HELMo
Haute Ecole
Libre Mosane

# Mes identifiants

Toutes les informations entourant vos identifiants HELMo sont reprises ici.

# Obtenir mes identifiants lors de mon arrivée à HELMo

Comment obtenir mes identifiants numériques lors de mon arrivée à HELMo?

## Pour les nouveaux étudiants

Après la validation de votre inscription et le paiement de votre acompte d'inscription, vous recevrez automatiquement vos identifiants HELMo et Microsoft sur l'adresse e-mail privée que mentionnée lors de votre inscription.

L'envoi des identifiant peut prendre jusqu'à 24h. Si vous payez vos frais d'inscription par virement bancaire, un délai de plusieurs jours peut s'ajouter ; ce délai comprend la réception de votre paiement, son traitement par le service financier et le traitement par le système informatique.

En cas de problème, adressez vous directement au secrétariat de votre institut.

## Pour les nouveaux membres du personnel

Après la signature de votre contrat, vous obtiendrez vos identifiants HELMo et Microsoft auprès de la personne relai de votre institut.

# Quelle est la durée de validité de mes identifiants HELMo?

Vos identifiants HELMo et Microsoft sont valides tout au long de votre cursus ou de la durée de votre contrat.

Hors circonstance particulière, vos identifiants HELMo et Microsoft **restent valides 6 mois* après la fin de votre cursus ou de votre contrat** afin de vous laisser le temps nécessaire pour récupérer vos données telles que vos fichiers, e-mails et attestations. Passé ce délai, votre compte sera automatiquement et définitivement désactivé ; plusieurs notifications vous parviendront pour vous en avertir.

* Certaines licences spécifiques seront désactivées avec effet immédiat.

> **Attention aux spams :** soyez vigilant, nous ne vous demanderont **jamais** de confirmer quoi que ce soit à propos de votre compte ou d'éviter une prétendue suppression en cliquant sur un lien reçu par e-mail.
> En cas de doute sur la légitimité d'un e-mail, vérifiez ou contactez le service informatique.

# Mot de passe perdu et problèmes de MFA

**Lisez ceci pour éviter le blocage de votre compte après un changement de mot de passe :**
Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

01

02

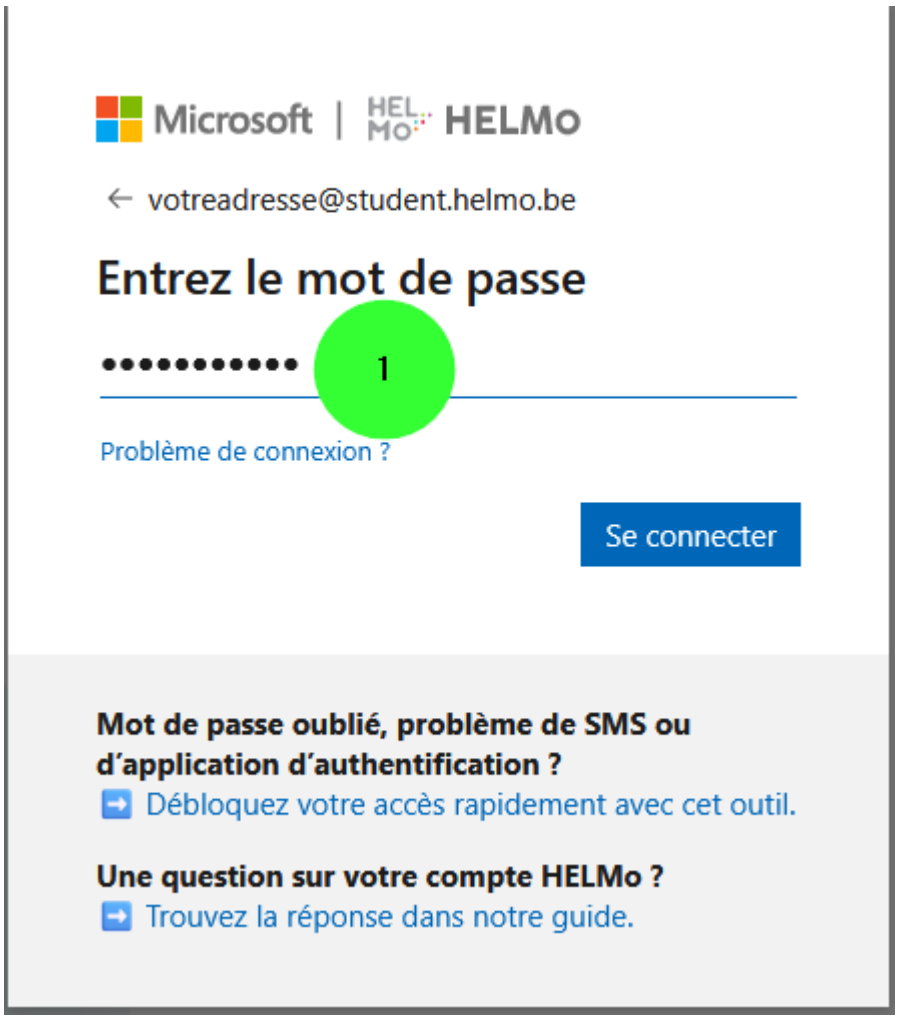
## Qu'est-ce que le MFA ?

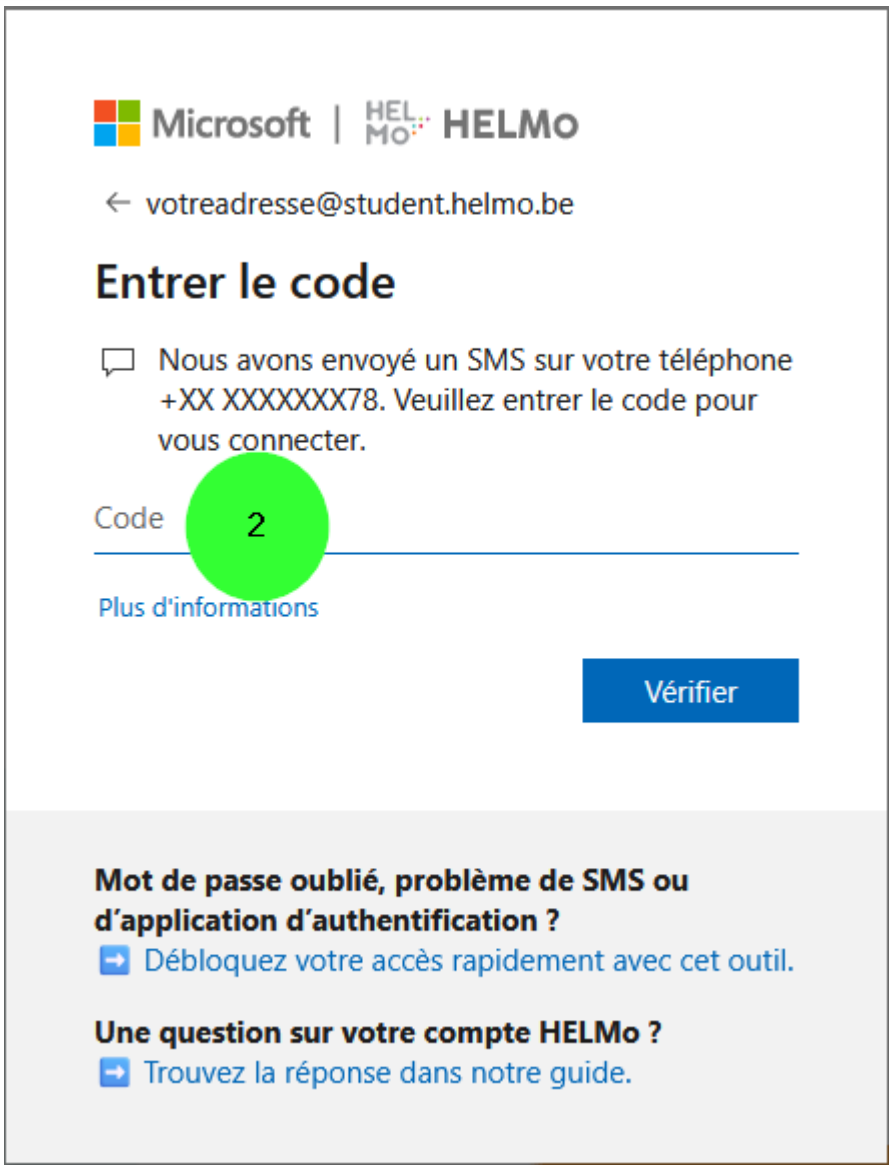
Le **MFA** (ou **authentification multifactorielle**) est une méthode utilisée pour **renforcer la sécurité de votre compte (pour le moment, uniquement la partie Microsoft)**.

Plutôt que de vous connecter uniquement avec votre **mot de passe**, Microsoft vous demande **une deuxième preuve** que c'est bien vous. Cela permet de mieux protéger vos informations personnelles.

Par exemple, après avoir encodé votre adresse e-mail HELMo :

- Vous entrez d'abord votre **mot de passe** (c'est la première étape).
- Ensuite, on vous demande un **code envoyé par SMS** ou généré par une **application d'authentification** (deuxième étape).


Microsoft | HELMo
votreadresse@student.helmo.be
Entrez le mot de passe
1
Problème de connexion ?
Se connecter
Mot de passe oublié, problème de SMS ou d'application d'authentification ?
Débloquez votre accès rapidement avec cet outil.
Une question sur votre compte HELMo ?
Trouvez la réponse dans notre guide.




C'est un peu comme **ajouter une deuxième serrure à votre porte** : même si quelqu'un connaît votre mot de passe, il ne pourra pas accéder à votre compte sans ce second élément, ce qui permet de limiter très fortement les risques de piratages.

Deux options sont proposées pour valider la seconde étape d'authentification :

- **Par SMS** : un code est envoyé à votre numéro de téléphone enregistré dans le système. Vous devez donc avoir accès à ce numéro au moment de la connexion.

- **Par application d'authentification** (comme Microsoft Authenticator, Authy ou Google Authenticator) :
  Il existe deux modes de fonctionnement selon l'application utilisée :
    - **Code à usage temporaire** : l'application génère un code qui change toutes les X secondes. Ce code doit être saisi lors de la connexion.
    - **Validation par notification** : une demande de connexion s'affiche dans l'application. Un numéro apparaît à l'écran de connexion et doit être saisi dans l'application pour valider l'accès.

- Vous rencontrez un problème avec votre mot de passe, rendez-vous **ici**.
- Vous n'avez plus accès à votre seconde méthode MFA, rendez-vous **ici**.
- Vous souhaitez configurer le MFA pour la première fois, redez-vous **ici**.

## J'ai perdu mon mot de passe HELMo et/ou Microsoft

### Obtenir un nouveau mot de passe en ligne

**Prérequis si vous êtes membre du personnel :**
1) Vous devez posséder un contrat de travail en cours d'exécution afin que votre compte HELMo soit actif.
2) Vous devez préalablement avoir renseigné une adresse e-mail privée pour permettre à nos services de vous envoyer un lien éphémère pour la création d'un nouveau mot de passe. Les membres du personnel peuvent renseigner cette donnée auprès du service des ressources humaines.

**Prérequis si vous êtes étudiant :**
1) Vous devez posséder une inscription valide à un cursus HELMo
2) Vous devez préalablement avoir renseigné une adresse e-mail privée pour permettre à nos services de vous envoyer un lien éphémère pour la création d'un nouveau mot de passe. Les étudiants peuvent renseigner cette donnée auprès du secrétariat de leur institut.

**Procédure de réinitialisation de votre mot de passe en ligne :**

Si vous rencontrez les prérequis énumérés ci-dessus, en cas de perte de votre mot de passe HELMo ou Microsoft, vous pouvez en définir un nouveau en vous rendant sur cette page : https://mon-espace.helmo.be/MotDePassePerdu/DemandeModifierMotDePasse

## Obtenir un nouveau mot de passe en institut

Le helpdesk informatique ne transmet pas de nouveau mot de passe.

Pour obtenir un nouveau mot de passe dans le cas où la récupération de mot de passe en ligne ne fonctionne pas, vous devez rencontrer une personne référente de façon à ce qu'elle puisse vous identifier et procéder au changement de mot de passe.

**Les étudiants** doivent s'adresser directement au secrétariat de leur institut.

**Les membres du personnel** peuvent s'adresser à la personne relai sur site.

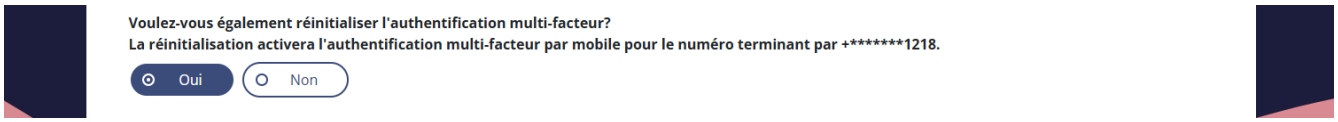
## Je souhaite modifier mon mot de passe HELMo et/ou Microsoft

Vous avez la possibilité de modifier votre mot de passe HELMo via le bouton "Mot de passe et sécurité" dans votre menu personnel sur la plateforme Mon Espace, soit directement via ce lien : https://mon-espace.helmo.be/ChangementMotDePasse/Employe/Index

## J'ai perdu mon moyen d'authentification multi-facteurs (MFA) Microsoft

Pour réinitialiser vos paramètres MFA, pour des raisons de sécurité, vous devez impérativement commencer par modifier votre mot de passe. Pour ce faire, suivre la procédure **"J'ai perdu mon mot de passe HELMo et/ou Microsoft"** **en veillant bien à suivre les instructions ci-après** :

Lors de cette procédure, après la réception de l'e-mail de réinitialisation de votre mot de passe, une option vous permettra de réinitialiser votre MFA :




Votre MFA sera réinitialisé avec les données que vous avez fournies au secrétariat lors de votre inscription ou au service GRH lors de la signature de votre contrat. Si ces données ne sont plus à jour, veuillez les contacter.

# Mauvais numéro de téléphone lié à mon compte Microsoft

le numéro de téléphone lié a votre compte Microsoft est le numéro que vous avez donné a l'administration de la Haute École lors de votre arrivée. Vous pouvez le consulter sur la page de votre profil dans mon espace.

Si le numéro de téléphone lié au compte Microsoft n'est pas ou plus correct, il est nécessaire de demander de le modifier.

- **Les étudiants** doivent s'adresser directement au secrétariat de leur institut.
- **Les membres du personnel** peuvent s'adresser à la personne relai sur site.

> Pour des raisons de sécurité, il est impératif de se présenter physiquement, toute demande de modification de numéro de téléphone par mail ou téléphone sera refusée.

**Une fois le numéro modifié**, vous pouvez directement réinitialiser votre mot de passe en prenant soins de cocher les deux options suivantes :

- "Oui" pour la réinitialisation du multi-facteur
- "Oui" pour la modification du mot de passe Microsoft

Le compte sera alors directement opérationnel, et le code de double authentification sera envoyé au nouveau numéro de téléphone.

> Le numéro de téléphone affiché dans le profile peut prendre 24h à se mettre à jour.

# 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.

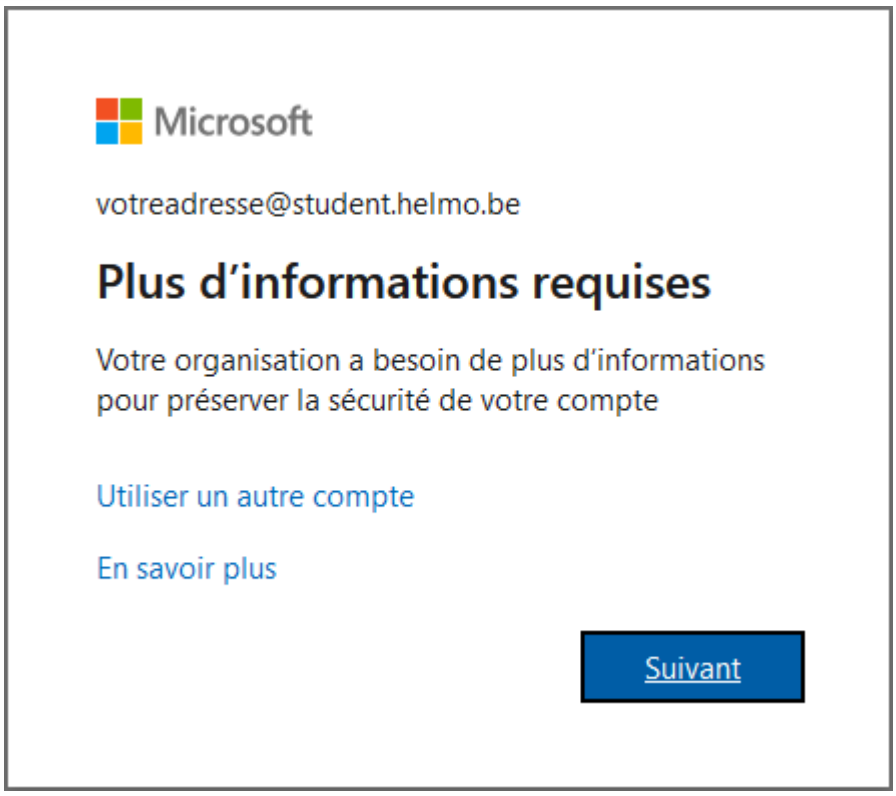
Si **vous ne disposez pas de ces applications**, nous vous conseillons d'installer Microsoft Authenticator qui est disponible sur Android (Play Store) et Apple (App Store).

| | |
|---|---|
| Android<br>go.microsoft.com/fwlink/p/?LinkId=722778 | Apple<br>go.microsoft.com/fwlink/p/?LinkId=722779 |

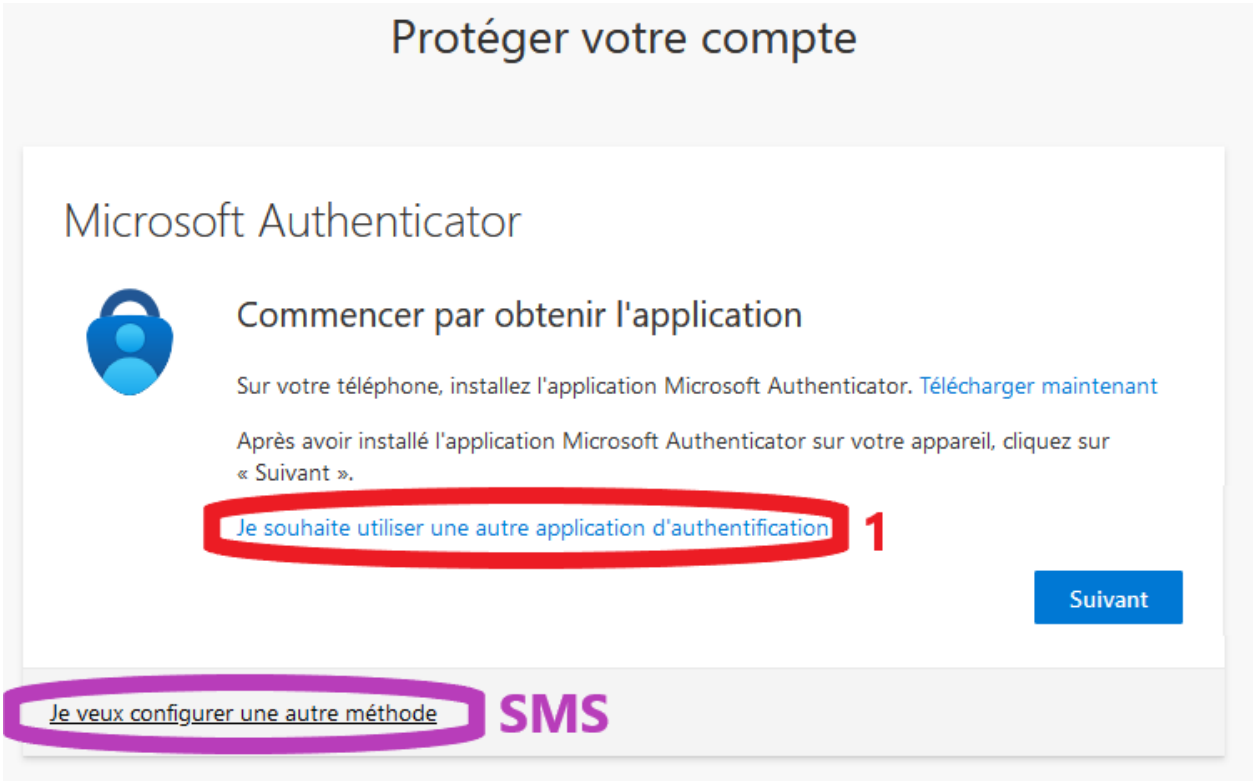
## Configuration

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 :

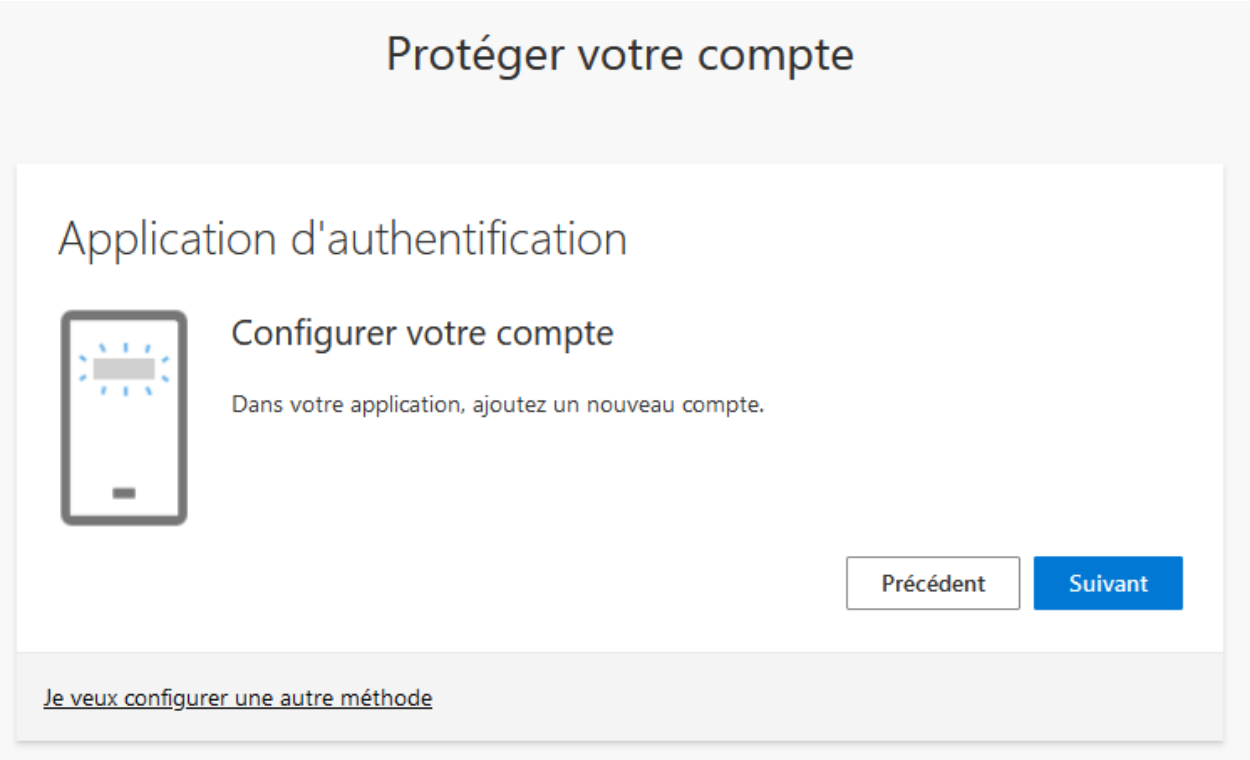



1. En cliquant sur « Suivant », la fenêtre suivante apparaît :



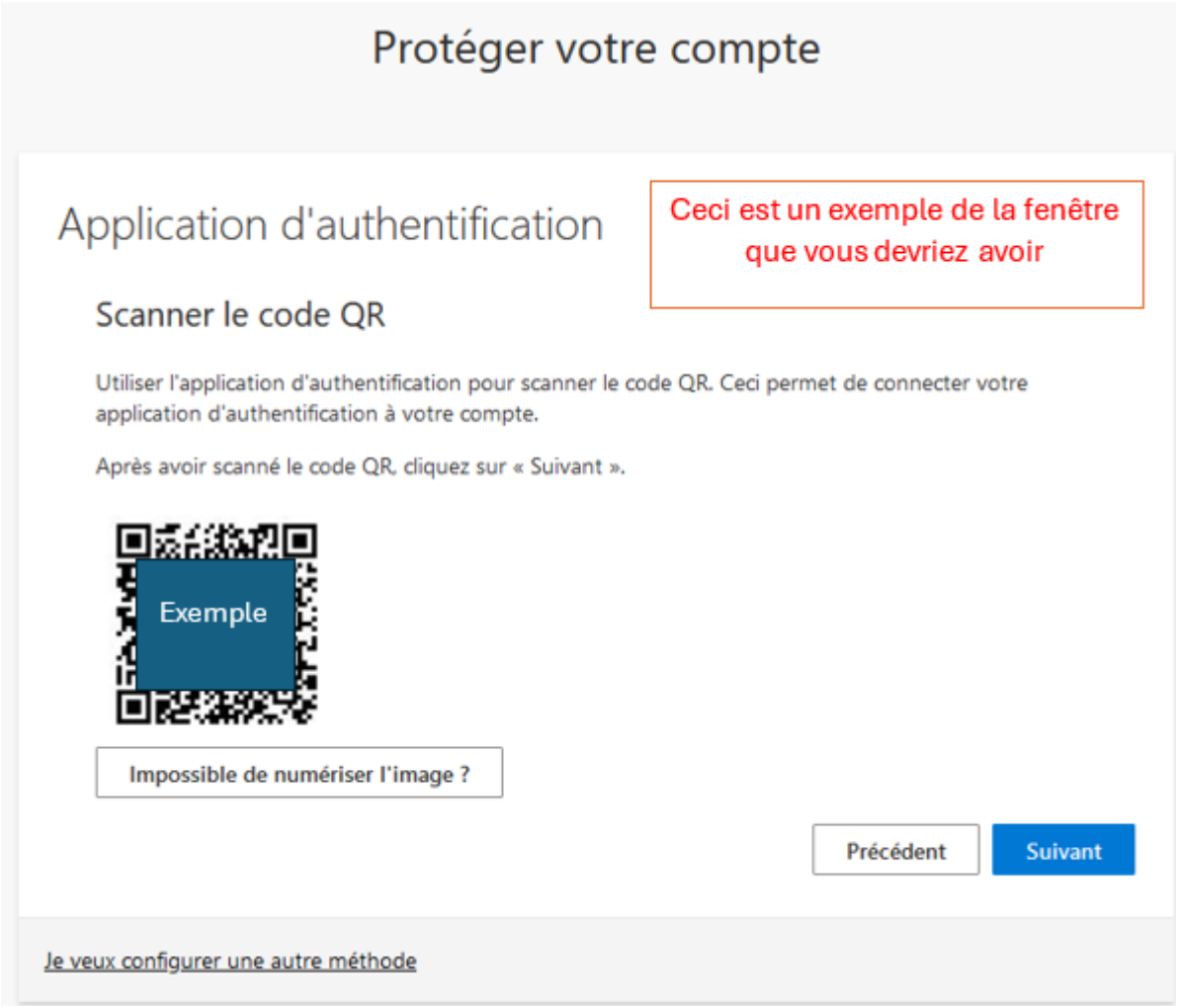
Si vous avez installé une application d'authentification, vous pouvez cliquer sur le lien mentionné « Je souhaite utiliser une autre application d'authentification » (qui fonctionne pour Microsoft Authenticator, Google Authenticator, ...). Si vous ne disposez pas d'un smartphone, il est possible d'encoder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

1. La fenêtre suivante apparaît alors :



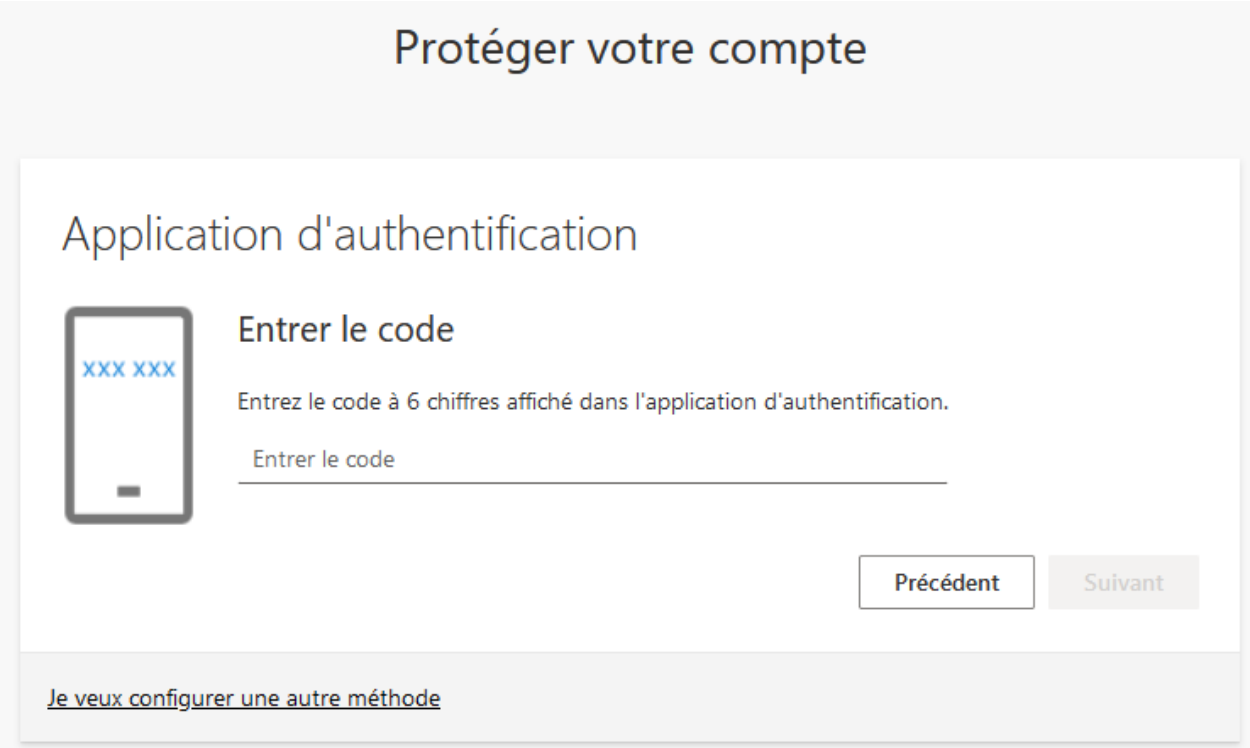
Il faut alors simplement cliquer sur Suivant

1. Le code QR apparaît sur la fenêtre suivante :



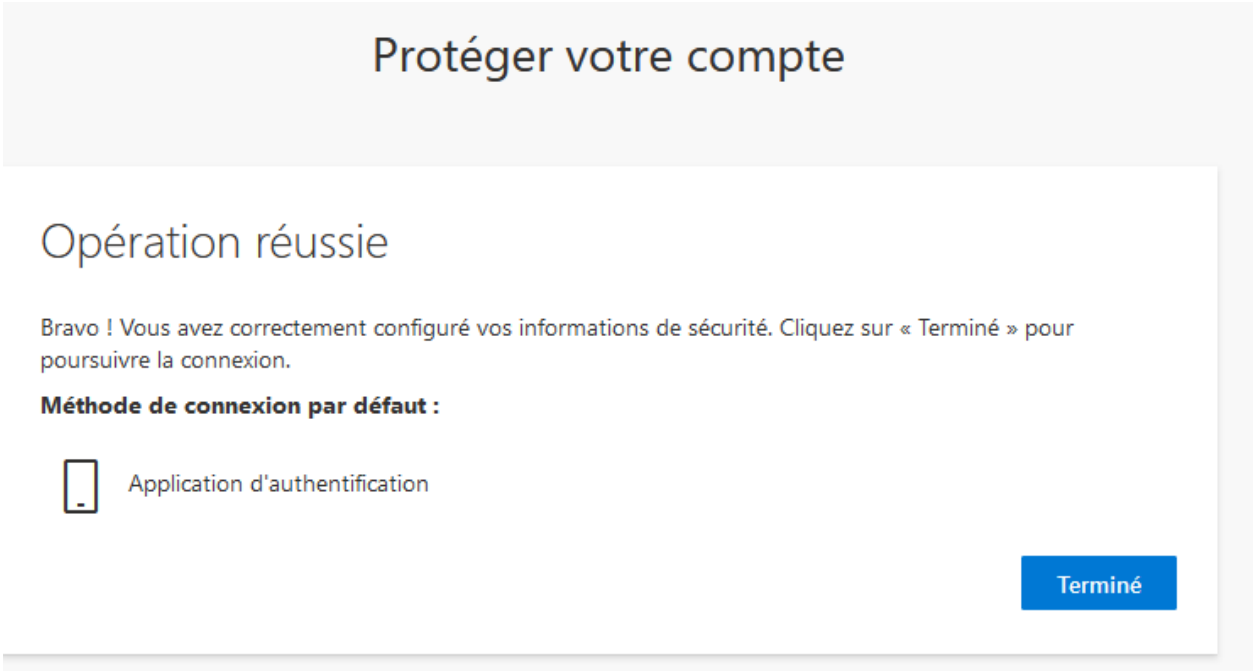
Il faut, ouvrir l'application d'authentification, et dans celle-ci, ajouter un compte (personnel s'il est demandé) et choisir Scanner un code QR. Présentez ensuite l'appareil photo de votre téléphone en regard de ce code. Cela provoquera automatiquement l'ajout du code dans l'application.

1. Etape de validation, la fenêtre suivante apparaît :



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



# Erreurs pendant ou après l'authentification

Retrouvez ici les erreurs d'authentification les plus récurrentes ainsi que les solutions pour les résoudre.

## Erreur "Bad Request - Request Too Long" après authentification

Il est possible que vous rencontriez le message d'erreur suivant après l'authentification sur l'une de nos plateforme :

```
Bad Request – Request Too Long
HTTP Error 400. The size of the request headers is too long.
```

Ce message survient lorsque votre cookie de session dépasse la taille maximale autorisée. Cela peut être consécutif d'une mise à jour sur la plateforme ou d'un problème lors du nettoyage des cookies par le navigateur.

Pour corriger ce problème, nous vous recommandons de supprimer les cookies faisant références aux sites HELMo suivants :
- mon-espace.helmo.be
- sso1.helmo.be

## Erreur "FatalProfileException" après l'authentification

Il arrive que vous rencontriez le message ci-dessous en tentant de vous authentifier sur une plateforme HELMo. **Ce message indique que votre réseau est configuré pour utiliser plusieurs adresses IP différentes lorsque vous naviguez sur internet.** Cette règle peu commune peut être configurée au niveau de votre fournisseur d'accès, au niveau du réseau de l'établissement dans lequel vous vous trouvez ou encore tout simplement au niveau du périphérique que vous utilisez pour vous connecter.

Par sécurité, notre système d'authentification bloque l'utilisation d'adresses multiples lors du processus d'authentification car elle peut être liée à une attaque informatique. Il est possible qu'un tiers tente d'usurper votre identité en interceptant vos requêtes Web et en les substituant par les siennes.

Pour résoudre le problème, il faut d'abord en identifier la provenance. Commencez par lancer une analyse anti-virus. Essayez ensuite de vous connecter avec un autre périphérique, ou avec le même périphérique depuis un autre réseau. Une fois que vous avez identifié la source du problème, tentez de savoir pourquoi cette règle est configurée et si c'est pertinent dans votre cas. Si ça ne l'est pas, il vaut mieux la désactiver. Dans le cas contraire, il faudra vous connecter à nos services depuis une autre source pour contourner le problème.

**Le message d'erreur :**

```
opensaml::FatalProfileException
```

```
The system encountered an error at Wed Jun 06 18:02:10 2018
To report this problem, please contact the site administrator at helpdesk@he

Please include the following message in any email:
opensaml::FatalProfileException at (https://www.helmo.be/Shibboleth.sso/SAML

Your client's current address (***.***.***.***) differs from the one used wh
```

## Parfois, je peux m'identifier et parfois cela ne fonctionne pas : blocage temporaire du compte

Pour des raisons de sécurité, nos systèmes bloquent automatiquement les comptes des utilisateurs lorsque plusieurs tentatives de connexion (au wifi, VPN, ou site HELMo) avec un mauvais mot de passe surviennent.

Les règles appliquées sont les suivantes : si j'effectue **5** tentatives de connexion infructueuses dans une période de **10** minutes, mon compte **sera bloqué automatiquement pour plusieurs minutes**.

Les conséquences du blocage sont :

- impossibilité de me connecter au Wifi.
- impossibilité de me connecter à Learn,
- impossibilité de me connecter à HELMo Connect,
- impossibilité d'utiliser l'application HELMo,
- impossibilité de me connecter en VPN (si une telle connexion est fournie par mon institut),

**Attention si vous avez changé votre mot de passe HELMo :**

Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

01

02

# Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

> **Attention : si vous avez changé votre mot de passe HELMo il est impératif de lire ceci pour éviter le blocage de votre compte !**

Pour des raisons de sécurité, nos systèmes bloquent automatiquement les comptes des utilisateurs lorsque plusieurs tentatives de connexion (au Wifi, VPN, ou site HELMo) avec un mauvais mot de passe surviennent.

Les règles appliquées sont les suivantes : si j'effectue **5** tentatives de connexion infructueuses dans une période de **10** minutes, mon compte **sera bloqué automatiquement pour plusieurs minutes**.

Les conséquences du blocage sont :

- impossibilité de me connecter au Wifi.
- impossibilité de me connecter en VPN (si une telle connexion est fournie par mon institut),

Si vous avez modifié votre mot de passe et qu'un portable (téléphone ou ordinateur) tente de se connecter automatiquement avec l'ancien mot de passe, **il est probablement la cause du blocage de votre compte**.

Il faut, dans ce cas, réinitialiser les profils Wifi sur vos appareils mobiles (téléphone et portable). Si vous utilisez l'application HELMo, il faut également se reconnecter.

- Pour supprimer le **profil wifi sous Windows**, vous pouvez consulter la vidéo suivante.
- Pour supprimer le **profil wifi sous MacOS**, vous pouvez consulter la vidéo suivante.
- Pour supprimer le **profil wifi sous Android**, vous pouvez consulter la vidéo suivante.

# Garder mes identifiants en sécurité

Quelques réflexes simples pour protéger vos identifiants et réagir en cas de piratage.

## 1. Repérez les faux sites

N'entrez **jamais** votre mot de passe HELMo si l'une de ces conditions n'est pas remplie :

- L'adresse se termine exactement par **.helmo.be** ou est **login.microsoftonline.com** (ex. : sso1.helmo.be, learn.helmo.be, webmail.helmo.be)
- La page est en **https** (cadenas dans la barre d'adresse)

La plupart des faux liens arrivent par e-mail : apprenez à reconnaître un e-mail frauduleux.

⚠ Vous avez entré votre mot de passe sur un site douteux ? Changez-le immédiatement.

## 2. Utilisez un gestionnaire de mots de passe

La règle : **un mot de passe long et unique par service**. Un gestionnaire de mots de passe le crée, le retient et le remplit pour vous. Vous n'avez plus qu'**un seul mot de passe maître** à retenir.

**KeePassXC** : gratuit, open-source, vos données restent chez vous

- Ordinateur (Windows, macOS, Linux) : keepassxc.org
- Android : KeePassDX
- iPhone : KeePassium

Astuce : placez votre fichier coffre-fort sur OneDrive pour l'ouvrir depuis tous vos appareils.

**Bitwarden** : le plus simple, synchronisé automatiquement

- Version web : vault.bitwarden.eu
- Applications et extensions navigateur : bitwarden.com/download

⚠ Le mot de passe maître ne peut pas être récupéré : choisissez une phrase longue et ne l'oubliez pas.

## 3. Activez l'authentification multifacteur (MFA)

Avec le MFA, un pirate qui vole votre mot de passe ne peut quand même pas se connecter : il lui manque le code de votre téléphone. C'est la protection la plus efficace contre le piratage.

- Activez-le **partout** : messagerie, réseaux sociaux, banque, cloud…
- Préférez une **application** aux SMS, moins sûrs :
  - **Microsoft Authenticator** (recommandé pour HELMo) : Android · iPhone
  - **Google Authenticator** : Android · iPhone
  - **Authy** : Android · iPhone

⚠ **Activez la sauvegarde de votre application MFA** : sans sauvegarde, perdre ou changer de téléphone peut vous bloquer l'accès à tous vos comptes.

- Microsoft Authenticator : Paramètres › Sauvegarde (compte Microsoft personnel ou iCloud)
- Google Authenticator : connectez-vous à votre compte Google dans l'application
- Authy : Paramètres › Comptes › Sauvegardes

À HELMo, le MFA est **obligatoire et activé par défaut**. Vous avez changé de téléphone sans sauvegarde ? Consultez Mot de passe perdu et problèmes de MFA.

## 4. Vérifiez si vos données ont fuité

Même les grandes plateformes se font pirater (Adobe, Dropbox…). Vos identifiants circulent peut-être déjà chez les pirates.

Vérifiez votre adresse e-mail (HELMo et privée) et **inscrivez-vous aux alertes** :

- haveibeenpwned.com
- monitor.mozilla.org

Votre adresse apparaît ? **Changez le mot de passe** concerné, partout où vous l'avez utilisé.

## 5. Protégez votre ordinateur

### Windows

- Microsoft Defender est intégré et suffisant pour la plupart des usages. Vérifiez qu'il est bien actif.
- Windows 10 n'est plus mis à jour depuis octobre 2025 : passez à Windows 11.
- Vous préférez un autre antivirus ? Consultez les comparatifs AV-Test ou AV-Comparatives. N'installez **jamais deux antivirus** en même temps.

### macOS

- La protection est intégrée (XProtect, Gatekeeper) : aucun antivirus supplémentaire n'est nécessaire.
- Installez les mises à jour macOS dès qu'elles sont proposées.
- Installez vos applications depuis l'App Store ou le site officiel de l'éditeur.

### Linux

- Faites régulièrement les mises à jour via le gestionnaire de paquets de votre distribution.
- Installez vos logiciels depuis les dépôts officiels (ou Flathub), jamais via des scripts trouvés au hasard.

**Dans tous les cas** : gardez votre système à jour et n'installez que des logiciels de source fiable.

Un doute sur un PC Windows ? Faites-le analyser gratuitement par un second antivirus, sans rien désinstaller :

- ESET Online Scanner
- Trend Micro HouseCall

# Personnes relais

Qui contacter en cas de problème avec vos identifiants?

## Personnes relais des étudiants

Les secrétariats sont les points de contact des étudiants dans la gestion de leurs identifiants.

## Personnes relais des membres du personnel

Si vous êtes membre du personnel, les personnes relais des membres du personnel peuvent, selon votre département, vous assister dans la gestion de vos identifiants.

# Ajouter une méthode MFA (authentification multi-facteurs) Microsoft

## Introduction

Pour protéger efficacement votre compte, il est fortement recommandé de configurer plusieurs méthodes d'authentification en plus du mot de passe. Cela garantit que vous pourrez toujours accéder à votre compte même si une méthode devient indisponible (par exemple, perte ou inaccessibilité de votre téléphone, ou problème avec l'application d'authentification). Ce guide vous accompagne pas à pas pour ajouter ces méthodes supplémentaires et sécuriser votre compte de manière fiable.

## 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.

## Étapes à suivre pour ajouter une méthode d'authentification

1. Cliquez sur « Informations de sécurité » de votre profil Microsoft.
2. Ajoutez une nouvelle méthode de connexion. Il est recommandé de configurer au minimum :
    - **Microsoft Authenticator** (application mobile pour générer des codes)
    - **Téléphone** (pour recevoir des codes par SMS ou appel)

## Bonnes pratiques et conseils

- Entrez toujours vos numéros de téléphone au format international : **+XX XXXXXXXX** (exemple : +32 474999888).
- Pour l'application d'authentification, utilisez la méthode **TOTP** (Time-based One-Time Password) pour plus de compatibilité et de simplicité. Pour ce faire :
    - Sélectionnez "Microsoft Authenticator" comme méthode à ajouter
    - Ensuite, ne cliquez pas sur "suivant" , mais plutôt sur l'option « Je souhaite utiliser une autre application d'authentification ».
    - Suivez la procédure détaillée disponible ici.
- 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.