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

Zzz

Guide de configuration des moyens d’identification électronique (MIE) et de la navigation sans couture à destination des établissements de santé

Version 0.3 - Février 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](#_Toc159338841)

[1.1 Présentation succincte du projet Pro Santé Connect sans couture et du POC technique 5](#_Toc159338842)

[1.2 Objectifs du guide 8](#_Toc159338843)

[1.3 Non-objectifs du guide 9](#_Toc159338844)

[2 Prise en charge des MIE conformes aux exigences de l’ANS dans Entra ID 10](#_Toc159338845)

[2.1 Utilisation des certificats X.509 de la carte CPx physique 10](#_Toc159338846)

[2.2 Utilisation d’une clé de sécurité FIDO2 10](#_Toc159338847)

[2.3 Utilisation de Windows Hello Entreprise 10](#_Toc159338848)

[2.4 Utilisation de Microsoft Authenticator 10](#_Toc159338849)

[2.5 Non prise en charge de la carte e-CPS 11](#_Toc159338850)

[2.6 MIE et navigation sans couture 11](#_Toc159338851)

[2.7 Axes d’extensibilité futurs prévisibles 12](#_Toc159338852)

[3 Configuration des MIE au niveau des appareils 13](#_Toc159338853)

[3.1 Activation du support des certificats X.509 de la carte CPx physique 13](#_Toc159338854)

[3.2 Activation du support des clés de sécurité FIDO2 17](#_Toc159338855)

[3.3 Activation de Windows Hello Entreprise 18](#_Toc159338856)

[3.4 Activation de Microsoft Authenticator 20](#_Toc159338857)

[4 Configuration des MIE dans Microsoft Entra ID 21](#_Toc159338858)

[4.1 Configuration des moyens d’authentification approuvés 21](#_Toc159338859)

[4.2 Configuration de l’authentification par certificats Microsoft Entra ID 21](#_Toc159338860)

[4.3 Configuration de l’authentification avec une clé de sécurité FIDO2 26](#_Toc159338861)

[4.4 Configuration de l’authentification avec Windows Hello Entreprise 27](#_Toc159338862)

[4.5 Configuration de l’authentification avec Microsoft Authenticator 28](#_Toc159338863)

# 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.

## Présentation succincte du projet Pro Santé Connect sans couture et du POC technique

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.

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

Description générée automatiquement

Dans le cadre des tests préliminaire, l’application de test PSC\_BAS, c.à.d. le portail de gestion des utilisateurs Bac à sable est mise à disposition à cette fin ; elle est accessible à l’adresse Internet <https://wallet.bas.psc.esante.gouv.fr/login-page>.

Un premier POC technique incluant le raccordement et la sécurisation avec Microsoft Entra ID vise à assoir la validité technique de la solution proposée dans le cadre de PSC sans couture, et de recueillir des retours qui auront pour vocation à permettre les évolutions et améliorations de la solution.

La délégation de l’authentification à Microsoft Entra ID est décrite dans le Guide de configuration de Pro Santé Connect à destination des établissements de santé. Elle suppose une approbation préalable de l’application PSC\_BAS dans le locataire Entra ID de l’ES retenu pour cette délégation.

Une fois celle-ci en place, en termes de parcours utilisateurs, lorsqu’un professionnel de Santé (PS) accède à ce service numérique (SN) depuis son navigateur, ce dernier est renvoyé vers PSC qui le redirige alors de façon transparente vers Microsoft Entra ID.

L’application de test permet de lancer cette cinématique en cliquant sur le bouton S’identifier avec EntraID.

Une image contenant texte, capture d’écran, Police, Page web

Description générée automatiquement

### Première authentification (appairage)

Si le PS n’a pas de session déjà ouverte avec Microsoft Entra ID, il se voit inviter à se connecter. Il utilise pour cela un moyen d’identification électronique (MIE) conforme avec les exigences établies par l’ANS et reconnu comme mécanisme d’authentification au niveau de ce locataire.

L’activation des différents MIE vis-à-vis desquels l’ANS invite les ES à conduire une évaluation ainsi que leur support dans Microsoft Entra ID sont couvert dans la suite de ce document.

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

Description générée automatiquement

Une fois authentifié par Microsoft Entra ID, avec le MIE conforme utilisé, et sur la base éventuellement d’une ouverture de session Windows avec la navigation sans couture, le PS est renvoyé vers PSC.

D’un point de vue technique, le protocole utilisé dans ces redirections et échanges est le standard de l’industrie OpenID Connect (OIDC) avec le flux de code d’autorisation (authorization code flow). (Le flux de code d'autorisation permet à l'application d'échanger un code d'autorisation contre des jetons d'ID pour représenter l'utilisateur authentifié et des jetons d'accès nécessaires pour appeler des API protégées.)

A ce stade, lors d’une première authentification, le PS n’accède pas directement au service numérique mais voit faire une proposition d’appairage du compte Microsoft Entra ID qui lui a été attribué par l’ES avec sa carte CPx ou son e-CPS.

Une image contenant texte, capture d’écran, Page web, logiciel

Description générée automatiquement

Si le PS confirme sa volonté de continuer en cliquant sur Appairer un compte avec la carte CPS, il est ensuite invité à utiliser sa carte CPX ou e-CPS. Une fois l’appairage réalisé, la mire précédente n’est plus affichée dans le parcours sans couture.

Seule est alors nécessaire de confirmer la validation de connexion.

Note concernant le parcours sans couture :il apparait préférable que le PS n’accède pas de façon totalement transparente au service numérique, afin de faciliter la gestion des sessions utilisées.

Exemple de cas d’usage : dans ce contexte, une secrétaire médicale pourrait laisser un accès rapide à son appareil à un des PS de son service : lors de l’accès au service numérique, la secrétaire choisirait sur l’écran intermédiaire de ne pas se connecter via son compte appairé, mais choisirait une authentification PSC. Cela permettrait au PS d’utiliser le poste de la secrétaire pour réaliser une tâche rapide et de se déconnecter par la suite.

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

Description générée automatiquement

Après avoir cliqué sur Confirmer, le PS accède au portail de gestion PSC BAS.

Une image contenant texte, capture d’écran, Caractère coloré, conception

Description générée automatiquement

### Authentification depuis l’ouverture de session d’un appareil Windows

Si l’authentification réalisée lors de l’ouverture de session satisfait aux exigences du Référentiel d’Identification Electronique (RIE), la mire de connexion Entra ID précédente n’est pas affiché dans le parcours sans couture et le PS bénéficie ici alors d’un accès transparent à l’ensemble des applications raccordés au FI local ainsi qu’à l’ensemble de l’écosystème PSC et ses services numériques (SN).

Une ouverte de session par carte à puce avec une carte CPx réalisée depuis un poste de travail Windows avec une jointure (hybride) à Entra ID permet de satisfaire aux exigences du RIE.

Pour l’accès à l’écosystème PSC, seule la confirmation de la validation de connexion est alors nécessaire pour les mêmes raisons qu’évoquées précédemment.

Pour plus d’informations, nous invitons le lectorat à consulter la page suivante sur le site de l’ANS : TBD.

## Objectifs du guide

Vis-à-vis du parcours précédent et de l’utilisation dans ce contexte de MIE conformes, l’objectif de ce guide est d’expliciter les éléments de configuration de Microsoft Entra ID associés aux MIE suivants retenus dans le périmètre du POC technique :

* Certificat basée sur Microsoft Entra ID avec une carte CPx physique ;
* Clé de sécurité FIDO2 (clé USB, carte à puce, etc.) ;
* Windows Hello Entreprise ;
* Microsoft Authenticator.

L’ensemble de ces MIE offrent à minima une authentification de type multifacteur (MFA).

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.

Ce guide vise également à couvrir de façon additionnelle les mécanismes additionnels permettant une navigation sans couture dès l’ouverture de session sur un appareil Windows pour l’accès à un SN déléguant l’authentification à PSC, Cf. section 1.1.2 Authentification depuis l’ouverture de session d’un appareil Windows.

Comme indiqué précédemment, si un appareil Windows 10 ou ultérieur est en effet enregistré auprès du locataire Microsoft Entra ID de l’ES, c.à.d. joint à Entra ID, de tels MIE peuvent également servir à l’ouverture d’une session nominative.

Une telle session nominative avec son identité provenant d’un FI tiers déjà appairé (ici Microsoft Entra ID) autorise alors l’accès en authentification unique (SSO) à un SN connecté à PSC au même titre qu’à une application de type client riche. Il s’agit de permettre une expérience de navigation sans couture à PSC aux applications web et lourds, dès l’ouverture de la session Windows au travers de mécanismes natifs de l’environnement Windows.

Il est à noter que les prérequis pour la mise en place de ces éléments pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS.

## 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.

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.

# Prise en charge des MIE conformes aux exigences de l’ANS dans Entra ID

## Utilisation des certificats X.509 de la carte CPx physique

Comme décrit précédemment en introduction de ce document, un PS peut utiliser le certificat X.509 de sa carte de professionnel de santé, ou carte CPx pour s’authentifier sur son locataire Entra ID et ainsi accéder à des services numériques connectés à PSC sans avoir besoin de se réauthentifier.

Le POC technique raccordement cible plus spécifiquement cette utilisation.

Documentation : carte d’identité professionnelle électronique du secteur de la santé : [<https://industriels.esante.gouv.fr/produits-services/cps-et-socle-technique/caracteristiques-de-la-cps3>](https://industriels.esante.gouv.fr/produits-services/cps-et-socle-technique/caracteristiques-de-la-cps3)

## Utilisation d’une clé de sécurité FIDO2

De la même façon, un PS peut utiliser une clé de sécurité FIDO2.

L’authentification FIDO2 ou Fast ID Online v2.0 est un standard ouvert pour l’authentification sans mot de passe, Cf. <https://fidoalliance.org/>.

Il permet aux PS et autres utilisateurs de se connecter à leurs appareils et applications à l’aide de l’authentification biométrique ou d’une clé de sécurité physique, sans avoir besoin d’un mot de passe traditionnel.

Le POC technique sécurisation cible plus spécifiquement cette utilisation. Dans ce cadre, la fourniture d’une clé de sécurité FIDO2 est à la charge de l’ES.

Le POC technique et les retours terrain et métier permettront d’affiner les exigences quant à la définition d’un MIE 2FA conforme de type clé FIDO2.

## Utilisation de Windows Hello Entreprise

Windows Hello Entreprise peut être utilisé à cet effet dans ce contexte comme clé de sécurité FIDO2.

La prise en charge de FIDO2 dans Windows Hello Entreprise offre une couche supplémentaire de sécurité et de commodité pour les PS et autres utilisateurs, tout en réduisant le risque d’attaques par mot de passe.

Windows Hello Entreprise utilise une méthode d’authentification à deux facteurs qui combine des informations d’identification spécifiques à l’appareil avec un mouvement biométrique ou code PIN. Ces informations d’identification sont liées au lié au FI, ici Microsoft Entra ID ,dans le contexte de ce guide, et peuvent être utilisées pour accéder à PSC et à ses services.

Documentation Microsoft :

* Windows Hello Entreprise : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/> ;

## Utilisation de Microsoft Authenticator

L’application Microsoft Authenticator peut enfin être utilisée dans ce contexte comme MIE 2FA conforme.

Elle 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

## Non prise en charge de la carte e-CPS

La carte e-CPS n’est PAS prise en charge dans le cadre proposé. Le flux « découplé » CIBA (Client-Initiated Backchannel Authentication, <https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html>) n’est en effet PAS pris en charge par la plateforme d’identité Microsoft Entra ID.

L’extension CIBA du protocole OpenID Connect (OIDC) n’est pas en effet pas intégré à date dans les environnements Microsoft.

Il convient de noter que la carte e-CPS reste cependant disponible avec PSC pour réaliser l’appairage.

Documentation : OpenID Connect on the Microsoft identity platform : <https://learn.microsoft.com/fr-fr/entra/identity-platform/v2-protocols-oidc>

## MIE et navigation sans couture

Il est possible de plus de tirer parti à la fois de l’authentification Microsoft Entra ID avec ces MIE et de la possibilité de jointure (hybride ou non) des appareils Windows 10 ou ultérieur avec un locataire Microsoft Entra ID pour offrir une navigation sans couture afin d’accéder à un service numérique connecté à PSC.

Ainsi, par exemple, l’ouverture de session Windows par carte à puce avec les cartes CPx physiques délivrées par l’ANS aux PS est utilisée par de (très) nombreux ES. Le projet Pro Santé Connect sans couture vise donc naturellement à capitaliser à la fois sur ce mécanisme et l’expérience utilisateur associée.

Pour autant, et comme déjà indiqué, les prérequis pour cette navigation sans couture ne font pas partie du cadre minimum défini par l’ANS. Ils sont néanmoins couvert dans la suite de ce document.

## Axes d’extensibilité futurs prévisibles

L’intégration courante de PSC avec Microsoft Entra ID telle que décrite dans ses modalités opérationnelles dans le cadre de cette expérimentation vise à établir une fondation technique pérenne qui pourra être étendue tant d’un point de vue fonctionnel que technique afin de répondre aux attentes exprimées par les ES et PS.

Ainsi, l’ouverture de session et la capacité de navigation sans couture résultante pourront être étendues par la suite après qualification et validation. Ainsi, par exemple, l’ouverture de session avec Microsoft Entra ID pourra être effectuée depuis une session de terminal Windows à distance avec les fonctionnalités proposées par Microsoft Entra Private Access pour l’intégration étendue avec les environnements existants en local.

La version courante du présent document n’aborde pas cette dimension et ce qu’elle suppose en termes de mise en œuvre. Nous invitons pour cela le lectorat à se reporter d’une façon générale au site de l’ANS pour une information à jour ainsi que vis-à-vis de la seconde dimension au Guide de configuration de Microsoft Entra Private Access à destination des établissements de santé pour les éléments de configuration associés et éventuels prérequis.

# Configuration des MIE au niveau des appareils

## Activation du support des certificats X.509 de la carte CPx physique

La carte CPx physique comme MIE permet d'adopter une authentification résistante à l’hameçonnage (phishing) et de s’authentifier avec un certificat X.509 émis par l'infrastructure de gestion de la confiance du secteur santé-social français, dite « IGC-Santé », c.à.d. l’infrastructure de gestion de clés cryptographiques (IGC) opérée par l'ANS.

Sa prise en charge suppose les opérations suivantes depuis un appareil Windows 10 ou ultérieur.

### Lecture de la carte CPx par Cryptolib

La « Cryptolib CPS (Windows) » un logiciel qui permet l’interfaçage entre des applications informatiques et la carte CPx. L’installation de la « Cryptolib CPS (Windows) » permet ici à Windows de lire la carte physique CPx.

Depuis un appareil Windows 10 ou ultérieur, procéder comme suit :

1. A l’aide d’un compte d’administrateur local, installer le logiciel Cryptolib comme décrit sur le lien suivant : <https://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-windows>.
2. Vérifier la lecture effective du certificat du PS dans CPS Gestion :

Une image contenant texte, Appareils électroniques, capture d’écran, nombre

Description générée automatiquement

### Lecture des champs du certificat de la carte CPS

Procéder comme suit :

1. Depuis le bureau Windows, ouvrir le dialogue Exécuter. Taper Touche Windows + R pour cela
2. Dans Ouvrir, taper la commande "*mmc.exe certmgr.msc*".

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

Description générée automatiquement

1. Cliquer sur OK. Le Gestionnaire de certificats utilisateur s’ouvre.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. Naviguer sous Certificats - Utilisateur actuel > Personnel > Certificats.
2. Deux certificats utilisateur sont présents sur la carte CPX et publiés dans le magasin de certificats utilisateur.
3. Sélectionner et afficher le certificat de type « Smart Card Logon » :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

* 1. Lire le Principal Name (PN).

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

* 1. Lire le Subject Key Identifier.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Documentation Microsoft :

* Certificats logiciels : <https://esante.gouv.fr/produits-services/certificats-logiciels>.

### Lecture de la carte CPx à l’ouverture de session Windows

Pour la navigation sans couture, la lecture de la carte CPS à l’ouverture de session Windows suppose un paramétrage du registre de Windows.

Ce paramétrage permet aux utilisateurs de voir apparaître un champ pour remplir un nom d’utilisateur lors de l’ouverture ou du déverrouillage de la session Windows par carte à puce. Ceci établit le lien entre l'identité enregistrée dans la carte CPS, représentée par le certificat X.509, et la paire de clés présente sur la carte, ainsi que l'identité utilisée au niveau de Windows.

Depuis un appareil Windows 10 ou ultérieur, procéder comme suit :

1. Exécuter l’éditeur du Registre(regedit.exe) depuis la barre Windows.
2. Se diriger vers : Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Polices\Microsoft\Windows.
3. Créer un nouveau dossier : SmartCardCredentialProvider.
4. Une fois le dossier créé, créer un nouveau fichier DWORD (32-bit) Value.
5. Renommer ce fichier X509HintsNeeded, puis passer la Value dataà 1.

Remarque :

* Un fichier de registre .reg peut être défini. Ce dernier est alors à exécuter directement depuis un invite de commande avec l’éditeur de registre (regedit.exe)

- ou -

* Pour un appareil Windows membre d’un domaine Active Directory, cette opération peut être automatisée au travers de l’application d’une stratégie de groupe (Group Policy Object ou GPO) de carte à puce.

Documentation Microsoft :

* Paramètres de Registre et de stratégie de groupe de carte à puce : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/smart-cards/smart-card-group-policy-and-registry-settings> ;
* Autoriser l’indicateur de nom d’utilisateur (clé de registre X509HintsNeeded) : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/smart-cards/smart-card-group-policy-and-registry-settings#allow-user-name-hint> .

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

Description générée automatiquement

Un champ apparait alors lors de la connexion par carte à puce, pour renseigner un nom d’utilisateur

Une image contenant peinture, texte, montagne, plein air

Description générée automatiquement

## Activation du support des clés de sécurité FIDO2

Le support d’une clé FIDO2 suppose les opérations suivantes depuis un appareil Windows 10 ou ultérieur. Le support depuis un appareil Android ou iOS n’est pas couvert dans la version courante de ce guide.

Depuis un appareil Windows 10 ou ultérieur, procéder comme suit :

1. A l’aide d’un compte d’administrateur local, ouvrir l’utilitaire Local Group Policy Editor.​   
   (Pour un déploiement centralisé, il faudra bien entendu faire l’équivalent à travers un Group Policy Object dans Active Directory, ou une stratégie de type OMA-DM - Open Mobile Alliance" "Device Management")

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

Description générée automatiquement

1. Dans Computer Configuration > Administrative Templates > System > Logon, activer le paramètre Turn on security key sign-in.​

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

Description générée automatiquement

Documentation Microsoft :

* Connexion Windows par clé de sécurité sans mot de passe : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-authentication-passwordless-security-key-windows>.

## Activation de Windows Hello Entreprise

La configuration de Windows Hello Entreprise peut être réalisée à l’aide des deux options suivantes pour un appareil Windows 10 ou ultérieur :

1. Le fournisseur de services de configuration (Configuration Service Provider ou CSP) PassportForWork couramment utilisé pour les appareils gérés par une solution de gestion des appareils mobiles (Mobile Device Management ou MDM), comme Microsoft Intune. Un CSP peut également être configuré avec des packages d’approvisionnement, qui sont généralement utilisés au moment du déploiement ou pour les appareils non gérés. Pour configurer Windows Hello Entreprise, utiliser le CSP PassportForWork.

Pour les appareils joints à Microsoft Entra et inscrits dans Microsoft Intune, vous pouvez utiliser des stratégies Intune pour gérer Windows Hello Entreprise. Il existe différentes façons d'activer et de configurer Windows Hello Entreprise dans Microsoft Intune, y compris l'utilisation d'une stratégie appliquée au niveau du locataire ou une stratégie de configuration d'appareil appliquée après l'inscription de l'appareil.

-ou-

1. Une stratégie de groupe (Groupe Policy Object ou GPO) utilisée pour les appareils avec une jointure (hybride) à Microsoft Entra ID et qui ne sont pas gérés par une solution de type MDM.

Pour configurer un appareil avec une stratégie de groupe, procéder comme suit :

1. Utiliser l'Éditeur de stratégie de groupe local.
2. Pour configurer plusieurs appareils joints à Active Directory, créer ou modifier un objet de stratégie de groupe (GPO) et utilisez les paramètres suivants :

* Chemin d'accès à la stratégie de groupe : Configuration ordinateur\Modèles d'administration\Composants Windows\Windows Hello Entreprise ou Configuration utilisateur\Modèles d'administration\Composants Windows\Windows Hello Entreprise
* Paramètre de stratégie de groupe : Utiliser Windows Hello Entreprise
* Valeur : Activé

Pour mémoire, les stratégies utilisateur ont la priorité sur les stratégies d’ordinateur. Si une stratégie utilisateur est définie, la stratégie d’ordinateur correspondante est ignorée. Si aucune stratégie utilisateur n'est définie, la stratégie de l'ordinateur est utilisée.

Les paramètres de stratégie de Windows Hello Entreprise sont appliqués à l'aide de la hiérarchie suivante :

* Utilisateur - Objet de stratégie de groupe,
* Ordinateur - Objet de stratégie de groupe,
* Utilisateur - Fournisseur de services de configuration PassportForWork,
* Appareil - Fournisseur de services de configuration PassportForWork.

Une fois ces paramètres configurés, vous pouvez passer à l'étape d'inscription à Windows Hello Entreprise.

Le processus d'approvisionnement Windows Hello Entreprise commence immédiatement après le chargement du profil utilisateur et avant que l'utilisateur ne reçoive son bureau. Pour que le processus d'approvisionnement commence, toutes les vérifications des prérequis doivent réussir, c’est-à-dire que le modèle de déploiement Windows Hello Entreprise (Cloud uniquement ou Hybride) doit avoir été choisir et déployé**.**

L'expérience de l'utilisateur commence une fois qu'un utilisateur s'est connecté. Le processus d'inscription Windows Hello Entreprise commence et l'utilisateur est guidé à travers une série d'étapes pour configurer et valider son code confidentiel, et pour créer une paire de clés asymétriques pour l'utilisateur. Une fois ces étapes terminées, l'utilisateur peut utiliser son code confidentiel ou un geste biométrique pour se connecter.

Nous recommandons d’éviter de mélanger les paramètres de stratégie de groupe et CSP pour Windows Hello Entreprise.

Windows Hello Entreprise peut être configuré par un objet de stratégie de groupe ou un fournisseur de solutions Cloud, mais pas une combinaison des deux !

Si vous combinez des paramètres de stratégie de groupe et de stratégie CSP, les paramètres CSP sont ignorés jusqu'à ce que tous les paramètres de stratégie de groupe soient effacés.

Documentation Microsoft :

* Vue d’ensemble de Windows Hello Entreprise: <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/>
* Configurer Windows Hello Entreprise : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/configure>.
* Fournisseurs de services de configuration pour les professionnels de l’informatique : <https://learn.microsoft.com/fr-fr/windows/configuration/provisioning-packages/how-it-pros-can-use-configuration-service-providers#csps-in-windows-configuration-designer>.
* Fournisseur de services de configuration PassportForWork : <https://learn.microsoft.com/fr-fr/windows/client-management/mdm/passportforwork-csp>.

## Activation de Microsoft Authenticator

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

Pour activer Microsoft Authenticator, suivez les étapes suivantes :

1. Suite au téléchargement et à l’installation de l'application Microsoft Authenticator sur l’appareil mobile, Cf. section 2.4 Utilisation de Microsoft Authenticator, 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.

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>

# Configuration des MIE dans Microsoft Entra ID

Microsoft Entra ID propose différents MIE pour gérer l’authentification de ces utilisateurs. De nombreuses méthodes peuvent être ainsi utilisées pour l’authentification multifacteur (MFA).

## Configuration des moyens d’authentification approuvés

Vous pouvez effectuer votre choix parmi la liste des méthodes d’authentification disponibles, en évaluant chacune d’elles sur le plan de la sécurité, de la facilité d’utilisation et de la disponibilité.

A ce propos, l’ES doit s’assurer que ces méthodes correspondent à des MIE autorisés et dûment configurés afin de permettre l’accès transparent à PSC et ses services.

L’ES aura à cible la charge de faire homologuer si nécessaire les MIE qu’il souhaite déployer et de leur compatibilité avec Microsoft Entra ID et les méthodes d’authentification proposées.

Afin de gérer les moyens d’authentifications autorisés pour les PS :

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.

Cette page permet de configurer les différents moyens d’authentification du projet Pro Santé Connect sans couture à intégrer dans le cadre des POC technique raccordement vs. sécurisation

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

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

C’est l’objet des sections suivantes.

Documentation Microsoft :

* Planifier un déploiement d'authentification multifacteur Microsoft Entra : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/howto-mfa-getstarted>

## Configuration de l’authentification par certificats Microsoft Entra ID

L’authentification basée sur les certificats Microsoft Entra permet d'authentifier les PS à l’aide de certificats X.509 sur leurs cartes à puce CPS3 directement auprès de Microsoft Entra ID quand ils ouvrent une session sur leur appareil Windows 10 ou ultérieur joint (en hybride) à Microsoft Entra ID. Aucune configuration spéciale n’est nécessaire sur l’appareil Windows pour accepter l’authentification par carte à puce au-delà de ce qui a été précisé précédemment, Cf. section 2.1 Utilisation des certificats X.509 de la carte CPx physique.

Prérequis :

* Les versions Windows des appareils Windows 10 ou ultérieurs prises en charge sont celles décrites pour la jointure à Microsoft Entra.

Cette prise en charge dans le cadre du projet Pro Santé Connect sans couture suppose l’application préalables des correctifs suivants selon les versions de Windows concernées :

* + [Windows 11 - KB5017383](https://support.microsoft.com/topic/september-20-2022-kb5017383-os-build-22000-1042-preview-62753265-68e9-45d2-adcb-f996bf3ad393) : <https://support.microsoft.com/topic/september-20-2022-kb5017383-os-build-22000-1042-preview-62753265-68e9-45d2-adcb-f996bf3ad393> ;
  + [Windows 10 - KB5017379](https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307) : <https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307> ;
  + [Windows Server 20H2- KB5017380](https://support.microsoft.com/topic/20-september-2022-kb5017380-os-builds-19042-2075-19043-2075-og-19044-2075-preview-59ab550c-105e-4481-b440-c37f07bf7897) : <https://support.microsoft.com/topic/20-september-2022-kb5017380-os-builds-19042-2075-19043-2075-og-19044-2075-preview-59ab550c-105e-4481-b440-c37f07bf7897> ;
  + [Windows Server 2022 - KB5017381](https://support.microsoft.com/topic/20-september-2022-kb5017381-os-build-20348-1070-preview-dc843fea-bccd-4550-9891-a021ae5088f0) : <https://support.microsoft.com/topic/20-september-2022-kb5017381-os-build-20348-1070-preview-dc843fea-bccd-4550-9891-a021ae5088f0> ;
  + [Windows Server 2019 - KB5017379](https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307) : <https://support.microsoft.com/topic/20-september-2022-kb5017379-os-build-17763-3469-preview-50a9b9e2-745d-49df-aaae-19190e10d307>

Documentation Microsoft :

* Présentation de l'authentification basée sur les certificats : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication>

### Configuration de l’authentification multifacteur (MFA)

Procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Authentification basée sur un certificat.
2. Sous Activer et cibler, sélectionner Activer.
   1. Sous Inclure, cliquer sur Sélectionner des groupes pour sélectionner des groupes spécifiques.
   2. Cliquer sur Ajouter des groupes.

Remarque : Nous ne recommandons PAS l’application à tous les utilisateurs. En effet, tous les utilisateurs déclarés dans le locataire ne disposant pas forcément d’une carte CPx, ce paramètre pourrait donc rendre certains comptes inaccessibles…

1. Peut-on recommander l’usage d’un groupe, ou ajouter une note précisant les risques ?
   1. Sélectionner le ou les groupes cibles, Cf. Guide de configuration de l’accès conditionnel pour les établissements de Santé.
   2. Cliquer sur Sélectionner.

Remarque : Une fois l’authentification basée sur les certificats activée sur le locataire Entra ID, tous les utilisateurs du locataire voient l’option de se connecter avec un certificat. Seuls les utilisateurs qui sont activés pour l’authentification basée sur les certificats peuvent s’authentifier à l’aide du certificat X.509.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Prendre connaissance du message et cliquer sur J’accepte.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. Sous Configurer :
   1. Dans Liaison d’authentification, pour Niveau de protection, sélectionner Authentification multifacteur afin de considérer l’authentification par certificat comme une authentification multifacteur (MFA).

Une image contenant texte, ligne, Police, nombre

Description générée automatiquement

* 1. Dans Liaison de nom d’utilisateur, indiquer l’ordre de priorité des champs à rechercher dans un certificat pour authentifier l’utilisateur. On utilisera ici le PrincipalName en priorité 1.

1. Les règles de liaison d’authentification mappent les attributs de certificat (émetteur ou OID de stratégie) à une valeur, et sélectionnent le niveau de protection par défaut pour cette règle. Plusieurs règles peuvent être créées pour aider à déterminer le niveau de protection pour les certificats clients. Celles-ci peuvent être configurées à l’aide des champs Sujet d’émetteur ou OID de stratégie dans le certificat.

A titre d’illustration, et de façon non obligatoire pour le POC technique, pour ajouter une règle personnalisée, sélectionner Ajouter une règle.

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

Description générée automatiquement

* + 1. Dans Attribut de certificat, cliquer sur Emetteur de certificat.
    2. Dans Identificateur d’émetteur de certificat, sélectionner CN=TEST AC IGC-SANTE.
    3. Dans Force de l’authentification, sélectionnez Authentification multifacteur.
    4. Dans Liaison d’affinité, sélectionner Basse.
    5. Cliquer sur Ajouter.

1. Lorsqu’invité à le faire, cliquer sur J’accepte pour terminer l’ajout de la règle.
2. Cliquer sur Enregistrer.

Documentation Microsoft :

* Comment configurer l’authentification Microsoft Entra basée sur certificat : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/how-to-certificate-based-authentication>.

### Déclaration des autorités de certification (AC)

Cette partie est obligatoire pour l’authentification basée sur un certificat /

Procéder comme suit :

1. Se diriger dans l’onglet Protection > Centre de sécurité.
2. Cliquer sur Autorités de certification.
3. Charger ensuite tous les certificats de la chaîne de confiance menant au certificat racine de l'infrastructure de gestion de la confiance du secteur santé-social français, dite « IGC – Santé », c.à.d. l’infrastructure de gestion de clés cryptographiques (IGC) opérée par l'ANS. L’IGC est ici celle de test pour le POC technique raccordement et le bac à sable PSC.

Il s’agit ici du certificat intermédiaire qui signe les certificats des cartes CPS et du certificat racine de l’AC.

* 1. Cliquer sur Charger pour charger le fichier de certificat.

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

Description générée automatiquement

* 1. Dans URL de la liste de révocation de certificats, renseigner la valeur :
* "http://igc-sante.esante.gouv.fr/CRL/ACI-EL-PP-TEST.crl" pour l’« IGC-Santé de test » ;

- ou -

* "http://igc-sante.esante.gouv.fr/CRL/ACI-EL-PP.crl" pour l’« IGC-Santé ».
  1. Laisser URL de la liste de révocation de certificats Delta. L’« IGC-Santé » ne propose pas de listes Delta.
  2. Cliquer sur Ajouter.

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

Description générée automatiquement

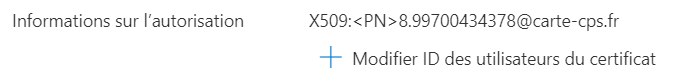
Documentation :

* Infrastructure de gestion de la confiance « IGC-Santé de test » : <http://igc-sante.esante.gouv.fr/PC_TEST/> ;
* Infrastructure de gestion de la confiance « IGC-Santé » : <https://igc-sante.esante.gouv.fr/PC>.

### Déclaration de l’attribut du certificat souhaité pour l’appairage utilisateur

Procéder comme suit :

1. Retourner dans la vue d’ensemble de Microsoft Entra ID.
2. Dans Utilisateurs, cliquer sur Tous les utilisateurs, puis dans la page sur un utilisateur cible pour le POC technique raccordement.
3. Cliquer sur Modifier des propriétés.
4. Cliquer surInformations sur l’autorisation, puis sur Modifier ID des utilisateurs du certificats.
5. Ajouter l’attribut à rechercher dans le certificat selon la syntaxe ci-dessous. Ici, pour le PrincipalName (PN)



Remarque : cet attribut ID des utilisateurs du certificat, ou CertificateUserID peut être peuplé via Entra Connect lors de la synchronisation des utilisateurs hybrides si celle-ci est en place dans l’ES entre son annuaire Active Directory en local et son locataire Entra ID, Cf. section Synchronisation d’annuaire avec un environnement Active Directory existant dans Socle technique minimal pour la mise en œuvre de PSC avec Microsoft Entra ID : <https://github.com/microsoft/prosanteconnect/blob/main/PREREQUISITES.md>.

Documentation Microsoft :

* Mappage à l’attribut certificateUserIds dans Microsoft Entra ID : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids> ;
* Synchroniser X509 :<PN>PrincipalNameValue : <https://learn.microsoft.com/fr-fr/entra/identity/authentication/concept-certificate-based-authentication-certificateuserids#synchronize-x509pnprincipalnamevalue>.

## Configuration de l’authentification avec une clé de sécurité FIDO2

### Autorisation de la configuration en libre-service ​

Procéder comme suit :

1. Depuis la page Stratégies des Méthodes d’authentification, cliquer sur Clé de sécurité FIDO2.
2. Activerla clé de sécurité FIDO2 pour Tous les utilisateurs.
3. Dans l’onglet Configurer,Autoriser la configuration libre-service**.** L’attestation et la restriction de clés sont optionnelles mais recommandées :
   1. Appliquer l’attestation : Les métadonnées de clé FIDO doivent être publiées et vérifiées auprès de la FIDO Alliance et également passer d’autres tests de validation par Microsoft.
   2. Appliquer les restrictions de la clé : Autorise ou interdit certaines clés FIDO selon leur AAGUID (identifiant indiquant le fabriquant et le modèle de la clé)

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

Description générée automatiquement

### Ajout de l’authentification par clé de sécurité FIDO2 en libre-service​

Pour les utilisateurs de test du POC technique sécurisation, procéder comme suit :

1. Se connecter sur le site <https://mysignins.microsoft.com> et se rendre dans Information de sécurité.
2. Cliquer sur Ajouter une méthode, sélectionner clé de sécurité et suivre la procédure d’enrôlement.

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

Description générée automatiquement

## Configuration de l’authentification avec Windows Hello Entreprise

Pour configurer Windows Hello Entreprise, procéder comme suit :

1. Paramètres des fonctionnalités : ces paramètres sont utilisés pour activer Windows Hello Entreprise et configurer les options de base.

Vous pouvez les trouver dans le chemin d'accès CSP suivant : ./Device/Vendor/MSFT/PassportForWork/{TenantId}/Policies/UsePassportForWork.

Pour un déploiement par stratégie de groupe (Group Policy Object ou GPO), les paramètres se trouvent :

|  |  |
| --- | --- |
| GPO | Configuration de l’ordinateur > Modèles d’administration > Composants > Windows > Windows Hello Entreprise  Configuration utilisateur > Modèles d’administration>Composants> Windows > Windows Hello Entreprise |

1. Paramètres de code confidentiel :ces paramètres sont utilisés pour configurer l'authentification par code confidentiel, comme la complexité et la récupération du code confidentiel.

Vous pouvez le trouver dans le chemin d'accès CSP suivant : ./Device/Vendor/MSFT/PassportForWork/{TenantId}/Policies/PINComplexity/devicetenantidpoliciespincomplexityexpiration.

Pour un déploiement par stratégie de groupe (GPO), les paramètres se trouvent :

|  |  |
| --- | --- |
| GPO | Configuration de l’ordinateur > Modèles d’administration > **Système > Complexité du code confidentiel** |

1. Paramètres biométrique : ces paramètres sont utilisés pour configurer l'authentification biométrique.

Vous pouvez le trouver dans le chemin d'accès CSP suivant : ./Device/Vendor/MSFT/PassportForWork/Biometrics/UseBiometrics.

Pour un déploiement par GPO, les paramètres se trouvent :

|  |  |
| --- | --- |
| GPO | Configuration de l’ordinateur > Modèles d’administration > Composants **> Windows > Windows Hello Entreprise** |

1. Paramètres carte à puce (smartcard) : ces paramètres sont utilisés pour configurer l'authentification par carte à puce (smartcard) utilisée conjointement avec Windows Hello Entreprise.

Vous pouvez les trouver dans le chemin d'accès CSP suivant : ./Device/Vendor/MSFT/PassportForWork/{TenantId}/Policies/UseHelloCertificatesAsSmartCardCertificates.

Pour un déploiement par stratégie de groupe (GPO), les paramètres se trouvent :

|  |  |
| --- | --- |
| GPO | Configuration de l’ordinateur > Modèles d’administration > Composants **> Windows > Windows Hello Entreprise** |

Pour chaque paramètre, vous pouvez choisir de l'activer, de le désactiver ou de ne pas le configurer. Si vous activez un paramètre, les utilisateurs doivent respecter les règles que vous définissez. Si vous désactivez un paramètre, les utilisateurs ne peuvent pas utiliser la fonctionnalité correspondante. Si vous ne configurez pas un paramètre, les utilisateurs peuvent choisir d'utiliser la fonctionnalité ou non.

Remarque : pour utiliser Windows Hello Entreprise, les utilisateurs doivent avoir un appareil compatible et l’ES doit avoir une licence appropriée pour Windows 10 Entreprise ou ultérieur.

Documentation Microsoft :

* Configurer Windows Hello Entreprise : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/configure> ;
* Windows Hello Entreprise paramètres de stratégie : <https://learn.microsoft.com/fr-fr/windows/security/identity-protection/hello-for-business/policy-settings?tabs=feature>.

## Configuration de l’authentification avec Microsoft Authenticator

Procéder comme suit :

1. Dans Microsoft Entra ID, accéder à l’emplacement Méthodes d’authentification > Stratégies.
2. Sous Microsoft Authenticator, choisir les options suivantes :
   1. Activer - Oui ou Non.
   2. Cible - Tous les utilisateurs ou les utilisateurs sélectionnés.
3. 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
4. Pour appliquer la nouvelle stratégie, cliquer sur Enregistrer.

Ceci conclut le présent guide.