

Utilisation de l'Authentification Multifactorielle (MFA) avec Microsoft via MS Authenticator

Objectif : Cette procédure a pour but de vous guider à configurer et utiliser l'authentification multifactorielle (MFA) avec les services Microsoft pour sécuriser votre compte.

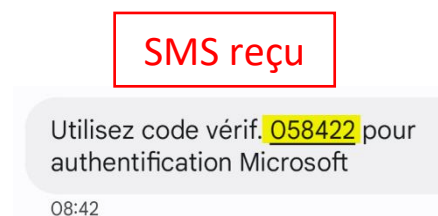
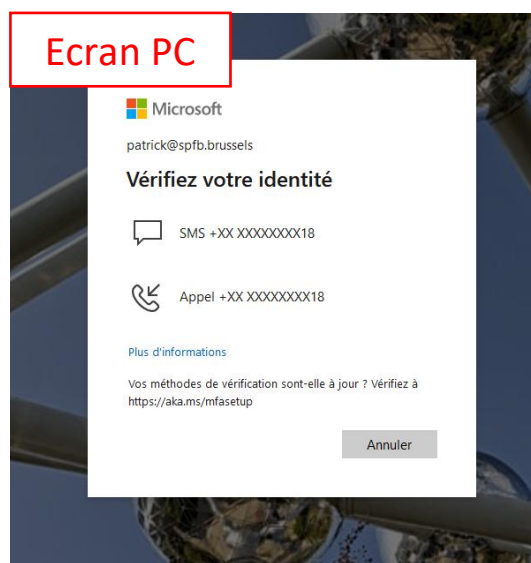
Étape 1 : Se connecter à vos paramètres de compte Microsoft 365

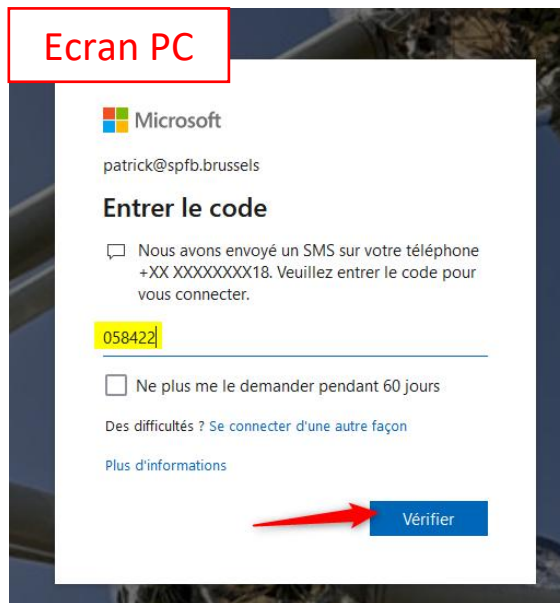
Pour vous connecter à votre compte Microsoft veuillez cliquer sur ce lien : <https://mysignins.microsoft.com/security-info>. Ou copiez et collez-le sur votre navigateur préféré. Il vous amènera directement dans la section « informations de sécurité » de votre compte.

Il est probable qu'un écran s'affiche (voir images ci-dessous) vous invitant à confirmer l'accès en utilisant un code de sécurité qui vous sera envoyé par SMS au numéro que vous avez déjà enregistré dans votre compte ou par courrier électronique à une adresse personnelle différente de celle de l'école.

Les paramètres de sécurité associés à votre compte Microsoft sont sécurisés afin d'empêcher toute modification par des personnes non autorisées.

Note : Si cet écran ne s'affiche pas, cela veut dire que le navigateur vous reconnaît via vos cookies et vous n'avez pas besoin de vous identifier à nouveau. Vous avez alors directement accès à la section « informations de sécurité » et vous pouvez passer directement à l'étape 2.

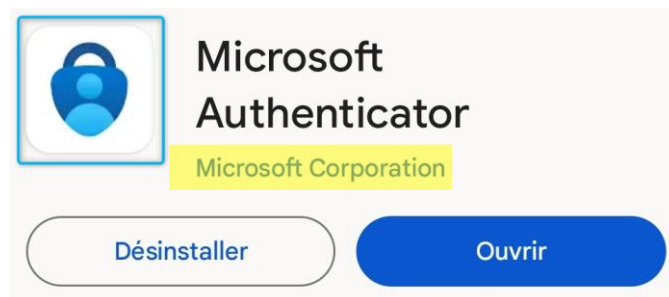




Vous aurez dès lors accès à la section « informations de sécurité ».

Etape 2 : Télécharger l'application MS Authenticator

Munissez-vous de votre GSM et installez l'application « **Microsoft Authenticator** » via le PlayStore (pour Android) ou l'AppStore (pour iPhone).



Important : vérifier bien qu'il s'agit de « Microsoft Authenticator » par Microsoft et non une autre application (certaines applications ont un logo très similaire, restez vigilant !)

Pour faciliter le téléchargement de l'application MS Authenticator (et vous assurer que c'est l'application correcte), vous pouvez scanner un de ces codes QR en fonction du type de smartphone que vous possédez. Ceci vous amènera directement sur la page de téléchargement de l'application.



Android
iPhone

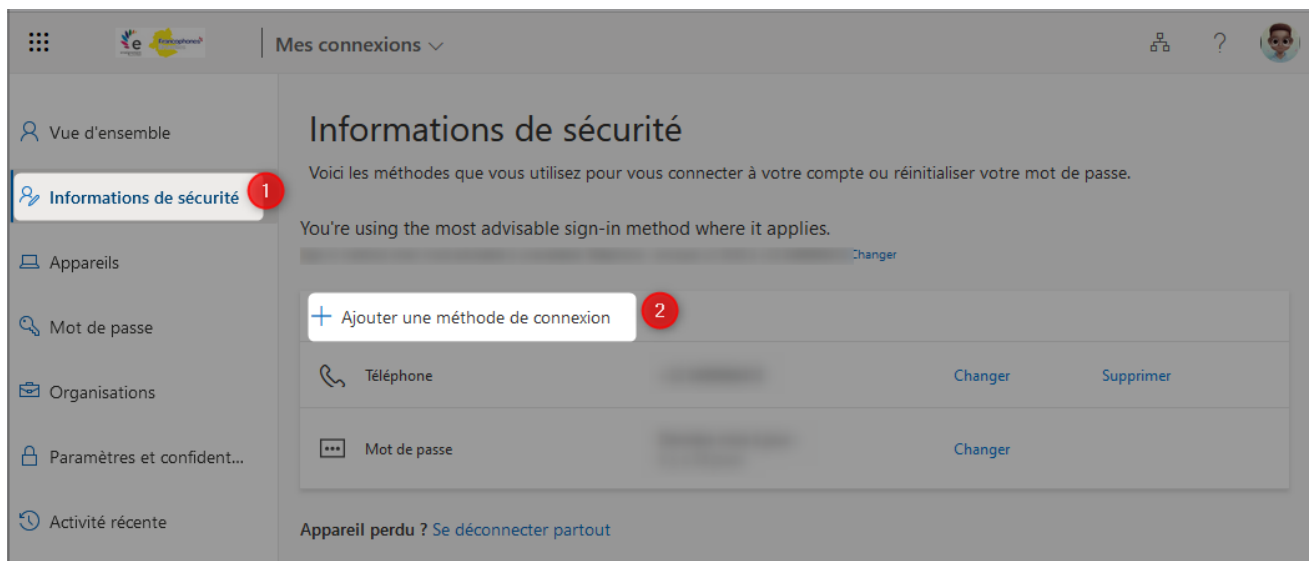


Une fois que l'application sera installée sur votre GSM vous pouvez passer à l'étape suivante.

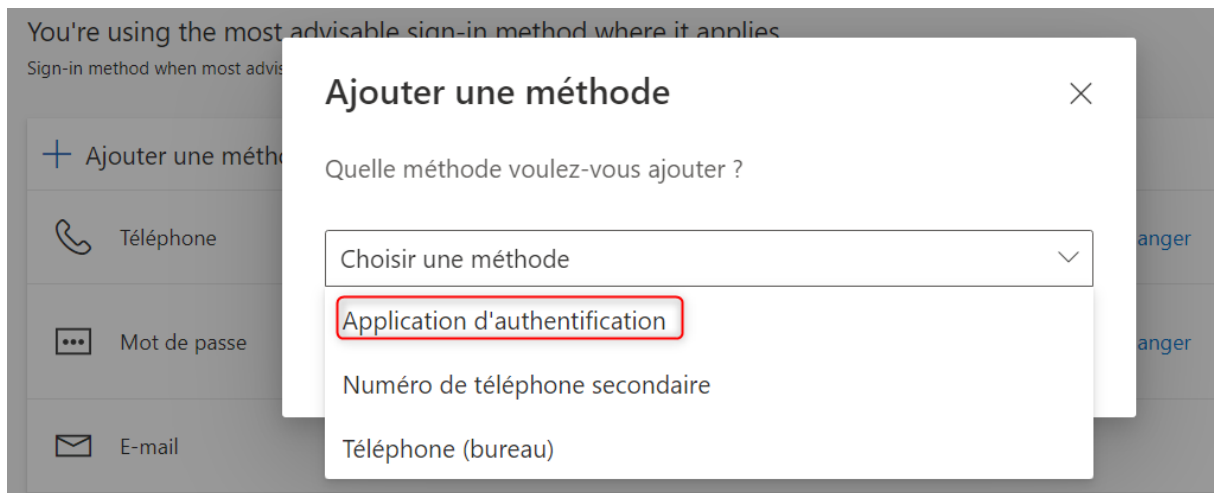
Etape 3 : configuration du MFA

A ce stade vous devriez avoir l'application « MS authenticator » installée sur votre GSM, et avoir la page « informations de sécurité » sous les yeux sur votre PC (voir étape 1).

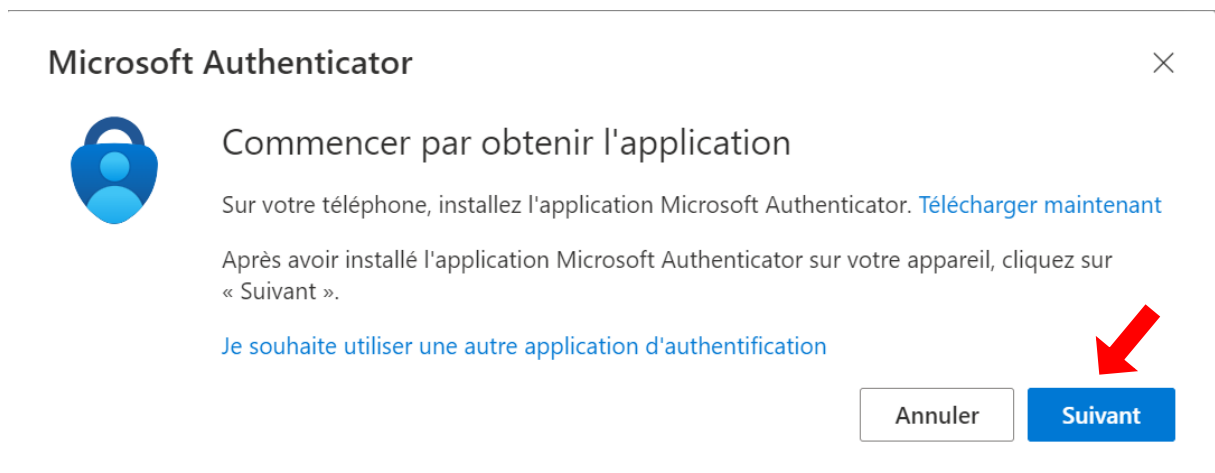
Pas 1 : Cliquez sur "Ajouter une méthode de connexion"



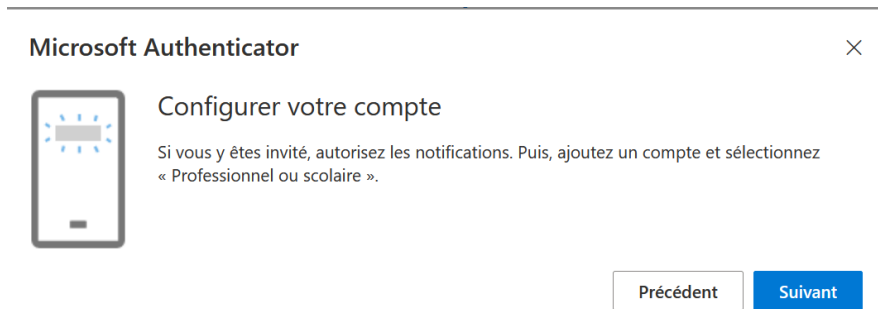
Pas 2 : Sélectionnez "**Application d'authentification**". Et confirmez votre choix en cliquant sur « **Ajouter** ».



Pas 3 : Vous aurez ensuite ce petit écran qui s'affiche qui vous guidera pour l'installation et la configuration de l'outil. Si vous avez suivi l'étape 2 correctement, l'application « Microsoft Authenticator » devrait être déjà installée sur votre GSM et pouvez dès lors cliquer sur « **suivant** ».

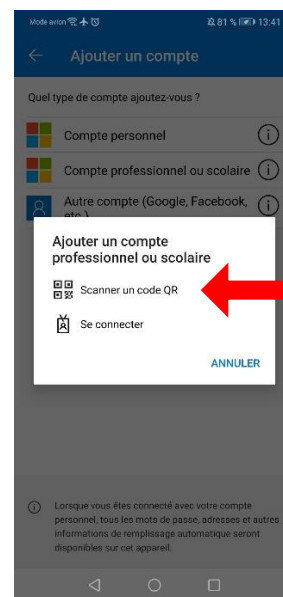
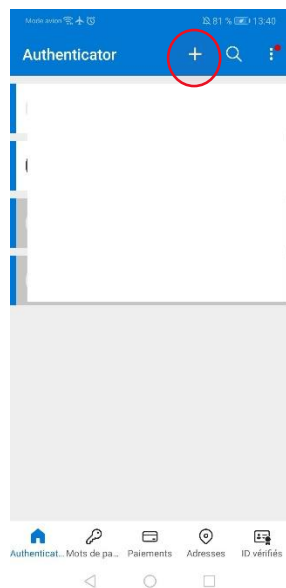


Pas 4 : Vous serez alors présentés avec cet écran qui s'affiche :



Il est temps de vous munir de votre GSM et d'ouvrir l'application « MS authenticator » que vous aurez installé au préalable (voir étape 2 plus haut).

Une fois l'application démarrée, cliquez sur le bouton « + » en haut à droite de l'écran. Indiquez ensuite « **Compte professionnel ou scolaire** » et finalisez par « **Scanner un code QR** ».

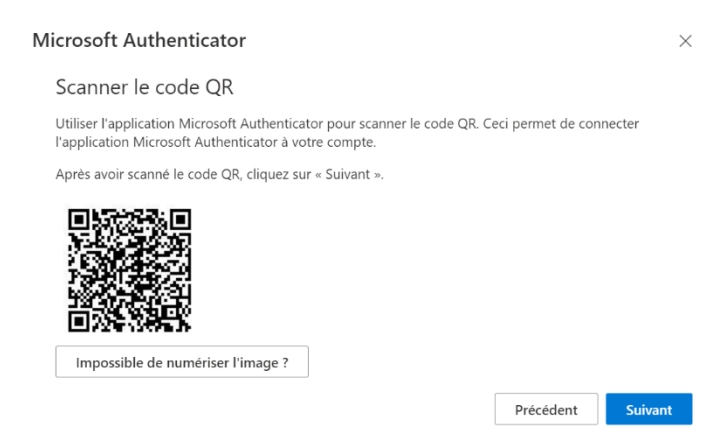


Note : Il est probable qu'à ce stade l'application MS Authenticator vous demande accès à votre camera, ceci est normal. En effet, sans accès à la caméra, vous ne pourrez pas scanner le code QR pour lier l'application à votre compte. Vous pouvez cliquer sur « seulement cette fois ci » si cela vous rassure.

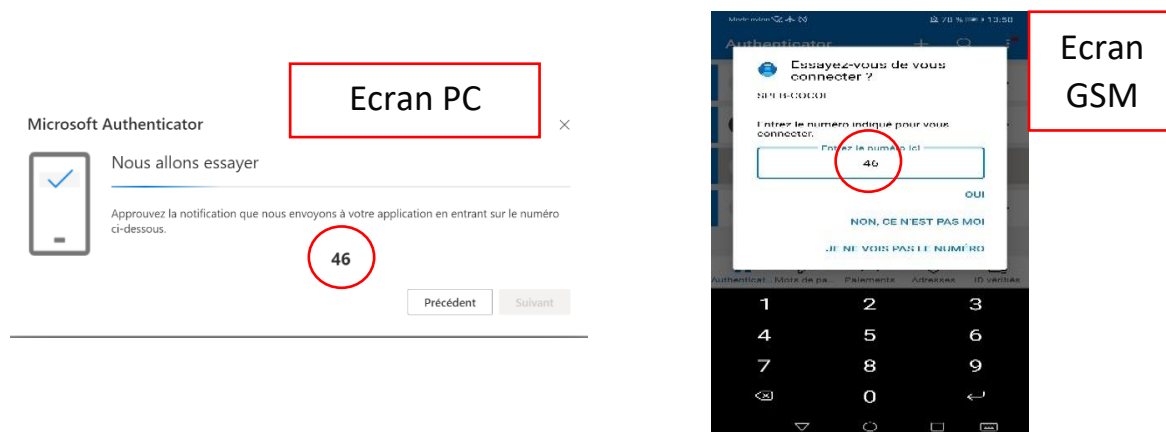
Une fois que votre GSM est prêt pour scanner le QR, vous pouvez revenir sur l'écran du PC, et cliquer sur « **suivant** » :



Pas 5 : Vous verrez alors un petit écran avec un code QR. Vous pouvez alors le scanner avec votre GSM (via l'application « MS Authenticator ») (voir pas 4)

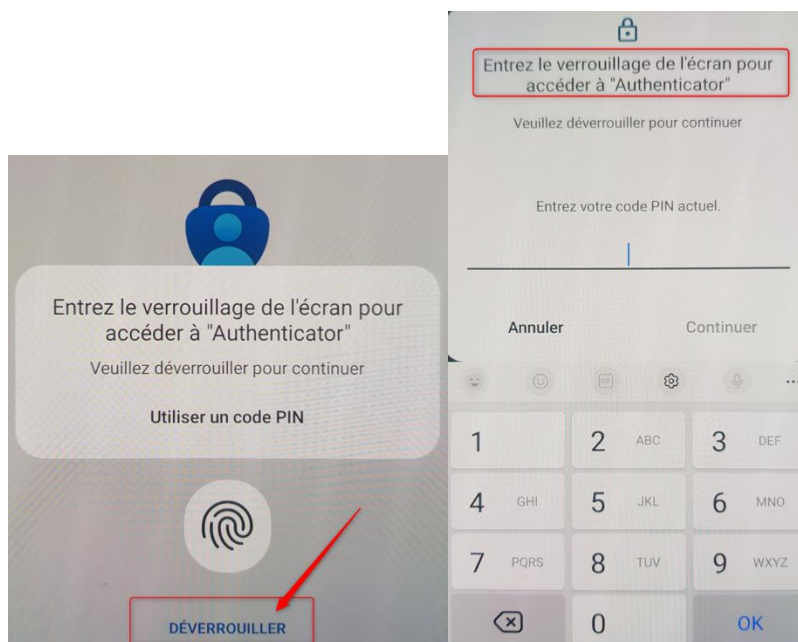


Pas 6 : Attendez la fin de l'activation. Vous aurez ensuite un écran qui s'affiche sur votre PC avec un chiffre. Toujours muni.e de votre GSM, indiquez sur l'application « MS Authenticator » le code généré à l'écran de votre PC.

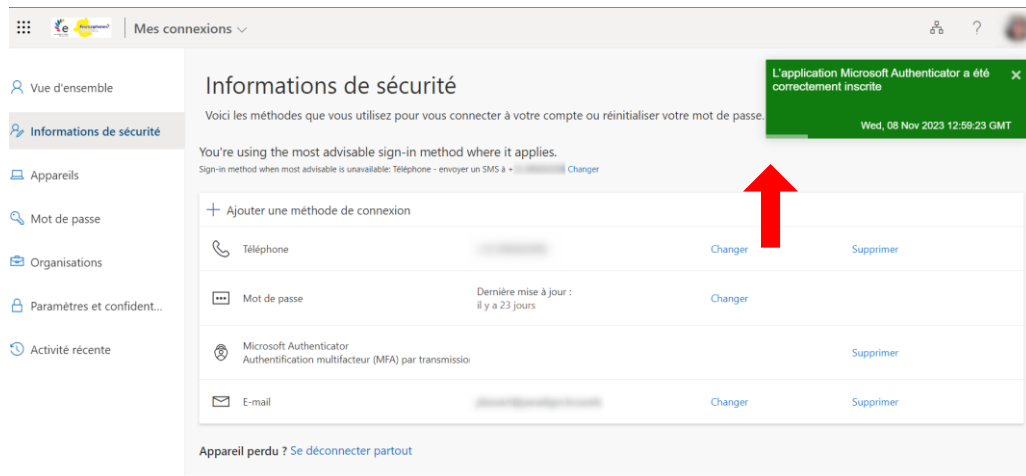


Terminez par cliquer sur « **Suivant** ».

Note : si vous avez un *code de verrouillage sur votre GSM* il est possible que l'application « MS Authenticator » vous demande de l'introduire afin de confirmer que vous êtes bien le propriétaire de ce GSM.

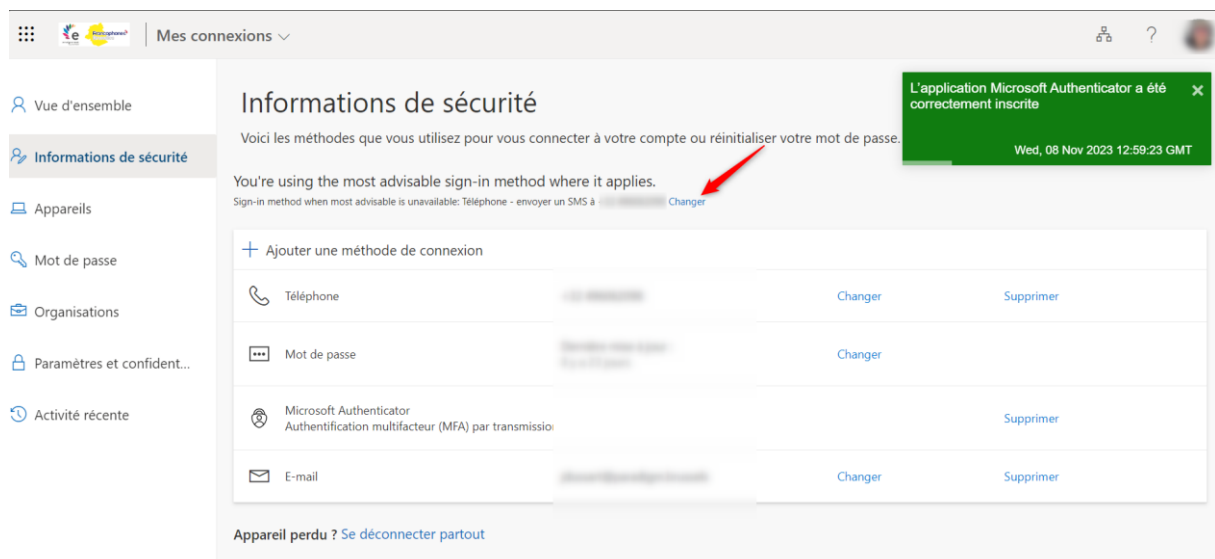


Pas 7 : Félicitations ! L'application est à présent configurée sur votre profil école.



Étape 4: favoriser l'application Microsoft Authenticator sur les autres méthodes

Pour finaliser cette procédure, sur votre PC, il faut à nouveau se rendre dans la partie « **Information de sécurité** » et définir la « **Méthode de connexion par défaut** » en appuyant sur le bouton « **Changer** ».



Dans la liste déroulante, veuillez sélectionner « **Authentification basée sur l'application – notification** » et ensuite « **Confirmez** ».

Cette modification vous permet d'être notifié.e via l'application « Microsoft Authenticator » lorsque quelqu'un essaie de se connecter à votre compte de l'école depuis un autre appareil que le vôtre ou lorsque vous devrez effectuer le MFA vous-même. Vous n'aurez qu'à cliquer sur la notification. À ce moment-là, il vous suffit de confirmer l'accès si vous êtes la personne qui tente de se connecter, ou de refuser l'accès si vous ne reconnaissez pas l'activité.

Conseils :

Assurez-vous de configurer le MFA sur un appareil de confiance.

Gardez vos informations de contact à jour pour recevoir les codes de vérification.

En cas de perte ou vol de votre appareil avec le MFA installé dessus, contactez votre secrétariat au plus vite.