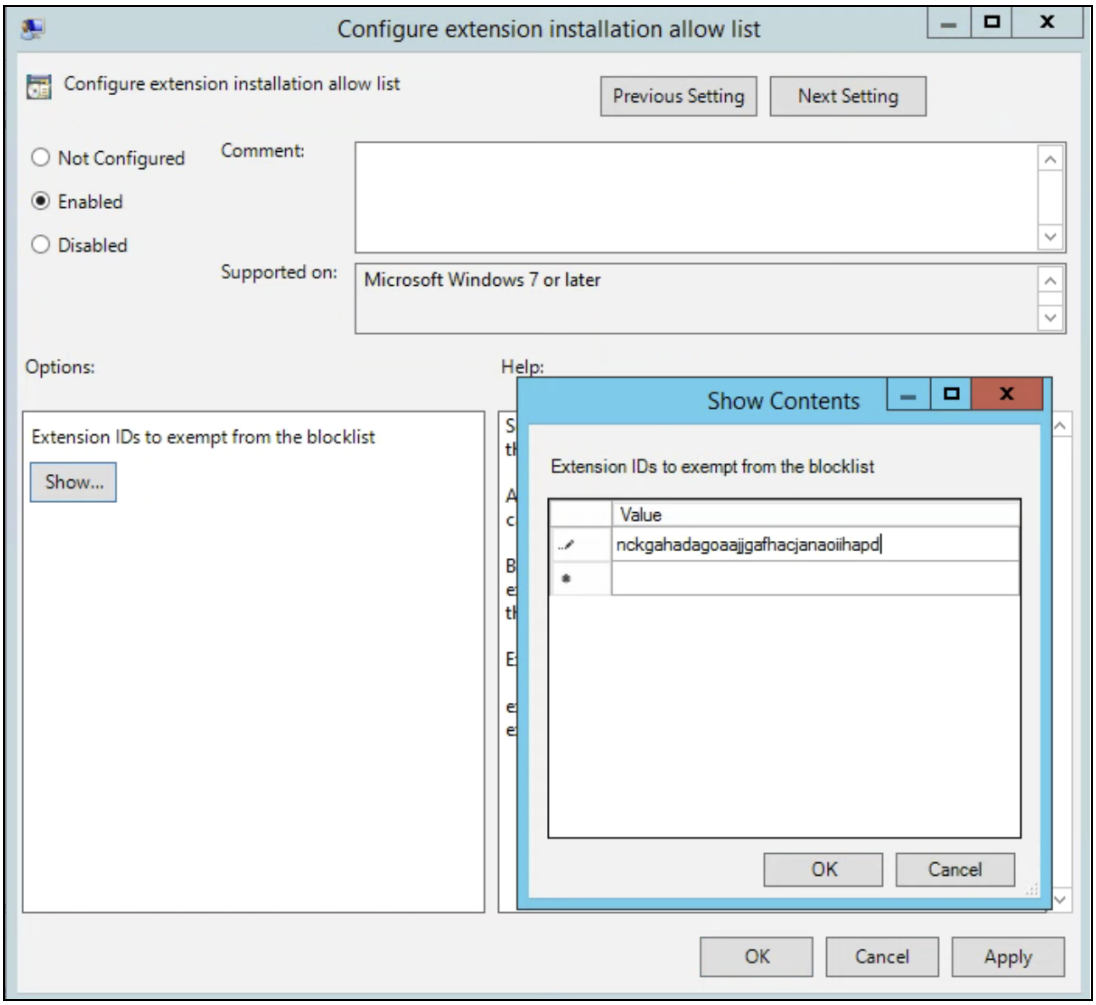
Remarques :

- Si vous ne trouvez pas l'ID d'application d'une extension, consultez-la dans le Chrome Web Store. Cherchez l'extension en question ; l'ID d'application se trouve à la fin de l'URL dans l'omnibox Chrome :



Exemple d'ID d'application se trouvant après google-hangouts/

- Saisissez ***** dans la règle pour empêcher l'installation d'extensions. Vous pouvez utiliser ce signe avec la règle "Configurer la liste d'autorisation concernant l'installation des extensions". De cette manière, vous autorisez l'installation de certaines extensions seulement par vos utilisateurs, et bloquez le reste.
- Vous pouvez ajouter à la liste de blocage une extension déjà installée sur la machine d'un utilisateur. L'extension sera désactivée et l'utilisateur ne pourra pas la réactiver. Elle ne sera pas désinstallée, simplement désactivée.



Configurer la liste d'autorisation concernant l'installation des extensions

Bloquer ou autoriser une extension

Pour bloquer une seule extension, ajoutez l'ID d'application de l'extension que vous voulez bloquer à la règle "Configurer la liste de blocage concernant l'installation des extensions". Toutes vos autres extensions pourront être installées.

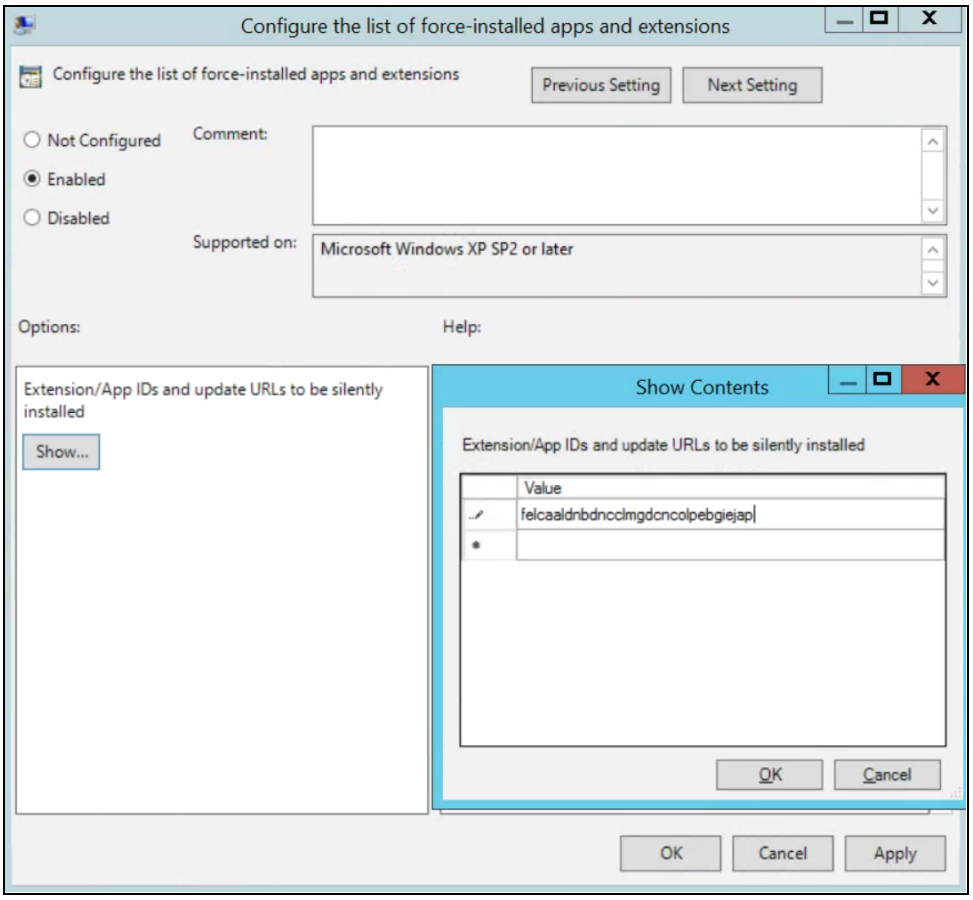
Pour autoriser seulement une extension :

1. Dans la section de contenu de la règle "Configurer la liste de blocage concernant l'installation des extensions", saisissez *****.
   Aucune extension de la liste ne pourra être installée.
2. Ajoutez l'ID d'application de l'extension autorisée à la règle "Configurer la liste d'autorisation concernant l'installation des extensions".

Installer d'office une extension

1. Dans l'éditeur de stratégie de groupe, accédez à **Google > Google Chrome > Extensions > Configurer la liste des applications et des extensions dont l'installation est forcée**.
2. Sélectionnez **Activé**.
3. Cliquez sur **Afficher**.
4. Saisissez l'ID ou les ID d'application de la ou des extensions que vous voulez installer d'office.

L'extension sera installée de façon autonome sans interaction de la part de l'utilisateur, qui ne pourra pas non plus désinstaller ni désactiver l'extension. Ce paramètre remplace toute règle de liste de blocage que vous pourriez avoir activée.



Configurer la liste des applications et des extensions installées d'office

Valider votre règle

Pour vérifier qu'une règle est valide et fonctionne comme prévu, appliquez-la sur une machine de test. Exécutez la procédure suivante sur la machine de test.

1. Accédez à l'adresse chrome://policy.
2. Cliquez sur le bouton "Actualiser les règles".
3. En haut à droite de la page, saisissez "ExtensionSettings" dans le filtre de règle pour n'afficher que la règle correspondante.
4. Cochez l'option "Afficher les règles non paramétrées".
5. Vérifiez que la colonne "État" de la règle affiche "OK".
6. Développez la règle en cliquant sur "Plus" et vérifiez que la valeur n'est pas vide.
7. Félicitations, vous disposez d'une règle valide.

Auto-héberger vos propres extensions

Le Chrome Web Store héberge les extensions et offre de nombreuses fonctionnalités de sécurité.

- Fonctionnalités telles que les lecteurs de code manuels et automatisés.
    - Celles-ci empêchent l'envoi de code malveillant à vos utilisateurs.

Vous avez cependant la possibilité d'héberger vos extensions sur votre propre serveur, séparément du Chrome Web Store. Voici quelques avantages et inconvénients liés à cette méthode :

Avantages :

- Le fait d'héberger vos propres extensions signifie que vous ne dépendez pas des règles et exigences du Chrome Web Store.
    - La vérification des extensions est moindre, et le risque de suppression de l'extension pour cause de violation des conditions d'utilisation est limité.

Inconvénients :

- La méthode d'auto-hébergement nécessite une configuration plus poussée et exige que vous hébergiez votre propre serveur de fichiers pour les fichiers d'extension.
- La validation de la sécurité des extensions et la mise à jour de celles-ci peuvent être complexes, alors que le Chrome Web Store effectue ces opérations automatiquement.

Si vous choisissez d'auto-héberger vos extensions, cette section vous explique comment procéder. Elle décrit comment empaqueter une extension et l'héberger sans utiliser le Chrome Web Store. Elle comprend également des instructions concernant le déploiement de ces extensions sur vos appareils et pour vos utilisateurs.

Alternatives à l'auto-hébergement des extensions

Options de publication des extensions

Comme alternative à l'auto-hébergement, envisagez de marquer les extensions internes sur le Chrome Web Store comme privées. Il existe trois options de publication des extensions : "Public", "Privé" et "Non répertorié". Voici un tableau qui reprend les avantages et les inconvénients de chaque option :

	Présent dans la recherche du Chrome Web Store ?	Exige une connexion ?	Compatible avec la gestion clouddu navigateur Chrome
Public	Oui	Non	Oui
Privé	Non	Oui	Oui
Non répertorié	Non	Non. Les utilisateurs ont besoin du lien pour installer l'extension	Oui

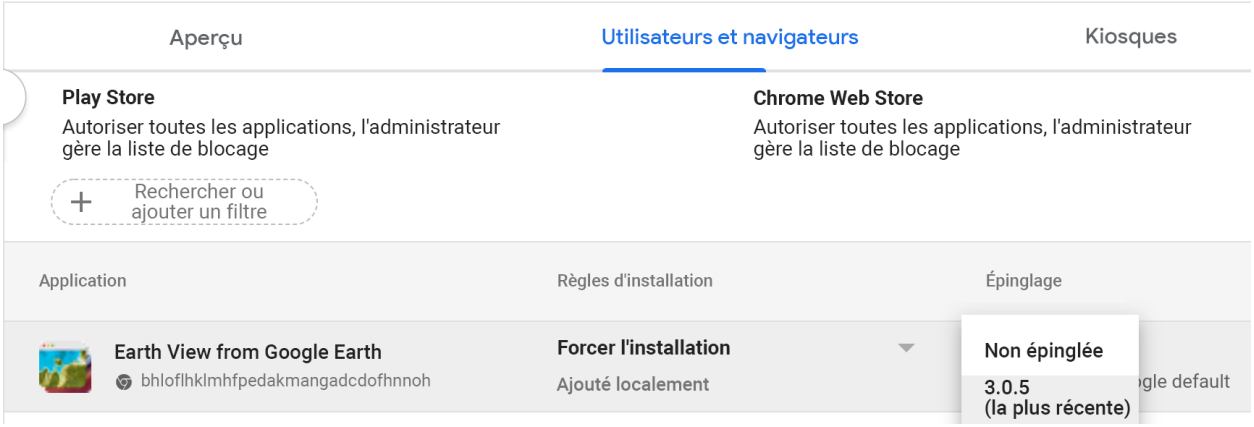
Pour plus d'informations, consultez ce blog qui décrit comment publier des extensions hors de la vue du public, sans devoir auto-héberger vos extensions.

- Notez que si vous gérez vos extensions via la console d'administration, vous devez configurer le paramètre d'autorisations du Chrome Web Store de manière à activer l'affichage des extensions privées pour vos utilisateurs.
    - Ce paramètre se trouve dans la console d'administration sous "Appareils" > "Chrome" > "Applications et extensions" > "Paramètres supplémentaires" > "Autorisations du Chrome Web Store" > activez l'option "Autoriser les utilisateurs à publier des applications privées limitées à votre domaine sur le Chrome Web Store".

Épingler une version spécifique d'une extension dans la console d'administration

La console d'administration Google propose maintenant quelques nouvelles options de gestion des extensions. D'abord, vous pouvez épingler une version d'une extension directement dans la console d'administration. Cette option offre plus de stabilité aux entreprises contraintes d'utiliser une version spécifique de l'extension. Il n'est pas recommandé, dans les bonnes pratiques, d'épingler d'anciennes versions des extensions. Si vous devez épingler une ancienne version, faites en sorte que cette mesure soit temporaire pour toujours disposer de la fonctionnalité et des mises à jour de sécurité les plus récentes. Cette fonctionnalité est disponible uniquement pour les extensions installées d'office. Pour en savoir plus, consultez cet article du centre d'aide.

1. Dans la console d'administration, accédez à **Appareils > Chrome > Applications et extensions > Utilisateurs et navigateurs**.
2. Sélectionnez l'unité organisationnelle qui contient l'extension que vous voulez épingler.
3. Sélectionnez (ou ajoutez) la ou les extensions que vous voulez gérer par version, puis, sous la colonne "Épinglage", sélectionnez la version que vous voulez épingler dans le menu déroulant et appuyez sur "Enregistrer".
    a. Notez qu'en épinglant une application ou une extension, elle ne recevra plus les mises à jour, y compris celles concernant la sécurité et la compatibilité.
    b. Vous pouvez aussi épingler uniquement la version de l'extension disponible sur le Chrome Web Store au moment de la configuration.
    c. Vous pouvez également épingler des applications et extensions auto-hébergées, et mettre à jour l'URL dans la console d'administration. Pour plus d'informations, consultez la section "Épingler des applications auto-hébergées" dans cette entrée du centre d'aide.



Épinglage de version dans la console d'administration

Exigences liées aux extensions auto-hébergées

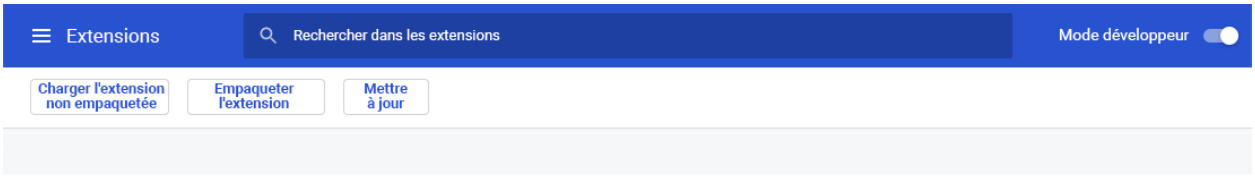
Pour héberger votre extension, vous avez besoin de vos propres services d'hébergement Web pour l'extension et de son fichier manifeste. Cet emplacement d'hébergement ne doit pas avoir besoin d'une authentification. Les appareils doivent pouvoir y accéder, où qu'ils se trouvent. Gardez cela en mémoire si vous voulez héberger le fichier sur votre référentiel interne.

Cette procédure implique que vous ayez déjà créé votre extension, que vous soyez à l'aise avec les fichiers XML, et que vous ayez des connaissances sur la stratégie de groupe et l'utilisation du registre Windows. La procédure ne s'applique pas aux extensions tierces que vous ne développez pas. Si vous souhaitez auto-héberger une extension tierce, parlez-en directement avec le fournisseur de l'extension.

Empaqueter votre extension

Les extensions doivent d'abord être empaquetées dans un fichier CRX. Si l'extension n'est pas empaquetée sous forme de fichier CRX, voici la marche à suivre :

1. Accédez à **chrome://extensions** dans la barre d'adresse de Chrome et activez le **Mode développeur**.

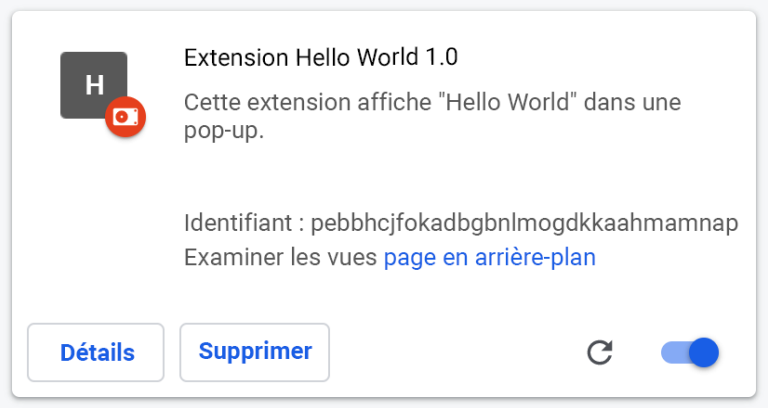


2. Une fois dans le mode développeur, créez le fichier CRX en cliquant sur **Empaqueter l'extension**.

3. Sélectionnez le répertoire où se situe votre source. Votre fichier CRX est alors créé, ainsi qu'un fichier PEM.

Conseil : Conservez le fichier PEM en sécurité, car il s'agit de la clé de votre extension. Vous en aurez besoin pour de futures mises à jour.

4. Faites glisser le CRX dans la fenêtre des extensions et vérifiez que le chargement fonctionne correctement.
    a. Notez que sur Windows et Mac, l'extension sera désactivée par défaut, mais que ce ne sera pas le cas sur Linux.
5. Testez l'extension et prenez note du champ d'identifiant et du numéro de version.
   Ces informations vous serviront par la suite.



5. Placez le fichier CRX à l'emplacement d'hébergement depuis lequel il sera téléchargé par les utilisateurs et les appareils.
    - Notez l'URL à laquelle le fichier est importé.
    - Cette information sera importante pour le fichier XML manifeste.
6. Pour créer un fichier XML manifeste avec l'identifiant d'application/extension, téléchargez l'URL, la version, et définissez ces trois champs :
    - **appid** (l'identifiant d'extension récupéré à l'étape 5)
    - **codebase** (l'emplacement de téléchargement du fichier CRX récupéré à l'étape 3)
    - **version** (la version de l'application/extension, qui doit correspondre à l'étape 5)

   Exemple de fichier XML manifeste :

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='abcdefghijklmnopqrstuvwxyz123456
'>
    <updatecheck codebase='https://example.com/chrome/helloworld.crx'
version='1.0' />
  </app>
</gupdate>
```

8. Importez le fichier XML finalisé à un emplacement d'où il pourra être téléchargé par vos utilisateurs et appareils, et notez bien l'URL.

Héberger votre extension

Le serveur qui héberge les fichiers .crx de votre extension doit utiliser des en-têtes HTTP appropriés pour permettre aux utilisateurs d'installer l'extension en cliquant sur un lien.
Google Chrome considère qu'un fichier peut être installé si l'une des conditions se vérifie :

- Le fichier dispose du type de contenu application/x-chrome-extension.
- Le suffixe du fichier est .crx et les deux conditions suivantes se vérifient :
    - Le fichier ne dispose pas de l'en-tête HTTP X-Content-Type-Options: nosniff.
    - Le fichier dispose de l'un des types de contenu suivants :
        - chaîne vide
        - "text/plain"
        - "application/octet-stream"
        - "unknown/unknown"
        - "application/unknown"
        - "*/*"

Lorsqu'un fichier pouvant être installé n'est pas reconnu, c'est généralement parce que le serveur envoie l'en-tête X-Content-Type-Options: nosniff. Cela peut aussi être dû au fait que le serveur envoie un type de contenu inconnu, qui ne figure pas dans la liste ci-dessus. Pour résoudre un problème d'en-tête HTTP, modifiez la configuration du serveur ou essayez d'héberger le fichier .crx sur un autre serveur.

Publier des mises à jour de vos extensions

Assurez-vous d'avoir apporté les modifications requises à votre extension et de l'avoir testée. Pour publier des mises à jour :

1. Modifiez le numéro de version du fichier manifeste JSON de l'extension pour qu'il soit supérieur à celui d'avant.
   Exemple :
   `"version": "versionString"`
   Si la `"version" est "1.0"`, vous pouvez la modifier en `"version":"1.1"` ou tout numéro supérieur à `"1.0"`.

2. Modifiez la `"version"` de `<updatecheck>` dans le fichier XML pour qu'elle corresponde au numéro que vous avez indiqué dans le fichier manifeste à l'étape précédente.
   Prenons cet autre exemple :
   ```
   <updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx'
   version='1.1' />
   ```

3. Recréez un fichier CRX qui inclut les nouveaux changements :
    a. Accédez à **chrome://extensions** dans la barre d'adresse de Chrome.
    b. Activez le **mode développeur**.

4. Créez le fichier CRX en cliquant sur **Empaqueter l'extension** et en sélectionnant le répertoire où se situe votre source.
   Remarque : Pour le fichier PEM, utilisez le fichier généré et enregistré la première fois que le fichier CRX a été créé.
5. Faites glisser le CRX dans la fenêtre des extensions et vérifiez que le chargement fonctionne correctement.
6. Testez l'extension.
7. Remplacez l'ancien fichier CRX et le fichier XML par le nouveau fichier.
   a. Il doit se trouver à l'emplacement hôte où les utilisateurs ou appareils ont téléchargé les fichiers auparavant.

Les modifications seront prises en compte lors du prochain cycle de synchronisation des règles.

URL de référence :

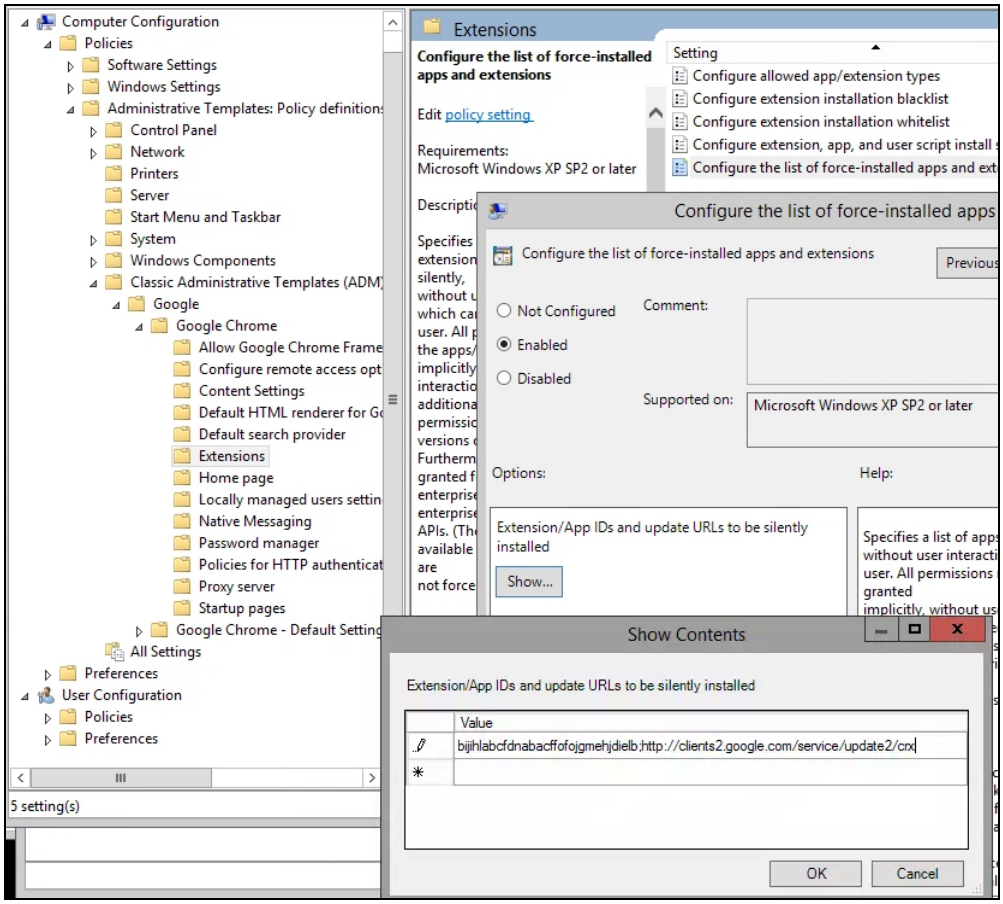
- Mise à jour automatique
- URL de mise à jour
- Manifeste de mise à jour

Distribuer des extensions hébergées en privé

Dans la stratégie de groupe : actuellement, la distribution d'extensions auto-hébergées ne peut s'effectuer que par le biais de la stratégie de groupe. Vous pouvez installer d'office une extension sur l'appareil d'un utilisateur à l'aide de la règle intitulée "Configurer la liste des applications et des extensions dont l'installation est forcée".

Pour les applications hébergées de manière privée (qui ne figurent donc pas dans le Chrome Web Store), utilisez une chaîne du type :
`pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml`

L'URL pointe vers le fichier **update.xml de l'application interne** plutôt que vers l'URL `clients2.google.com` publique.



Règle GPO "Configurer la liste des applications et des extensions dont l'installation est forcée" (Show Contents [Afficher le contenu])

Les règles peuvent ensuite être appliquées aux utilisateurs et aux machines que vous avez sélectionnés Un certain délai peut s'écouler avant que la règle prenne effet. Accélérez le processus en exécutant "gpupdate" sur la machine de l'utilisateur.

Gérer les extensions à l'aide de la gestion cloud du navigateur Chrome

Gérez le navigateur Chrome pour vos machines Windows, Mac et Linux au même endroit, et accédez à une vue complète sur l'état du navigateur Chrome dans votre environnement. La gestion cloud du navigateur Chrome représente une méthode idéale pour gérer les paramètres du navigateur Chrome. Accédez à cette console sans frais supplémentaires. Toutes les sections de ce document qui font référence à la console d'administration Google sont accessibles avec cette fonctionnalité de Chrome. Grâce à la console, vous pouvez obtenir rapidement les informations suivantes :

- Versions du navigateur Chrome actuellement déployées dans votre parc
- Extensions installées sur chaque navigateur
- Règles appliquées à chaque navigateur
- Pour en savoir plus sur la gestion des extensions dans la gestion cloud du navigateur Chrome, consultez cette vidéo.

Autres ressources

Les ressources suivantes vous aideront à gérer le navigateur Chrome dans votre organisation :

- Page de destination de la gestion cloud du navigateur Chrome
- Lot Enterprise du navigateur Chrome
- Liste des règles Chrome
- Notes de version de Chrome Enterprise
- Stratégies de gestion des mises à jour du navigateur Chrome
- Chrome Enterprise Help Center
- Définir Chrome comme navigateur par défaut (Windows 10)
- Article de blog Chrome Insider
- La transition des extensions Chrome vers Manifest V3