Microsoft logo white text versionMise en œuvre Pro Santé Connect avec Microsoft Entra ID

Zzz

Guide de configuration de Microsoft Authenticator à destination des établissements de santé

Version 0.4a - Septembre 2024

Cette page est intentionnellement laissée vide.

Avertissement

Les informations contenues dans le présent document, y compris les URL et autres références à des sites Internet, sont susceptibles d'être modifiées sans préavis. Sauf indication contraire, les exemples de sociétés, d'organisations, de produits, de noms de domaine, d'adresses électroniques, de logos, de personnes, de lieux et d'événements décrits dans le présent document sont fictifs et aucune association avec une société, une organisation, un produit, un nom de domaine, une adresse électronique, un logo, une personne, un lieu ou un événement réel n'est voulue ou ne doit être déduite. Il incombe à l'utilisateur de se conformer à toutes les lois applicables en matière de droits d'auteur.

A drawing of a face

Description automatically generated

Attribution 4.0 International (CC BY 4.0)

Microsoft et tous les contributeurs vous accordent une licence pour ce document sous la licence [Creative Commons Attribution 4.0 International Public License](https://creativecommons.org/licenses/by/4.0/legalcode), Cf. fichier [LICENSE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE), et vous accordent une licence pour tout code dans le référentiel sous la licence MIT, Cf. fichier [LICENSE-CODE](https://github.com/microsoft/prosanteconnect/blob/main/LICENSE-CODE).

Microsoft, Windows, Microsoft Azure et/ou d'autres produits et services Microsoft référencés dans le document peuvent être des marques commerciales ou des marques déposées de Microsoft aux États-Unis et/ou dans d'autres pays. La licence de ce document ne vous donne pas le droit d'utiliser les noms, logos ou marques de Microsoft. Les directives générales de Microsoft en matière de marques sont disponibles à l'adresse suivante : <http://go.microsoft.com/fwlink/?LinkID=254653>.

Des informations sur la protection de la vie privée sont disponibles à l'adresse suivante : <https://privacy.microsoft.com/fr-fr/>

Microsoft et tous les contributeurs se réservent tous les autres droits, que ce soit au titre de leurs droits d'auteur, de leurs brevets ou de leurs marques respectives, que ce soit de manière implicite, par préclusion ou de toute autre manière.

Contenu

[1 Introduction 5](#_Toc176967282)

[1.1 Objectifs du guide 5](#_Toc176967283)

[1.2 Non-objectifs du guide 5](#_Toc176967284)

[2 Configuration de Microsoft Authenticator au niveau des appareils 7](#_Toc176967285)

[2.1 Installation de l’application Microsoft Authenticator 7](#_Toc176967286)

[2.2 Activation de Microsoft Authenticator 7](#_Toc176967287)

[3 Configuration de l’authentification avec Microsoft Authenticator dans Microsoft Entra ID 9](#_Toc176967288)

# Introduction

Pro Santé Connect (PSC) est le fédérateur d’identités des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire Partagé des Professionnels de Santé (RPPS). Ce service socle est proposé par l’Agence du Numérique en Santé (ANS) en sa qualité d’autorité compétente.

Dans le cadre du déploiement de PSC, différents retours terrains ont mis en lumière la nécessité de faire évoluer le service pour simplifier les parcours d’accès aux services connectés à PSC ; notamment dans les contextes des ES.

L’objectif du projet Pro Santé Connect sans couture est d’étudier, de définir puis d’implémenter des mesures organisationnelles et techniques permettant de fluidifier l’accès à ces services numériques dans le contexte des ES.

Pour fluidifier la navigation, une fédération/délégation peut être ainsi mise en place entre le fournisseur d’identités (FI) local de l’ES et PSC selon les contextes. Microsoft Entra ID.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Le POC technique prend en charge la délégation de l’authentification à Microsoft Entra ID. Pour plus d’informations, nous invitons le lectorat à consulter le Portail Industriels de l’ANS : Délégation à un fournisseur d'identité local : <https://industriels.esante.gouv.fr/produits-et-services/pro-sante-connect/delegation-un-fournisseur-d-identite-local>.

Dans ce contexte, l’application Microsoft Authenticator peut enfin être utilisée comme un moyen d’identification électronique (MIE) 2FA conforme. (Le POC technique sécurisation cible plus spécifiquement cette utilisation.)

## Objectifs du guide

L’objectif de ce guide est d’expliciter dans ce contexte les éléments de configuration de Microsoft Authenticator.

## Non-objectifs du guide

La configuration de la délégation de l’authentification PSC auprès du FI tiers Microsoft Entra ID n’est pas couverte en tant que telle dans ce guide. Cette dernière fait l’objet du Guide de configuration de Pro Santé Connect à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Microsoft Authenticator n’est pas le seul MIE conforme dans le cadre du POC technique. Les MIE suivants sont également retenus dans le périmètre du POC technique :

* Certificat X.509 avec une carte CPx physique ;
* Clé de sécurité FIDO2 (clé USB, carte à puce, etc.) ;
* Windows Hello Entreprise.

La configuration de ces MIE n’est pas couverte dans ce guide. Cette dernière fait l’objet des guides suivants :

* Guide de configuration des cartes CPx à destination des établissements de santé ;
* Guide de configuration des clés de sécurité FIDO2 à destination des établissements de santé ;
* Guide de configuration de Windows Hello Entreprise à destination des établissements de santé.

Nous invitons le lectorat à s’y reporter.

De plus, ce guide ne donne pas de préconisations sur la stratégie de déploiement à opérer au sein d’un ES pour par exemple déployer ces nouveaux MIE auprès de ses PS et autres utilisateurs ; celle-ci étant sous la responsabilité de l’ES.

Il pourra le cas échéant renvoyer le lectorat sur les guides de planification disponibles dans la documentation Microsoft.

Par ailleurs, cette même expérience d’authentification unique peut être étendue à d’autres types de dispositifs comme les services de terminaux Windows. Ceci requiert la mise en œuvre additionnelle de Microsoft Entra Private Access, un produit de type ZTNA (Zero Trust Network Access) centré sur l'identité. Cette mise en œuvre est couverte dans le Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

Enfin, l’accès à PSC depuis une session Entra ID et/ou Windows ouverte avec un MIE conforme, est permis au travers d’un accès conditionnel Entra ID afin d’assurer le respect d’un ensemble d’exigences comme la force d’authentification requise. Un tel accès conditionnel est indépendant de la configuration de la navigation sans couture. La mise en œuvre des politiques d’accès conditionnel attendues est couverte dans le Guide de configuration de l’accès conditionnel à destination des établissements de santé. Nous invitons le lectorat à s’y reporter.

# Configuration de Microsoft Authenticator au niveau des appareils

La prise en charge de Microsoft Authenticator suppose les opérations suivantes depuis un appareil mobile Android ou iOS.

## Installation de l’application Microsoft Authenticator

Procéder comme suit :

1. Depuis votre appareil mobile, télécharger l’application. L’application Microsoft Authenticator est téléchargeable sur :

* Les appareils Android depuis le store Google Play à l’adresse Internet suivante : <https://go.microsoft.com/fwlink/p/?linkid=2168850&clcid=0x40c&culture=fr-fr&country=fr>.

Ce QR code peut être scanné à cet effet :

Une image contenant motif, texte, point, monochrome

Description générée automatiquement

* Les appareils iOS depuis l’Apple Store à l’adresse Internet suivante : <https://go.microsoft.com/fwlink/p/?linkid=2168643&clcid=0x40c&culture=fr-fr&country=fr> .

Ce QR code peut être scanné à cet effet :

Une image contenant motif, point, pixel, mots croisés

Description générée automatiquement

1. Procéder à l’installation de l’application.

## Activation de Microsoft Authenticator

Procéder comme suit :

1. Ouvrir l'application Microsoft Authenticator et sélectionner le bouton + pour ajouter un compte.
2. Choisir Compte professionnel ou scolaire et suivre les instructions pour se connecter avec le compte Microsoft Entra ID souhaité. Vous pouvez ajouter votre compte en vous connectant avec vos informations d'identification de compte professionnel ou scolaire, en scannant un code QR, ou en vous connectant avec vos informations d'identification.
3. Une fois le compte ajouté, un message s’affiche demandant d'appuyer sur un numéro dans l'application. Entrer le numéro sir l'écran de connexion dans la boîte de dialogue Microsoft Authenticator.
4. Choisir Approuver et fournir votre code confidentiel ou votre biométrie pour terminer le processus de connexion.
5. À ce stade, vous pouvez être invité à scanner un code QR fourni par l’ES pour configurer un compte d'authentification multifacteur dans l'application. Suivre les instructions fournies pour compléter cette étape.

A ce stade, il est nécessaire d’ activer la connexion par téléphone. Procéder comme suit :

1. Dans **Microsoft Authenticator**, sélectionner le compte enregistré ci-dessus.
2. Sélectionner **Activer la connexion par téléphone**.
3. Suivre les instructions de l’application pour terminer de s’inscrire à la connexion sans mot de passe.

Une fois ces étapes terminées, Microsoft Authenticator peut être utilisé pour se connecter au compte Entra ID configuré sans avoir besoin d'un mot de passe traditionnel.

Pour utiliser l'authentification sans mot de passe avec Microsoft Authenticator, certaines conditions préalables doivent être remplies, notamment l'installation de la dernière version de Microsoft Authenticator sur des appareils exécutant Android ou iOS, et l'activation de l'authentification multifacteur (MFA) Microsoft avec les notifications Push autorisées comme méthode de vérification.

Documentation Microsoft :

* Activer la connexion sans mot de passe avec Microsoft Authenticator :  
  <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-phone>
* Ajouter votre compte professionnel ou scolaire à l’application Microsoft Authenticator : <https://support.microsoft.com/fr-fr/account-billing/ajouter-votre-compte-professionnel-ou-scolaire-%C3%A0-l-application-microsoft-authenticator-43a73ab5-b4e8-446d-9e54-2a4cb8e4e93c> ;
* Vous connecter à vos comptes à l’aide de l’application Microsoft Authenticator : <https://support.microsoft.com/fr-fr/account-billing/vous-connecter-%C3%A0-vos-comptes-%C3%A0-l-aide-de-l-application-microsoft-authenticator-582bdc07-4566-4c97-a7aa-56058122714c>.

# Configuration de l’authentification avec Microsoft Authenticator dans Microsoft Entra ID

Procéder comme suit :

1. Depuis un navigateur, aller sur le Centre d’administration Microsoft Entra à l’adresse Internet <https://entra.microsoft.com>, puis sur la vue d’ensemble Identité de Microsoft Entra ID. L’adresse <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView> peut être utilisée pour un accès direct.
2. Se diriger dans l’onglet Protection > Méthodes d’authentification > Stratégies.
3. Sous Microsoft Authenticator, choisir les options suivantes :
   1. Activer - Oui ou Non.
   2. Cible - Tous les utilisateurs ou les utilisateurs sélectionnés.
4. Chaque groupe ou utilisateur ajouté est activé par défaut pour utiliser Microsoft Authenticator dans les modes de notifications sans mot de passe et push (mode « Tout »). Pour modifier le mode, pour chaque ligne pour le Mode d’authentification, choisir Tout ou Sans mot de passe. Le choix d’une notification Push empêche l’utilisation des informations d’identification de connexion par téléphone
5. Pour appliquer la nouvelle stratégie, cliquer sur Enregistrer.

Ceci conclut le présent guide.