



Déploiement de l'extension IMTLazarus dans Google Workspace et mesures de sécurité

Administrateurs IMTLazarus



Indice

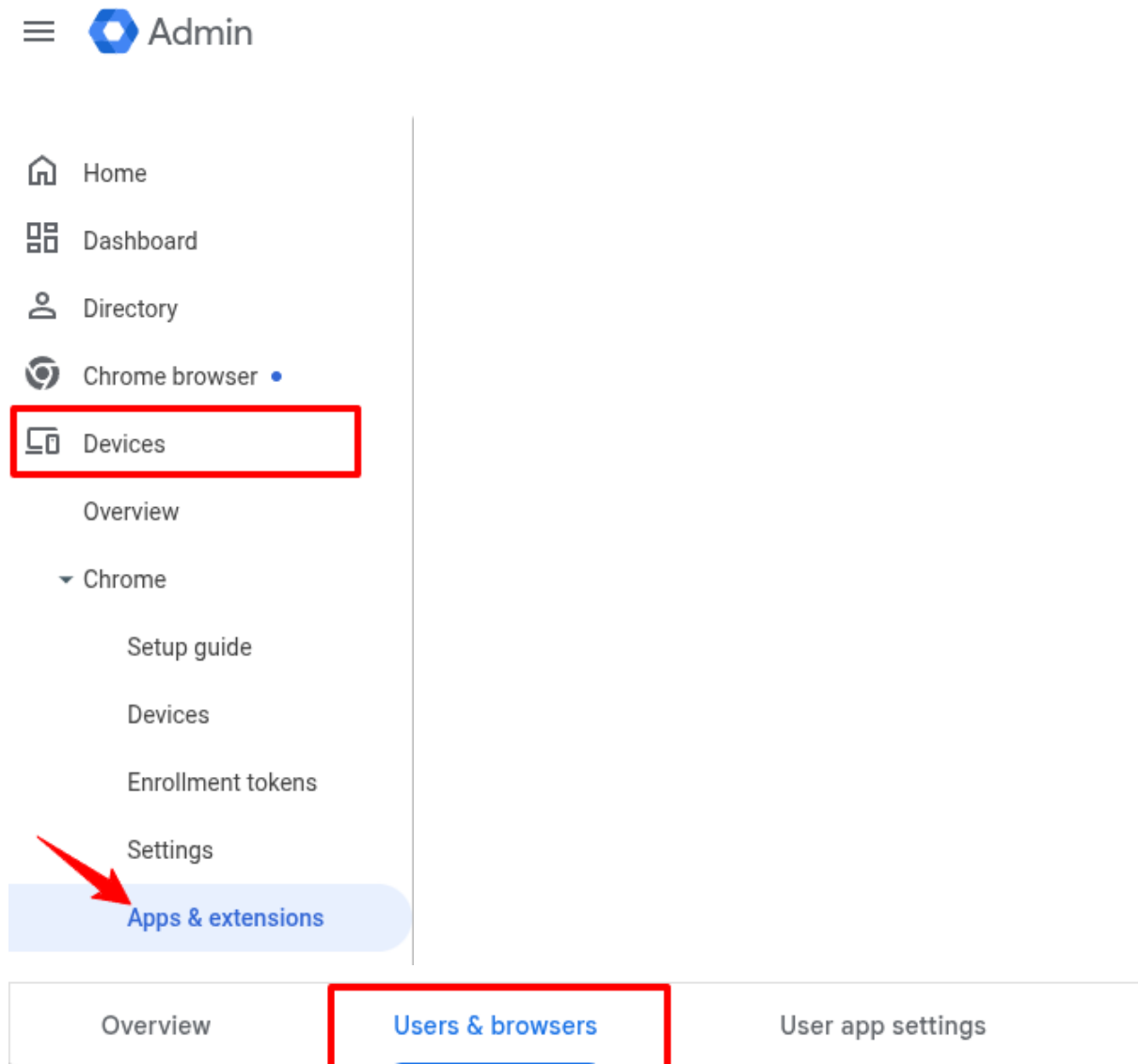
1. Déploiement L'extension IMTLazarus :	2
2. Empêcher la connexion avec des comptes extérieurs au domaine et en mode navigation privée :	6
3. Empêcher les utilisateurs de mettre fin aux processus avec le gestionnaire de tâches Chrome :	9
4. Autorisations d'enregistrement des équipements :	9
5. Empêcher la connexion en tant qu'invité :	11
6. Empêcher le mode développeur :	12
7. Désactiver l'exécution de JavaScript dans la barre d'outils du navigateur :	13
8. Configurez la géolocalisation dans Google Workspace :	14
9. Désactiver la synchronisation Chrome :	15

Introduction

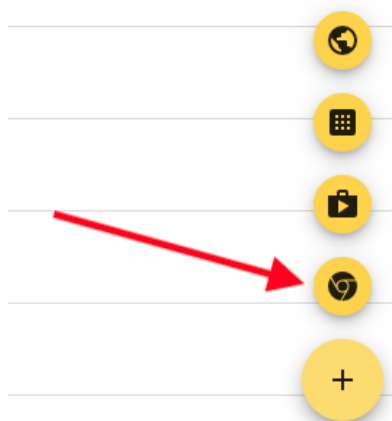
Pour qu'IMTLazarus fonctionne correctement sur les appareils Chrome, IMTLazarus recommande d'effectuer les actions suivantes dans la Console [d'administration Google Workspace](#). La première étape est obligatoire. Les étapes suivantes sont recommandées pour empêcher les utilisateurs de contourner la sécurité et pour que IMTLazarus fonctionne correctement.

1. Déploiement L'extension IMTLazarus :

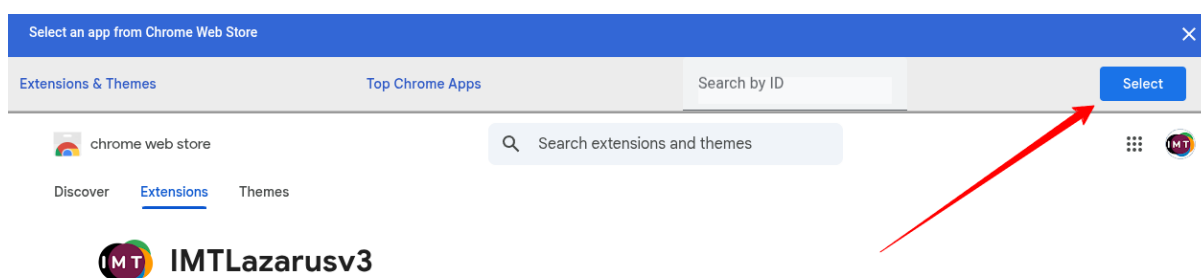
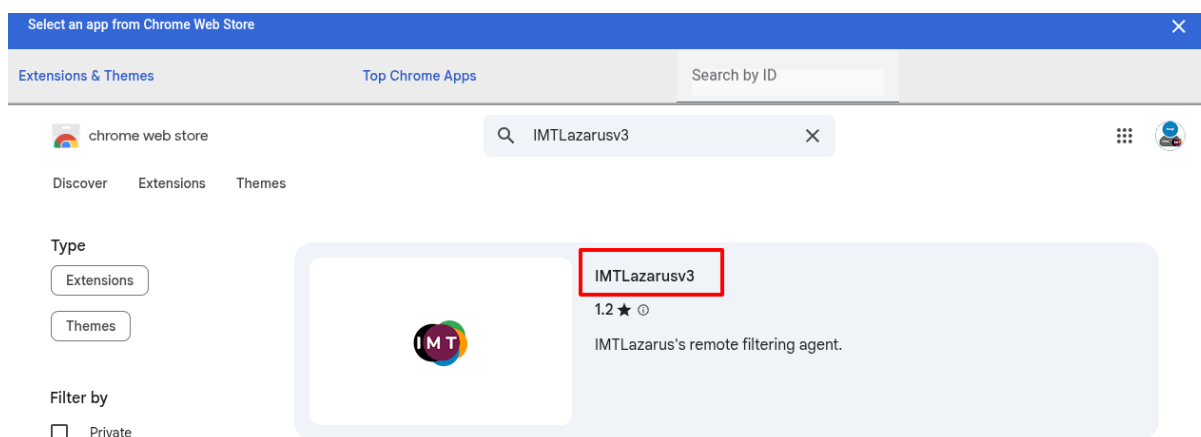
Dans la console d'administration Google Workspace, dans le menu de gauche, développez le menu Appareils > Chrome > Applications et extensions Chrome et cliquez sur Utilisateurs et navigateurs :



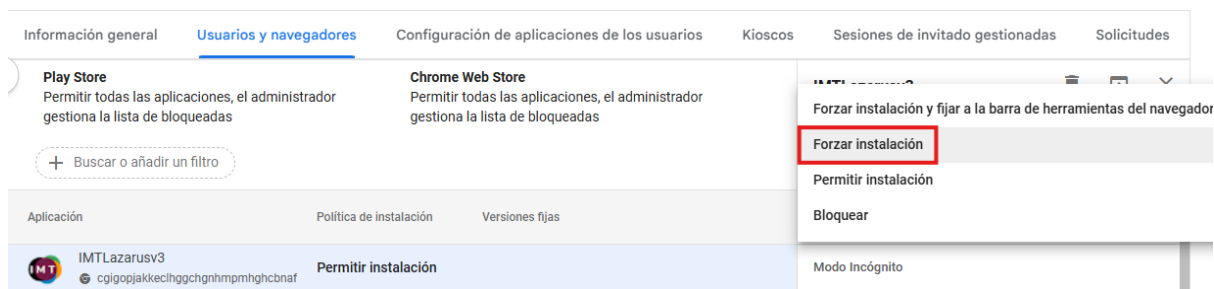
Une fois sur cet écran, sur le côté gauche de l'écran, vous sélectionnez l'unité organisationnelle sur laquelle vous souhaitez travailler. Ensuite, dans l'onglet UTILISATEURS ET NAVIGATEURS, cliquez sur le bouton jaune « + » situé en bas à droite de l'écran, puis sur l'icône Chrome :



Cela ouvrira une nouvelle fenêtre intitulée « Sélectionnez une application dans le Chrome Web Store » à partir de laquelle vous devrez rechercher l'extension « IMTLazarus« v3 », cliquez dessus puis sur le bouton « Sélectionner » en haut à droite de la fenêtre :

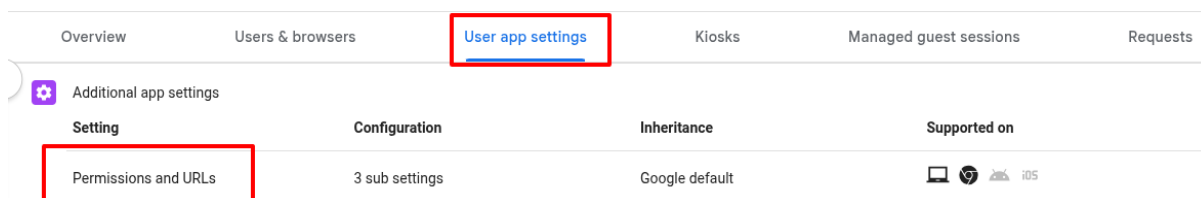


Une fois l'extension disponible, vérifiez que vous avez sélectionné l'unité organisationnelle appropriée, sélectionnez la stratégie d'installation « Forcer l'installation » et cliquez sur le bouton « ENREGISTRER » qui apparaîtra en haut à droite de l'écran pour enregistrer les modifications.



Si vous avez installé une ancienne version de l'extension IMTLazarus, supprimez-la depuis cet écran :

Sans quitter cet écran, cliquez sur l'onglet « Paramètres de l'application utilisateur » et, dans la section « Paramètres supplémentaires de l'application », cliquez sur le paramètre « Autorisations et URL » :



Vérifié que Vous n'avez PAS coché les paramètres suivants.:

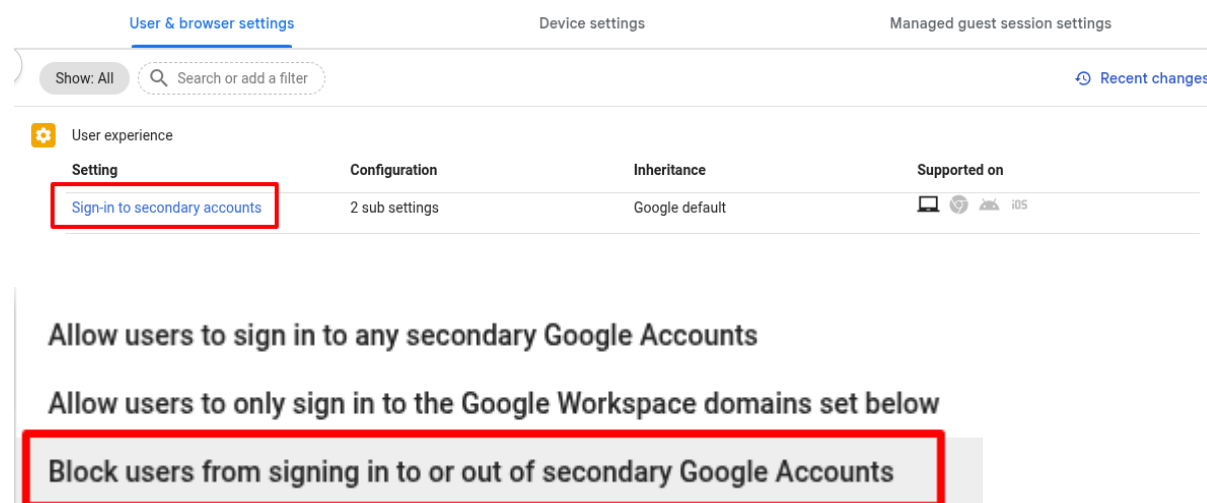
- Capture de bureau
- Bloquer les requêtes Web
- Requête Web

2. Empêcher la connexion avec des comptes extérieurs au domaine et en mode navigation privée :

Dans la console d'administration Google Workspace, développez le menu Appareils > Chrome > Paramètres et cliquez sur l'onglet « Paramètres des utilisateurs et des navigateurs ».

Une fois sur cet écran, sur le côté gauche de l'écran et sélectionnez l'unité organisationnelle au sein de laquelle vous souhaitez travailler.

Accédez à la section « Expérience utilisateur » et cliquez sur « Connexion aux comptes secondaires ». Sélectionnez ensuite l'option « Bloquer la connexion ou la déconnexion des utilisateurs aux comptes Google secondaires ». Pour appliquer les modifications, cliquez sur le bouton « Enregistrer » en haut à droite de l'écran.



The screenshot shows the 'User & browser settings' tab in the Google Workspace Admin console. Under the 'User experience' section, the 'Sign-in to secondary accounts' setting is highlighted with a red box. Below this, three options are listed: 'Allow users to sign in to any secondary Google Accounts', 'Allow users to only sign in to the Google Workspace domains set below', and 'Block users from signing in to or out of secondary Google Accounts'. The third option is also highlighted with a red box.

Setting	Configuration	Inheritance	Supported on
Sign-in to secondary accounts	2 sub settings	Google default	Android, iOS

Allow users to sign in to any secondary Google Accounts

Allow users to only sign in to the Google Workspace domains set below

Block users from signing in to or out of secondary Google Accounts

Sans quitter cet écran, dans la section « Gestion de Chrome pour les utilisateurs connectés », sélectionnez l'option « Appliquer toutes les stratégies utilisateur lorsque les utilisateurs se connectent à Chrome et fournir une expérience Chrome gérée ».

Chrome management for signed-in users

Setting	Configuration	Inheritance	Supported on
Chrome management for signed-in users	Apply all user policies when users sign into Chrome, and provide a managed Chrome experience	Inherited	   

Dans la section « Alimentation et arrêt », sélectionnez « Paramètres de veille » et, dans le paramètre « Verrouiller l'écran en cas de mise en veille ou de fermeture du couvercle », sélectionnez l'option « Verrouiller l'écran » :

Configuration	Action on lid close Sleep ▼
	Lock screen on sleep or lid close Lock screen ▼ Before Chrome 106, only sleep will trigger locking. In Chrome 106+, sleep or lid close will trigger locking.
	AC idle action Sleep ▼

Dans la section « Sécurité », cliquez sur le paramètre « Mode navigation privée » et sélectionnez l'option « Interdire le mode navigation privée » :

Security

Setting	Configuration	Inheritance	Supported on
Incognito mode	Disallow incognito mode	Locally applied	   

Sans quitter l'onglet PARAMÈTRES UTILISATEUR ET NAVIGATEUR où vous vous trouvez, accédez à la section « Expérience utilisateur » et, dans le paramètre « Accès par connexion multiple », sélectionnez l'option « Bloquer l'accès via plusieurs connexions pour les utilisateurs de cette organisation ».

User experience

Setting	Configuration	Inheritance	Supported on
Multiple sign-in access	Block multiple sign-in access for users in this organization	Locally applied	   

Déploiement de l'extension IMTLazarus dans Google Workspace et mesures de sécurité

Administrateurs IMTLazarus

3. Empêcher les utilisateurs de mettre fin aux processus avec le gestionnaire de tâches Chrome :

Sans quitter l'onglet PARAMÈTRES UTILISATEUR ET NAVIGATEUR, accédez à la section « Applications et extensions », sélectionnez l'option « Empêcher les utilisateurs de mettre fin aux processus avec le gestionnaire de tâches Chrome » et cliquez sur le bouton « Enregistrer » pour enregistrer les modifications.

 Apps and extensions 

Setting	Configuration	Inheritance	Supported on
Task manager	Block users from ending processes with the Chrome task manager	Locally applied	   iOS

4. Autorisations d'enregistrement des équipements :

Pour empêcher les utilisateurs de réinitialiser leurs appareils aux paramètres d'usine et ainsi désinstaller IMTLazarus et toute autre application, il est nécessaire d'activer l'enregistrement obligatoire des appareils. De cette façon, si une telle opération se produisait (une réinitialisation ou un « nettoyage » de l'appareil Chrome), l'utilisateur serait contraint de s'inscrire à la console d'administration pour pouvoir l'utiliser.

Pour ce faire, dans la console d'administration Google Workspace, dans le menu de gauche, développez le menu Appareils > Chrome > Paramètres et cliquez sur l'onglet Utilisateurs et navigateurs.

Une fois sur cet écran, sur le côté gauche de l'écran et Sélectionnez l'unité organisationnelle avec laquelle vous souhaitez travailler..

Dans l'onglet PARAMÈTRES UTILISATEUR ET NAVIGATEUR, accédez à la section « Contrôles d'inscription » et cliquez sur le paramètre « Autorisations d'inscription » pour le définir sur « Ne pas autoriser les utilisateurs de cette

Déploiement de l'extension IMTLazarus dans Google Workspace et mesures de sécurité

Administrateurs IMTLazarus

organisation à inscrire de nouveaux appareils ou à réinscrire des appareils existants ».

Cliquez sur le bouton « Enregistrer » pour sauvegarder les modifications.

Sans quitter l'écran, accédez à l'onglet PARAMÈTRES DE L'APPAREIL, puis à la section « Inscription et accès » et cochez les options suivantes :

- Réinscription forcée : forcer l'appareil à se réinscrire avec les informations d'identification de l'utilisateur après effacement.
- Nettoyage haute pression : Ne pas autoriser le déclenchement du nettoyage haute pression.



Enrollment and access

Setting	Configuration	Inheritance	Supported on
Forced re-enrollment	Force device to re-enroll with user credentials after wiping	Locally applied	   iOS
Asset identifier input after zero touch enrollment	Do not allow asset ID and location to be entered for devices enrolled via zero touch enrollment	Google default	   iOS
Powerwash	Do not allow powerwash to be triggered	Locally applied	   iOS

Ainsi, si un utilisateur effectue une réinitialisation d'usine, il devra retourner l'appareil aux administrateurs informatiques afin que ceux-ci puissent le réinscrire manuellement avec un compte d'administrateur.

5. Empêcher la connexion en tant qu'invité :

Dans la même fenêtre, cliquez sur l'onglet PARAMÈTRES DE L'APPAREIL, puis accédez à la section « Paramètres de connexion », puis, dans le paramètre « Mode invité », sélectionnez l'option « Désactiver le mode invité » et cliquez sur le bouton Enregistrer en bas de l'écran pour enregistrer les modifications.



Sign-in settings ⓘ

Setting	Configuration	Inheritance	Supported on
Guest mode	Disable guest mode	Locally applied	   iOS

6. Empêcher le mode développeur :

Dans la console d'administration Google Workspace, dans le menu de gauche, développez le menu Appareils > Chrome > Paramètres et cliquez sur Utilisateurs et navigateurs.

Une fois sur cet écran, sur le côté gauche de l'écran et Sélectionnez l'unité organisationnelle avec laquelle vous souhaitez travailler.

Accédez à la section « Expérience utilisateur » et, dans le paramètre « Outils de développement », configurez l'option « Disponibilité des outils de développement » sur « Ne jamais autoriser l'utilisation des outils de développement intégrés » et l'option « Mode développeur de la page des extensions » sur « Ne pas autoriser l'utilisation des outils de développement sur la page des extensions » :

Configuration

Developer tools availability

Never allow use of built-in developer tools

Extensions page developer mode

Do not allow use of developer tools on extensions page ▼

7. Désactiver l'exécution de JavaScript dans la barre d'outils du navigateur :

Pour empêcher les étudiants d'utiliser du code JavaScript pour tenter de contourner la sécurité, nous devons ajouter une configuration supplémentaire.

Dans la console d'administration Google Workspace, dans le menu de gauche, développez le menu Appareils > Chrome > Paramètres et cliquez sur l'onglet Utilisateurs et navigateurs. Sélectionnez l'unité organisationnelle à laquelle vous souhaitez appliquer la restriction.

Accédez à la section « Contenu » et cliquez sur le paramètre « Blocage d'URL ». Dans la section de configuration, ajoutez « javascript://* » (sans les guillemets) dans le champ « URL bloquées ».

Configuration

Blocked URLs
javascript://*

Maximum of 1000 URLs in blocklist. Put each URL on its own line. For example
example.org
https://example.com

N'oubliez pas de cliquer sur le bouton Enregistrer pour enregistrer les modifications.

8. Configurez la géolocalisation dans Google Workspace :

Pour activer la géolocalisation des appareils, vous devez configurer le paramètre suivant dans la console d'administration Google Workspace. Dans le menu de gauche, développez « Appareils » > « Chrome » > « Paramètres » et cliquez sur l'onglet « Utilisateurs et navigateurs ». Sélectionnez ensuite l'unité organisationnelle concernée.

Dans la section Sécurité, cliquez sur le paramètre « Géolocalisation » et sélectionnez l'option « Autoriser les sites à détecter la géolocalisation des utilisateurs ».



Security

Setting

Configuration

Geolocation

Allow sites to detect users' geolocation

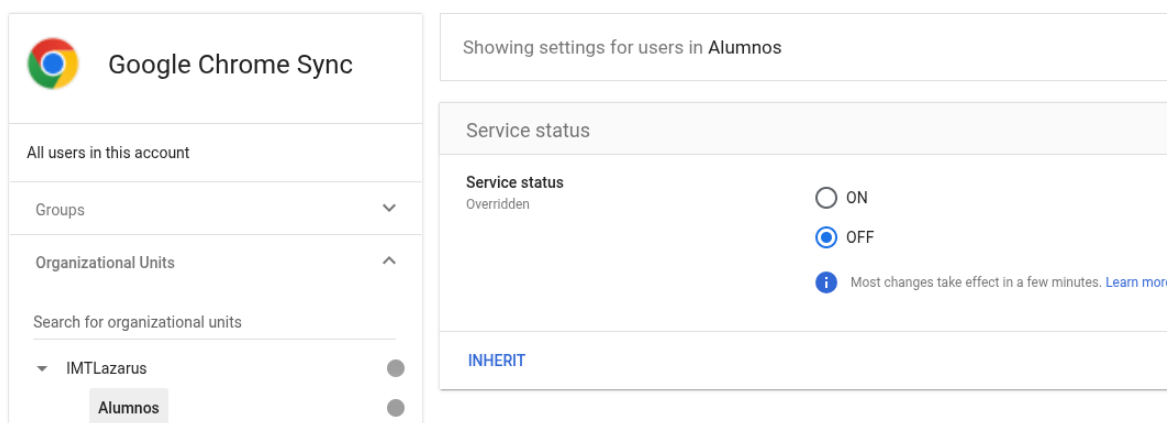
Enfin, cliquez sur le bouton « Enregistrer » pour enregistrer les modifications.

9. Désactiver la synchronisation Chrome :

Pour empêcher les étudiants de désactiver l'extension, nous devons désactiver la synchronisation Chrome depuis la console.

Dans le menu de gauche, développez Applications > Services Google supplémentaires > Paramètres de synchronisation Google Chrome. Sélectionnez l'unité organisationnelle à laquelle vous souhaitez appliquer les paramètres et choisissez l'option « État du service ».et réglez-le sur « OFF ».

Apps > Additional Google services > Settings for Google Chrome Sync > Service Status



The screenshot shows the 'Service Status' page for Google Chrome Sync. On the left, the 'Organizational Units' list is expanded, showing 'IMTLazarus' and 'Alumnos'. The main content area shows the 'Service status' for 'Alumnos' is set to 'OFF'. Below this, there is an 'INHERIT' link.