



Authentification Multi Facteur (MFA)

Procédure
d'enrôlement de
votre compte avec
votre smartphone.

Table des matières

Comment fonctionne l'Authentification Multi Facteur (MFA) :.....	2
1. L'enrôlement avec une application d'authentification	3
2. Ajout d'une nouvelle méthode d'authentification.....	13
3. Changer la méthode d'authentification par défaut	18
FAQ.....	19

Afin de sécuriser l'accès à la messagerie de l'extérieur du CHU en mode Web l'authentification multi facteur (MFA) est nécessaire.

Comment fonctionne l'Authentification Multi Facteur (MFA)

Elle s'appuie sur deux éléments qui vous caractérise :

1. Quelque chose que vous savez : C'est généralement un mot de passe ou un code PIN. C'est la première étape de l'authentification et c'est quelque chose que vous devez mémoriser.
2. Quelque chose que vous avez : Cela pourrait être votre téléphone mobile, une clé de sécurité physique, ou une carte à puce. Après avoir entré votre mot de passe, un code d'authentification unique peut vous être envoyé sur votre téléphone.

L'utilisation de l'authentification multi-facteur peut sembler un peu plus compliquée que l'utilisation d'un simple mot de passe, mais elle offre une protection bien supérieure. Même si quelqu'un parvient à deviner ou à voler votre mot de passe, il lui sera très difficile d'obtenir également votre deuxième facteur d'authentification. Cela rend l'authentification multi-facteur essentielle pour protéger l'accès au système d'information de l'établissement.

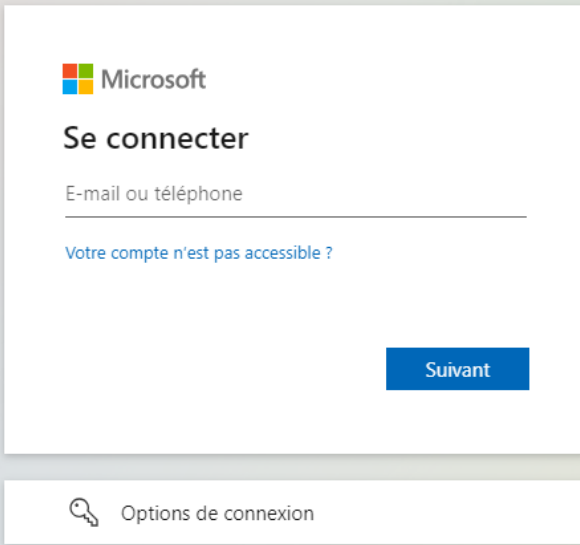
Le but de cette documentation est de vous guider dans la mise en œuvre de ce mode d'authentification sécurisée

1. L'enrôlement avec une application d'authentification

A effectuer uniquement sur un poste du CHU connecté au réseau CHU

Vous devez associer votre téléphone avec votre compte Microsoft CHU, ceci correspond à l'étape d'enrôlement qui consiste à définir votre mode d'authentification multi-facteur. [Cliquez ici pour effectuer l'enrôlement](https://mysignins.microsoft.com/security-info/) (https://mysignins.microsoft.com/security-info/) et suivez la procédure ci-dessous.

- a. Si vous n'êtes pas directement connecté à votre profil Microsoft Office365 suivez les étapes ci-dessous :
 - Identifiez-vous avec votre adresse mail et votre mot de passe du CHU.




Microsoft

Se connecter

E-mail ou téléphone

[Votre compte n'est pas accessible ?](#)

Suivant

 [Options de connexion](#)

- Saisissez votre mot de passe



← testot@chu-montpellier.fr

Entrez le mot de passe

Mot de passe

[J'ai oublié mon mot de passe](#)

Se connecter



testot@chu-montpellier.fr

Plus d'informations requises

Votre organisation a besoin de plus d'informations pour préserver la sécurité de votre compte

[Utiliser un autre compte](#)

[En savoir plus](#)

Suivant

b. Si vous êtes déjà connecté à votre compte Microsoft Office365 :

Cliquez sur « Ajouter une méthode de connexion »

https://mysignins.microsoft.com/security-info

Mes connexions

Vue d'ensemble

Informations de sécurité

Appareils

Mot de passe

Organisations

Paramètres et confident...

Activité récente

Informations de sécurité

Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification [Changer](#)

+ Ajouter une méthode de connexion

...	Mot de passe	Dernière mise à jour : il y a 14 jours	Changer
...	Microsoft Authenticator Authentification multifacteur (MFA) par transmission	SM-A415F	Supprimer

Appareil perdu ? [Se déconnecter partout](#)

Ajouter une méthode

Quelle méthode voulez-vous ajouter ?

Choisir une méthode


- Application d'authentification
- Téléphone

- A cette étape vous devez télécharger sur votre smartphone l'application **Microsoft Authenticator** disponible dans les stores App Store ou Play Store

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Microsoft Authenticator



Commencer par obtenir l'application

Sur votre téléphone, installez l'application Microsoft Authenticator. [Télécharger maintenant](#)

Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

[Je souhaite utiliser une autre application d'authentification](#)

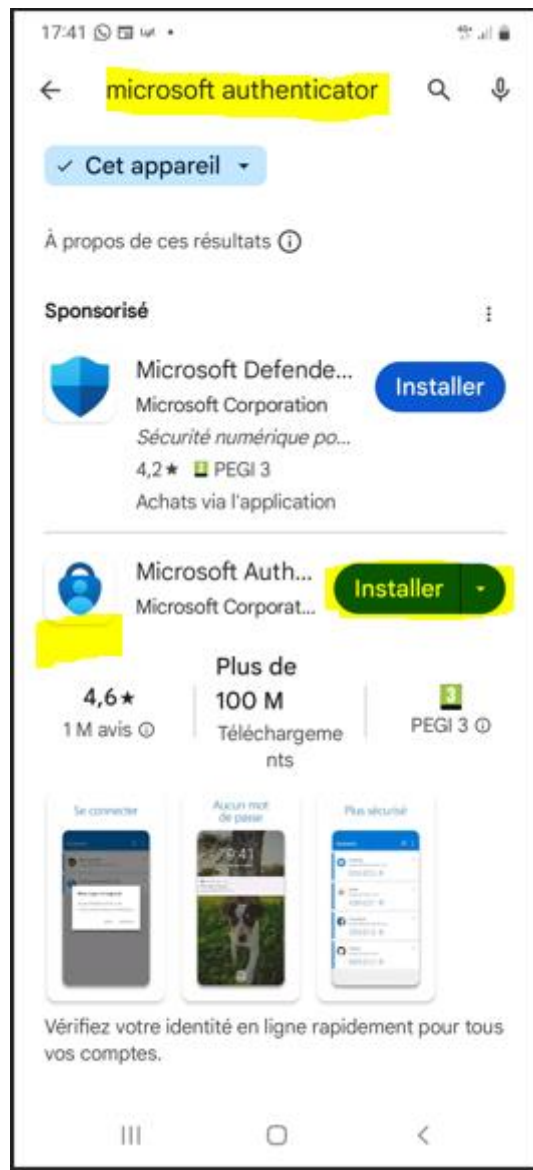
[Suivant](#)

[Je veux configurer une autre méthode](#)


NB : Sur un PC ou un MAC ne cliquez pas sur « Télécharger maintenant », ce lien étant là uniquement si vous faite l'enrôlement directement à partir de votre smartphone.

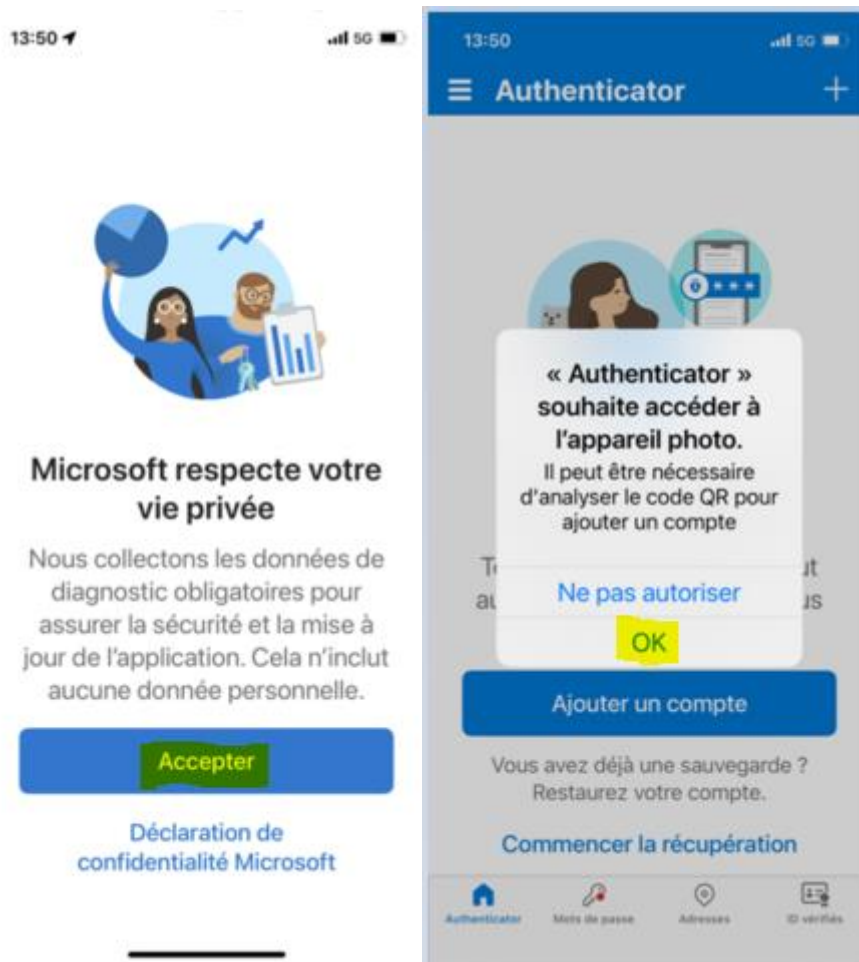
Sur votre Smartphone :

Smartphone Android, ouvrez Play Store et recherchez Microsoft Authenticator.
iPhone, ouvrez App Store et recherchez Microsoft Authenticator.

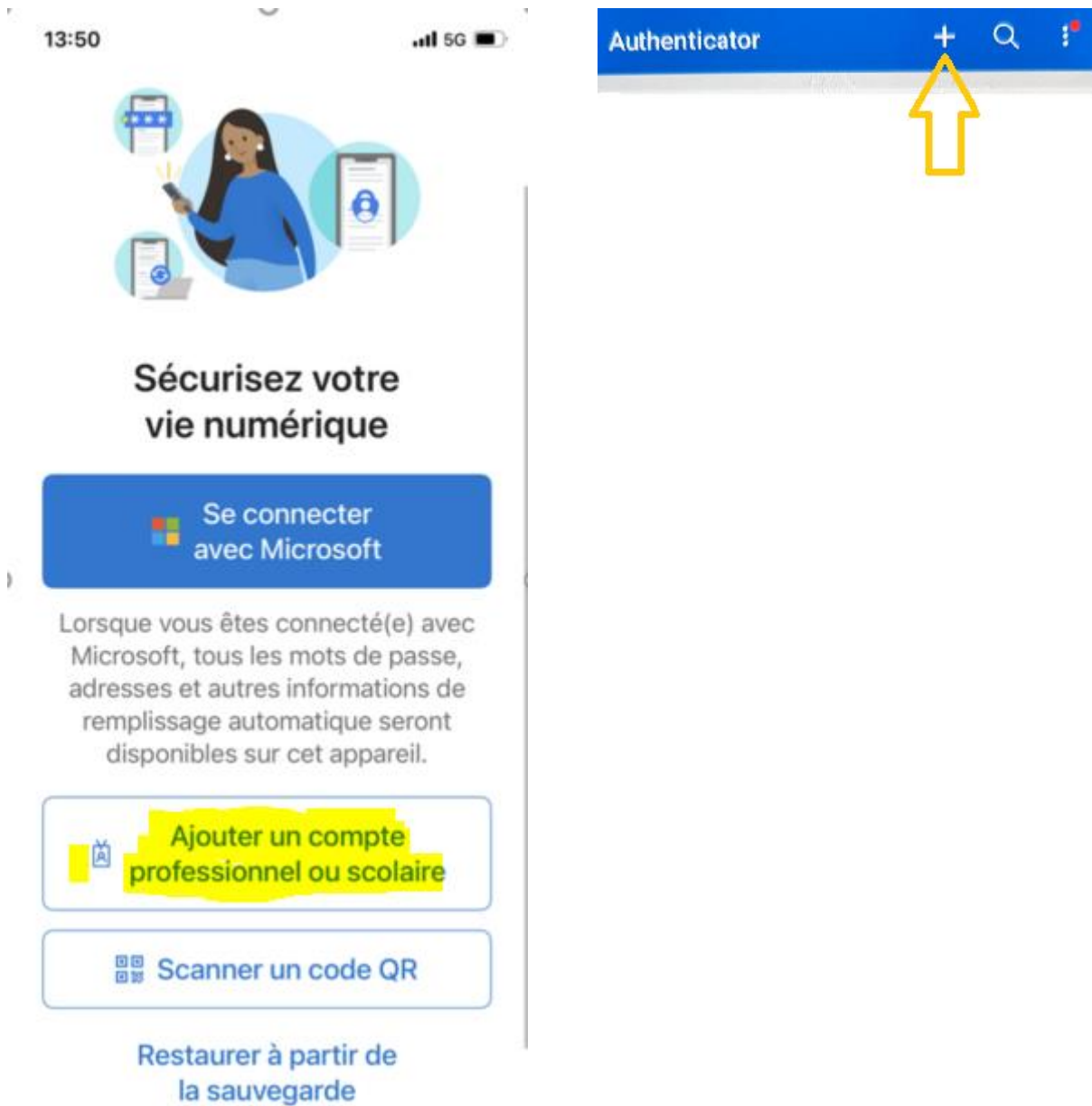


- Cliquez sur le bouton « Installer »

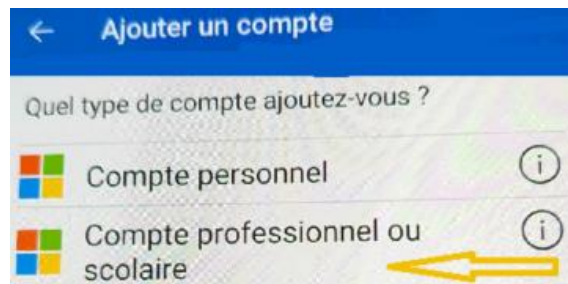
- Ouvrez l'application Authenticator  acceptez les demandes d'autorisation d'utilisation de l'appareil photo et les conditions de respect de la vie privée.



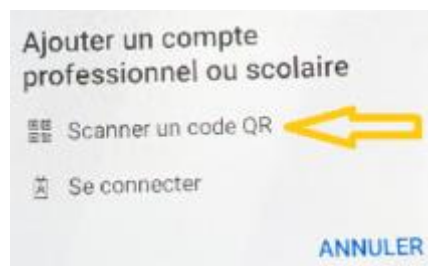
- Cliquez sur « Ajouter un compte professionnel ou scolaire » ou sur l'icône « + » si vous avez déjà un compte enregistré dans cette application.



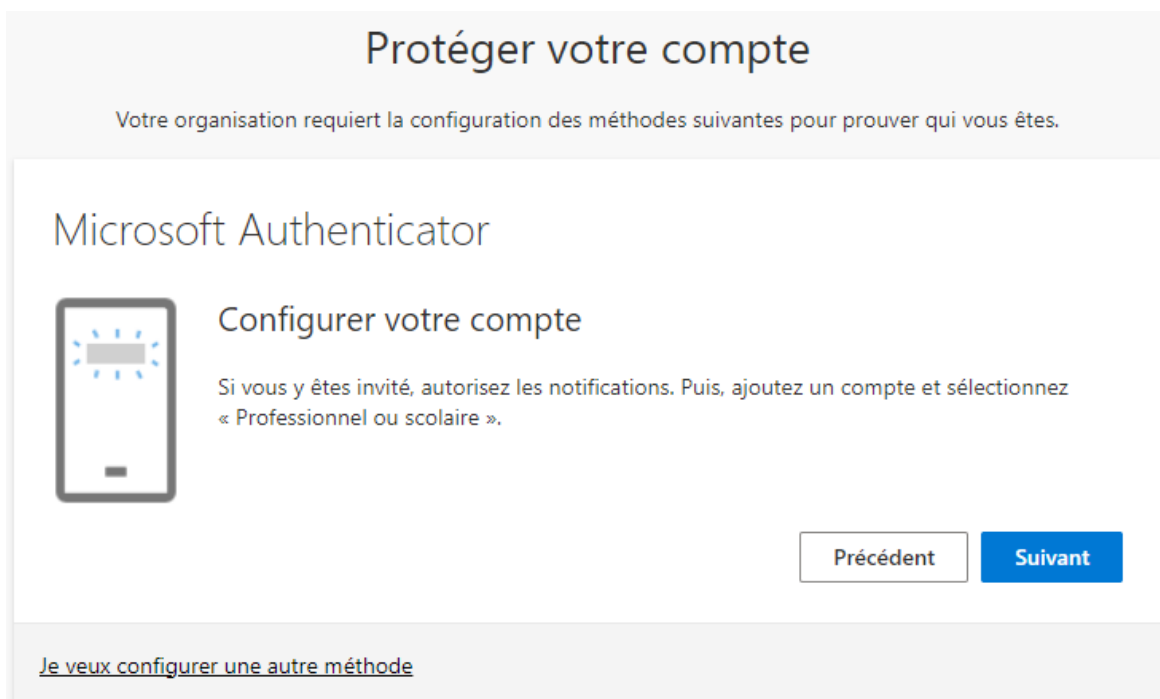
- Sélectionnez « Compte professionnel ou scolaire »



- Sélectionner « Scanner un code QR » :



Sur l'écran du PC/MAC :



- Scanner avec votre smartphone le QR code **afficher sur votre écran**

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Microsoft Authenticator

Scanner le code QR

Utiliser l'application Microsoft Authenticator pour scanner le code QR. Ceci permet de connecter l'application Microsoft Authenticator à votre compte.

Après avoir scanné le code QR, cliquez sur « Suivant ».



Impossible de numériser l'image ?

Précédent


Suivant

[Je veux configurer une autre méthode](#)

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Microsoft Authenticator



Nous allons essayer

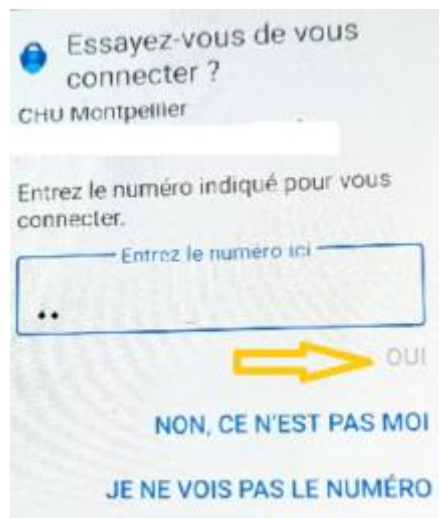
Approuvez la notification que nous envoyons à votre application en entrant sur le numéro ci-dessous.

1

Précédent Suivant

[Je veux configurer une autre méthode](#)

- Saisissez sur votre smartphone le numéro affiché à l'écran :



Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Microsoft Authenticator



✓ Notification approuvée

Précédent

Suivant

[Je veux configurer une autre méthode](#)

Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

Opération réussie

Bravo ! Vous avez correctement configuré vos informations de sécurité. Cliquez sur « Terminé » pour poursuivre la connexion.

Méthode de connexion par défaut :



Microsoft Authenticator

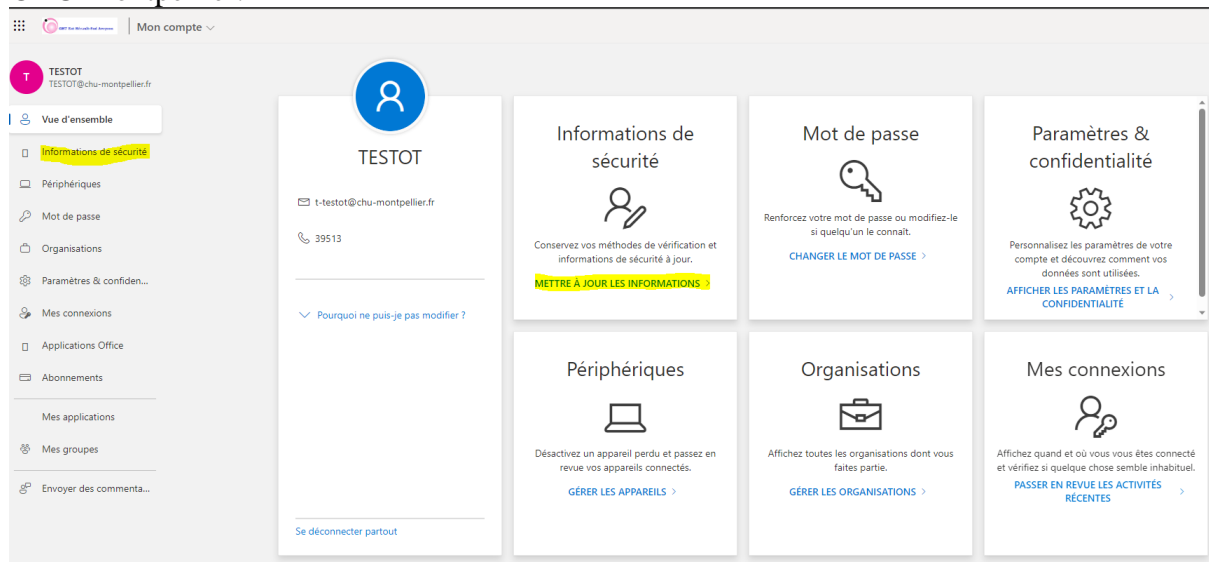
Terminé

Votre compte est maintenant enrôlé avec votre smartphone. Cet enrôlement vous permettra d'accéder à la messagerie du CHU en mode Web lorsque vous serez connecté en dehors du réseau de l'établissement (Chez vous, en déplacement, en 4G, en Wifi public). Ainsi, lors de l'accès à la messagerie Outlook Web il vous sera demandé de saisir le code fourni par l'application Authenticator.

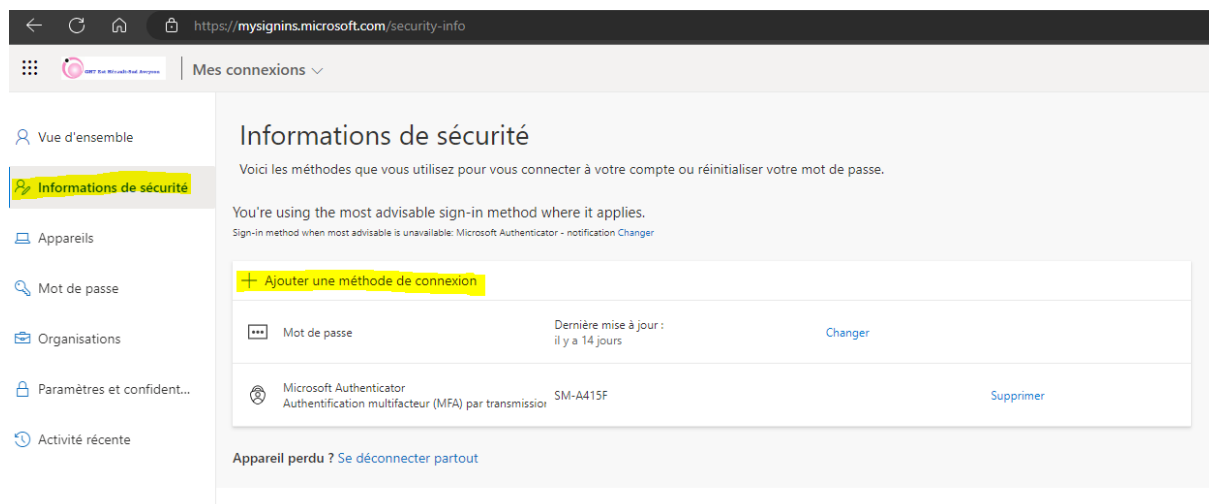
NB : Cet enrôlement permettant l'authentification par MFA, deviendra la méthode officielle d'accès aux ressources informatiques en dehors du réseau CHU. Elle sera appliquée prochainement pour effectuer votre connexion pour le télétravail.

2. Ajout d'une nouvelle méthode d'authentification (Optionnel)

A la suite de l'étape précédente, vous avez atteint l'écran de gestion de votre compte Microsoft Office365. A partir de cet écran vous pouvez gérer plusieurs paramètres associés à votre compte CHU Montpellier.



La suite de cette documentation se limitera à décrire la gestion de vos informations de sécurité.



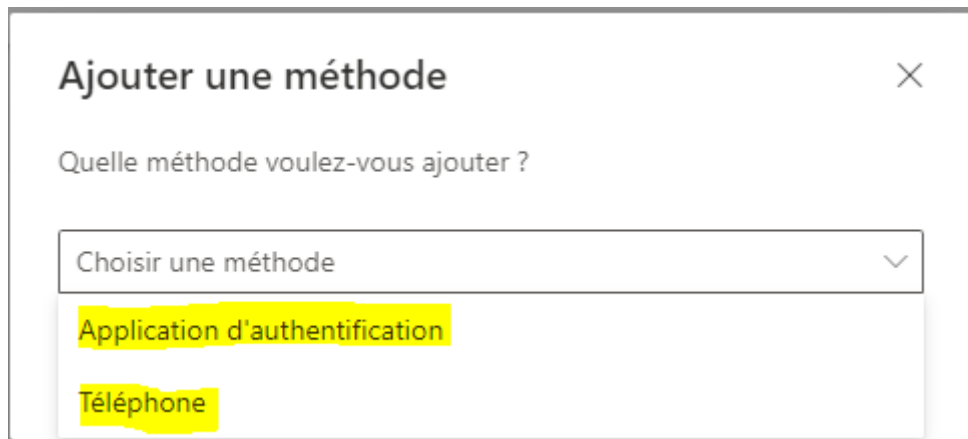
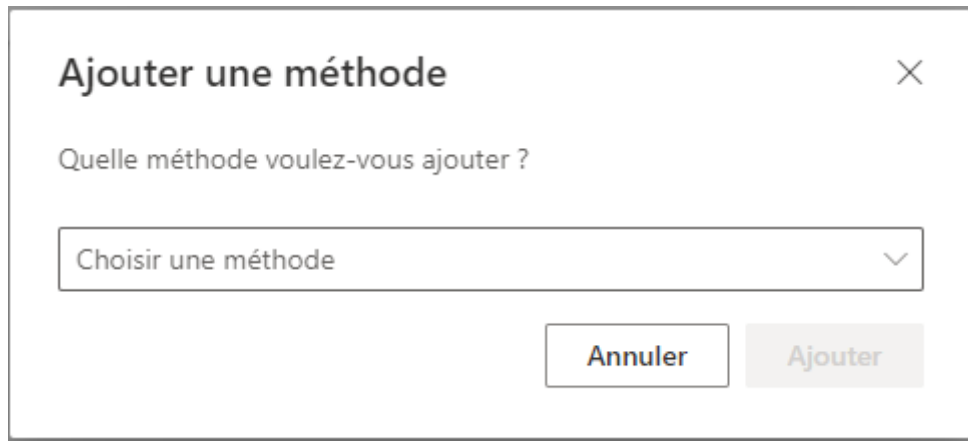
Sur cet écran vous pouvez constater que vous avez deux méthodes de connexion enregistrées :

- Mot de passe : Méthode standard, elle ne peut pas être supprimée.

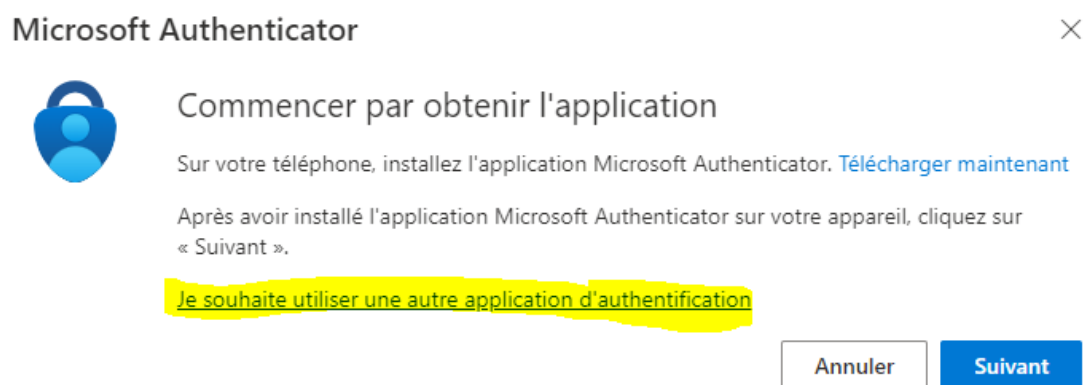
NB : Le changement de mot de passe ne fonctionne pas par cet accès pour le CHU, ne l'utilisez pas.

- Microsoft Authenticator : Il s'agit de la méthode enregistrée lors de votre enrôlement à l'étape précédente.

Vous pouvez ajouter une nouvelle méthode d'authentification en cliquant sur « Ajouter une méthode de connexion »



- Application d'authentification : Cette méthode est identique à la méthode précédente effectuée lors de l'enrôlement mais avec l'application Authenticator de Google que vous pouvez télécharger sur les stores PlayStore ou AppStore d'Apple.



Le procédé est identique au procédé effectué lors de l'enrôlement avec Microsoft Authenticator

- Téléphone : Ce choix vous permet de recevoir un SMS avec le code de sécurité (OPT). Ce choix nécessite que vous saisissez votre numéro de téléphone portable.

Téléphone

Vous pouvez prouver votre identité en recevant un code sur votre téléphone.

Quel numéro de téléphone voulez-vous utiliser ?

France (+33) 06.....

Recevoir un code

Des frais relatifs aux messages et aux données peuvent s'appliquer. Si vous choisissez Suivant, cela signifie que vous acceptez [Conditions d'utilisation du service](#) et [Déclaration sur la confidentialité et les cookies](#).

Annuler Suivant

[Les Déclarations sur la confidentialité et les cookies](#) cités dans le lien ci-dessus sont des conditions générales des systèmes Microsoft. Dans le cas de votre utilisation en tant que professionnel du CHU de Montpellier, il s'agit d'une utilisation d'un compte professionnel dont les conditions sont décrites dans le chapitre « [Produits fournis par votre organisation – information destinées aux utilisateurs finaux](#) ».

Le numéro de téléphone que vous allez fournir sera conservé en France.

Dans le cadre du traitement de vos données à caractère personnel, vous pouvez exercer vos droits octroyés par RGPD^[1] et (LIL)^[2] à tout moment et sans justification auprès du DPO (délégué de la protection des données) du CHU de Montpellier (dpo@chu-montpellier.fr)


^[1] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

^[2] Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

Veillez saisir les caractères affichés dans la zone surlignée en jaune

Téléphone

Please show you are not a robot.



Enter characters

Précédent Suivant

Veillez saisir le code reçu par SMS dans la zone surlignée en jaune

Téléphone

Nous venons d'envoyer un code à 6 chiffres à +33 0603548865.
Entrez le code ci-dessous.

Entrer le code

[Renvoyer le code](#)

Précédent Suivant

Téléphone



Vérification terminée. Votre téléphone a été enregistré.

Terminé

3. Changer la méthode d'authentification par défaut

Informations de sécurité

Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification **Changer**

+ Ajouter une méthode de connexion

Téléphone		Changer	Supprimer
Mot de passe	Dernière mise à jour : il y a 14 jours	Changer	
Microsoft Authenticator Authentification multifacteur (MFA) par transmission			Supprimer

Modifier la méthode par défaut

Quelle méthode voulez-vous utiliser pour vous connecter ?

Authentification basée sur l'application – notification

Téléphone - envoyer un SMS à [redacted]


Authentification basée sur l'application – notification

FAQ

Q : Impossible d'installer Microsoft Authenticator "Cette application ne fonctionnera pas sur cet appareil "

R : Votre téléphone est trop ancien cependant vous pouvez utiliser Google Authenticator en sélectionnant dans l'écran ci-dessous l'option surligné en jaune

Microsoft Authenticator



Commencer par obtenir l'application

Sur votre téléphone, installez l'application Microsoft Authenticator. [Télécharger maintenant](#)

Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

Je souhaite utiliser une autre application d'authentification

Q : Je ne peux pas scanner le QR code

R : Utilisez une des solutions suivantes


- 1- Utilisez l'application appareil photo sur votre smartphone pour scanner le QR code

Microsoft Authenticator

Scanner le code QR

Utiliser l'application Microsoft Authenticator pour scanner le code QR. Ceci permet de connecter l'application Microsoft Authenticator à votre compte.

Après avoir scanné le code QR, cliquez sur « Suivant ».



Impossible de numériser l'image ?

Entrez les informations suivantes dans votre application :

Code :

URL : <https://mobileappcommunicator.auth.microsoft.com/activate/276339021/WEU>

Q : Je n'ai pas de Smartphone

R : Vous pouvez vous enrôler avec votre téléphone. Dans ce cas vous devrez saisir votre numéro de téléphone. Ainsi vous recevrez le code d'accès par SMS



A screenshot of a mobile application dialog box titled "Ajouter une méthode" (Add a method). The dialog has a close button (X) in the top right corner. Below the title, the text "Quelle méthode voulez-vous ajouter ?" (Which method do you want to add?) is displayed. A dropdown menu is open, showing two options: "Application d'authentification" (Authentication application) and "Téléphone" (Phone). The "Téléphone" option is highlighted with a yellow background and circled in blue. The "Application d'authentification" option is also highlighted with a yellow background.