

Comment configurer l'authentification à facteurs multiples



01 Introduction

L'activation de l'authentification à facteurs multiples (MFA) est une recommandation courante de Microsoft pour la protection des comptes. L'objectif est de rendre encore plus difficile l'usurpation de comptes Microsoft.

Le fonctionnement est simple, lors de la connexion au compte, il faut entrer son adresse mail, son mot de passe et un code unique obtenu par un autre moyen (via une application spécifique sur le smartphone ou via un SMS par exemple). Cette étape supplémentaire n'est pas systématiquement nécessaire : en effet, lorsque vous utilisez vos appareils habituels, la vérification est effectuée une seule fois au début et n'est plus redemandée que tous les 60 jours.

Par contre, la connexion à votre compte Microsoft depuis un nouveau périphérique nécessite la validation en encodant le code supplémentaire obtenu.

Prérequis

La méthode d'authentification supplémentaire que le service informatique vous conseille est l'utilisation d'**une application d'authentification** comme Google Authenticator, Microsoft Authenticator ou Authy.

Si **vous disposez déjà d'une telle application**, vous pouvez passer à l'étape Configuration ci-dessous, nous ajouterons le compte HELMo directement dans votre application préexistante.

Si **vous ne disposez pas de ces applications**, nous vous conseillons d'installer Microsoft Authenticator qui est disponible sur Android (Play Store) et Apple (App Store).



Android



Apple

go.microsoft.com/fwlink/p/?LinkId=722778 go.microsoft.com/fwlink/p/?LinkId=722779

Configuration

Nous procédons aux activations MFA par étape. A un moment donné, la connexion à votre compte Microsoft nécessitera d'accomplir les étapes suivantes :

1. Apparition de la fenêtre suivante :



votreadresse@student.helmo.be

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](#)

1. En cliquant sur « Suivant », la fenêtre suivante apparaît :

Protéger votre compte

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](#)

1

[Suivant](#)

[Je veux configurer une autre méthode](#)


SMS

Si vous avez installé une application d'authentification, vous pouvez cliquer sur le lien mentionné « Je souhaite utiliser une autre application d'authentification » (qui fonctionne pour Microsoft Authenticator, Google Authenticator, ...). Si vous ne disposez pas d'un smartphone, il est possible d'encoder votre numéro de téléphone pour recevoir un code par SMS.

1. La fenêtre suivante apparaît alors :

Protéger votre compte

Application d'authentification



Configurer votre compte

Dans votre application, ajoutez un nouveau compte.

PrécédentSuivant

[Je veux configurer une autre méthode](#)

Il faut alors simplement cliquer sur Suivant

1. Le code QR apparaît sur la fenêtre suivante :


Protéger votre compte

Application d'authentification

Scanner le code QR

Utiliser l'application d'authentification pour scanner le code QR. Ceci permet de connecter votre application d'authentification 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](#)

Il faut, ouvrir l'application d'authentification, et dans celle-ci, ajouter un compte (personnel s'il est demandé) et choisir Scanner un code QR. Présentez ensuite l'appareil photo de votre téléphone en regard de ce code. Cela provoquera automatiquement l'ajout du code dans l'application.

1. Etape de validation, la fenêtre suivante apparaît :

Protéger votre compte

Application d'authentification



Entrer le code

Entrez le code à 6 chiffres affiché dans l'application d'authentification.

Entrer le code

[Je veux configurer une autre méthode](#)

Dans votre application d'authentification, si le code de 6 chiffres ne s'affiche pas directement, choisissez le compte ajouté et le code apparaîtra. Il faut entrer le code dans l'interface pour valider le l'installation est bien fonctionnelle.

1. La configuration est alors terminée

Protéger votre compte

Opération réussie

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

Méthode de connexion par défaut :



Application d'authentification

Terminé