Tokens Matériels Classiques pour Entra ID MFA – Méthode Graph API avec Self-Service et Support des Tokens SHA-256

Pour renforcer la sécurité et simplifier l'administration, Microsoft a introduit la politique d'authentification pour Microsoft Entra ID. Cette politique permet aux administrateurs de gérer les paramètres d'authentification multi-facteurs (MFA) et de réinitialisation de mot de passe en libre-service (SSPR) depuis un emplacement unique, améliorant ainsi l'expérience utilisateur. Avec la migration désormais terminée, examinons les principales améliorations apportées à cette politique.

D'après la documentation Microsoft, la fonctionnalité « Hardware OATH Tokens (Preview) » a reçu plusieurs mises à jour importantes, notamment :

Suppression de l'exigence d'administrateur global.

Les utilisateurs finaux peuvent désormais s'attribuer et activer eux-mêmes des tokens directement depuis leur page « Informations de sécurité ».

Support des tokens SHA-256, annoncé précédemment mais désormais pleinement implémenté.

De plus, Microsoft Entra ID dispose maintenant d'une nouvelle API Microsoft Graph (en préversion) pour gérer les tokens dans Azure. Les administrateurs peuvent utiliser l'API Graph avec des rôles de moindre privilège pour gérer les tokens dans cette préversion. Cependant, il n'existe pas d'option pour gérer les tokens matériels OATH directement via le centre d'administration Entra dans cette version. La gestion se fait exclusivement via les API Graph. Les tokens ajoutés via Graph apparaîtront aux côtés des autres dans le centre d'administration, mais ne pourront être gérés que via les API.

Dans cet article, nous allons démontrer comment les administrateurs peuvent utiliser le nouveau dépôt de tokens matériels pour permettre aux utilisateurs de s'auto-attribuer un token matériel à leur compte via la page « Informations de sécurité ».

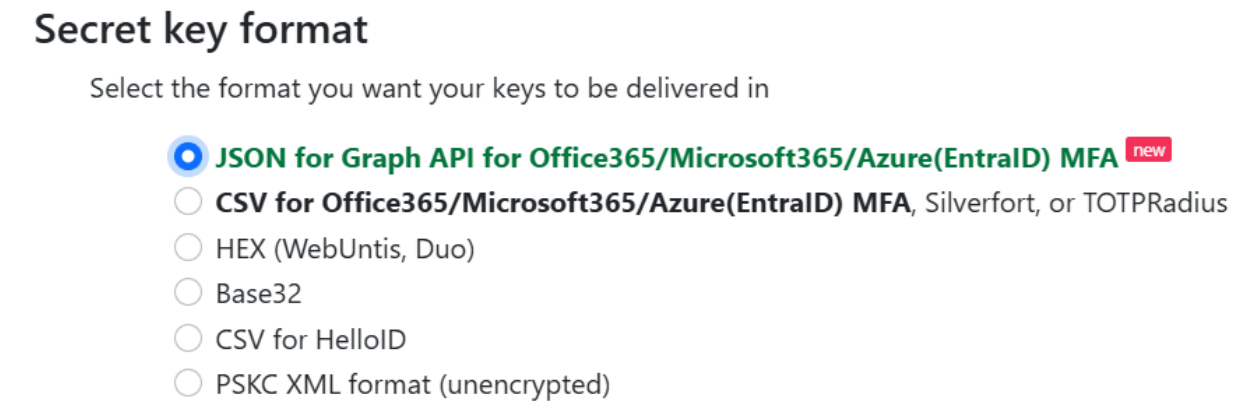
Prérequis

Voici ce qu'il faut pour effectuer cette configuration :

Une licence Microsoft Entra ID Premium P1 ou P2

Un ou plusieurs tokens matériels TOTP Token2. Cette méthode prend en charge les modèles SHA-1 et SHA-256.

Un fichier JSON pour vos tokens. Vous pouvez demander ce fichier depuis la page de commande après livraison (option actuelle, comme illustré ci-dessous).



N'oubliez pas d'envoyer votre clé publique GPG/PGP lors de la demande de fichier JSON pour garantir la sécurité de la transmission des données sensibles (la plupart des emails étant encore non sécurisés).

Alternativement, vous pouvez convertir vos anciens fichiers CSV en format JSON à l'aide de ce script.

Activer les Tokens OATH matériels dans la politique d'authentification

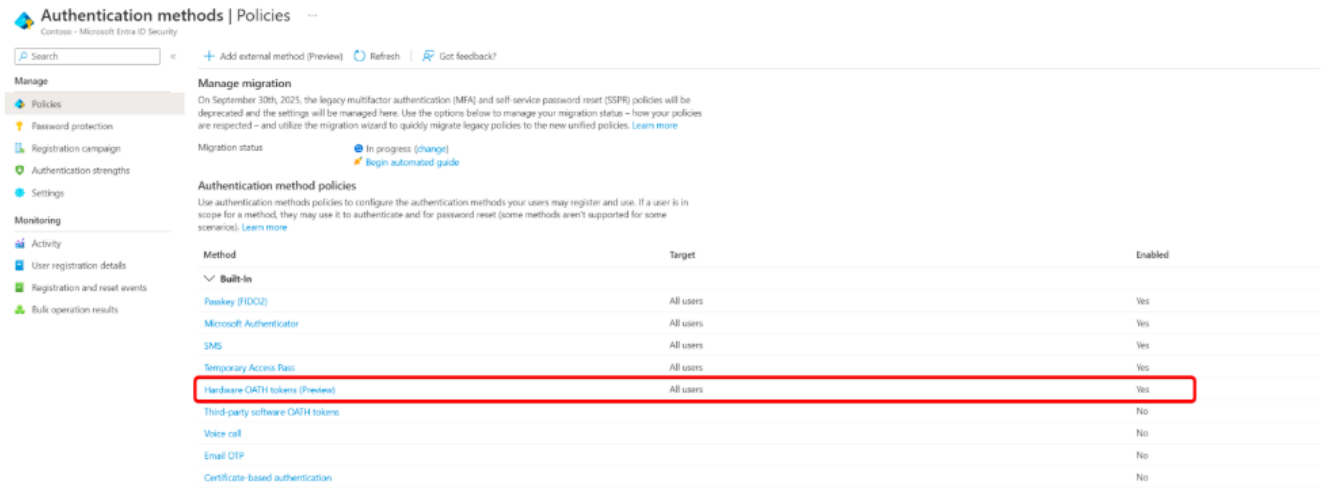
Assurez-vous d'abord que les tokens matériels sont activés pour votre locataire. L'emplacement de configuration peut varier selon que vous avez migré ou non vers la nouvelle politique d'authentification. En supposant que la migration est faite, vérifiez que la méthode est activée pour tous les utilisateurs ou pour un groupe spécifique.

Étapes :

Connectez-vous au centre d'administration Microsoft Entra avec des droits d'administrateur de la politique d'authentification.

Allez dans **Sécurité** > **Méthodes d'authentification** > **Tokens OATH** matériels (Preview).

Activez la méthode, sélectionnez les groupes d'utilisateurs, puis cliquez sur « **Enregistrer** ».



Obtenir le Fichier JSON

Microsoft Entra ID supporte les tokens OATH-TOTP (SHA-1 et SHA-256) qui se régénèrent toutes les 30 ou 60 secondes. Les clients peuvent acheter ces tokens auprès de Token2. Le fichier JSON contient des données telles que :

Le champ « HashFunction » avec la valeur "hmacsha1" (SHA-1) ou "hmacsha256" (SHA-256), selon le modèle du token. L'algorithme est renseigné automatiquement.

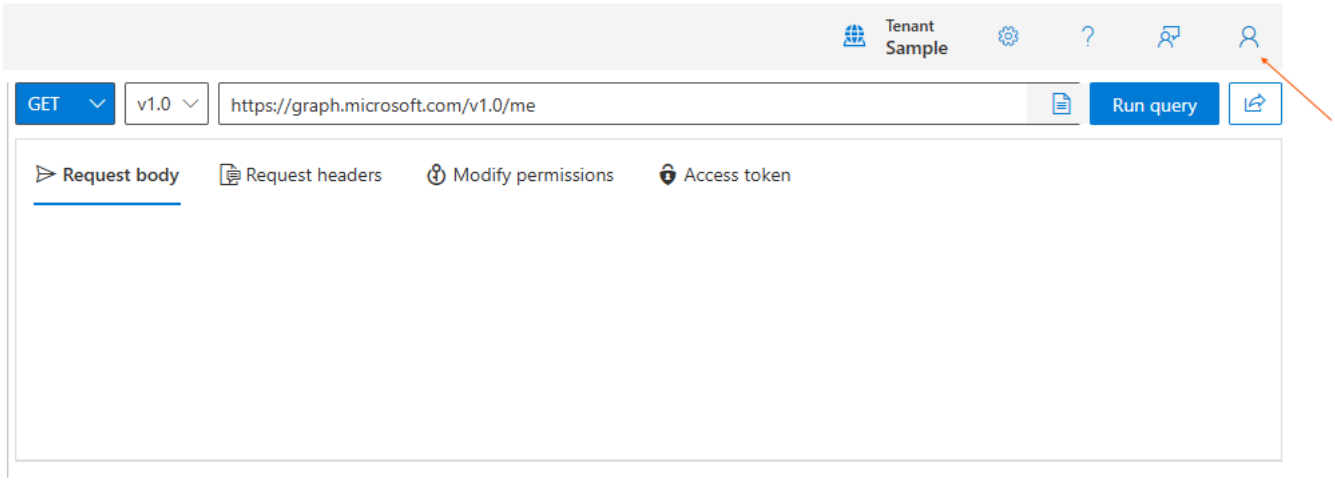
```json
{
    "@context": "#$delta",
    "value": [
        {
            "@contentId": "1",
            "serialNumber": "*************",
            "manufacturer": "Token2",
            "model": "C202",
            "secretKey": "********************************",
            "timeIntervalInSeconds": 30,
            "hashFunction": "hmacsha1"
        }
    ]
}
```

Ajouter de Nouveaux Tokens au Locataire

Nous allons maintenant ajouter les tokens au locataire pour les rendre disponibles en self-service. Ils ne seront pas attribués directement à un utilisateur, mais ajoutés au dépôt public du locataire. Pour cela, nous utiliserons Graph Explorer.

Graph Explorer est un outil interactif idéal pour tester les requêtes de l'API Microsoft Graph sans configuration préalable. Pour des intégrations avancées, vous pouvez enregistrer une application dans Entra ID, obtenir des access tokens et utiliser des permissions spécifiques (ex. : Policy.ReadWrite.AuthenticationMethod). Par exemple, nous avons développé un portail PHP illustrant la gestion des tokens avec cette API.

Accédez à Graph Explorer : https://developer.microsoft.com/en-us/graph/graph-explorer



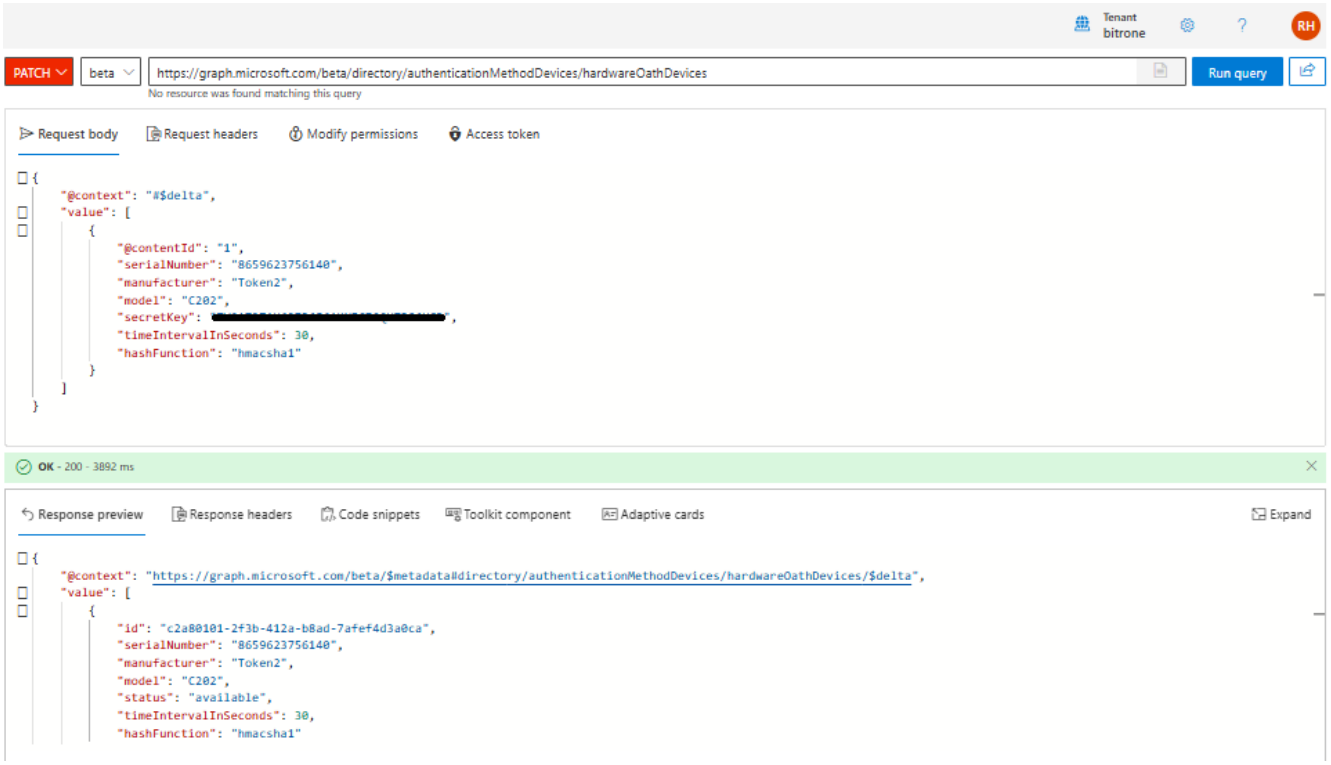
Connectez-vous avec vos identifiants.

Accordez l'autorisation « Policy.ReadWrite.AuthenticationMethod » dans l'onglet « Modify permissions ».

Pour uploader des tokens, utilisez la méthode PATCH avec les données du fichier JSON à l'adresse suivante :
https://graph.microsoft.com/beta/directory/authenticationMethodDevices/hardwareOathDevices

Ouvrez le fichier JSON, copiez le contenu et collez-le dans le champ « Request body » de Graph Explorer.

Cliquez sur « Run query ».



Le token sera disponible immédiatement en self-service. Vous pouvez vérifier le dépôt courant avec cette requête :

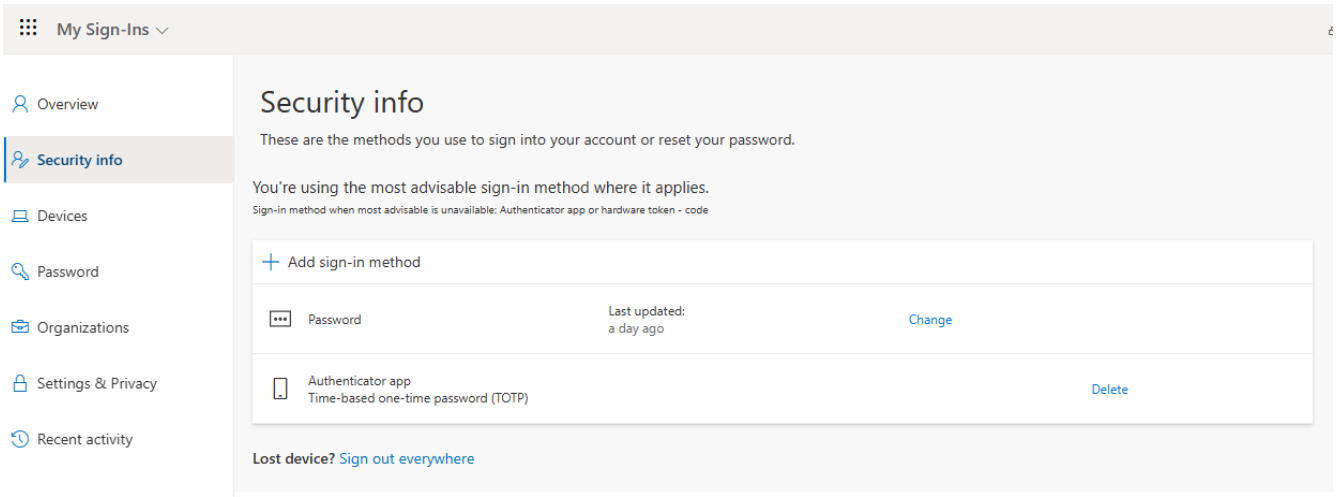
GET https://graph.microsoft.com/beta/directory/authenticationMethodDevices/hardwareOathDevices

Pour l'utilisateur final, le processus est simple. Les instructions suivantes (jusqu'à la section « Conclusion des instructions utilisateur ») décrivent la procédure d'enrôlement en self-service. Cette section peut être copiée pour être incluse dans la documentation utilisateur. Vous pouvez aussi télécharger en format PDF

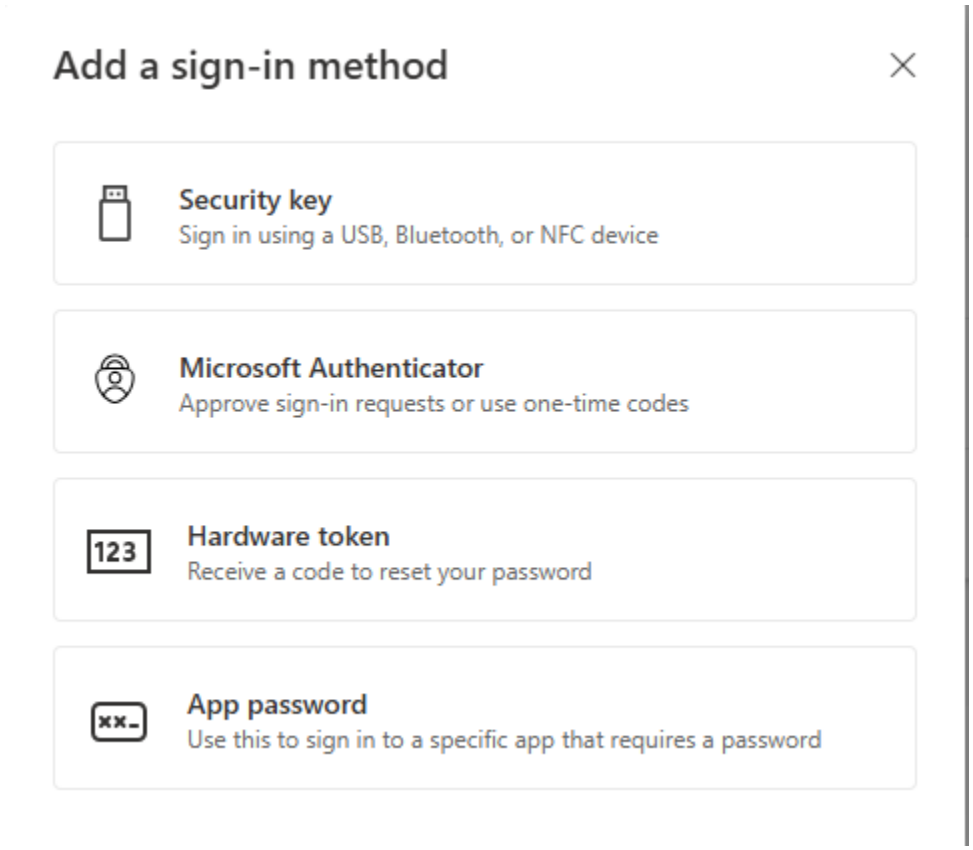
Procédure D'enregistrement Token Utilisateur

Depuis la page « Informations de sécurité », l'utilisateur :

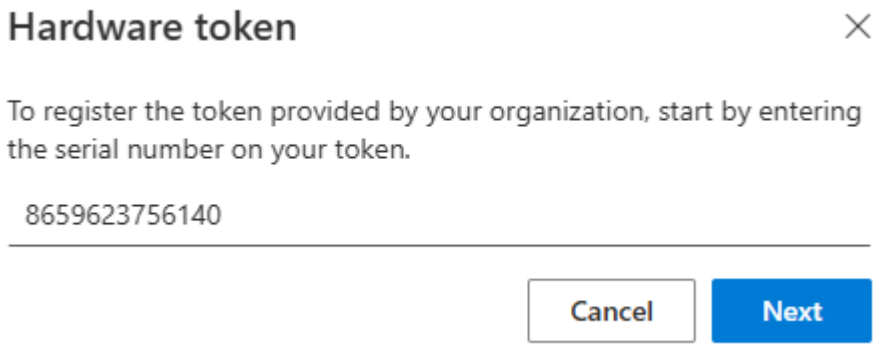
Clique sur « Ajouter une méthode de connexion ».



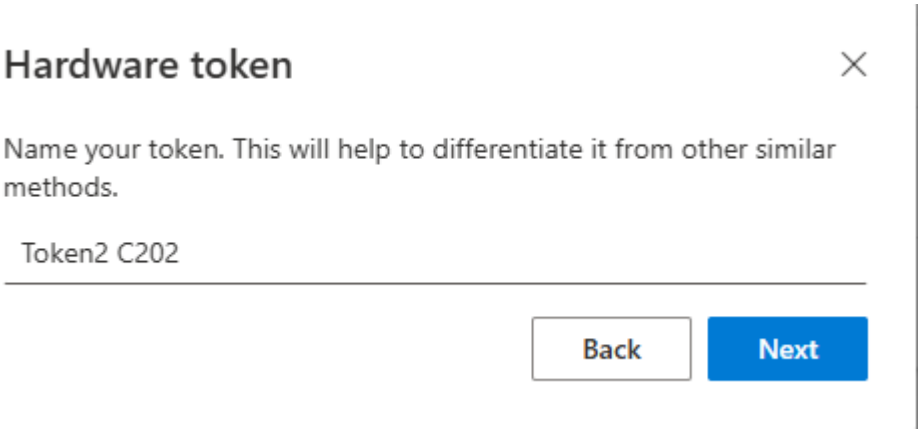
Choisit « Token matériel » comme méthode.



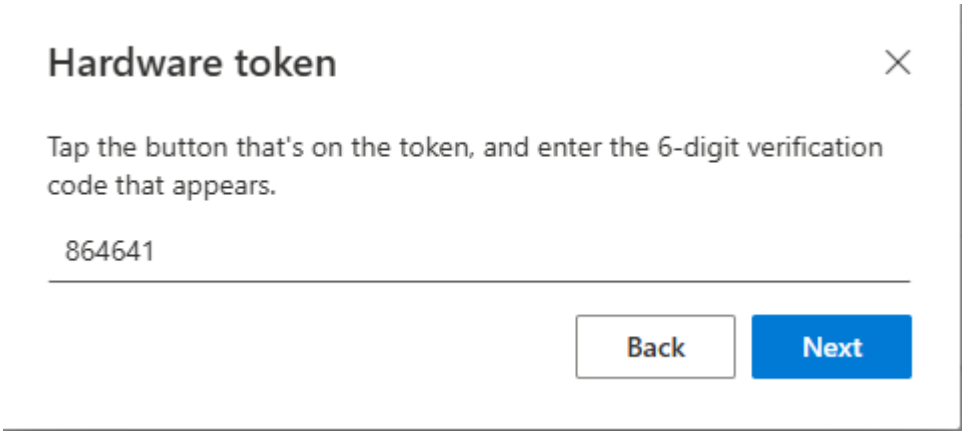
Saisit le numéro de série (au dos du token).



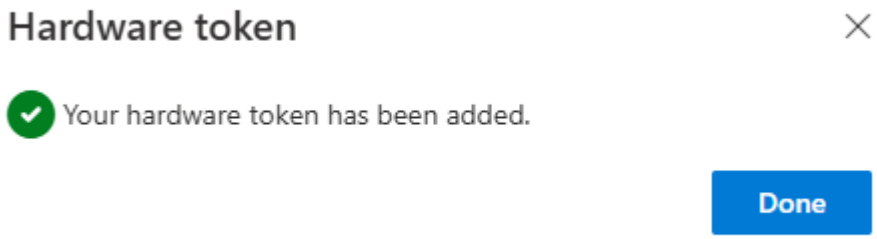
Nommez le token.



Entre un code OTP à 6 chiffres généré par le token.

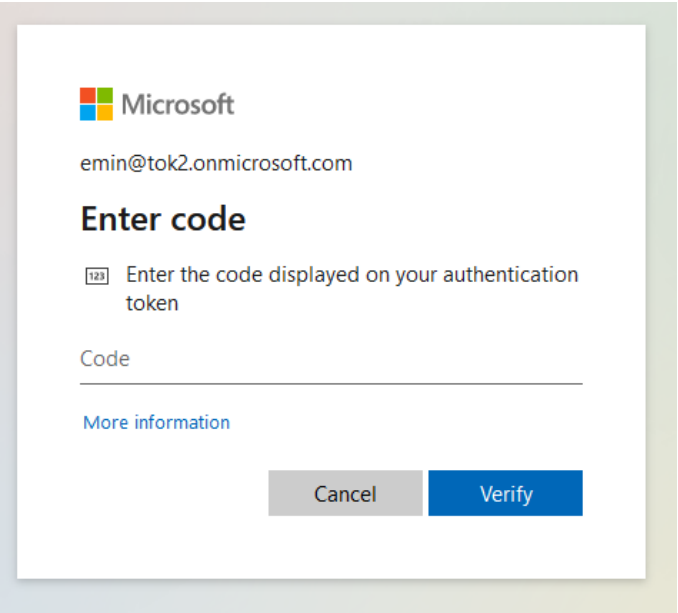


Si tout est correct, le token est ajouté au compte.



Connexion

Une fois activé et défini comme méthode MFA par défaut, le token TOTP permet à l'utilisateur de se connecter. La page de connexion demandera un « Code d'authentificateur » et acceptera l'OTP du token.

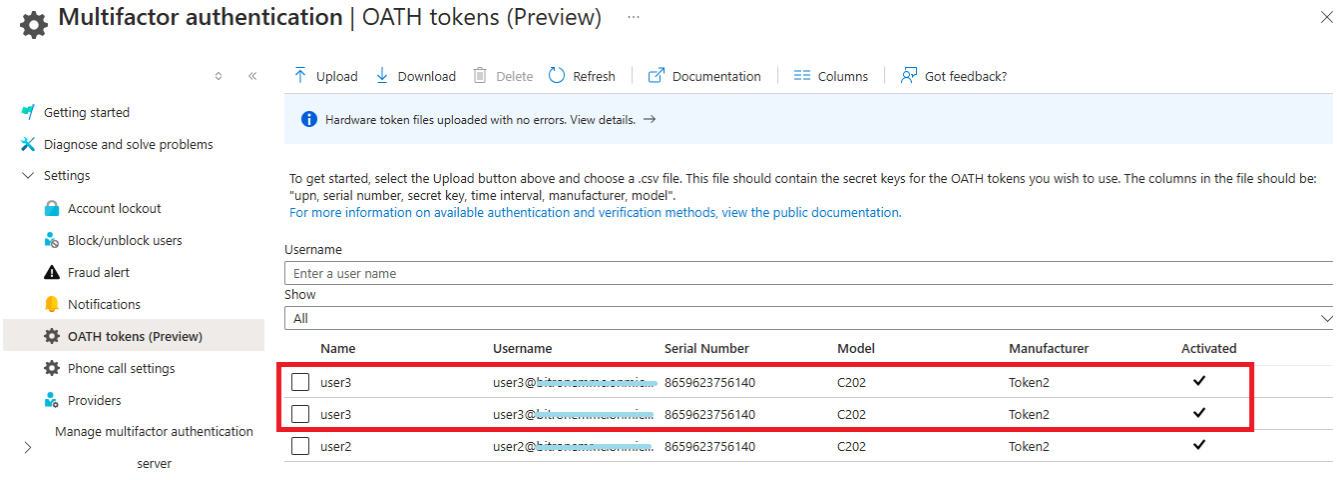


Conclusion des instructions utilisateur

Résolution des Problèmes

Le chargement de tokens via CSV autorisait les doublons. Ce n'est plus le cas avec JSON : numéro de série et seed doivent être uniques.

Un utilisateur peut avoir deux entrées du même token si celui-ci n'est pas supprimé du centre d'administration après ajout via Graph API. Supprimez l'ancien token selon la documentation Microsoft.



Vous pouvez identifier et supprimer le token hérité en suivant les étapes décrites dans la documentation Microsoft

FAQ

Comment gérer les tokens matériels dans Microsoft Entra ID ? Dans cette préversion, uniquement via Microsoft Graph API. Ils s'affichent dans le centre d'administration, mais ne peuvent y être gérés que s'ils viennent de la première préversion.

Ajouter un token dans le nouveau portail désactive-t-il l'ancien ? Non. Il reste actif dans les deux portails jusqu'à suppression. Il ne s'affiche pas dans la section « Hardware OATH Tokens (Preview) » tant qu'il n'est pas ajouté via « Informations de sécurité ».

Peut-on ajouter un token dans le nouveau portail s'il existe encore dans l'ancien ? Oui, mais les doublons sont interdits en JSON. Si le token existe déjà, il faut modifier son numéro de série et sa seed pour le différencier (voir exemple ci-dessous).

Peut-on importer des tokens sans intervention utilisateur ? Oui. L'admin peut uploader via Graph API, mais l'utilisateur doit activer manuellement le token en saisissant numéro de série, nom et OTP sur la page « Informations de sécurité ».

Délai d'activation maximum ? Pas de limite officielle, mais il est conseillé de ne pas dépasser 2 ans pour éviter une dérive de temps.

Le nouveau mode permet-il les doublons comme l'ancien ? Non, mais on peut contourner la limite en ajoutant un zéro au numéro de série et « AA » à la seed (AA = zéro en base32). Le Graph API considérera alors le token comme unique.

Exemple JSON original :

```
{
  "@context": "#$delta",
  "value": [
    {
      "@contentId": "1",
      "serialNumber": "865923712",
      "manufacturer": "Token2",
      "model": "C202",
      "secretKey": "JBSWY3DPEHPK3PXPJBSWY3DPEHPK3PXP",
      "timeIntervalInSeconds": 30,
      "hashFunction": "hmacsha1"
    }
  ]
}
```

doublon

```
{
  "@context": "#$delta",
  "value": [
```

```
    {
      "@contentId": "2",
      "serialNumber": "86592371200",
      "manufacturer": "Token2",
      "model": "C202",
      "secretKey": "JBSWY3DPEHPK3PXPJBSWY3DPEHPK3PXPAA",
      "timeIntervalInSeconds": 30,
      "hashFunction": "hmacsha1"
    }
  ]
}
```


Les tokens SHA-256 sont-ils plus sûrs ? Oui, théoriquement. SHA-256 a une longueur de 256 bits contre 160 pour SHA-1, le rendant moins vulnérable aux collisions. Mais dans le cadre TOTP basé sur HMAC, la différence de sécurité est moindre. Cela dit, nous recommandons d'éviter le TOTP si possible, et de préférer les clés FIDO2, plus résistantes au phishing et plus sûres.