Documentation

GPO - Blocage des gestionnaire de mot de passe.docx

1. Définition de l'environnement

1.1. Environnement

1.1.1. 1er machine - Serveur

Cette machine fonctionne sur Windows Server 2022 avec les services : Active Directory Domain Services, DNS, DHCP. Un ordinateur est relié (console) au domaine et un utilisateur avec un rôle « Administrateur du domaine ».

1.1.1. 2nd machine - Console

Cette machine, fonctionnant sur Windows 11 va me servir pour la batterie de vérification, elle est reliée au domaine du serveur (gpotest.local). Les logiciels Google Chrome, Mozilla Firefox et Microsoft Edge sont installés.

2. Configuration

2.1. Téléchargement des ADMX/ADML

Le fichier **ADMX** est un fichier **XML** qui définit la **structure technique** des paramètres de stratégie de groupe. Il spécifie les clés de Registre impactées, les types de données et les valeurs possibles, mais sans les descriptions textuelles spécifiques à une langue. Il remplace l'ancien format. Tandis que le fichier **ADML** est un fichier **XML** qui contient les **ressources linguistiques** (textes, descriptions, noms affichables) associées à un fichier ADMX. Chaque fichier ADML est spécifique à une langue (par exemple, fr-FR pour le français) et permet à l'Éditeur de stratégie de groupe d'afficher les informations dans la langue de l'administrateur.

2.1.1. Mozilla Firefox

La fondation Mozilla a pris le choix d’héberger ses ADMX sur le site GitHub, permettant un accès et un visuel simple sur la fonctionnalité de ce modèle d’administration. Voici le lien permettant d’accéder au dépôt.

> https://github.com/mozilla/policy-templates/releases

Il suffira de cliquer sur « policy_templates_vX.X.zip », (soit X le numéro de version de ce modèle), afin de télécharger le fichier.

2.1.2. Google Chrome

De son côté Google a pris le choix de l'héberger sur ses propres serveurs, il faudra donc se rendre sur ce lien :

> “ https://www.chromium.org/administrators/policy-templates/

Puis de cliquer sur la mention « ZIP file of ADM/ADMX/JSON templates and documentation », afin de télécharger le fichier « policy_templates.zip ».

2.1.3. Microsoft Edge

Enfin pour Microsoft Edge le modèle d'administration est trouvable sur ce lien :

> “ https://www.microsoft.com/fr-fr/edge/business/download?cs=3457492030&form=MA13FJ

Sous la mention « Téléchargement » des trois cartes avec pour titre, l'architecture du processeur présent dans les ordinateurs. La mention « Télécharger la politique de Windows 64 bits » figure en cliquant dessus, il suffira de choisir « Accepter et télécharger » afin d'obtenir le modèle d'administration, du navigateur Edge.

2.2. Mise en place des ADMX

2.2.1. Mozilla Firefox

Pour ce navigateur, il faudra se rendre dans l'archive, choisir le système d'exploitation où l'on souhaite établir des politiques, dans mon cas Windows, puis glisser le fichier « firefox.admx » et « mozilla.admx » dans le dossier :

> “ C:\Windows\SYSVOL\sysvol\domain.local\Policies**PolicyDefinitions**

Bien remplacer « domain.local » par le domaine de l'Active Directory.

Ensuite, il faudra glisser le dossier correspondant à la langue au même endroit dans mon cas j'ai glissé le dossier « fr-FR ».

2.2.2. Google Chrome

Pour Google Chrome cela diffère au niveau de l'architecture des dossiers présents dans l'archive, il faudra se rendre dans le dossier « windows » pour configurer les machines fonctionnant sous le système d'exploitation de Microsoft, puis dans « admx » pour enfin faire la même manipulation que précédemment. Glissez les fichiers « chrome.admx » et « google.admx », dans le dossier « PolicyDefinitions ». De même pour le dossier « fr-FR » qui contient désormais les « ADML » de Firefox ainsi que de Google Chrome.

2.2.3. Microsoft Edge

Microsoft Edge, est non pas livrer avec un modèle d'administration sous le format .zip mais sous le format .cab, qui est une extension signifiant que le fichier est compressé et contient des données liées à des installations comme des pilotes de périphériques ou des fichiers système. Sur le système Windows cette extension est automatiquement reconnue.

Double-cliquez, sur le fichier.cab afin d'accéder à un fichier nommer « MicrosoftEdgePolicyTemplates » extraire vers un dossier où l'on pourra le retrouver facilement afin de faire une seconde extraction.

Désormais, ouvrez le fichier précédemment extrait, même chose que les derniers navigateurs un dossier « windows » est présent, en y accédant on remarque un dossier « admx », glissez « msedge.admx », « msedgeupdate.admx » et « msedgewebview2.admx » dans le répertoire :

> C:\Windows\SYSVOL\sysvol\domain.local\Policies**PolicyDefinitions**

Bien remplacer « domain.local » par le domaine de l'Active Directory.

Glissez ensuite le dossier « fr-FR » dans le même emplacement.

2.3. Définition des stratégies

2.3.1. Mozilla Firefox

Titre	Etat
Ne pas autoriser la révélation des mots de passe dans les connexions enregistrées	Activé
Désactiver Pocket	Activé
Désactiver l'importation de profil	Activé
Exceptions du gestionnaire de mots de passe	Activé

Activer le remplissage automatique des méthodes de paiement	Désactivé
Proposer d’enregistrer les identifiants	Désactivé
Proposer d’enregistrer les identifiants (par défaut)	Désactivé
Gestionnaire de mots de passe	Désactivé

Ne pas oublier de glisser la GPO sous le nom de domaine de l’AD, et d’appliqué la stratégie de groupe.

2.3.2. Google Chrome

Titre	Etat	Contenu
Liste des types à exclure de la synchronisation	Activé	• passwords • payments
Importer les mots de passes enregistrés du navigateur par défaut à la première exécution	Désactivé	

Titre (Règles trouvable dans « Gestionnaire de mots de passe »)	Etat
Activer la suppression des mots de passe indéchiffrables	Activé
Activer l’enregistrement des mots de passe dans le gestionnaire de mots de passe	Désactivé
Activer l’enregistrement des clés d’accès dans le gestionnaire de mots de passe	Désactivé
Activer le partage des identifiants de l’utilisateur avec d’autres utilisateurs	Désactivé

2.3.3. Microsoft Edge

Titre	Etat	Contenu
Configuration de la liste des types exclus de la synchronisation	Activé	• passwords • edgeWallet
Importer automatiquement les données et les paramètres d’un autre navigateur lors de la première exécution	Désactivé	
Activer le remplissage automatique pour les instruments de paiement	Désactivé	
Autoriser l’importation des mots de passe enregistrés	Désactivé	

Titre (Règles trouvable dans « Gestionnaire de mots de passe et protection »)	Etat
Activer l’exportation des mots de passe enregistrés à partir du gestionnaire de mots de passe	Désactivé
Autoriser les utilisateurs à obtenir une suggestion de mot de passe fort chaque fois qu’ils créent un compte en ligne	Désactivé
Activer l’enregistrement des mots de passe pour le Gestionnaire de mot de passe	Désactivé

Ne pas oublier de glisser la GPO sous le nom de domaine de l’AD, et d’appliqué la stratégie de groupe.

2.4. Vérification

Pour la vérification, je vais me servir de ma console sous Windows 11. Embarquant déjà les navigateurs configurés par GPO.

Si la machine était déjà allumée il serait nécessaire de faire cette commande dans le terminal :

> gpupdate /force

Afin de forcer l’actualisation des stratégies de groupe de l’utilisateur connecté sur l’ordinateur console.

Du coté de Firefox une fois Pocket désactivé cela ne permet plus de synchronisation de données de compte Mozilla et bloque donc la synchronisation de mot de passe. De plus, une page s’affiche montrant l’inaccessibilité du gestionnaire de mot de passe.

image.png

Pour Google Chrome comme pour Edge, une fois, la liste d’exclusion établit les mots de passe et les coordonnées bancaires ne sont plus synchronisées. De plus, il n’est pas possible d’enregistrer deux mots de passe, mais ceux déjà présent au sein du navigateur resteront sauf si dans un futur le fichier SQLite contenant les mots de passe est supprimé via un script lors du démarrage.

Une image contenant texte, capture d’écran Le contenu généré par l’IA peut être incorrect.

image.png

Revision #3
Created 2026-09-23 09:05:25 UTC by Eythan
Updated 2026-09-23 10:06:25 UTC by Eythan