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

Guide de configuration de Windows Hello Entreprise 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](#_Toc176967594)

[1.1 Objectifs du guide 6](#_Toc176967595)

[1.2 Non-objectifs du guide 6](#_Toc176967596)

[2 Configuration de Windows Hello Entreprise au niveau des appareils 8](#_Toc176967597)

[3 Configuration de l’authentification avec Windows Hello Entreprise 11](#_Toc176967598)

# 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. Cette dernière est décrite dans le Guide de configuration de Pro Santé Connect à destination des établissements de santé.

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, Windows Hello Entreprise constitue un moyen d’identification électronique (MIE) retenu dans le périmètre du POC technique. (Le POC technique sécurisation cible plus spécifiquement cette utilisation.)

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/>.

Ainsi, l’ouverte de session avec Windows Hello Entreprise depuis un poste de travail Windows avec une jointure (hybride) à Entra ID permet au Professionnel de Santé (PS) de bénéficier 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) dans le cadre de cette délégation de l’authentification.

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.

## Objectifs du guide

L’objectif de ce guide est d’expliciter dans ce contexte les éléments de configuration de l’authentification avec Windows Hello Entreprise sur Microsoft Entra ID.

## 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.

Windows Hello Entreprise 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.) ;
* Microsoft Authenticator.

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 Microsoft Authenticator 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 Windows Hello Entreprise au niveau des appareils

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>.
* 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>

Enfin, pour les appareils avec jointure hybride à Entra ID, l’erreur à la connexion en WHFB suivante peut être rencontrée :

« Vos informations d’identification n’ont pas pu être vérifiées »

Les modalités de correction de cette erreur sont décrite dans l’article Erreur « Vos informations d’identification n’ont pas pu être vérifiées » lors de la connexion à Windows avec Windows Hello Entreprise : <https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/user-profiles-and-logon/your-credential-could-not-be-verified-error-when-logging-on-to-windows-by-using-whfb>.

Deux opérations sont à également réaliser pour en complément :

1. Installer un objet serveur Kerberos, Cf. Installer le module AzureADHybridAuthenticationManagement: <https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-passwordless-security-key-on-premises#install-the-azureadhybridauthenticationmanagement-module> ;
2. Configurer les postes à l'aide de Microsoft Intune ou via une stratégie de groupe (Group Policy Object ou GPO) pour permettre la connexion avec l'Active Directory en local, Cf. Guide de déploiement de l’approbation Kerberos cloud : <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/deploy/hybrid-cloud-kerberos-trust>.

# 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>.

Windows Hello Entreprise peut être configuré plus simplement, soit au niveau du locataire (dans intune, Devices/windows enrollment/windows hello for business), soit en suivant le guide Paramètres de profil Identity Protection dans Intune pour Windows Hello Entreprise : <https://learn.microsoft.com/fr-fr/mem/intune/protect/identity-protection-windows-settings>.

Ceci conclut le présent guide.