

Multi Factor Authentication (MFA) pour accéder à l'environnement client de Partena Professional – Manuel utilisateur

Sommaire

I. Qu'est-ce que la <i>MFA</i> et pourquoi est-elle importante ?	2
II. Quoi doit l'utiliser ? Quand l'activer ?	2
III. Comment procéder ?	2
1. Démarrage – Option A : Partena Authenticator	4
2. Démarrage – Option B : Microsoft Authenticator	11
3. Démarrage – Option C : Google Authenticator	14
IV. Comment gérer vos méthodes d'authentification (ajout / modification / suppression) ?	14
V. Comment résoudre un problème (<i>troubleshooting</i>) ?	15
VI. Besoin d'aide ?	15

I. Qu'est-ce que la MFA et pourquoi est-elle importante ?

La MFA *Multi Factor Authentication* (Authentification multifactorielle – MFA) ajoute une vérification supplémentaire à votre mot de passe (p. ex. par e-mail ou via une application). L'accès reste ainsi protégé, même si votre mot de passe tombe entre de mauvaises mains.

II. Qui doit l'utiliser ? Quand l'activer ?

- **Qui ?** Utilisateurs du portail client.
- **Quand ?** Lors de la connexion. Vous pouvez **reporter** l'activation à **1 reprise** au maximum ; à la 2^{ème}, la configuration sera **obligatoire**.
- **Prérequis :** votre smartphone, une connexion Internet et votre adresse e-mail.
- **Conseil :** utilisez votre adresse e-mail comme méthode de back-up (au cas où votre smartphone ne serait pas disponible).

III. Comment procéder ?

Vous avez le choix entre les 3 applications de vérification suivantes :

Partena Authenticator	Microsoft Authenticator (TOTP*)	Google Authenticator (TOTP*)
Authentification via un code QR à scanner	Code à 6 chiffres qui change toutes les 30 secondes	Code à 6 chiffres qui change toutes les 30 secondes

* **TOTP = Time-based One-Time Password (mot de passe à usage unique limité dans le temps) :** code à 6 chiffres généré par l'application et renouvelé toutes les 30 secondes.

Pourquoi installer une énième application sur mon GSM ?

Toutes les méthodes actuelles exigent que vous introduisiez un code en plus de votre mot de passe. Vous recevez ce code par e-mail ou par le biais d'applications connues.

Nous avons cherché à améliorer l'expérience utilisateur. Imaginez que vous n'ayez plus besoin **ni d'un mot de passe ni d'un code supplémentaire et que vous puissiez quand même vous connecter à vos applications en toute sécurité**. C'est désormais possible grâce à l'application d'authentification de Partena Professional. Après avoir associé l'application/appareil à votre compte, vous pouvez vous connecter simplement en **scannant le code QR avec l'application d'authentification de Partena Professional**. En d'autres termes, vous ne devrez plus introduire ni mot de passe, ni code à usage unique.

Est-ce sûr?

Ce mode de connexion est totalement sûr, étant donné que votre application/appareil est associé à votre compte. L'application est installée sur votre smartphone et vous recevez un élément (code QR) pour établir la connexion. Cela suffit pour satisfaire aux conditions *MFA*.

III. Comment utiliser la nouvelle application?

Installez la nouvelle application à partir de l'App Store



- iPhone : recherchez l'Authenticator app Partena Professional et installez-la sur votre appareil.
- Android : recherchez l'Authenticator app Partena Professional et installez-la sur votre appareil.

1. Démarrage – Option A : Partena Authenticator

1. Connectez-vous au portail. Le système affiche automatiquement l'écran **Activation MFA requise** lorsqu'aucune méthode n'a encore été configurée.



Partena
PROFESSIONAL

Activation MFA requise

Pour des raisons de sécurité, vous devez activer l'authentification multifacteur (MFA) pour votre compte.

Vous pouvez ignorer l'activation de MFA pour votre compte **un total de 1 fois**.

Activer MFA maintenant

[Ignorer l'activation MFA](#)

2. Le système vous demandera d'introduire le code d'accès que vous avez reçu par e-mail. Il s'agit de notre méthode de back-up.



Partena
PROFESSIONAL

Enregistrement d'un e-mail MFA

Saisissez le code d'accès à usage unique que vous avez reçu dans votre boîte mail pour enregistrer votre e-mail comme méthode MFA.

[Le code d'accès à usage unique a été renvoyé](#)

Terminer l'Enregistrement

[Annuler](#)

Cliquez sur Terminer l'enregistrement.

3. Si vous avez reçu le code d'accès, allez à l'étape 4. Votre adresse e-mail a été enregistrée avec succès comme méthode MFA.

Que faire si vous n'avez pas reçu le code d'accès ? Nous voyons 2 raisons possibles à cela.

- L'adresse e-mail connue dans notre système n'est plus correcte.
- L'adresse e-mail est correcte, mais vous ne retrouvez pas l'e-mail dans votre boîte de réception.

1. L'adresse e-mail est correcte, mais vous ne retrouvez pas l'e-mail.

Si vous n'avez pas reçu le code d'accès, cliquez sur « Renvoyer le code d'accès ».



Partena
PROFESSIONAL

Enregistrement d'un e-mail MFA

Saisissez le code d'accès à usage unique que vous avez reçu dans votre boîte mail pour enregistrer votre e-mail comme méthode MFA.

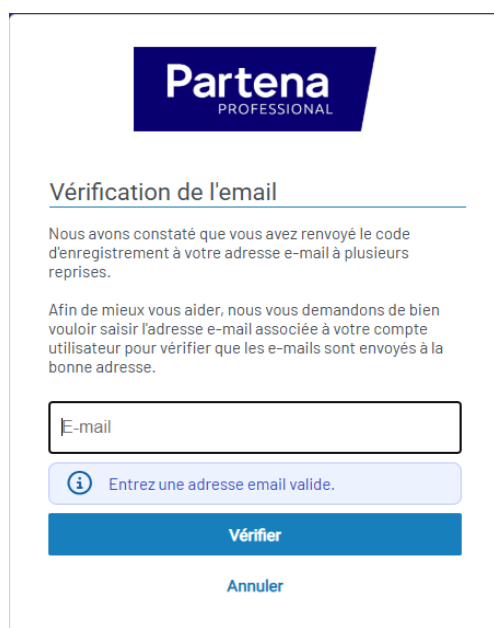
Code d'accès

[Renvoyer le code d'accès](#)

Terminer l'Enregistrement

[Annuler](#)

Si vous ne recevez pas de code d'accès dans votre boîte mail, vous pouvez demander à nouveau le code plusieurs fois. Ensuite, vous verrez l'écran suivant :



Partena
PROFESSIONAL

Vérification de l'email

Nous avons constaté que vous avez renvoyé le code d'enregistrement à votre adresse e-mail à plusieurs reprises.

Afin de mieux vous aider, nous vous demandons de bien vouloir saisir l'adresse e-mail associée à votre compte utilisateur pour vérifier que les e-mails sont envoyés à la bonne adresse.

E-mail

[Entrez une adresse email valide.](#)

Vérifier

[Annuler](#)

Nous vérifions ici si votre adresse e-mail correspond à celle enregistrée dans nos systèmes.

Si elle correspond, vous verrez alors l'écran suivant :



Partena
PROFESSIONAL

L'adresse e-mail correspond

Votre adresse e-mail est correcte, mais il semble que vous n'ayez pas reçu notre message. Veuillez vérifier votre dossier Spam/Indésirables.

S'il n'y figure pas, assurez-vous auprès de votre service IT que les e-mails de Partena ne sont pas bloqués. Vous pourrez ensuite poursuivre la procédure.

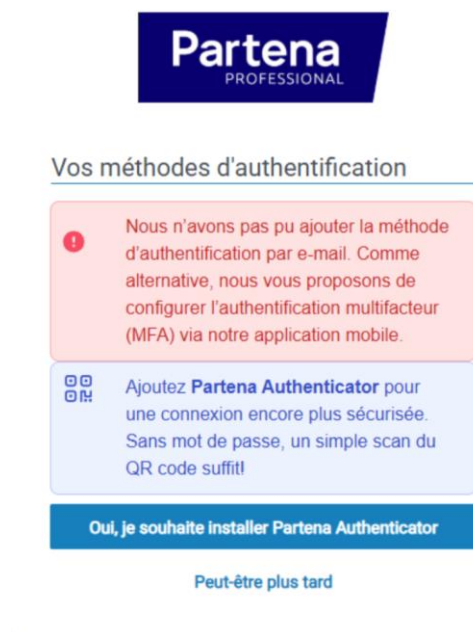
☎ 02/549.33.99
✉ digitalsupport@partena.be

J'ai vérifié et souhaite continuer

Le courriel se trouvait dans mon dossier Spam

Si l'e-mail se trouvait dans le dossier SPAM, vous pouvez continuer.

Si ce n'est pas le cas, vous verrez l'écran suivant (après avoir cliqué sur « J'ai vérifié et je souhaite continuer »).



Partena
PROFESSIONAL

Vos méthodes d'authentification

! Nous n'avons pas pu ajouter la méthode d'authentification par e-mail. Comme alternative, nous vous proposons de configurer l'authentification multifacteur (MFA) via notre application mobile.

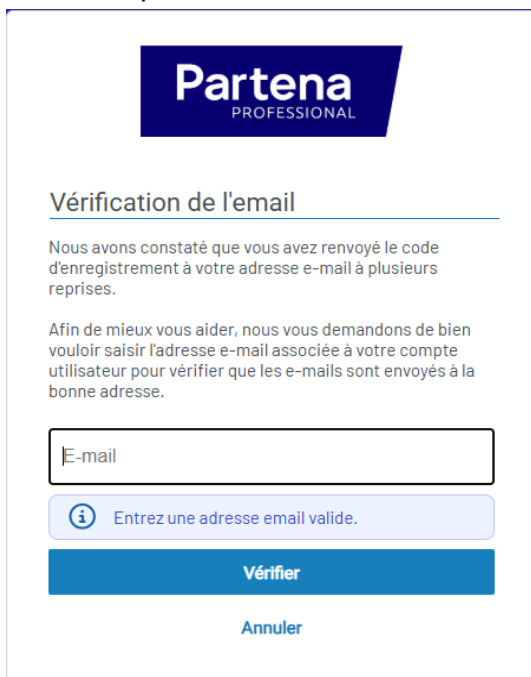
📱 Ajoutez **Partena Authenticator** pour une connexion encore plus sécurisée. Sans mot de passe, un simple scan du QR code suffit!

Oui, je souhaite installer Partena Authenticator

[Peut-être plus tard](#)

Cet écran vous permet de passer l'étape de l'e-mail et d'installer directement l'application **Partena Authenticator** (voir étape suivante : étape 4).

2. Si l'adresse e-mail que vous avez indiquée ne correspond pas à celle enregistrée dans nos systèmes, vous pouvez saisir l'adresse correcte ; celle-ci remplacera alors l'adresse actuellement enregistrée dans nos systèmes.



Partena
PROFESSIONAL

Vérification de l'email

Nous avons constaté que vous avez renvoyé le code d'enregistrement à votre adresse e-mail à plusieurs reprises.

Afin de mieux vous aider, nous vous demandons de bien vouloir saisir l'adresse e-mail associée à votre compte utilisateur pour vérifier que les e-mails sont envoyés à la bonne adresse.

 Entrez une adresse email valide.

Vérifier

[Annuler](#)

Ensuite, cliquez sur « Vérifier »



Partena
PROFESSIONAL

L'adresse e-mail ne correspond pas

L'adresse e-mail saisie ne correspond pas à celle enregistrée dans votre dossier.

Veuillez utiliser le bouton Continuer afin de modifier votre adresse e-mail vers:

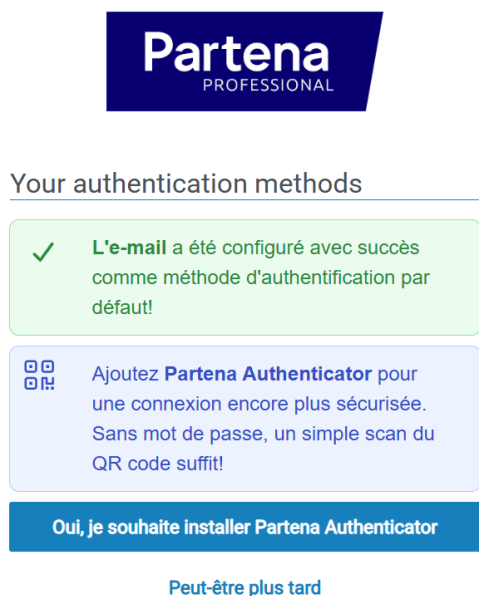
Continuer

Retour

Cliquez sur « Continuer » pour modifier votre nouvelle adresse e-mail (correcte) dans nos systèmes :



Ensuite, vous pouvez poursuivre avec l'étape 4.



4. Votre adresse e-mail a été enregistrée avec succès comme méthode *MFA*. Le système vous demande ensuite d'installer Partena Authenticator. Cliquez sur « Oui, je souhaite installer Partena Authenticator ».



Your authentication methods

✓ **L'e-mail** a été configuré avec succès comme méthode d'authentification par défaut!

 Ajoutez **Partena Authenticator** pour une connexion encore plus sécurisée. Sans mot de passe, un simple scan du QR code suffit!

Oui, je souhaite installer Partena Authenticator

Peut-être plus tard



Associez votre application Partena Professional Auth

Pour pouvoir lier votre téléphone en tant que méthode d'authentification, vous devez d'abord télécharger l'application Partena Professional Auth correspondante dans Google Play ou App Store.




Continuer

Annuler

5. Sur votre smartphone :
- Installez **Partena Authenticator** (App Store / Google Play) si l'application ne figure pas encore sur votre smartphone.
6. Après avoir cliqué sur Continuer, un code QR apparaît sur l'écran de votre ordinateur. Prenez votre smartphone et ouvrez l'application Partena Authenticator. Appuyez sur le bouton Associer cet appareil et scannez le code QR qui apparaît à l'écran. L'application associe immédiatement votre appareil à votre compte utilisateur.



Associez votre application Partena Professional Auth

Scannez la clé de couple avec l'application Partena Professional Auth



02310418030178
Clé de couple manuel

Annuler



7. Donnez un nom à la méthode (p. ex. Partena App) et cliquez sur Définir nom.



Nom de l'application Partena Professional Auth

Veuillez fournir un nom approprié pour l'application mobile Partena Professional Auth associée

Nom

Définir Nom

8. Vous pouvez ensuite ajouter une autre méthode d'authentification (**cf. infra**). Vous pouvez également conserver ces 2 méthodes (Partena Authenticator) et l'adresse e-mail en back-up.



Vos méthodes d'authentification



Application Partena Professional Auth

Défaut



E-mail

frederic@sigmail.com

Cliquez sur une méthode pour la mettre à jour.

Cliquez sur "Ajouter une méthode" pour ajouter une méthode supplémentaire.

[Ajouter une méthode](#)

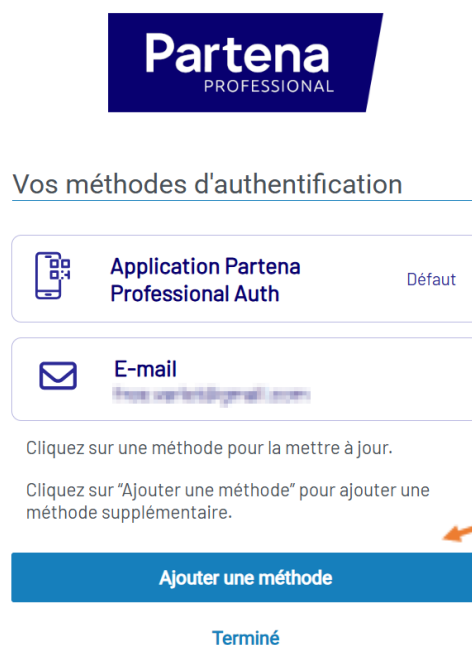
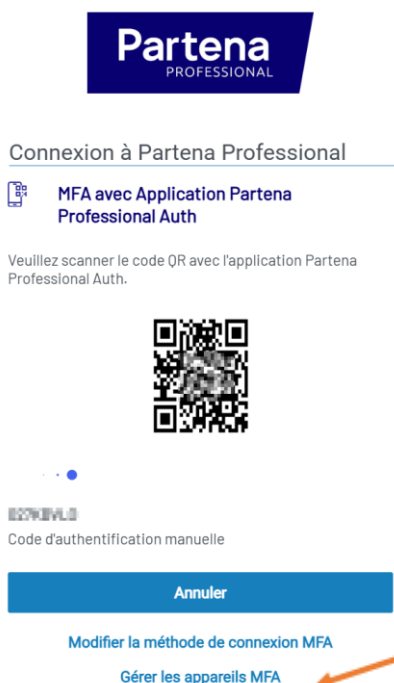
Terminé

2. Démarrage – Option B : Microsoft Authenticator

1. Connectez-vous au portail. Le système affiche automatiquement l'écran **Activation MFA requise** lorsqu'aucune méthode n'a encore été configurée.



2. Après avoir enregistré votre adresse e-mail, cliquez sur Ajouter une méthode.



3. Cliquez sur Autres applications d'authentification et sélectionnez par exemple Microsoft Authenticator.



Partena
PROFESSIONAL

Ajouter une nouvelle méthode MFA

Sélectionnez la méthode d'authentification multifacteur (MFA) que vous souhaitez associer à votre compte.

- Application Mobile**
Utilisez l'application officielle Partena Professional Auth pour s'authentifier à l'aide d'un code QR
- E-mail**
Recevez un e-mail avec un code d'accès à usage unique pour vous authentifier.
- Autres applications d'authentification**
Utilisez une application d'authentification avec un code d'accès à usage unique pour vous authentifier.

[Annuler](#)

4. Sur votre smartphone :
- Installez **Microsoft Authenticator** (App Store / Google Play) si l'application ne figure pas encore sur votre smartphone.
 - Ouvrez l'application → appuyez sur + → choisissez **Autre compte (TOTP)** → **scanner code QR**.
 - Pas d'appareil photo / appareil non compatible ?** Cliquez sur **Impossible de scanner l'image ?** et copiez la clé et l'URL pour configurer l'application manuellement.
5. Scannez le code QR sur le portail (ou saisissez la clé manuellement).
L'application ajoute un compte avec un code à 6 chiffres qui change toutes les 30 secondes.



Partena
PROFESSIONAL

Enregistrement TOTP MFA

Scannez le QR code dans l'application d'authentification de votre choix ou saisissez manuellement la clé de configuration.

Ci-dessous, le QR code de configuration :

Clé de configuration manuelle :
W5ACTUJ2X0SLR3K3PTJSLDEB2TMT

[Continuer le couplage TOTP](#)

6. Donnez un nom à votre nouvelle méthode d'authentification (p. ex. Microsoft Authenticator) et cliquez sur Définir nom.



Nommez votre méthode d'authentification

Veuillez fournir un nom reconnaissable pour votre méthode MFA.

Nom

Définir Nom

7. Vous disposez à présent de 3 méthodes d'authentification (ou de 2 si vous n'avez pas choisi l'option A). Cliquez sur Terminé pour terminer le processus.



Vos méthodes d'authentification



Application Partena Professional Auth

Défait



E-mail

free.worid@gmail.com



Authentificateur TOTP

Cliquez sur une méthode pour la mettre à jour.

Cliquez sur "Ajouter une méthode" pour ajouter une méthode supplémentaire.

Ajouter une méthode

Terminé

Conseil : si vous changez de smartphone, ajoutez **d'abord** le nouvel appareil à l'aide de l'ancien (répétez les étapes 3 à 9), puis supprimez l'ancien appareil.

3. Démarrage – Option C : Google Authenticator

1. Connectez-vous au portail. Dans **Activation MFA requise**, sélectionnez **Authentificateur (TOTP) → Google Authenticator → Suivant**.
2. Sur votre smartphone :
 - Installez **Google Authenticator** (App Store / Google Play) si nécessaire.
 - Ouvrez l'application → appuyez sur + → choisissez **Scanner code QR** (ou **Saisir une clé de configuration**).
3. Scannez ensuite le code QR sur le portail.
 - **Pas d'appareil photo / Impossible de scanner l'image ?** Cliquez sur **Impossible de scanner l'image ?** et copiez la clé (ainsi que l'URL/l'éditeur s'ils sont disponibles) pour configurer l'application manuellement. Dans Google Authenticator, sélectionnez **Type : Basé sur le temps (TOTP)**.
4. L'application ajoute un compte avec un **code à 6 chiffres** qui change toutes les 30 secondes.
5. Introduisez le code sur le portail → **Continuer**.
6. **Renommez la méthode** (p. ex. « Samsung privé ») → **Enregistrer**.
7. **(Facultatif)** Définir comme **méthode par défaut** ou laisser Microsoft Authenticator comme méthode par défaut si vous l'utilisez déjà.
8. **Ajoutez E-mail comme méthode de back-up** (recommandé) pour pouvoir vous connecter si votre smartphone n'est pas disponible.

Conseil : synchronisez Google Authenticator avec votre compte Google, afin de pouvoir restaurer plus facilement vos comptes *TOTP* lorsque vous changez d'appareil.
Vérifiez les politiques internes en la matière avant d'activer la synchronisation Cloud.

IV. Comment gérer vos méthodes d'authentification (ajout / modification / suppression) ?

- **Ajouter :** cliquez sur **Ajouter une méthode**.
- **Modifier / Renommer / Supprimer :** cliquez sur la méthode existante.
- **Définir par défaut :** ouverture de la méthode → **Définir la méthode MFA par défaut**.



V. Comment résoudre un problème (*troubleshooting*) ?

Oubli du smartphone / batterie déchargée

- Cliquez sur l'écran MFA **Modifier la méthode** ► **E-mail**.

Code refusé

- Attendez la **rotation suivante** (le code change toutes les **30 secondes**).
- Vérifiez que l'**heure** de votre smartphone est réglée **automatiquement**.
- Veillez à utiliser le **dernier compte ajouté** si vous en avez plusieurs dans l'application.

Le code QR n'apparaît pas / est illisible

- Utilisez la fonction **Impossible de scanner l'image ?** pour procéder à une saisie **manuelle** (clé + URL) dans l'application.

Nouveau téléphone

- Connectez-vous à partir d'un ordinateur et **ajoutez la nouvelle application comme nouvelle méthode**.
 - Avec l'ancien appareil :
 - Saisissez le code *TOTP* de votre ancien appareil.
 - Sélectionnez Autres applications d'authentification.
 - Maintenant, utilisez votre nouvel appareil (Microsoft Authenticator ou Google Authenticator), cf. point 4
 - Sans l'ancien appareil :
 - Modifiez la méthode de connexion MFA et choisissez E-mail.
 - Saisissez le code *TOTP* reçu par e-mail.
 - Sélectionnez Autres applications d'authentification.
 - Maintenant, utilisez votre nouvel appareil (Microsoft Authenticator ou Google Authenticator), cf. point 4
- **Essayez d'établir une connexion MFA.**
- **Supprimez l'ancienne méthode** associée à l'ancien téléphone.
 - **Restez connecté à votre messagerie électronique** tout au long du processus.

Aucun accès à aucune méthode

- **Contactez la *Digital Support Team*** (coordonnées ci-dessous) pour réinitialiser vos méthodes de connexion MFA.

VI. Besoin d'aide ?

1. **Consultez d'abord [nos questions fréquentes](#).**
2. **Toujours bloqué ?** Contactez la *Digital Support Team*.
 - **Tél.** : 02 549 33 99
 - **E-mail** : digitalsupport@partena.be