HEL MO
Haute Ecole Libre Mosane

Ajouter une méthode d'authentification supplémentaire (MFA)

Objectifs

Cette procédure explique comment ajouter une méthode d'authentification à un compte Microsoft lorsqu'une méthode est déjà configurée afin de pouvoir s'authentifier en cas de problème avec sa méthode principale

Les méthodes privilégiées sont :

1. **Par application** : une application mobile permettant de valider une connexion à l'aide d'un numéro qu'il faut introduire dans l'application. Celle recommandée est Microsoft Authenticator mais il existe également Google Authenticator, Aegis Authenticator, ...
2. **TOTP** : code temporaire à 6 chiffres généré par une application d'authentification. Ce code change régulièrement et peut être configuré dans plusieurs application d'authentification (Microsoft Authenticator, Authy, Google Authenticator, ...)
3. **Clé d'accès** : permet de valider la connexion à l'aide des moyens de déverrouillage du smartphone (code PIN, empreinte digitale, reconnaissance faciale)

> Les méthodes d'authentification par **SMS** et par **appel téléphonique (GSM)** sont amenées à disparaître progressivement. Il est donc recommandé de configurer dès maintenant une méthode privilégiées.

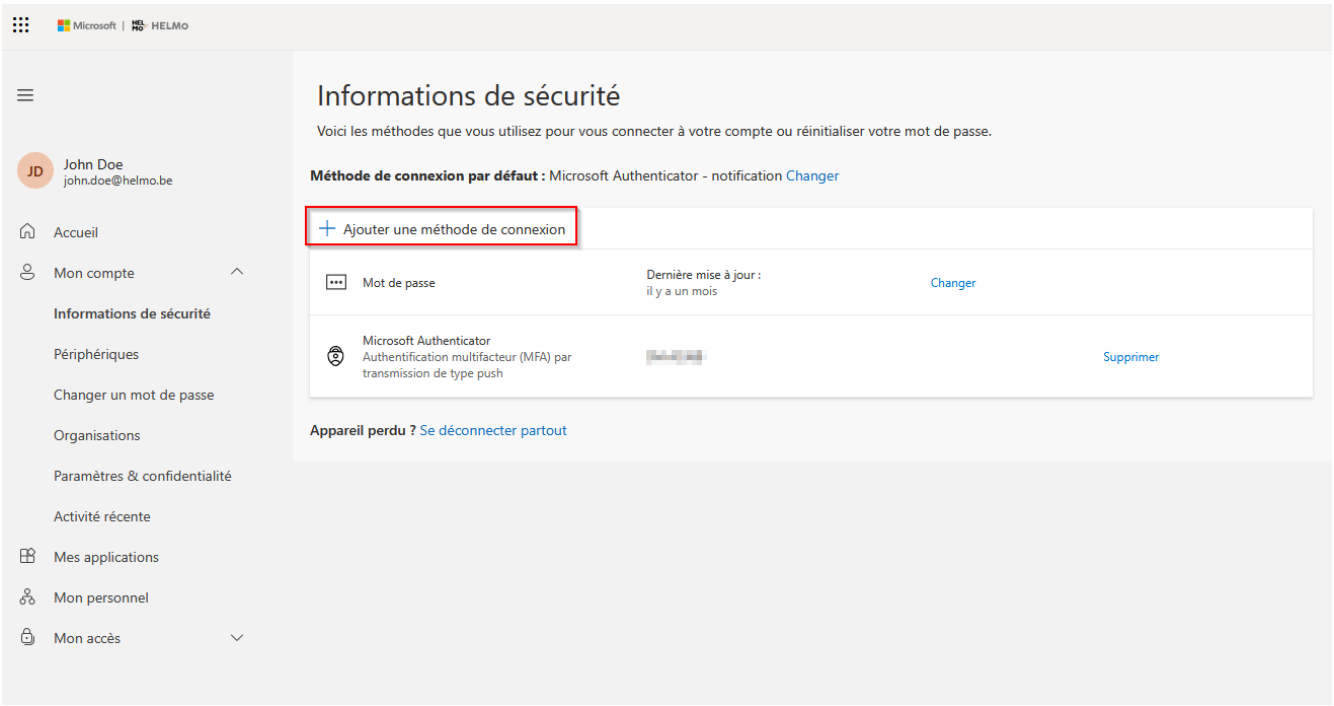
Étapes

Avant de commencer

> Vous devez déjà avoir accès à votre compte via une méthode fonctionnelle pour pouvoir en ajouter une nouvelle. Si vous n'y parvenez pas, consultez la page Mot de passe perdu et problèmes de MFA avant de poursuivre.

> Seule la méthode Microsoft Authenticator et la méthode TOTP (Jeton d'accès) sont expliquées ci-dessous, ces méthodes étant les méthodes recommandées.

- Ouvrez un navigateur Internet.
- Accédez à la page suivante : https://mysignins.microsoft.com/security-info
- Connectez-vous avec votre compte Microsoft professionnel.
- Validez la connexion avec votre méthode d'authentification habituelle.



- Cliquez sur **« Ajouter une méthode de connexion »**
- Ouvrez la liste des méthodes proposées.
- Sélectionnez la méthode souhaitée. Privilégiez la méthode via Microsoft Authenticator permettant de configurer l'authentification via l'application et celle via TOTP ainsi que la méthode par Clé d'accès

Optionnel – Installer Microsoft Authenticator

Si c'est la première fois que vous utiliser Microsoft Authenticator, il vous faut le configurer. Si vous avez déjà l'application configurée, veuillez passer à l'étape suivante.

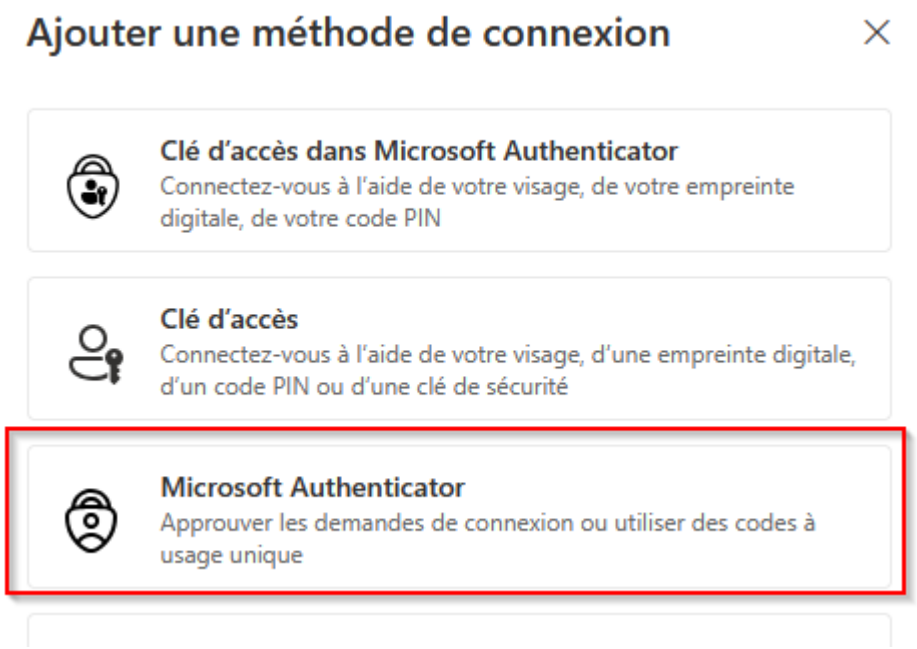
- Installez l'application Microsoft Authenticator sur votre smartphone.
- Suivez les instructions affichées à l'écran.
- Ouvrez Microsoft Authenticator sur votre smartphone.
- Ajoutez un compte professionnel ou scolaire si cela est demandé.
- Scannez le QR code affiché à l'écran de votre ordinateur.
- Terminez la configuration en suivant les instructions.
- Validez le test de connexion si celui-ci est proposé.

Configurer une méthode par application

Cette méthode permet d'utiliser une application d'authentification compatible pour entrer le numéro affiché dans l'application afin de confirmer la tentative de connexion. Dans cet exemple, Microsoft Authenticator est utilisé.

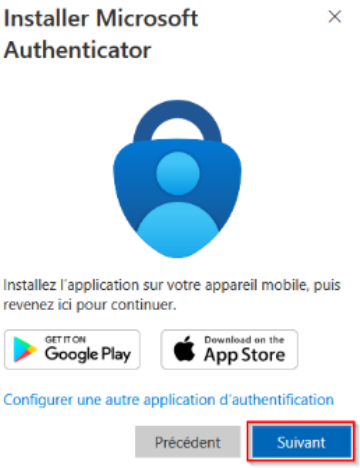
https://www.youtube.com/embed/4FqMbpueYUQ

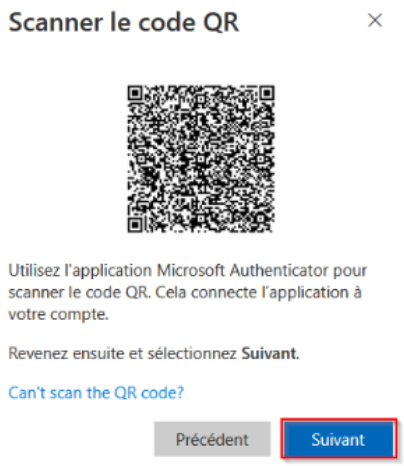
- Sélectionner Microsoft Authenticator



Si vous désirer utiliser une autre application que Microsoft Authenticator, veuillez ensuite sélectionner "Configurer une autre application d'authentication" et suivre les instructions

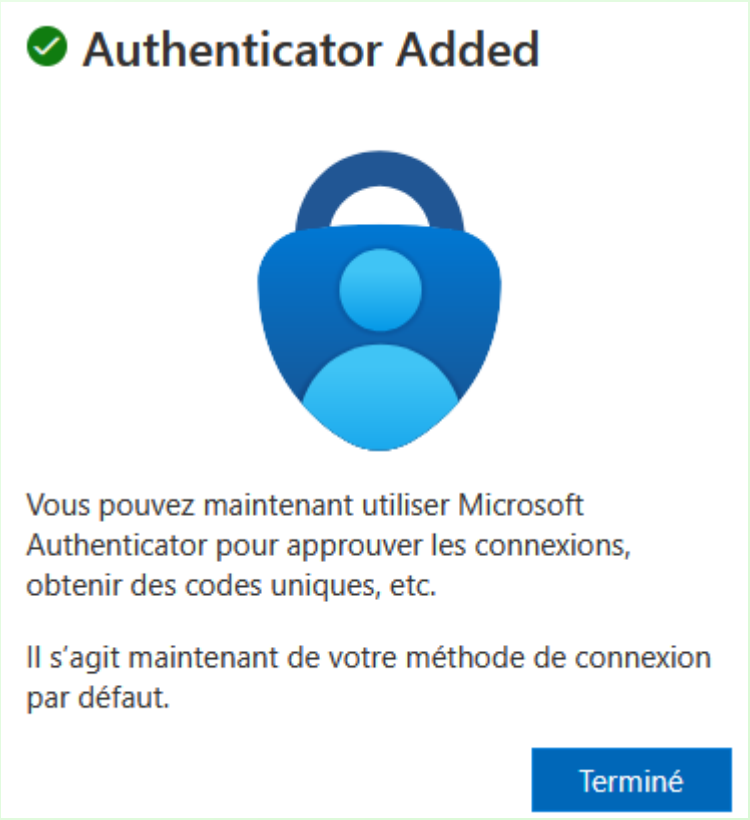
- Cliquez sur **« Suivant »**.
- Suivre les instructions affichées
- Scanner le QR code
- Cliquez sur **« Suivant »**.
- Il est ensuite proposer de tester la connexion avec un numéro à introduire dans l'application, recopier ce numéro dans l'application







L'authentification via Microsoft Authenticator est alors bien configurée !

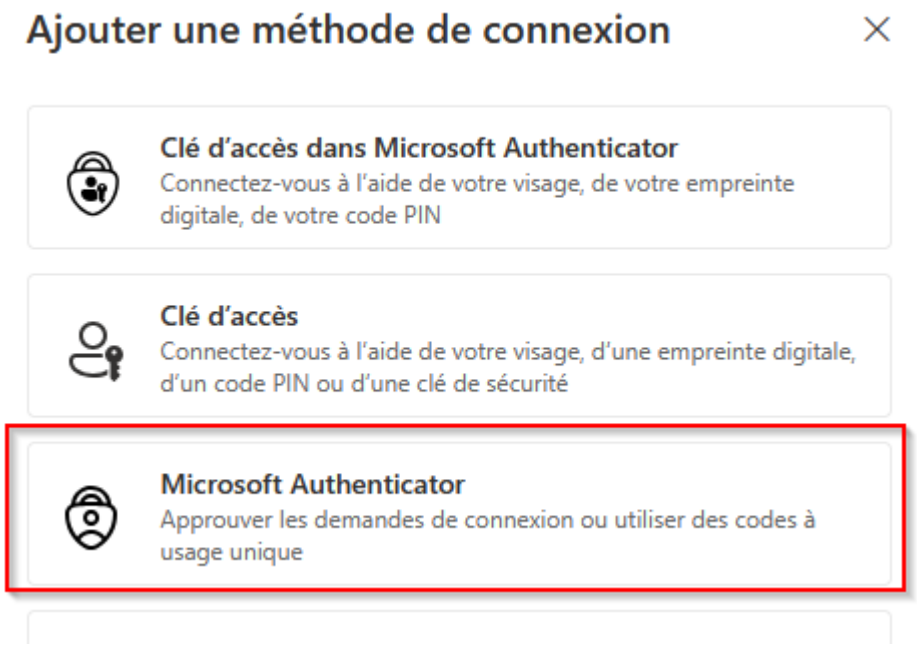


Configurer une méthode TOTP

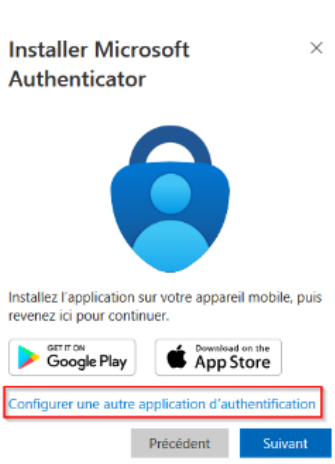
Cette méthode permet d'utiliser une application d'authentification compatible pour générer des codes temporaires à 6 chiffres. Dans cet exemple, Microsoft Authenticator est utilisé.

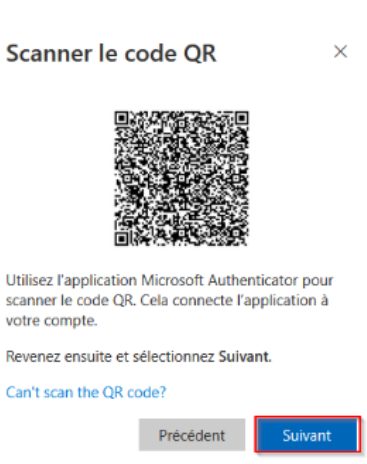
https://www.youtube.com/embed/B1dSGa-1WG0

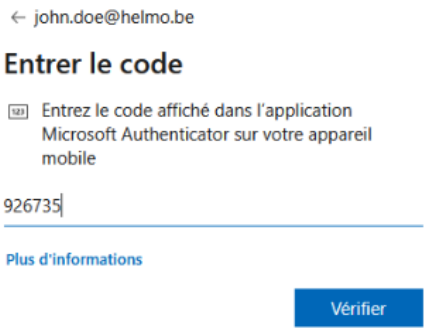
- Sélectionner Microsoft Authenticator



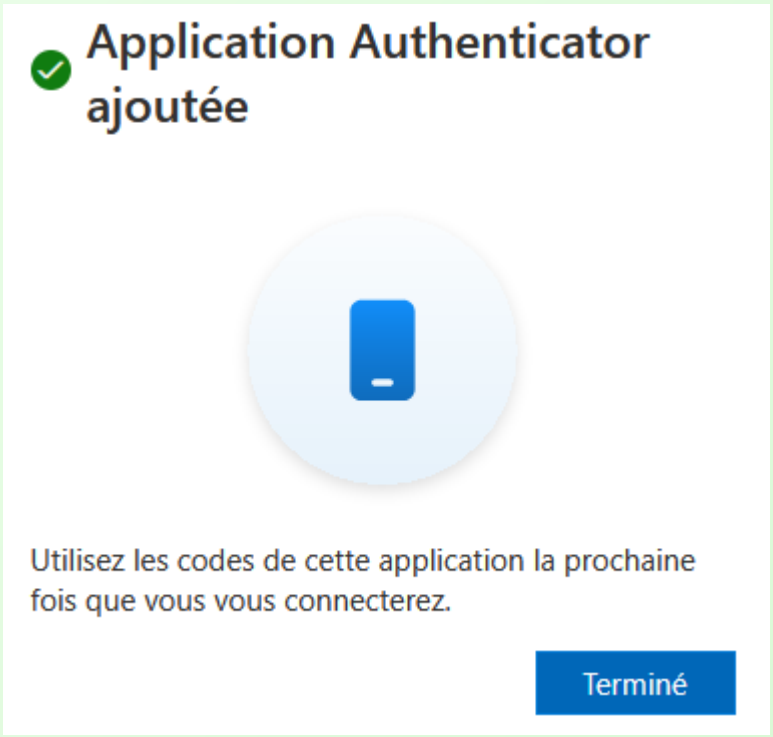
- Sélectionnez **« Configurer une autre application d'authentification »**
- Suivez les instructions affichées.
- Microsoft propose alors un QR code, ouvrez Microsoft Authenticator.
- Ajoutez un compte en scannant le QR code.
- Scanner le QR code
- Cliquez sur **« Suivant »**.
- Microsoft propose de tester l'authentification, récupérez le code temporaire généré par l'application.
- Saisissez ce code sur la page Microsoft







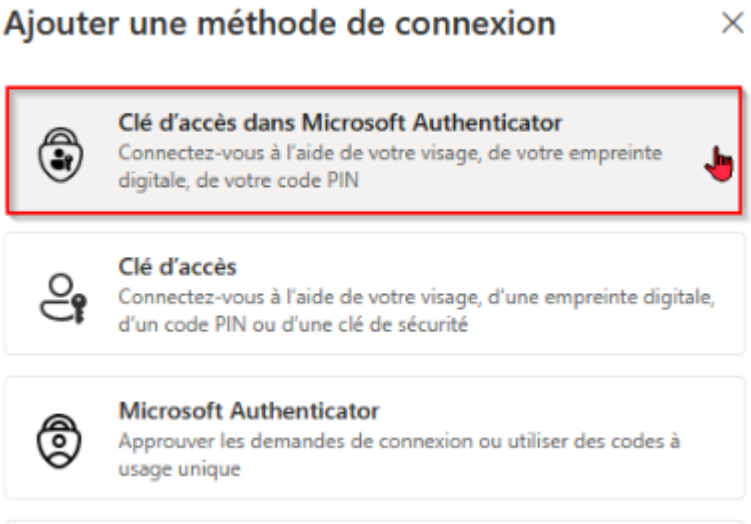
L'authentification par TOTP est alors bien configurée !



Configurer une méthode clés d'accès dans Microsoft Authenticator

Cette méthode permet de valider la connexion à l'aide des moyens de déverrouillage du smartphone (code PIN, empreinte digitale, reconnaissance faciale) via l'application Microsoft Authenticator.

- Sélectionner Clé d'accès dans Microsoft Authenticator



- Vérifier que votre appareil dispose bien d'Android 14 ou d'IOS 17 au minimum et que votre application est mise à jour
- Cliquer sur suivant
- Suivez les instructions dans l'application

HEL MO
Haute Ecole Libre Mosane

Create a passkey in Microsoft Authenticator



Une clé d'accès vous permet de vous connecter plus facilement et en toute sécurité avec votre visage, votre empreinte digitale ou votre code PIN.

Vérifiez que votre appareil dispose d'Android 14 ou d'iOS 17 au minimum, et que l'application Authenticator est mise à jour vers la dernière version.

Vous devez ajouter votre compte dans Authenticator ? Ajoutez-le dès maintenant.

Précédent Suivant

Terminer la création de votre clé d'accès dans Authenticator



1. Dans Authenticator, sélectionnez votre compte professionnel ou scolaire, **p.gualtieri.test@helmo.be**.
2. Sélectionnez **Créer une clé d'accès** et suivez les instructions de l'application.

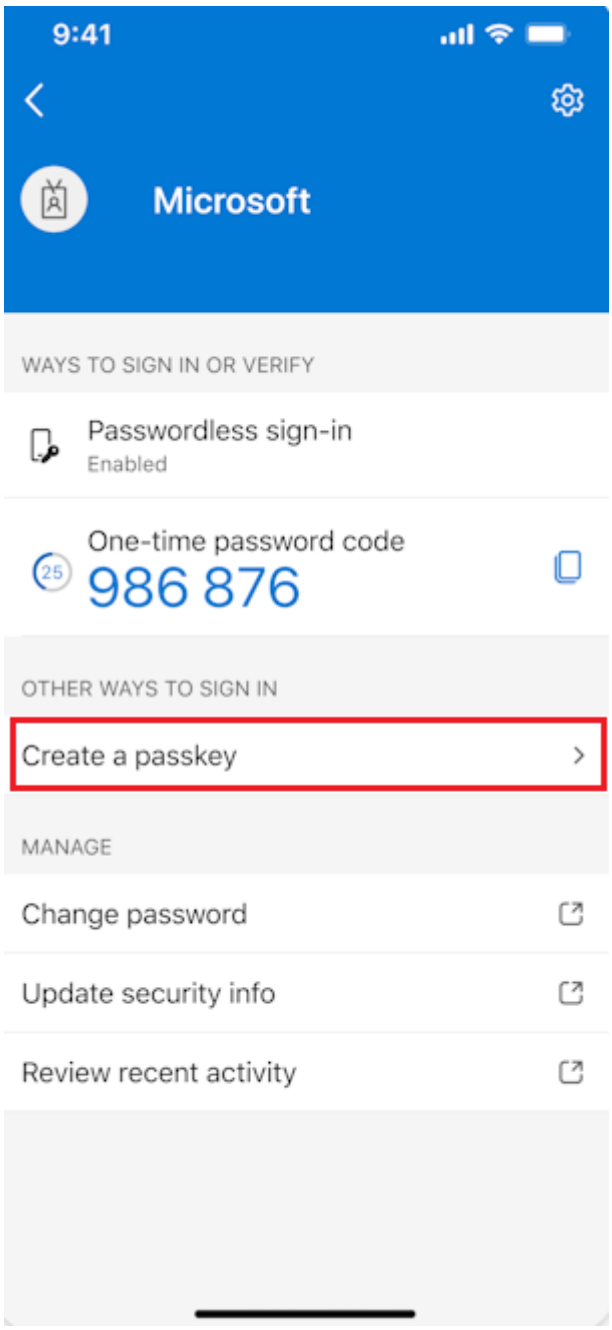
Vérifiez que votre appareil dispose d'Android 14 ou d'iOS 17 au minimum, et que l'application Authenticator est mise à jour vers la dernière version.

Vous devez ajouter votre compte dans Authenticator ? Ajoutez-le dès maintenant.

Vous rencontrez des problèmes ?

Précédent | Suivant

- Dans Microsoft Authenticator, sélectionner votre adresse mail Helmo
- Cliquer sur l'option **Créer une clé d'accès** (Create a passkey).



- Suivre les instructions affichées par l'application.

Changer la méthode d'authentification par défaut

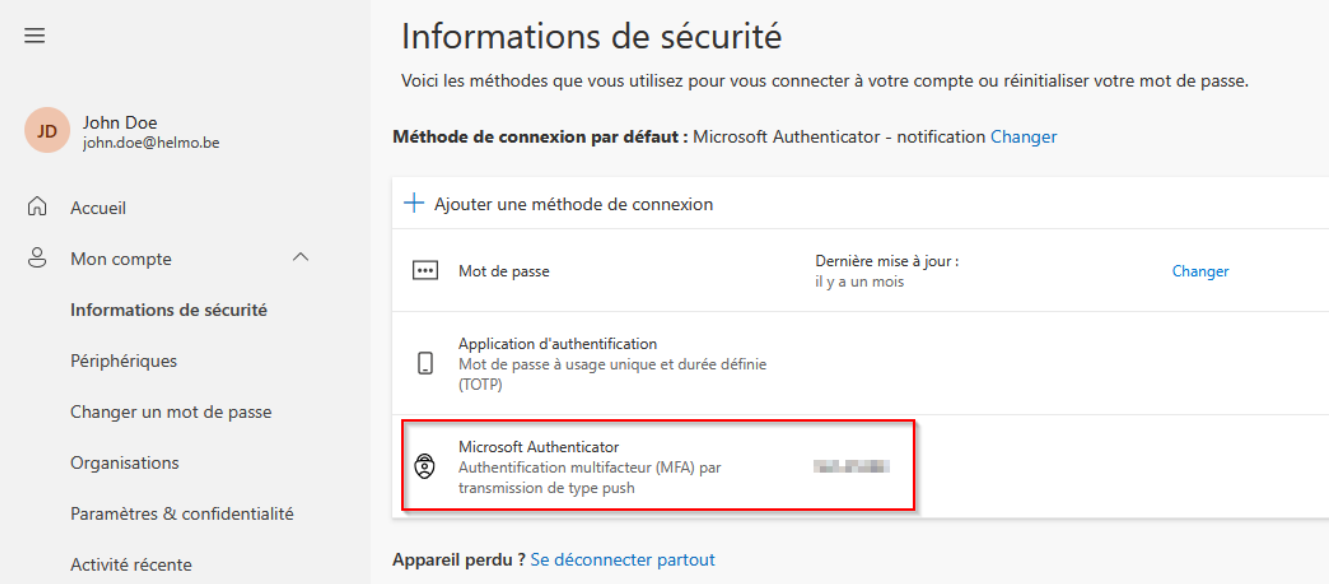
Si vous le désirez, vous pouvez faire de cette nouvelle méthode d'authentification votre méthode par défaut. Elle sera proposée en priorité lorsque vous tenterez de vous connecter.

- Revenez à la page « Informations de sécurité ».

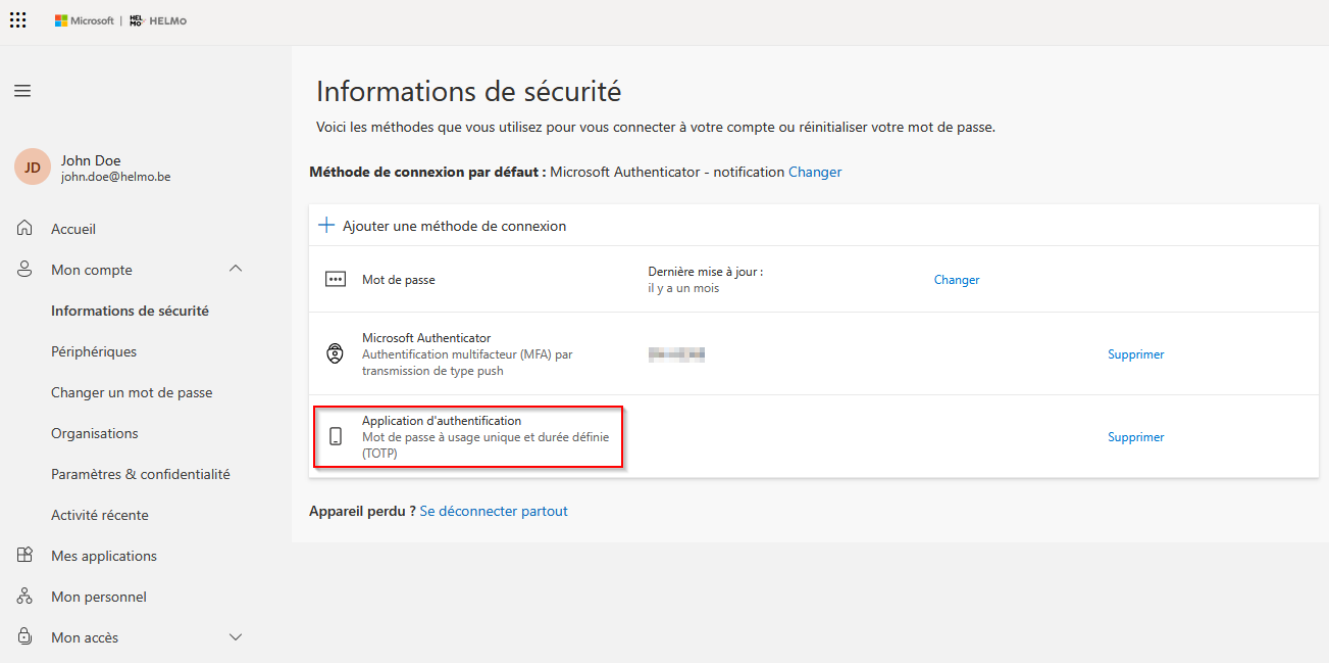
- Vérifiez que la nouvelle méthode apparaît dans la liste.

https://www.youtube.com/embed/je86S5-yUd4

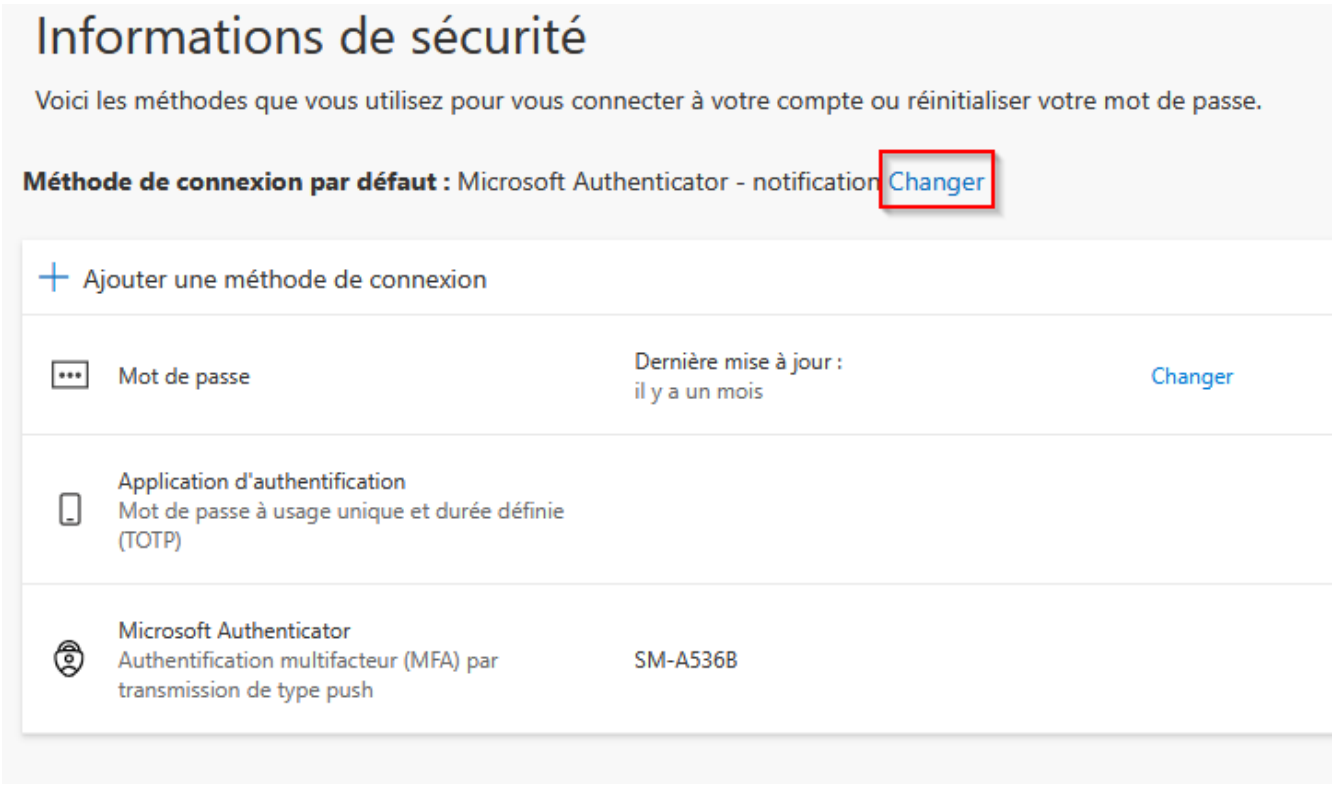
1) Méthode Microsoft Authenticator



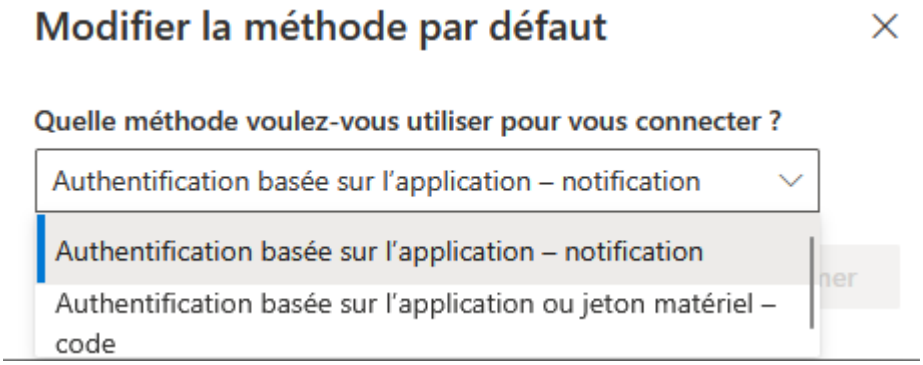
2) Méthode TOTP



- Sélectionner l'option "**Changer**"



- Sélectionner la nouvelle méthode (notification pour Microsoft Authenticator et code pour TOTP)



Vous avez bien ajouté votre méthode d'authentification comme authentification par défaut !

Conseils

- Vérifiez toujours que chaque méthode fonctionne correctement après l'avoir configurée pour éviter tout blocage futur.
- Si possible, conservez au moins deux méthodes différentes pour garantir un accès sécurisé en toutes circonstances.

Résolution des problèmes

- **Le QR code ne fonctionne pas/tourne en rond :** vérifiez que vous utilisez une application compatible et que votre GSM à une bonne connexion internet. Passez sur la 4G au besoin.
- **Le code TOTP est refusé :** saisissez le code le plus récent et vérifiez que la date et l'heure de votre smartphone sont réglées automatiquement.
- **Vous changez de smartphone :** configurez et testez votre méthode sur le nouvel appareil avant de supprimer l'ancienne.
- **Vous n'avez plus accès à votre méthode actuelle :** utilisez une autre méthode déjà configurée ou contactez le support informatique.