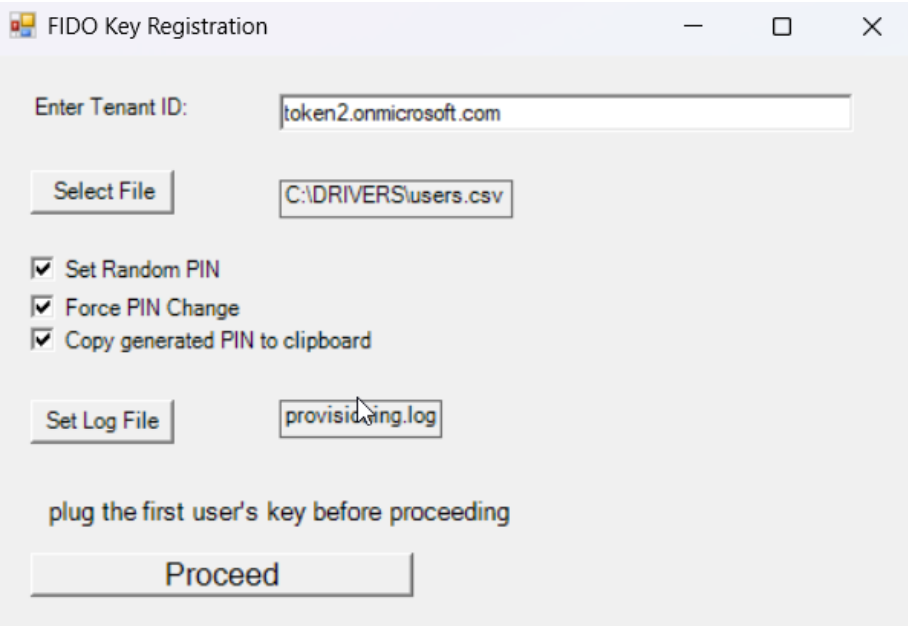
Enregistrement automatisé des clés FIDO2 pour Entra ID – Solution PowerShell

Vue d'ensemble

Cet outil permet d'enregistrer des clés de sécurité FIDO2 pour plusieurs utilisateurs en traitant leurs informations à partir d'un fichier CSV. Il prend en charge la définition de PINs aléatoires, la gestion des clés et l'enregistrement des opérations. Le script est créé en PowerShell et repose sur le module DSInternals.Passkey, qui exploite les nouvelles API de provisionnement FIDO2 au sein de Microsoft Entra ID. L'outil offre une interface graphique pour une interaction conviviale.

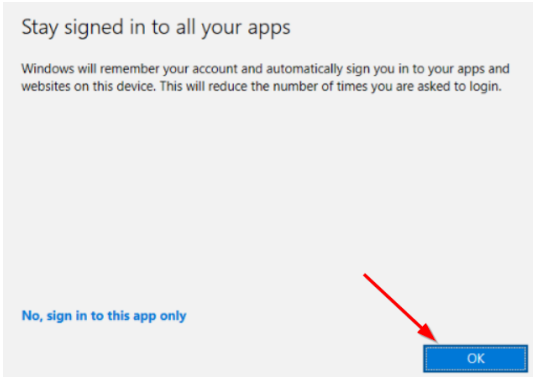


Prérequis

En raison d'un léger problème avec l'API Graph, ce script peut échouer si l'utilisateur cible dispose déjà d'une clé FIDO2 enregistrée. L'objectif principal de cette solution est d'activer en masse les clés pour les utilisateurs qui n'ont pas encore de clé FIDO2.

- **Matériel requis** : La solution fonctionne avec toute clé FIDO2.1 compatible, mais certaines fonctionnalités sont spécifiques à certaines révisions. La définition des PINs et l'obligation de changement de PIN ne sont disponibles que pour les clés avec un firmware FIDO2.1 Final, et les numéros de série des clés sont disponibles uniquement avec la série PIN+.
- **Logiciel requis** : PowerShell 5.1 ou version ultérieure, module Microsoft.Graph et module DSInternals.PassKeys. Le script installera automatiquement les modules requis.
- **Fichiers requis** :
    - read_serial_t2.exe : Utilitaire pour lire le numéro de série des clés FIDO.

    - fido2-manage.exe : Outil pour gérer les clés FIDO2.
      (les deux sont inclus dans l'archive avec le script PowerShell)
- **Fichier d'entrée** : Un fichier CSV avec une colonne nommée UPN (User Principal Name).
- **Autorisations** : Le script doit être exécuté en tant qu'administrateur (en raison des limitations de l'API native FIDO2 de Windows). Le compte Entra doit disposer des autorisations appropriées pour l'API Graph (UserAuthenticationMethod.ReadWrite.All).
- **Compte Entra avec autorisations appropriées** :
    - Un compte disposant des autorisations appropriées pour lancer l'API Graph est nécessaire.
    - Si le compte à utiliser est protégé par FIDO2/Passkey, la fenêtre PowerShell ne peut pas être utilisée pour se connecter.
    - Connectez-vous plutôt à une application (par exemple, MS Teams, même si le compte n'est pas sous licence pour celle-ci) avec Passkey.
    - Choisissez « Se connecter à toutes vos applications » (au lieu de « Se connecter uniquement à cette application »).



    - Cette action ajoutera le compte à la liste des identifiants connectés, vous permettant de simplement choisir un compte connecté lorsqu'il vous est demandé.

Fonctionnalités

- Définir des PINs aléatoires ou personnalisés pour les clés FIDO2.
- Forcer le changement de PIN après le provisionnement (si activé, les utilisateurs devront définir un nouveau PIN lors de la première utilisation).
- Copier automatiquement les PINs générés dans le presse-papiers.
- Enregistrer les résultats dans un fichier spécifié.
- Gérer les erreurs de manière conviviale avec des invites visuelles.

Utilisation de l'outil

1. **Lancer l'outil**

Exécutez le script PowerShell (EnrollFIDO2.ps1). Une interface graphique apparaîtra. Assurez-vous que votre stratégie d'exécution PowerShell autorise l'exécution de scripts. Si nécessaire, exécutez Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted ou une commande similaire avant d'exécuter le script.

2. **Configurer l'ID du locataire**

Entrez l'ID du locataire (par exemple, tenantname.onmicrosoft.com) dans le champ de saisie. Cette valeur sera mémorisée pour la prochaine exécution.

3. **Sélectionner le fichier CSV d'entrée**

Cliquez sur le bouton « Sélectionner le fichier » et choisissez un fichier CSV valide contenant les UPNs des utilisateurs. Exemple de format du fichier :

```
UPN
user1@token2.swiss
user2@token2.swiss
```

4. **Configurer les options de PIN**

   - Définir un PIN aléatoire : Cochez cette case pour générer un PIN aléatoire à 6 chiffres pour chaque clé.
   - Copier le PIN dans le presse-papiers : Cochez cette case pour copier automatiquement chaque PIN généré dans le presse-papiers.
   - Forcer le changement de PIN : Cochez cette case pour imposer un changement de PIN sur la clé.

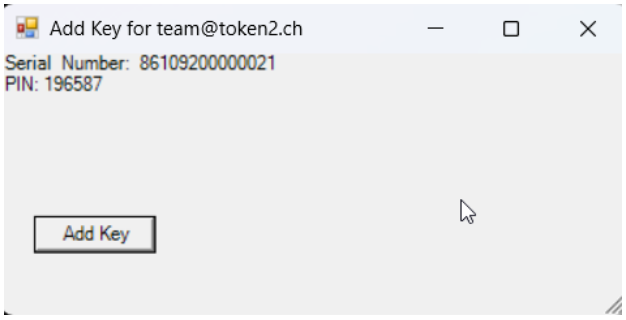
5. **Définir le chemin du fichier journal**

Cliquez sur le bouton « Définir le fichier journal » pour choisir où enregistrer les journaux des opérations.

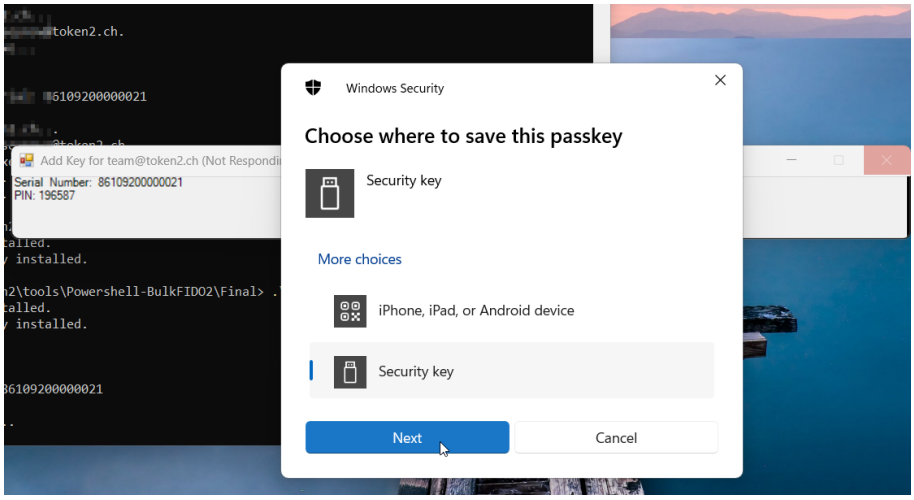
6. **Procéder à l'enregistrement**

Cliquez sur le bouton « Procéder » pour démarrer le processus d'enregistrement. L'outil effectuera les opérations suivantes pour chaque utilisateur :

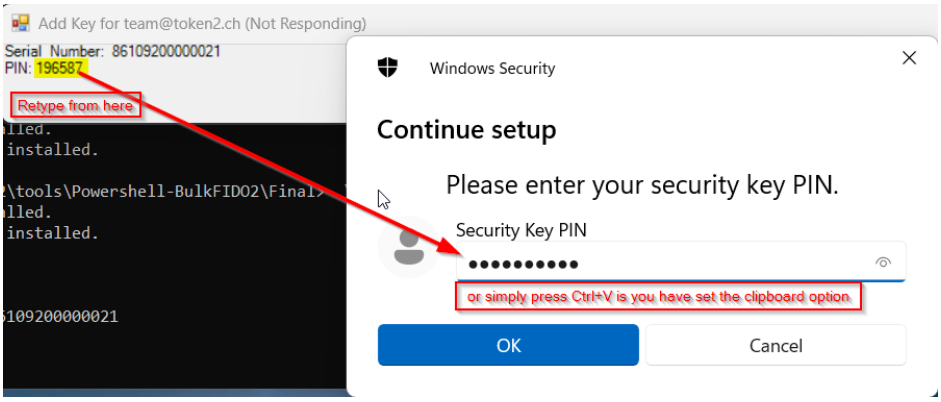
   - Lit le numéro de série de la clé FIDO.
   - Définit éventuellement un PIN aléatoire.
   - Affiche une fenêtre de dialogue avec les informations ci-dessus pour vérification. Si tout est correct, cliquez sur « Ajouter la clé » pour poursuivre.



- En cliquant sur "Ajouter la clé", la clé FIDO est enregistrée pour l'utilisateur via l'API Graph. Cette étape repose sur les boîtes de dialogue natives de création de passkey FIDO du système d'exploitation Windows et ne peut pas être entièrement automatisée.



Pour faciliter l'approvisionnement, le script peut copier chaque nouveau code PIN dans le presse-papiers, ce qui vous permet d'utiliser Ctrl+V dans la fenêtre concernée. Le code PIN sera également affiché dans une fenêtre redimensionnée afin d'éviter qu'il ne soit masqué par la boîte de dialogue native.



Enregistre les résultats dans le fichier spécifié. Remarque : si vous avez sélectionné l'option de code PIN aléatoire, il se peut que vous deviez consulter ce fichier journal ultérieurement pour communiquer le code PIN à l'utilisateur final

Invites interactives

Après le traitement de chaque utilisateur, l'outil affiche une invite :

« Préparez la clé suivante et cliquez sur OK pour continuer. »

Insérez la clé suivante et cliquez sur OK pour poursuivre. Si le dernier utilisateur est atteint, l'outil se termine sans invites supplémentaires.

Gestion des erreurs

- **ID du locataire manquant** : Affiche une erreur si l'ID du locataire n'est pas fourni.
- **CSV invalide** : Invite l'utilisateur à sélectionner un fichier CSV valide si le fichier sélectionné est manquant ou invalide.
- **Erreurs de lecture de la clé** : Alerte l'utilisateur si aucun numéro de série valide n'est détecté.
- **Erreurs de provisionnement** : Fournit des messages d'erreur détaillés si un problème survient lors de l'enregistrement de la clé.

Journaux

L'outil crée ou ajoute à un fichier journal avec les détails suivants pour chaque utilisateur :

- UPN (User Principal Name)
- Numéro de série de la clé FIDO
- PIN (si défini)
- Statut du changement forcé de PIN

Exemple de contenu du fichier journal généré par l'outil (notez que le format est toujours CSV ; nous avons simplement changé l'extension en .log pour le différencier du fichier de la liste des utilisateurs, qui sera attendu en .csv) :

```
UPN,Numéro de série,PIN,ForcePINChange
user1@token2.ch,86109200000021,142375,True
user2@token2.ch,86109400000020,497210,True
```

Important : Si vous avez sélectionné l'option de PIN aléatoire, vous devrez peut-être vous référer à ce fichier journal plus tard pour communiquer le PIN à l'utilisateur final. Ce fichier journal est le seul endroit où les PINs aléatoires sont stockés, donc manipulez-le avec soin.

Dépannage

- **Aucun numéro de série détecté** : Assurez-vous que la clé FIDO est correctement connectée et réessayez l'opération. Seules les clés de la série PIN+ disposent de l'API pour lire le numéro de série.

- **Erreur de connexion à l'API Graph** : Vérifiez l'ID du locataire fourni et assurez-vous que vos autorisations API Graph sont appropriées.
- **L'outil ne se lance pas** : Assurez-vous que les modules requis sont installés et exécutez le script avec les autorisations appropriées.

Fonctionnalités avancées

- **Complexité du PIN** : Les PINs aléatoires évitent les numéros séquentiels, les chiffres répétés ou les palindromes.
- **Intégration du presse-papiers** : Copie automatiquement les PINs pour une utilisation rapide.

Démo

La vidéo ci-dessous démontre l'outil en action, montrant le processus et la rapidité. L'enregistrement de 4 clés pour 4 utilisateurs a pris environ 2 minutes.

https://youtu.be/jGwds-du-5Y

Support

Si vous rencontrez des problèmes ou avez besoin d'aide, contactez-nous avec les informations suivantes :

- Messages d'erreur affichés lors de l'opération.
- Une copie du fichier journal généré pour analyse.

Téléchargement

Vous pouvez télécharger l'outil d'enregistrement des clés FIDO2 pour Microsoft Entra ID depuis notre dépôt GitHub. Le dépôt contient tous les scripts, exécutables et la documentation nécessaires pour commencer.

https://github.com/token2/fido2_bulkenroll_entraid