

# Gestion de compte Azure Active Directory sur poste Windows

## Table des matières

Présentation de l'entreprise **2**

Contexte **3**

Liste des solutions **4**

Choix de la solution **6**

Projet **7**

Suppression d'un compte collaborateur.....**8**

**Installation de Windows / Ajout du compte principal..... 16**

Liaison au domaine Azure Active Directory / Ajout du compte principal..... **29**

Ajout d'un compte collaborateur ..... **33**

En raison du RGPD et donc de la protection des données à caractères personnels, le site de base de données ne sera pas présenté, mais uniquement la procédure concernant les postes WINDOWS

## Présentation de l'entreprise

SFEIR est un pure player du digital, basée à Paris, Lille, Luxembourg Strasbourg, Nantes, Bordeaux et Bruxelles, regroupant près de 700 développeurs spécialisés dans le développement d'applications de pointe. Nos langages de prédilection : Java, JavaScript, Go, .NET, NodeJS et Python. Pionner du cloud en France, nous accompagnons nos clients dans leur transformation numérique et pensons des solutions efficaces pour leurs utilisateurs.

#Front-End #Back-End #Cloud #Mobile #Data #IoT #DevOps #Assistants #UX-UI

Nous sommes fiers d'être développeurs. Nous partageons la même culture, ainsi que des valeurs qui nous sont chères : partage, humilité, bienveillance.

Notre process de recrutement : les PlayOffs, 3 tests d'évaluation technique en peer-programming (Algorithme, Langage, IaC).

Angelo, SFEIRIEN depuis 3 ans - Developpeur Agile Web

« Lorsque j'ai passé les PlayOffs, c'était une expérience très enrichissante. J'ai rencontré des évaluateurs brillants, bienveillants, où j'ai appris des choses, en mode coaching ».

En quoi SFEIR est différent ?

Nicolas, SFEIRIEN depuis 8 ans - Software Architect & Team Leader

“C'est un état d'esprit. L'humain avant tout. La fierté d'être développeur. Le salaire au-dessus du marché aussi. Les consultants sont pris en considération. Nous appartenons à une famille. Tout le monde est facile à vivre et toujours prêt à aider. Chez SFEIR, nous donnons à chacun la possibilité de se développer. Il y a souvent un fossé entre ce qu'une entreprise communique & la réalité quotidienne. Pas chez SFEIR.”

## Contexte

Comme indiqué dans la présentation de l'entreprise, SFEIR est un pure player du digital basée à Paris, Lille, Luxembourg Strasbourg, Nantes, Bordeaux et Bruxelles, regroupant près de 700 collaborateurs.

En raison de la présence d'une unique équipe DSI, composée de M Guillaume LEFELLE, administrateur réseau, et de l'alternant M Stanick LI, basée sur Paris, la possibilité d'administrer efficacement les postes collaborateurs est restreinte. A cela s'ajoutent les contraintes physiques et humaines, rendant la tâche difficile.

Ainsi, l'équipe SIS de SFEIR est à la recherche d'une solution permettant d'administrer efficacement l'accès aux comptes et aux postes des collaborateurs situés dans les autres agences, hors Paris.

Liste de solutions

- Azure Active Directory (Azure AD) est un service d'annuaire cloud fourni par Microsoft dans le cadre de sa suite de services Azure. Il s'agit d'un service d'authentification et d'autorisation qui permet aux entreprises de gérer l'identité et l'accès de leurs utilisateurs à diverses applications cloud et services. Azure AD offre un large éventail de fonctionnalités de sécurité, de gestion des identités et des accès, notamment :

L'authentification unique (SSO) pour permettre aux utilisateurs d'accéder à plusieurs applications avec un seul nom d'utilisateur et un seul mot de passe.

La gestion des identités et des accès pour créer, gérer et supprimer des comptes utilisateur, des groupes et des rôles.

La gestion des appareils pour contrôler l'accès aux ressources en fonction des paramètres de sécurité des appareils.

La surveillance et la protection de l'accès aux ressources pour détecter les menaces potentielles et protéger les données confidentielles.

La gestion de l'application pour contrôler l'accès aux applications cloud.

Azure AD peut être intégré à un large éventail de services cloud et de plateformes, notamment Office 365, Azure, Dynamics 365, et de nombreux autres services tiers.

- Scaleway est un fournisseur de services d'infrastructure cloud qui propose une gamme complète de solutions d'hébergement pour les entreprises et les particuliers. Fondée en 2015, Scaleway est une filiale d'Iliad, une entreprise française de télécommunications.

Scaleway propose une large gamme de services cloud, allant des serveurs dédiés aux instances de machines virtuelles, en passant par les solutions de stockage et de base de données. Les clients peuvent également profiter de services de conteneurs et d'orchestration, ainsi que de solutions de mise en réseau et de sécurité pour garantir la disponibilité et la sécurité de leurs applications.

Scaleway dispose également de centres de données en France, aux Pays-Bas et en Pologne, permettant aux clients de choisir l'emplacement de leurs données pour se conformer aux réglementations en matière de confidentialité et de sécurité des données.

En plus de ses offres cloud, Scaleway propose également des solutions d'edge computing, qui permettent aux entreprises de traiter les données sur site et de les envoyer ensuite dans le cloud pour un traitement ultérieur. Scaleway est connu pour ses tarifs compétitifs et sa flexibilité, permettant aux clients de choisir des solutions sur mesure adaptées à leurs besoins spécifiques.

- JumpCloud est une plateforme de gestion des identités et des accès basée sur le cloud, conçue pour permettre aux entreprises de sécuriser et de gérer les accès de leurs utilisateurs à toutes leurs ressources informatiques, qu'il s'agisse de serveurs, de postes de travail, d'applications ou de réseaux.

JumpCloud propose une solution d'annuaire cloud centralisée qui permet aux administrateurs informatiques de créer et de gérer les comptes utilisateur, de définir les politiques d'accès et de suivre les activités des utilisateurs. La solution prend en charge une large gamme de protocoles d'authentification, notamment LDAP, RADIUS et SAML, pour garantir une intégration transparente avec les applications et services existants.

JumpCloud offre également une solution de gestion des systèmes d'exploitation qui permet aux administrateurs de gérer les postes de travail et les serveurs à partir d'un seul et même portail. Cette solution comprend des fonctionnalités telles que le déploiement à distance de logiciels, les mises à jour système automatiques et la gestion des correctifs de sécurité.

Enfin, JumpCloud propose également des solutions de gestion des identités pour les appareils mobiles, ainsi qu'une solution de gestion des accès privilégiés pour contrôler et surveiller l'accès des administrateurs aux ressources sensibles.

Dans l'ensemble, JumpCloud est une solution de gestion des identités et des accès complète et évolutive, qui convient aux entreprises de toutes tailles et de tous secteurs d'activité.

- OneLogin est une plateforme de gestion des identités et des accès basée sur le cloud, qui permet aux entreprises de sécuriser l'accès à leurs applications web et mobiles, ainsi que d'autres ressources, telles que des serveurs, des postes de travail, des réseaux et des données.

OneLogin permet aux administrateurs de gérer les comptes d'utilisateur, les politiques d'accès et les mots de passe, et de suivre les activités des utilisateurs à partir d'une interface centralisée. La plateforme prend en charge une large gamme de protocoles d'authentification, notamment SAML, OpenID Connect, OAuth 2.0 et LDAP, permettant ainsi une intégration facile avec les applications et les services existants.

OneLogin offre également une solution de gestion des accès privilégiés pour contrôler et surveiller l'accès des administrateurs aux ressources sensibles. La plateforme fournit des outils de conformité pour aider les entreprises à respecter les réglementations en matière de sécurité des données, telles que GDPR et HIPAA.

OneLogin dispose également d'une fonctionnalité de provisionnement automatisé pour simplifier le processus de création et de gestion des comptes utilisateur. La plateforme offre également une intégration avec des solutions de gestion de la mobilité d'entreprise (EMM) pour la gestion des appareils mobiles.

Dans l'ensemble, OneLogin est une solution de gestion des identités et des accès complète et évolutive, qui convient aux entreprises de toutes tailles et de tous secteurs d'activité. La plateforme est connue pour sa facilité d'utilisation, son intégration transparente et sa sécurité de pointe.

## Choix de la solution

Azure AD est un service de gestion des identités et des accès basés sur le cloud, qui offre de nombreux avantages par rapport aux services LDAP traditionnels :

Intégration avec les services cloud de Microsoft : Azure AD est étroitement intégré avec les services cloud de Microsoft tels que Office 365, Dynamics 365 et Azure. Cela facilite la gestion des identités et des accès pour les utilisateurs de ces services.

Sécurité avancée : Azure AD offre une sécurité de pointe, avec des fonctionnalités telles que l'authentification multifactorielle, la protection contre les attaques par force brute et la gestion des risques d'accès.

Évolutivité : Azure AD est conçu pour être facilement évolutif, et peut facilement s'adapter aux besoins des entreprises en pleine croissance.

Coût : Azure AD offre des options tarifaires flexibles pour répondre aux besoins de toutes les entreprises, de la petite entreprise à la grande entreprise.

Gestion centralisée des identités et des accès : Azure AD offre une gestion centralisée des identités et des accès pour tous les services, applications et systèmes de l'entreprise, offrant ainsi une solution unifiée pour les administrateurs informatiques.

Intégration avec des services tiers : Azure AD prend en charge les normes d'authentification modernes telles que SAML et OAuth, ce qui facilite l'intégration avec des services tiers tels que Salesforce et Dropbox.

En résumé, Azure AD est un choix judicieux pour les entreprises qui souhaitent une solution de gestion des identités et des accès évolutive, sécurisée et facilement intégrable avec les services cloud de Microsoft.

**SFEIR utilise également Azure AD depuis sa création et présente actuellement un partenariat avec Microsoft, facilitant le choix de la solution.**

## PROJET

Mettre en place une solution sécurisée des postes collaborateurs et une gestion facile de celle-ci.

La connexion à un poste Windows avec un compte Azure AD présente plusieurs avantages pour les entreprises qui utilisent déjà Azure AD pour la gestion de leurs identités et de leurs accès :

**Authentification unique** : Les utilisateurs peuvent accéder à leur poste de travail et à toutes les applications web et cloud associées à leur compte Azure AD à l'aide d'une seule authentification.

**Gestion centralisée des identités** : Les administrateurs peuvent gérer les comptes utilisateur, les politiques d'accès et les mots de passe à partir d'une interface centralisée, ce qui facilite la gestion des utilisateurs et la mise en œuvre des politiques de sécurité.

**Sécurité accrue** : La connexion à un poste Windows avec un compte Azure AD offre une sécurité accrue, car les comptes utilisateurs sont protégés par l'authentification multifactorielle, la protection contre les attaques par force brute et la gestion des risques d'accès.

**Facilité d'intégration** : Azure AD est étroitement intégré avec les services cloud de Microsoft tels qu'Office 365 et Azure, ce qui facilite l'intégration avec ces services et permet aux utilisateurs d'accéder facilement à leurs applications et services associés à leur compte Azure AD.

**Flexibilité** : Les comptes Azure AD peuvent être configurés pour autoriser l'accès aux postes de travail Windows à partir de n'importe quel emplacement, ce qui offre une plus grande flexibilité pour les utilisateurs en déplacement.

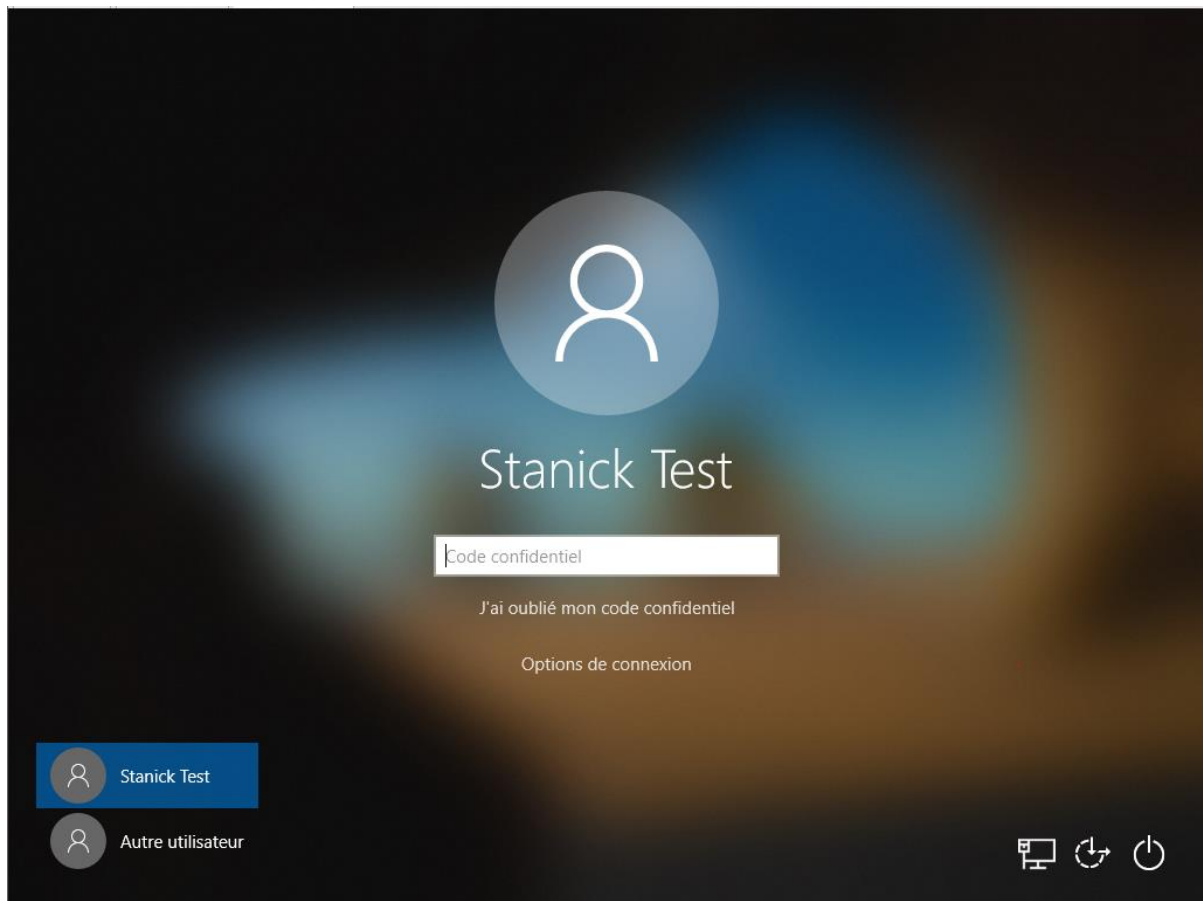
En résumé, la connexion à un poste Windows avec un compte Azure AD offre une gestion centralisée des identités, une sécurité accrue, une authentification unique et une facilité d'intégration pour les utilisateurs qui utilisent déjà Azure AD pour la gestion de leurs identités et de leurs accès.

[Suppression de compte collaborateur du poste](#)

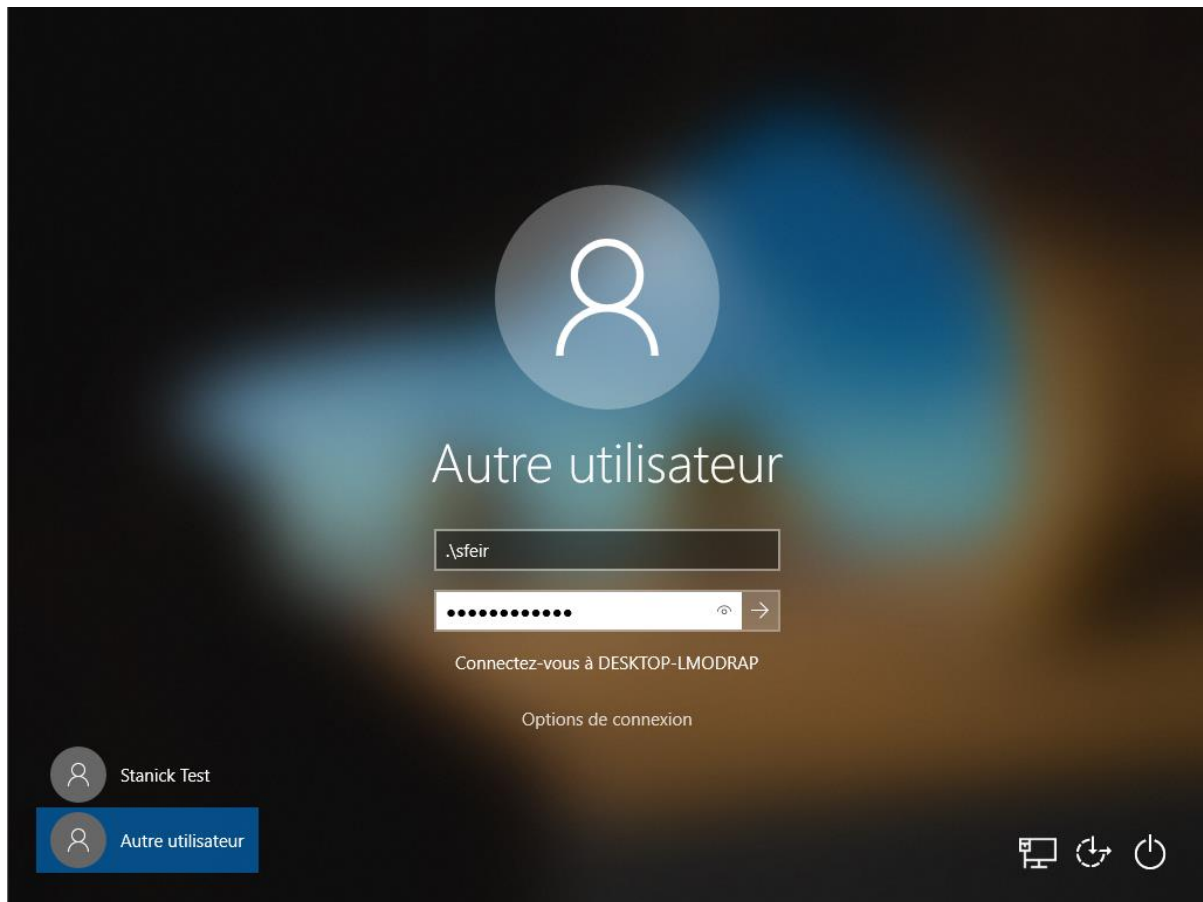
Lorsqu'un collaborateur n'a plus besoin du poste pour quelque raison (départ de la société, prêt terminé), il convient de supprimer ses accès au poste, mais également les données le concernant.

Possible également de **formater** son poste et repartir de zéro.

Dès lors, nous revenons sur le compte principal, que ce soit l'admin local ou le compte admin du domaine afin de supprimer le compte du collaborateur.







Dans Autres utilisateurs, sélectionner le compte à supprimer et cliquer sur le bouton associé.

Paramètres

Accueil

Rechercher un paramètre

Comptes

Vos informations

E-mail et comptes

Options de connexion

Accès Professionnel ou Scolaire

**Autres utilisateurs**

Synchroniser vos paramètres

Autres utilisateurs

Utilisateurs d'entreprise ou d'école

Ajouter un utilisateur professionnel ou scolaire

AzureAD\StanickTest

Administrateur

AzureAD\adminSIS

Administrateur

Autres utilisateurs

Ajouter un autre utilisateur sur ce PC

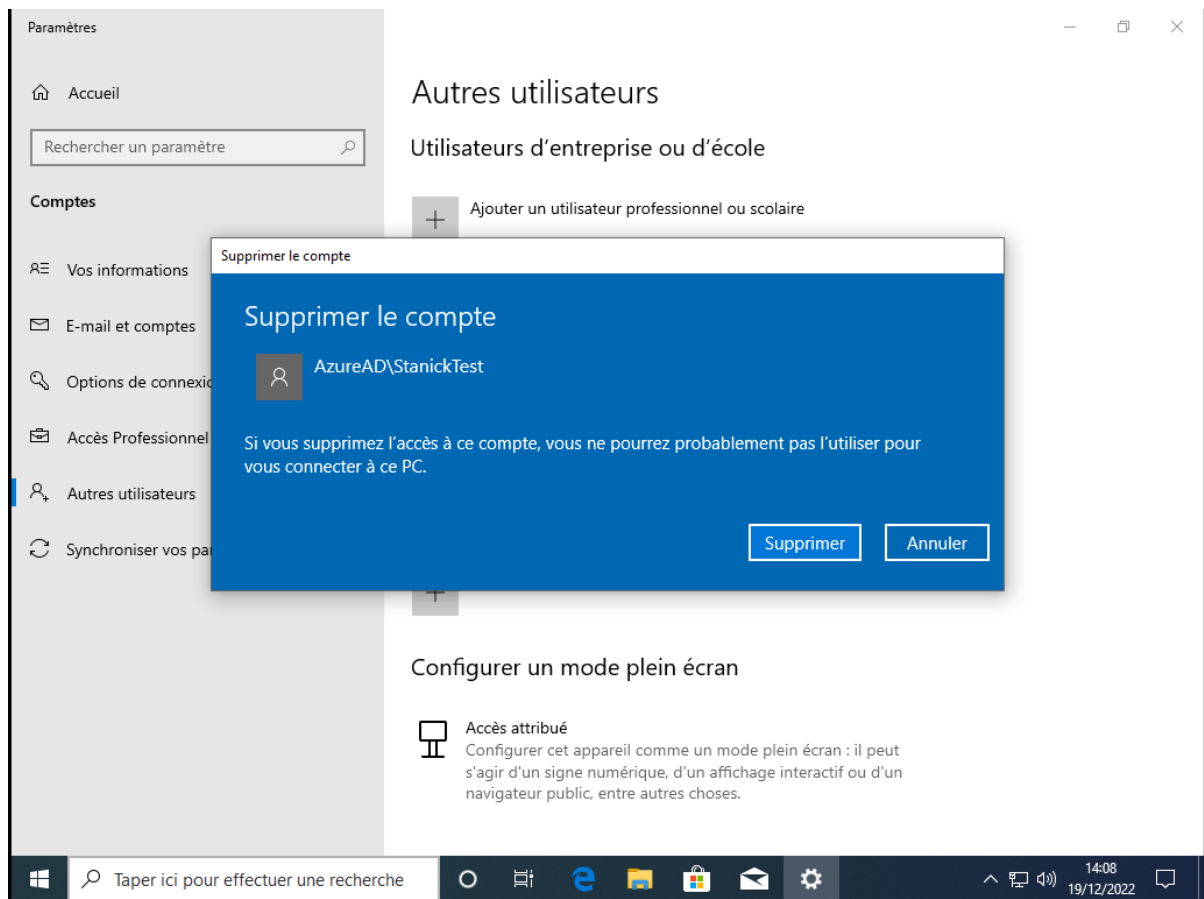
Accès attribué

Configurer cet appareil comme un mode plein écran : il peut s'agir d'un signe numérique, d'un affichage interactif ou d'un navigateur public, entre autres choses.

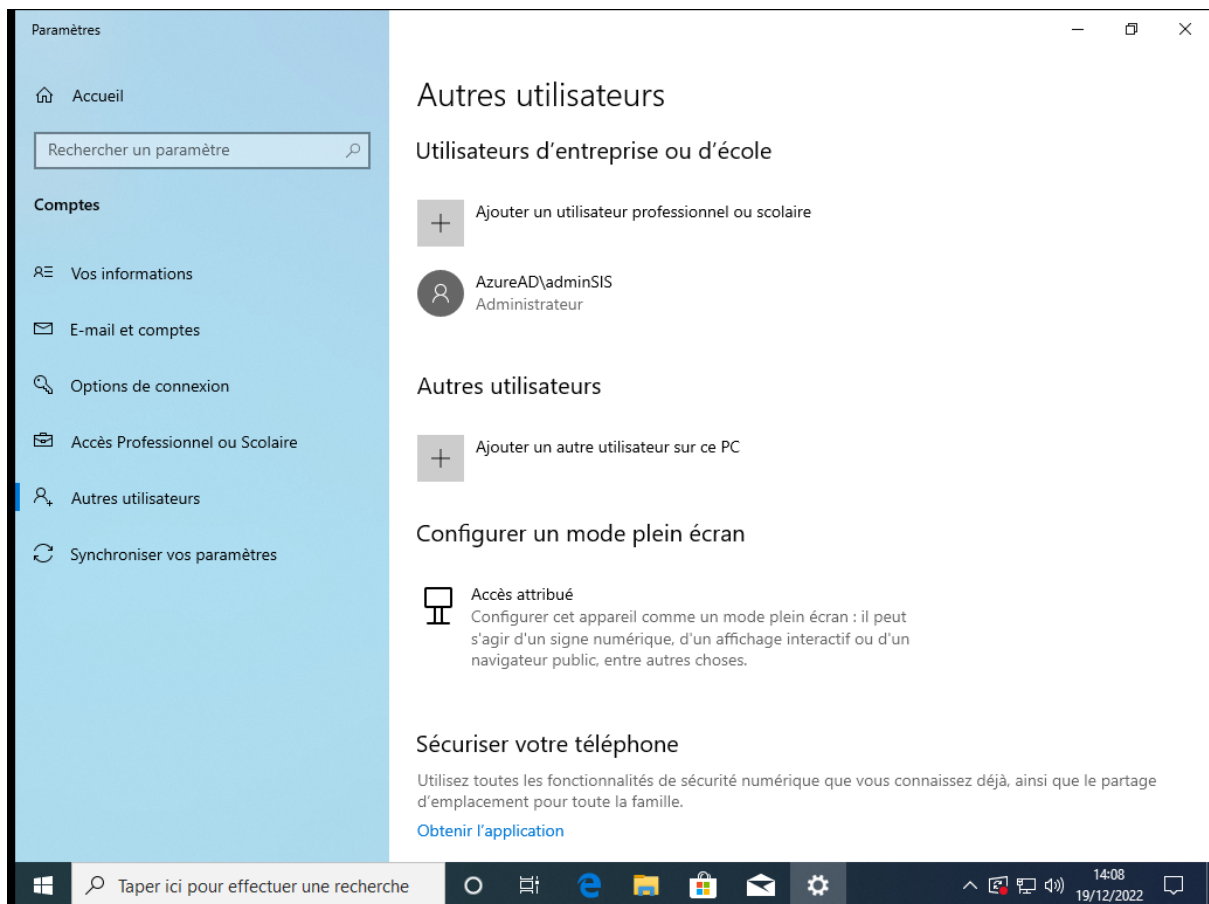
Sécuriser votre téléphone

Utilisez toutes les fonctionnalités de sécurité numérique que vous connaissez déjà, ainsi que le partage



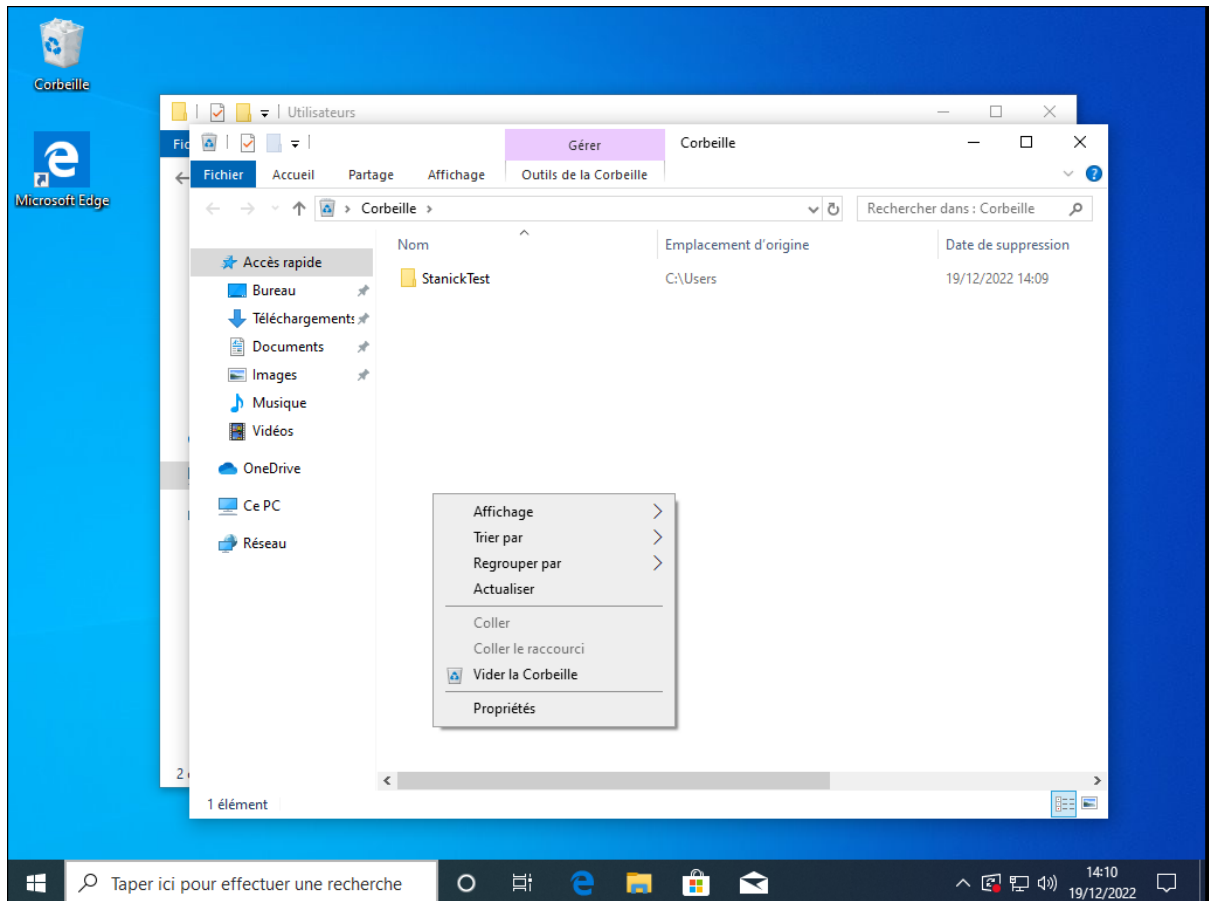
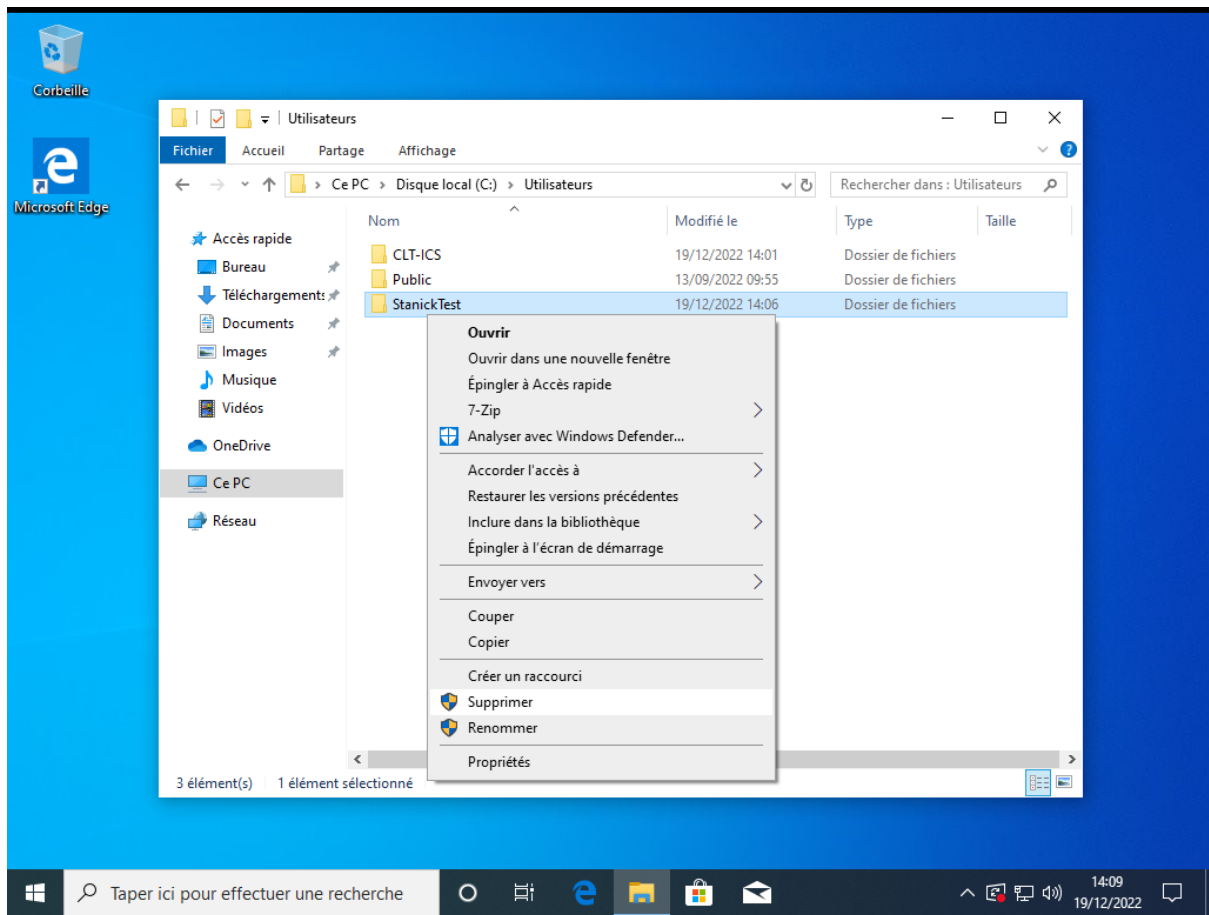


Le compte collaborateur est désormais supprimé, il faut également en faire de même pour ses données.

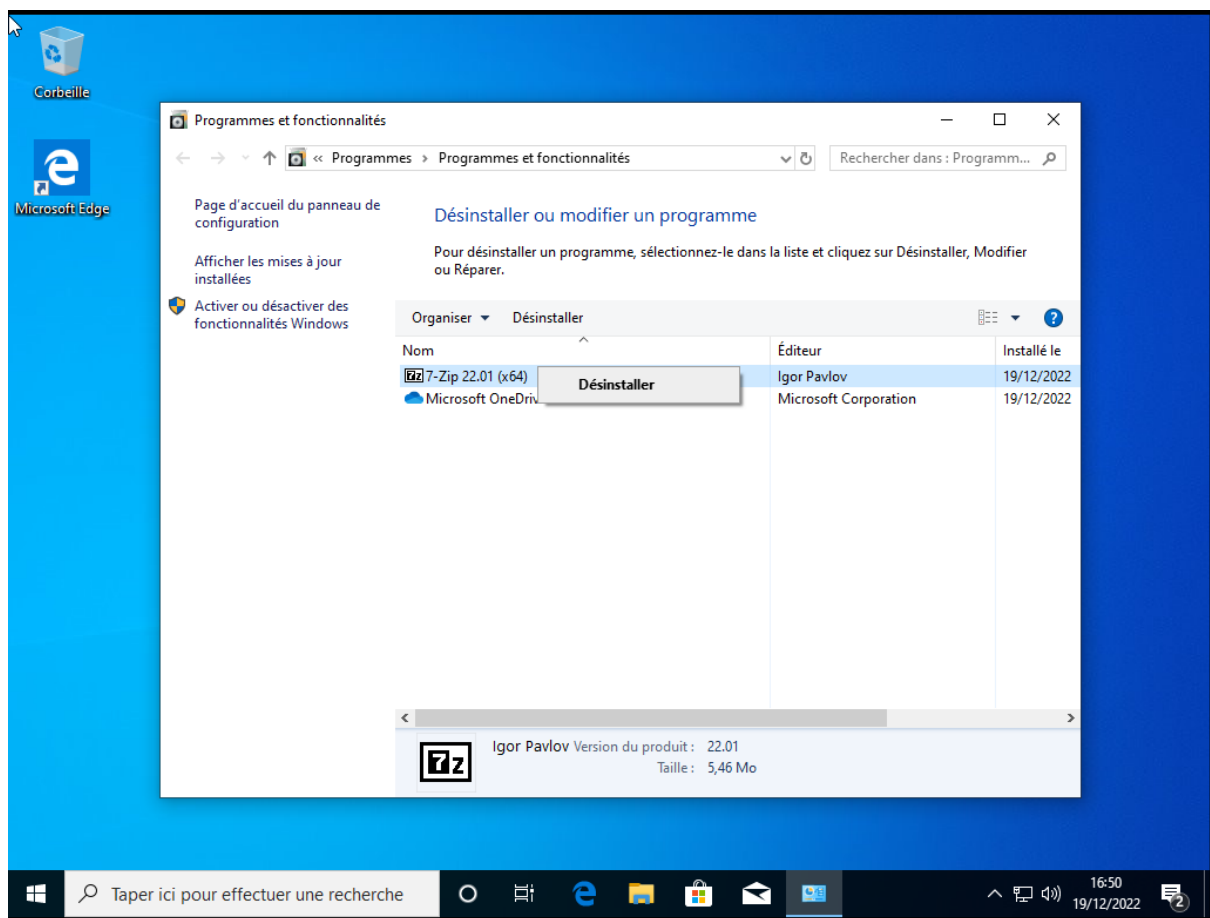


Dans l'explorateur de fichiers, accéder à la partie Utilisateurs et supprimer le dossier associé au nom du collaborateur ayant utilisé le poste.

Confirmer en supprimant ce même dossier dans la corbeille.

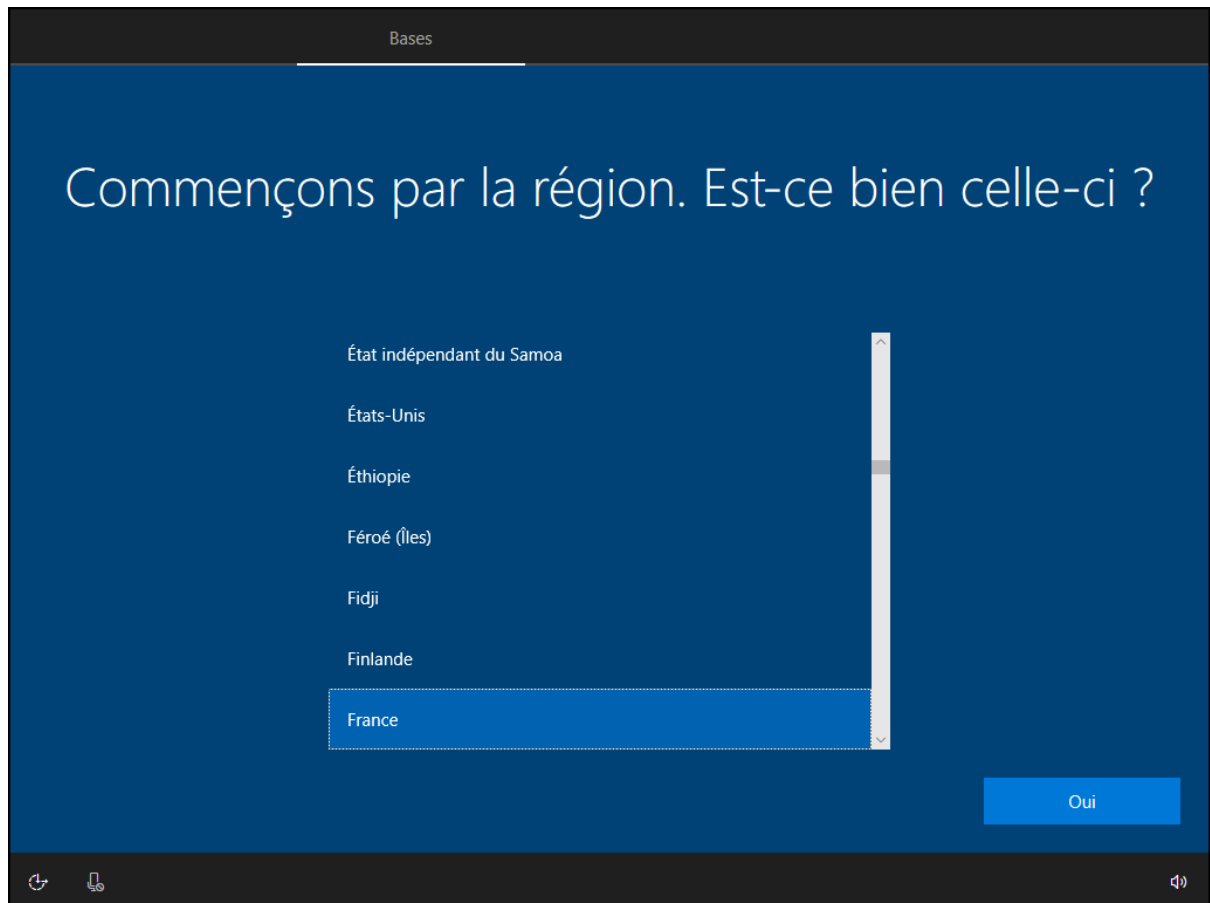


Vérifier dans Programmes et fonctionnalités les éventuelles applications à désinstaller.



## Installation de Windows / Ajout direct du compte principal

Lors d'une installation neuve de Windows, les paramètres de base sont à configurer tels que la région, la langue d'affichage, la disposition du clavier, le réseau (partie coupée en raison de la connexion filaire/Ethernet) et les mises à jour.





# Est-ce la bonne disposition de clavier ?

Si vous utilisez également un autre disposition de clavier, vous pouvez l'ajouter après.

Français

Belge (virgule)

Français (Belgique)

Français (Suisse)

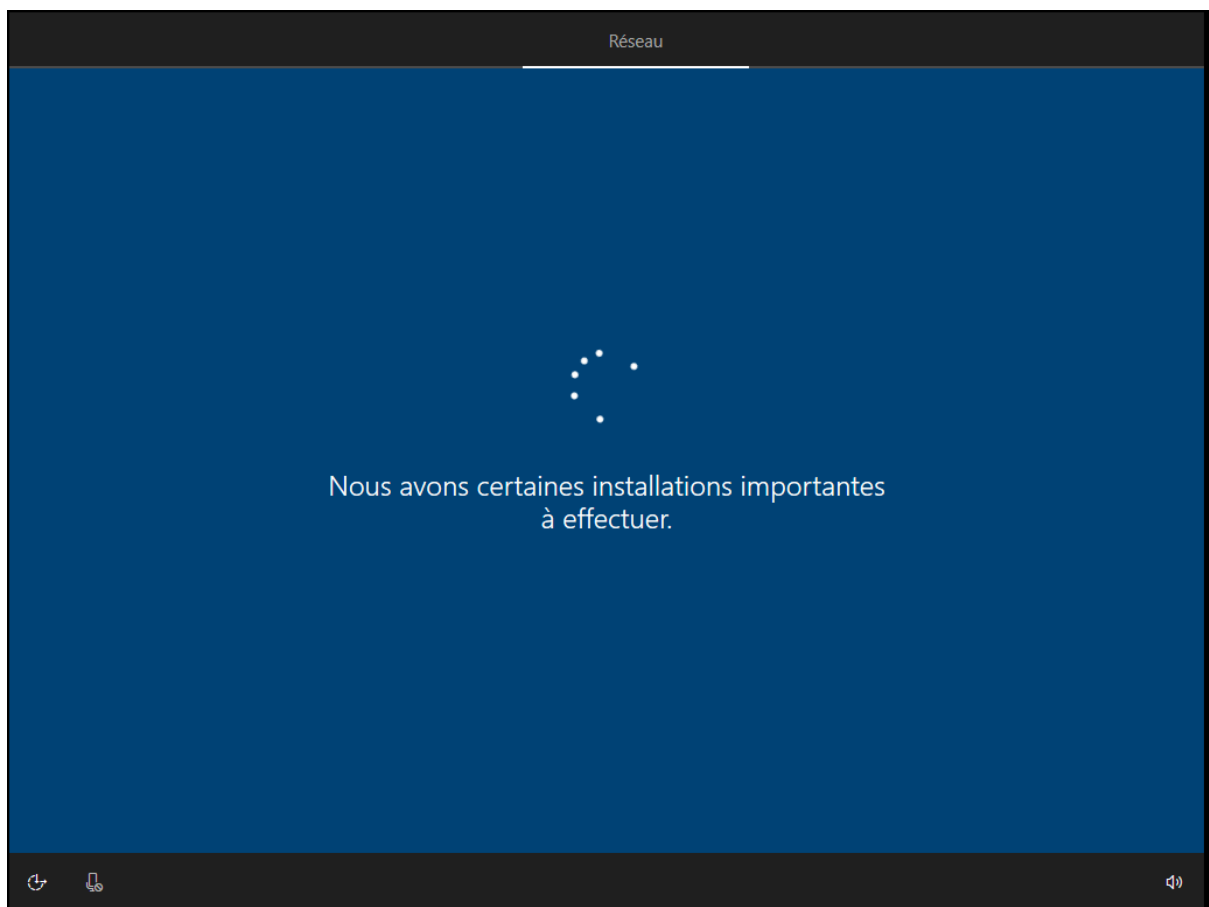
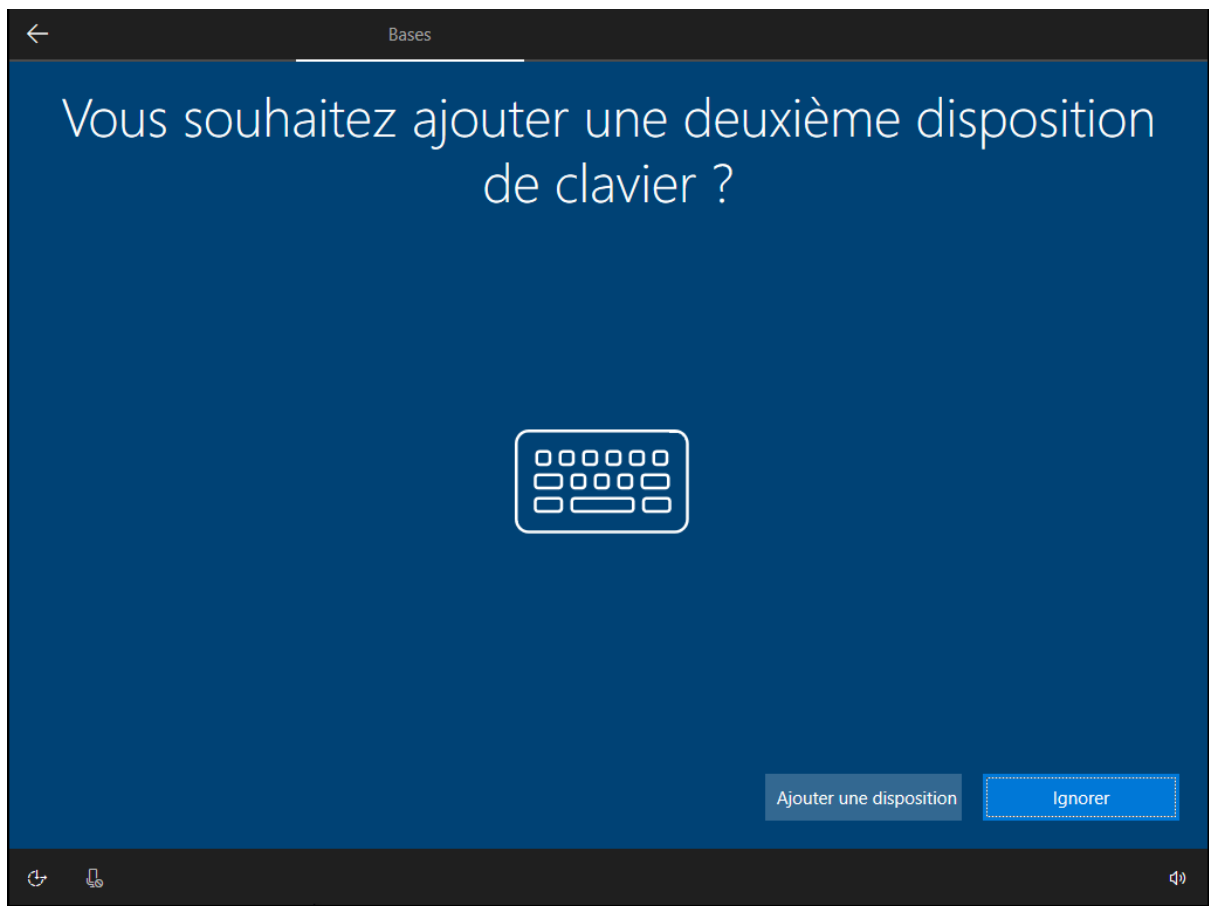
Français traditionnel (Canada)

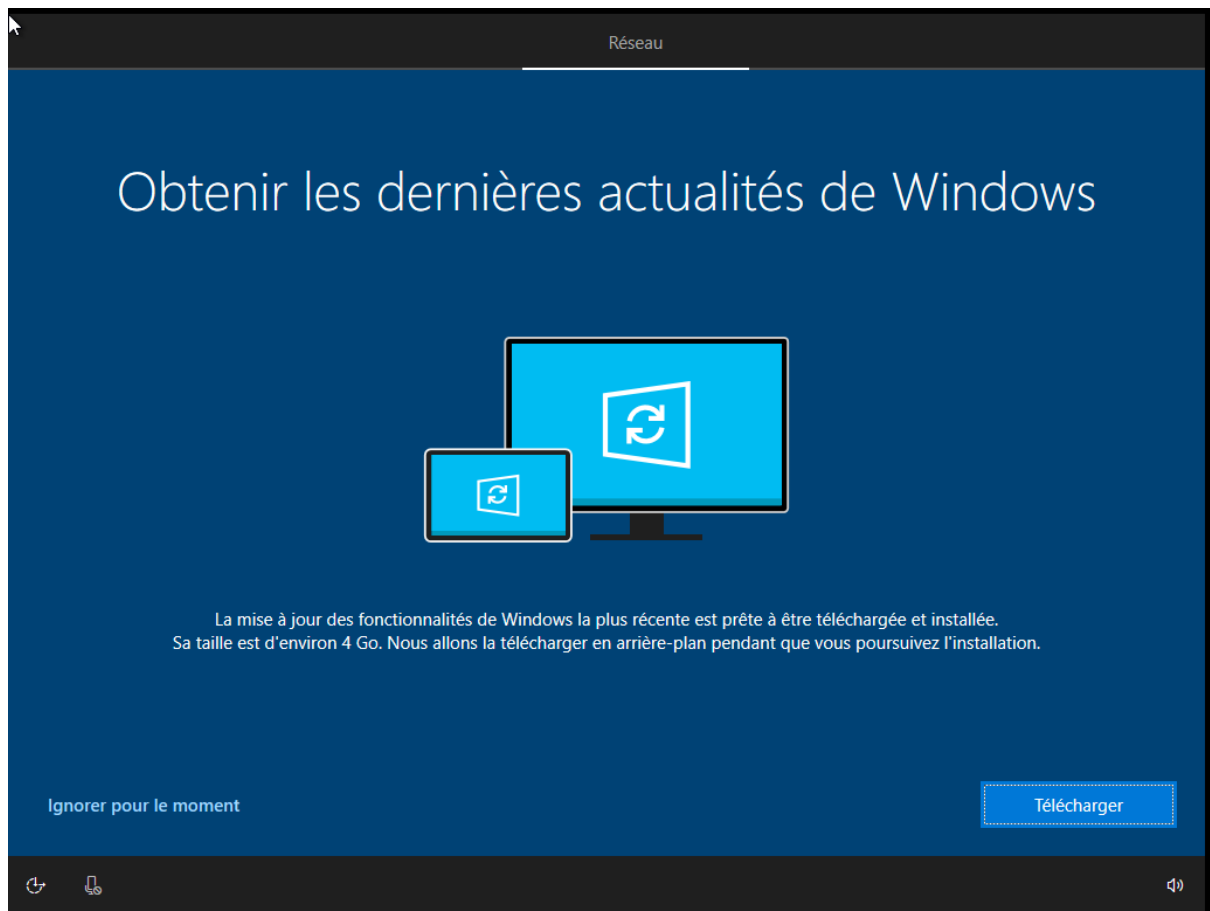
Albanais

Allemand

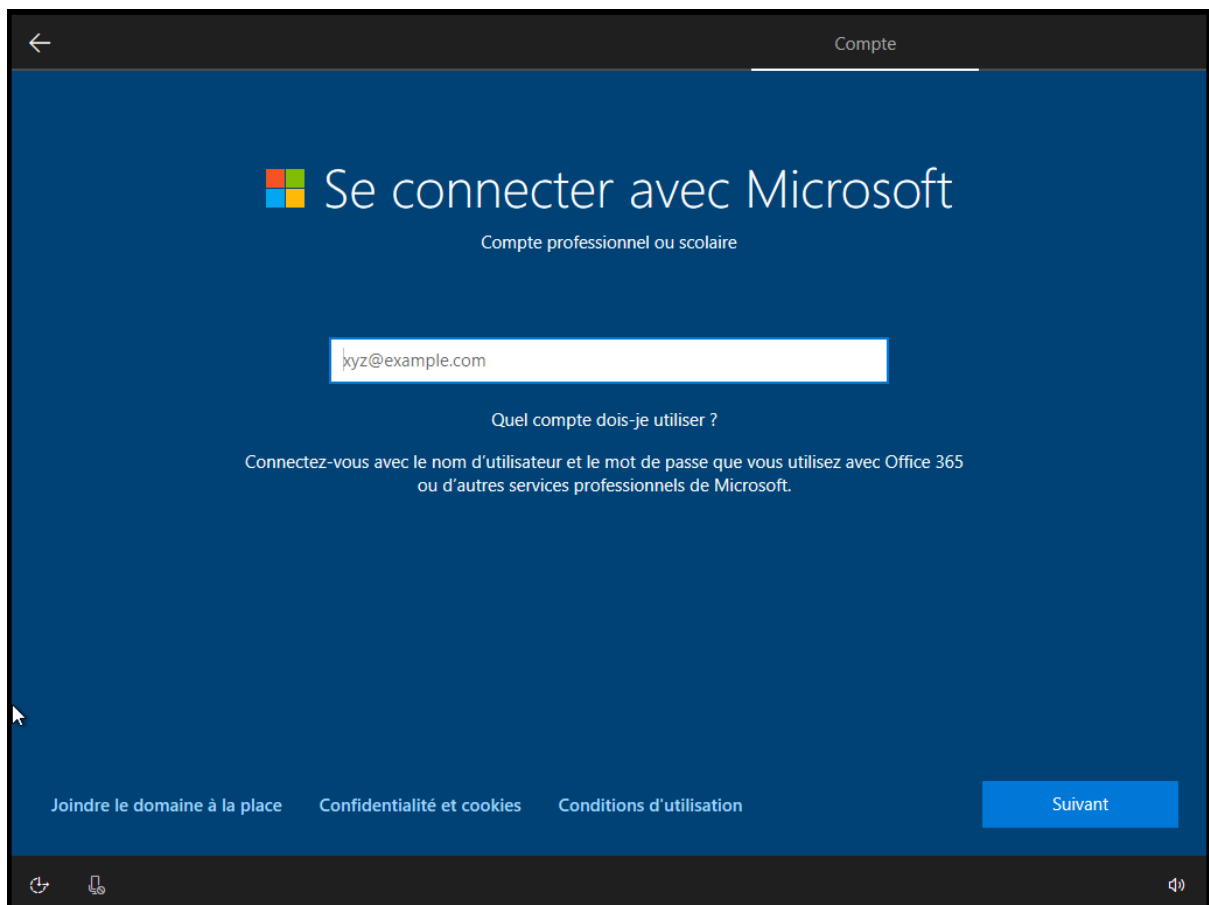
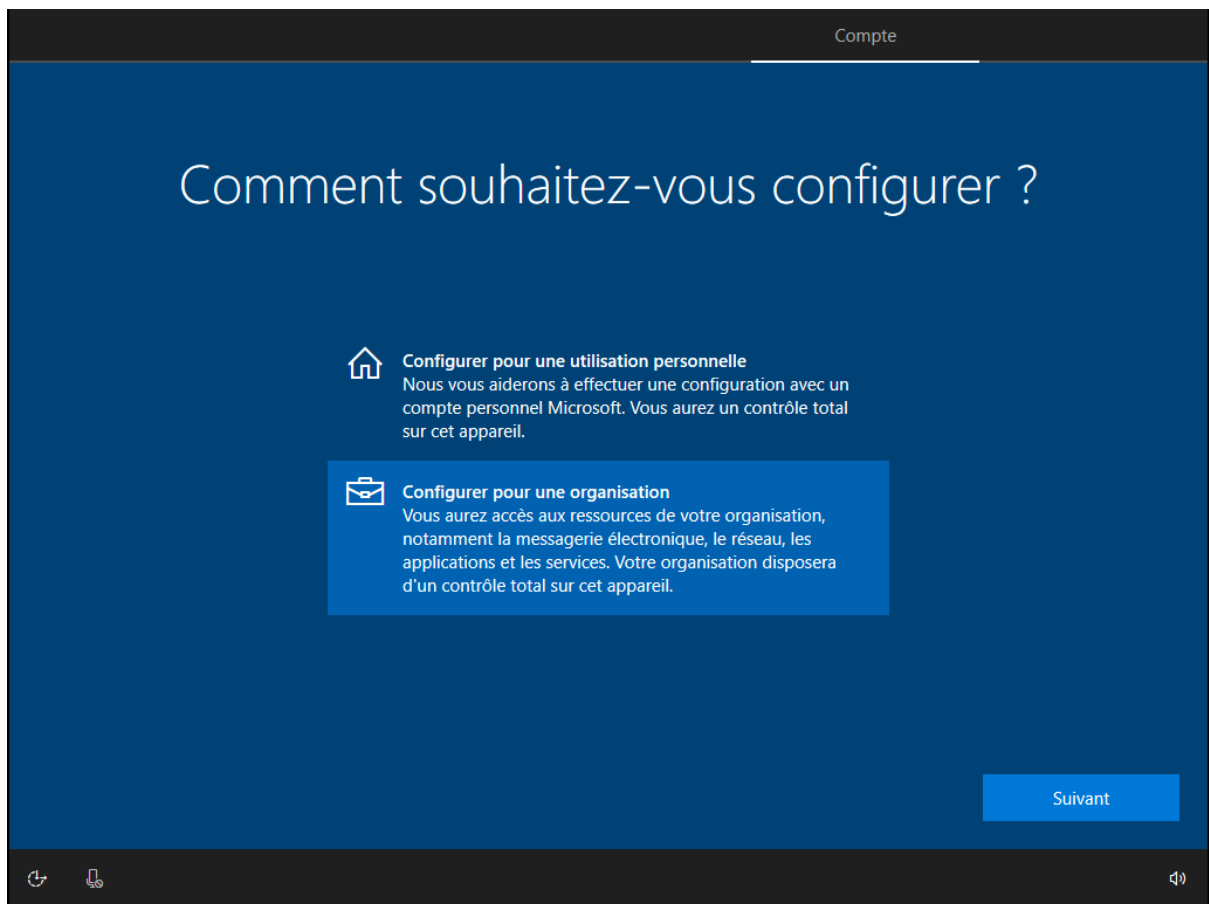
Oui








Dans la section de configuration de compte, sélectionner Configurer pour une organisation et saisir les informations de connexion.



Compte




# Entrez votre mot de passe

Entrer le mot de passe pour sis.azure@sfeir.com

[Mot de passe oublié ?](#)

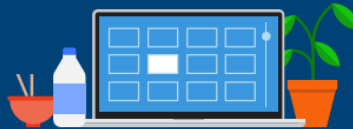
Retour

Suivant



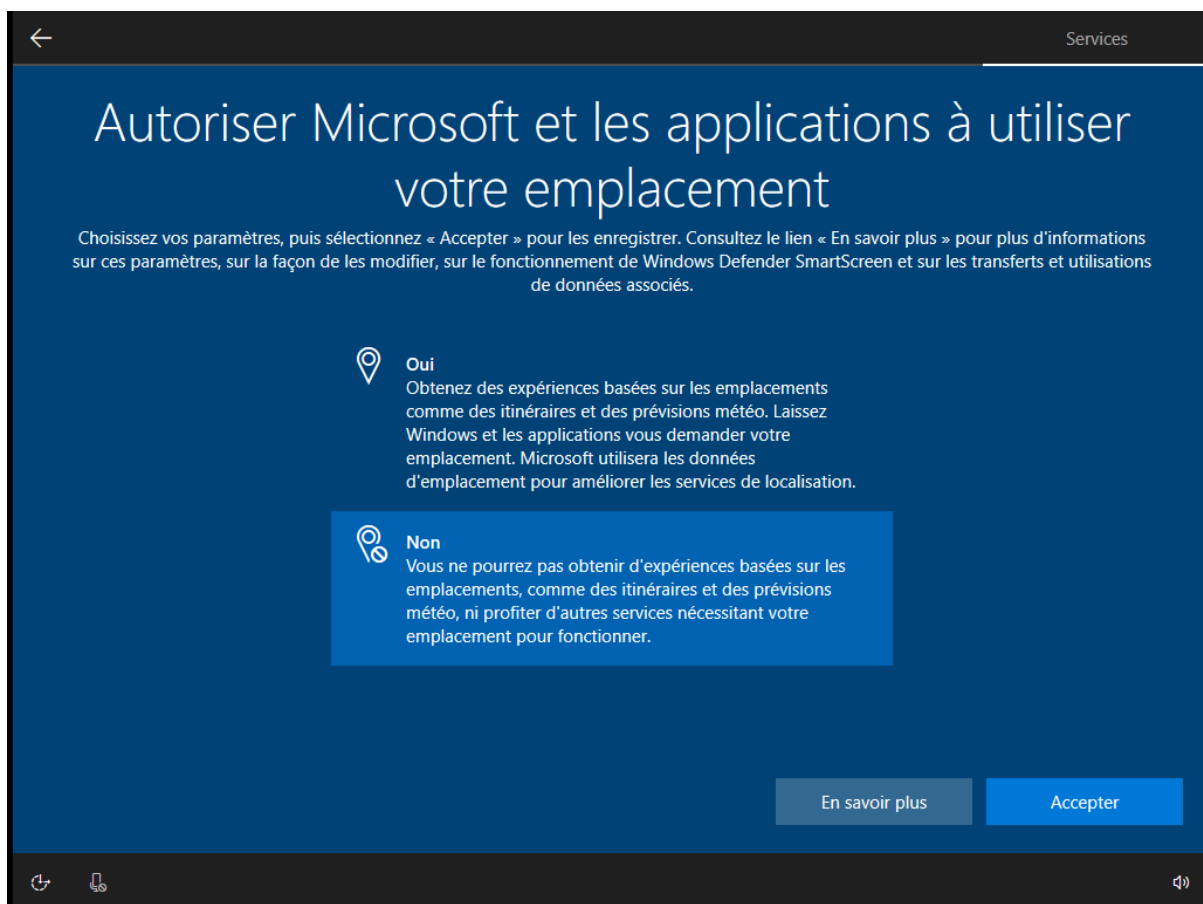
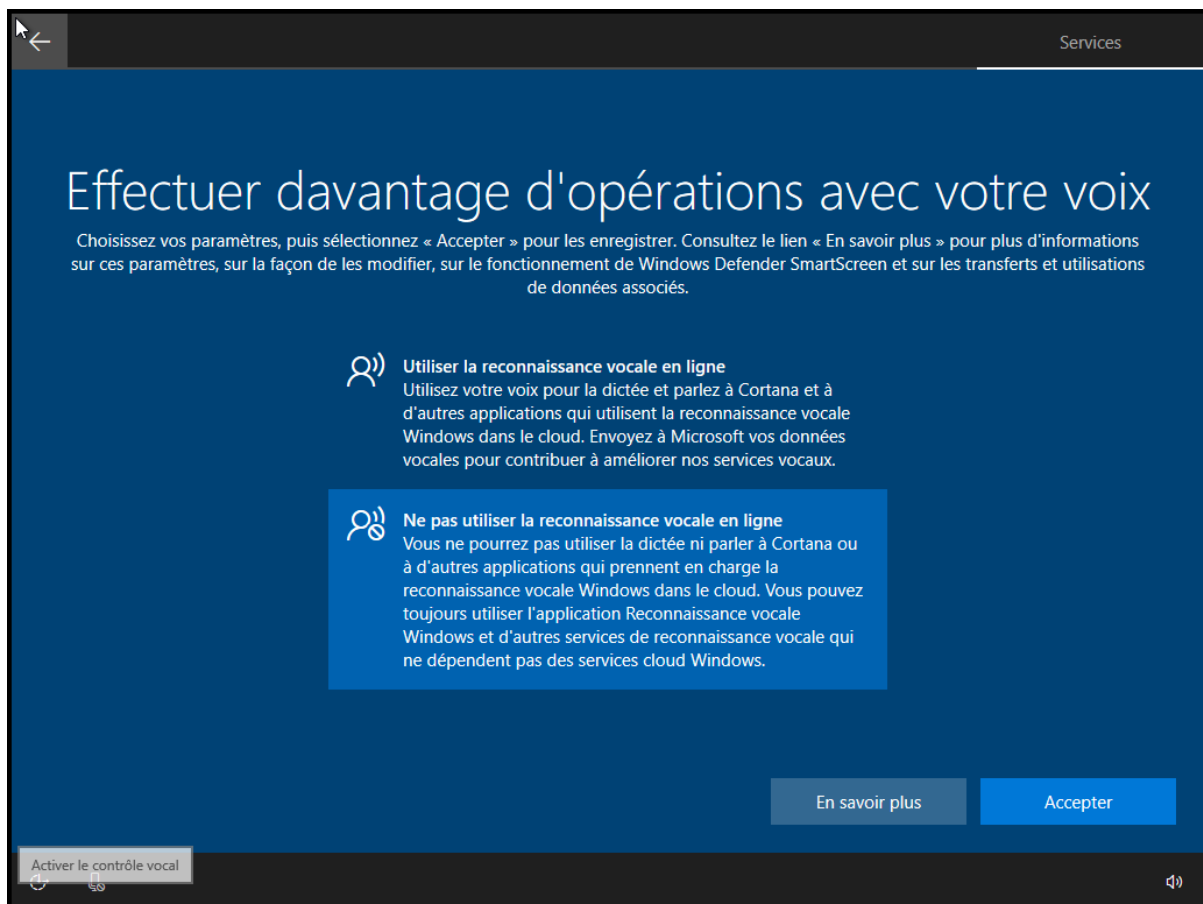
D'autres paramètres optionnels (historique, reconnaissance vocale, localisation, diagnostic, écriture manuscrite et publicité ciblée) sont à confirmer.

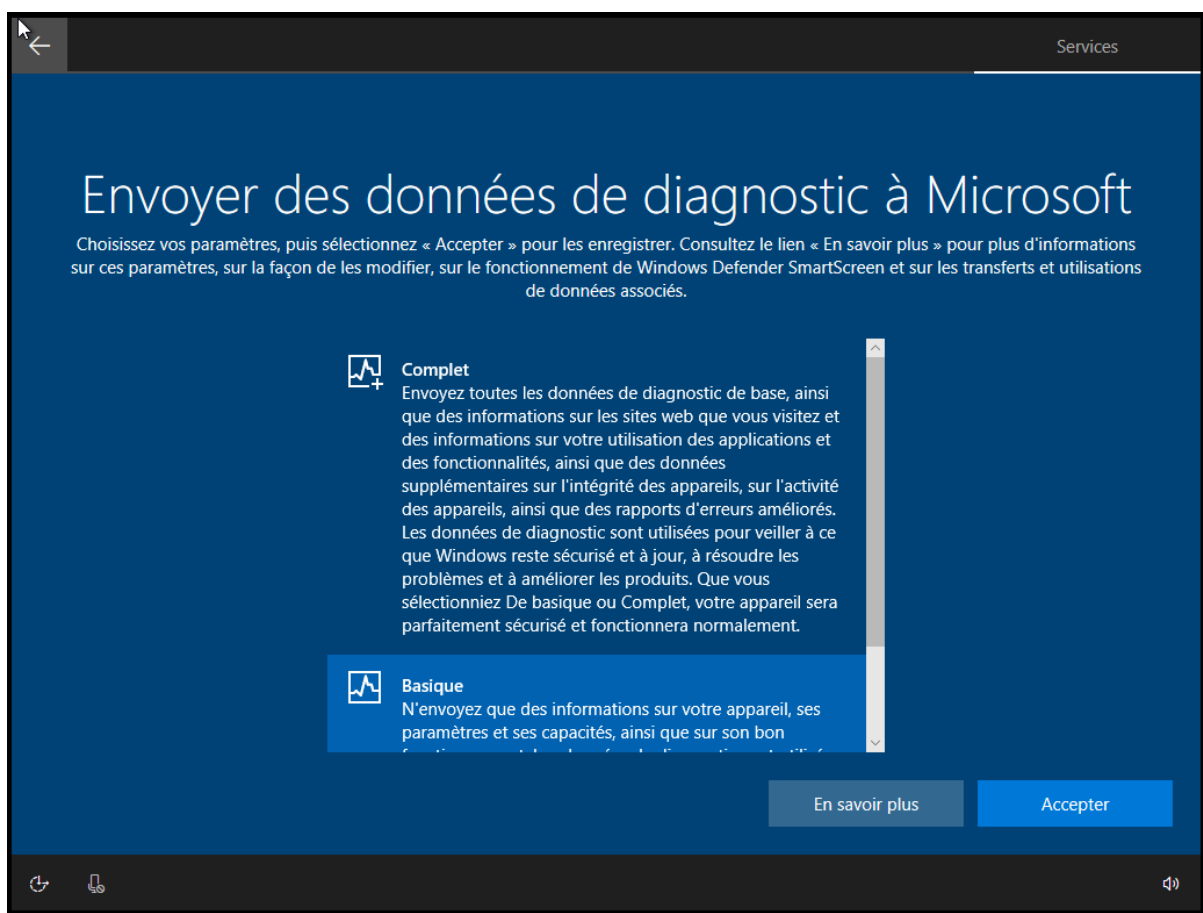
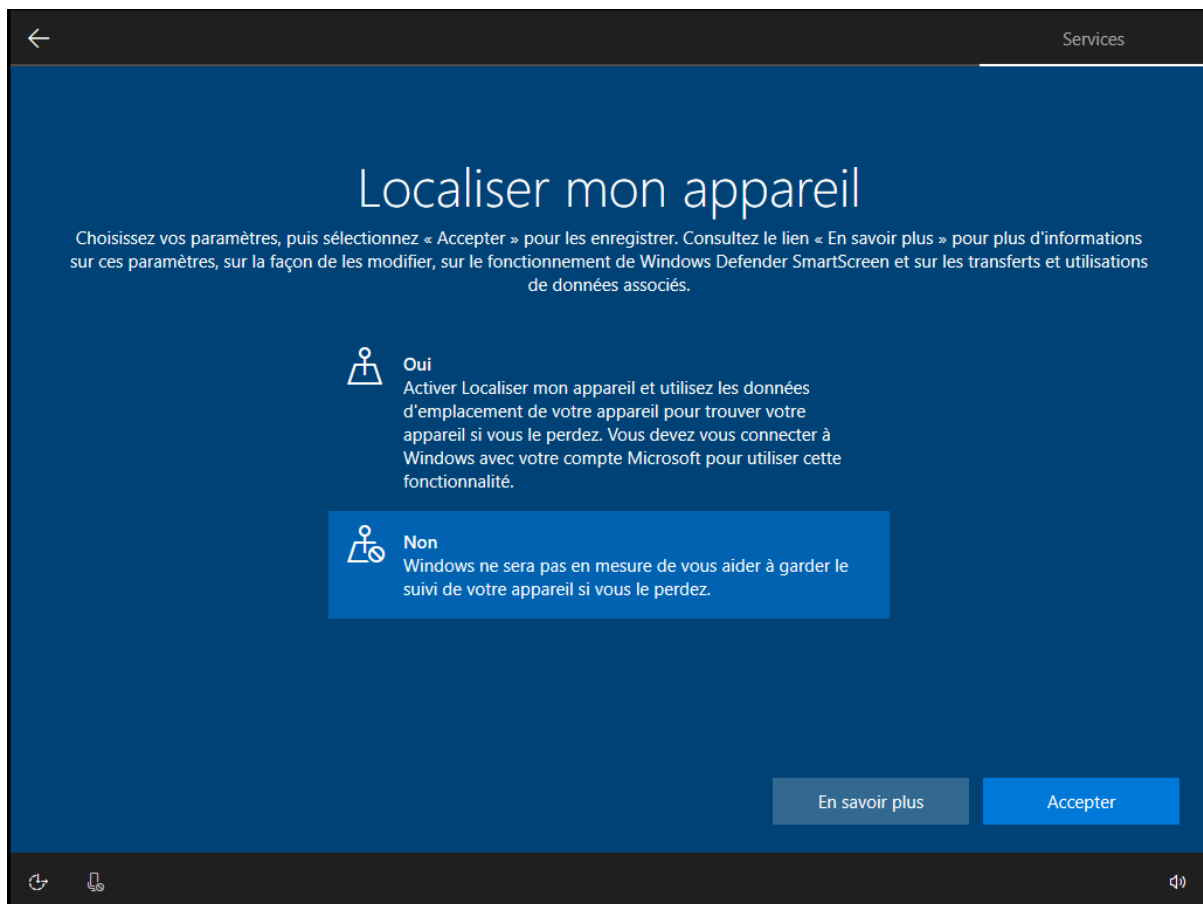
# En faire plus sur les appareils avec l'historique des activités



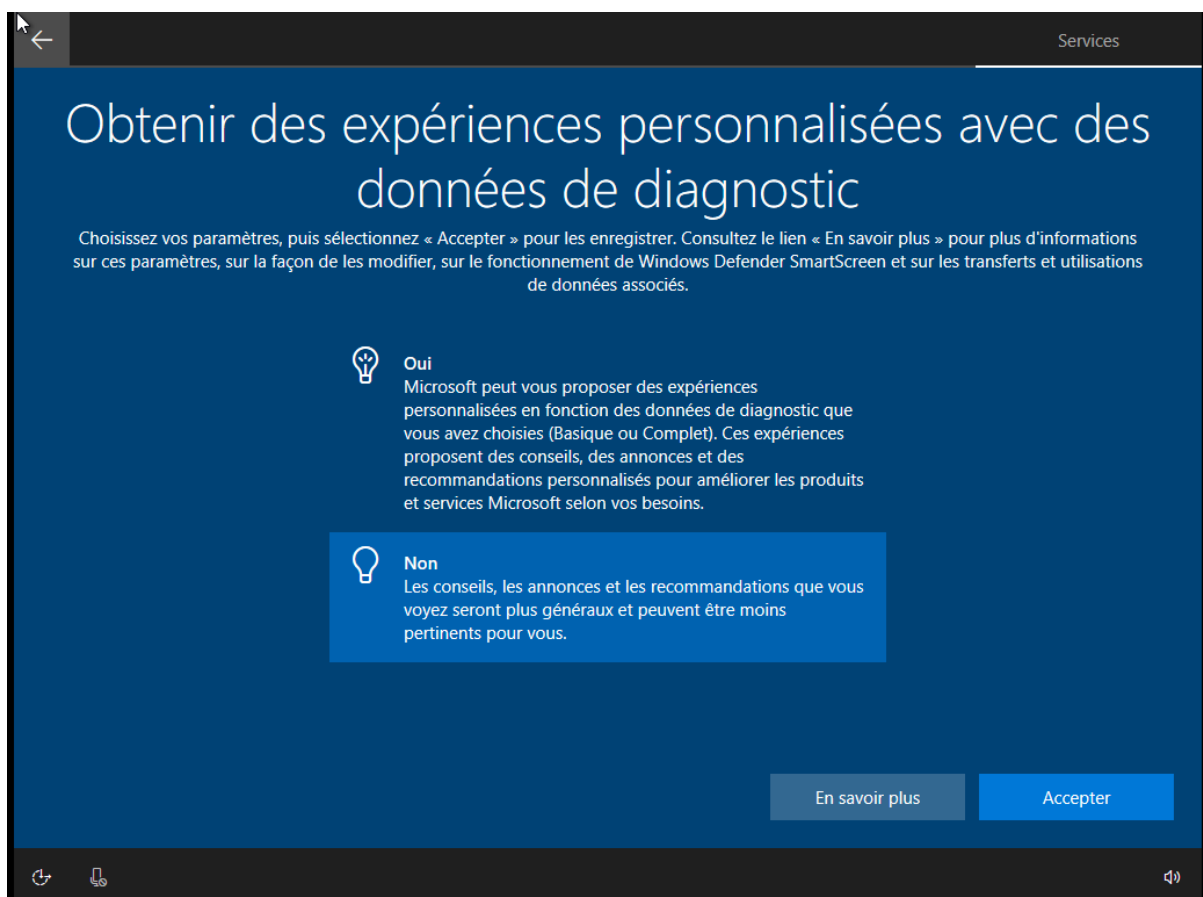
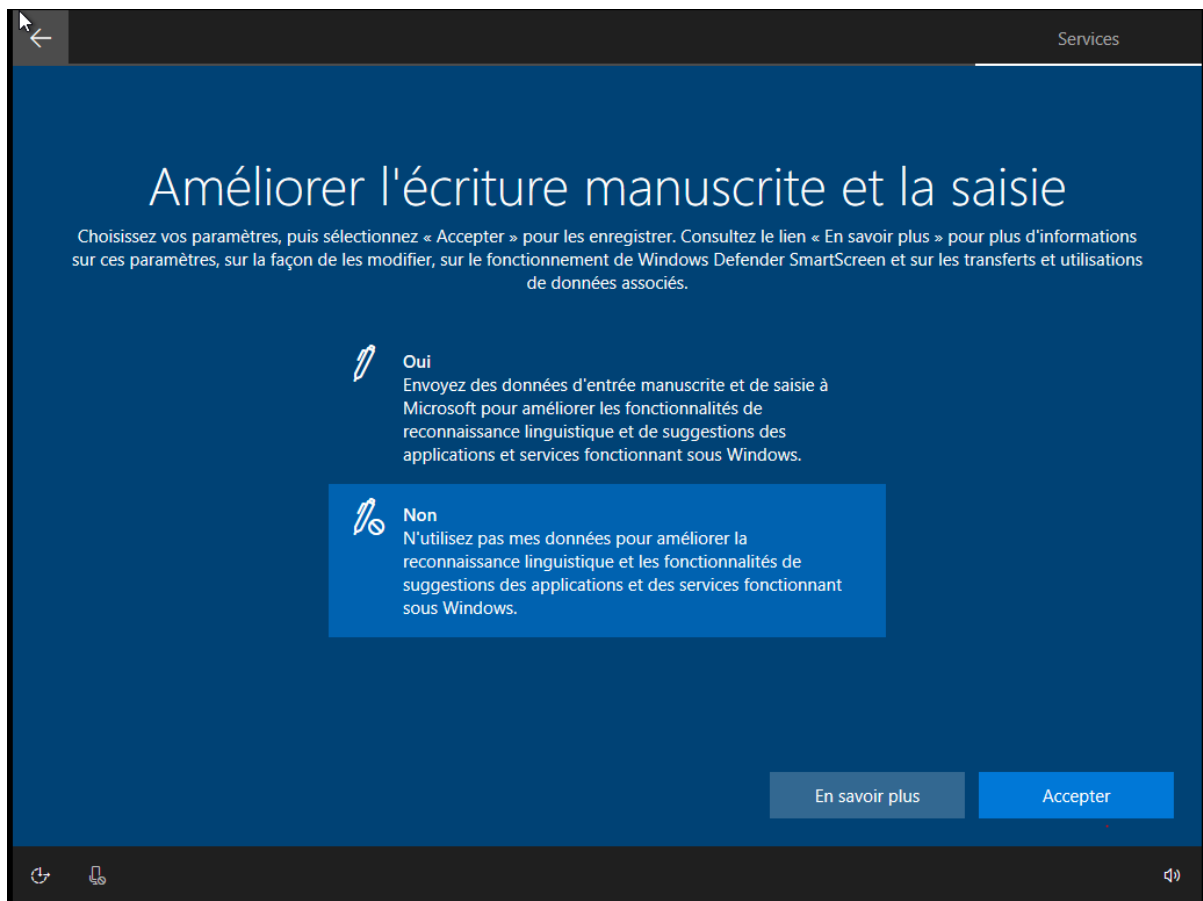
Si vous voulez utiliser la chronologie et d'autres fonctionnalités Windows pour vous aider à poursuivre ce que vous faisiez, même lorsque vous changez d'appareil, envoyez à Microsoft l'historique de vos activités, y compris les informations sur les sites web que vous visitez et la manière dont vous utilisez les applications et les services. Sélectionnez **En savoir plus** pour découvrir comment les produits et services Microsoft utilisent ces données pour personnaliser vos expériences tout en respectant votre vie privée.

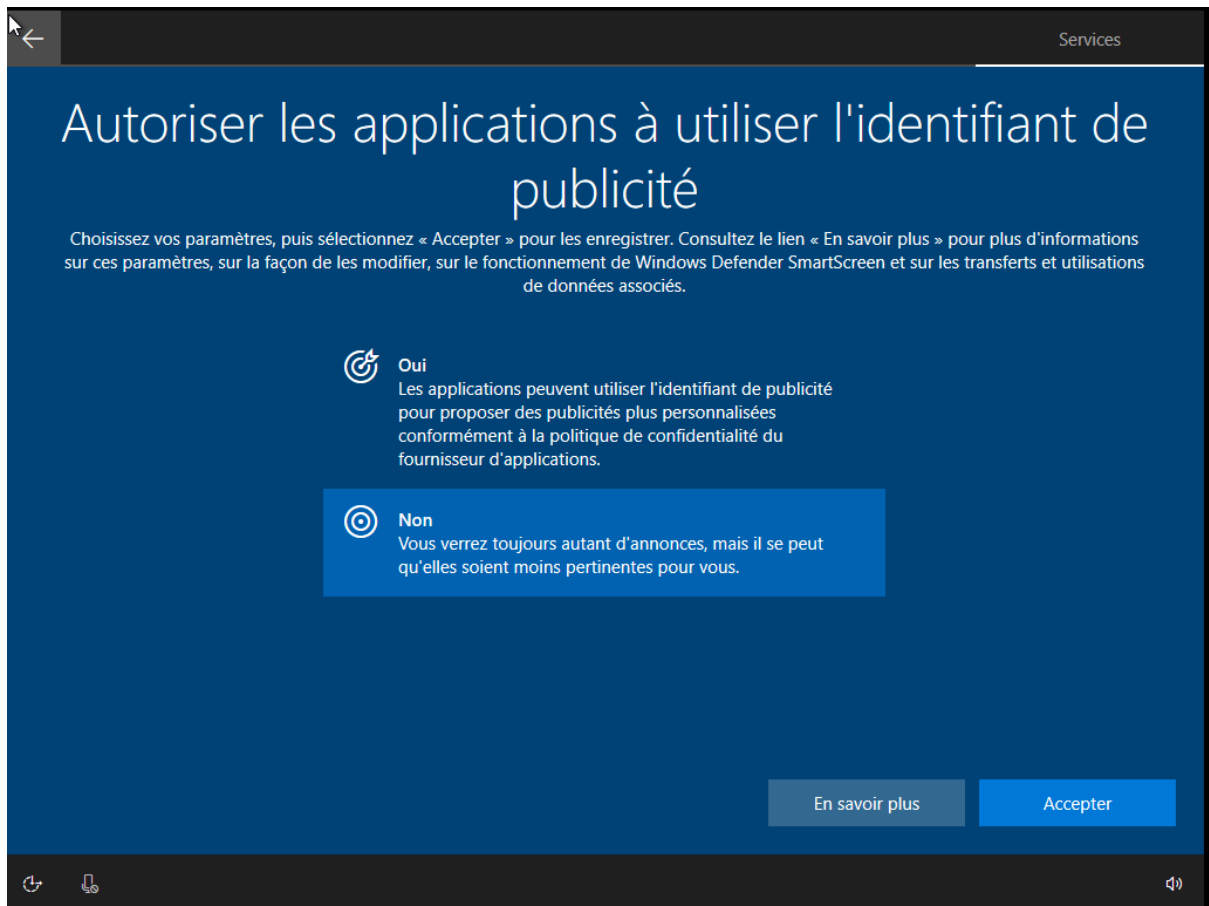
[En savoir plus](#)[Non](#)[Oui](#)











Suite à l'installation de Windows, le compte principal demande une protection plus sécurisée. Toutefois, en raison de l'organisation particulière de SFEIR avec une seule équipe SIS parmi les 7 entités de la société, l'étape d'authentification double est rejetée.

## Utiliser Windows Hello avec votre compte

Votre organisation requiert la configuration de votre compte professionnel ou scolaire avec la reconnaissance des visages Windows Hello, Fingerprint ou PIN.

Si vous avez déjà configuré Windows Hello sur cet appareil, nous l'ajouterons automatiquement à ce compte. Vous serez peut-être invité à revérifier avec Windows Hello.

Si votre organisation requiert un code PIN plus complexe, Windows vous invitera à le changer.



OK



sis.azure@sfeir.com

### Plus d'informations requises

Votre organisation a besoin de plus d'informations pour préserver la sécurité de votre compte

[Utiliser un autre compte](#)

Suivant

[Conditions d'utilisation](#) [Confidentialité et cookies](#) [Accessibilité : partiellement conforme](#) ...

## Un problème est survenu

Impossible de définir votre code confidentiel. Il est parfois utile d'essayer de nouveau. Vous pouvez également passer cette étape pour le moment et y revenir plus tard.

Pour plus d'informations sur les erreurs survenant lors de la configuration du code confidentiel :  
<https://aka.ms/PINErrors>

Pour obtenir de l'aide supplémentaire, contactez votre support technique et communiquez-leur les informations suivantes.

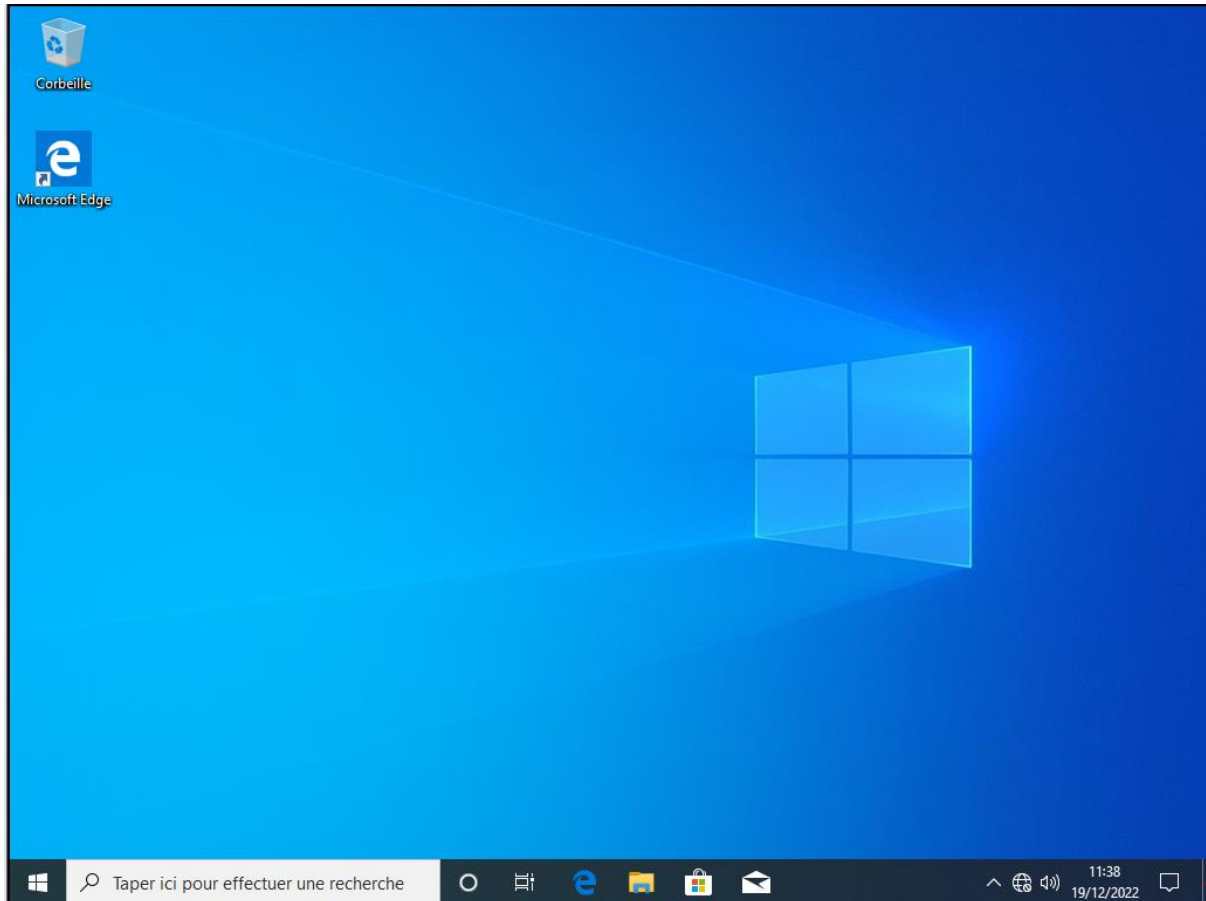
Code d'erreur : 0x801c044f  
ID de corrélation : 1547bcbd-13ae-0000-a4e1-4715ae13d901  
Horodateur : 2022-12-19T13:52:09.614Z

Réessayer



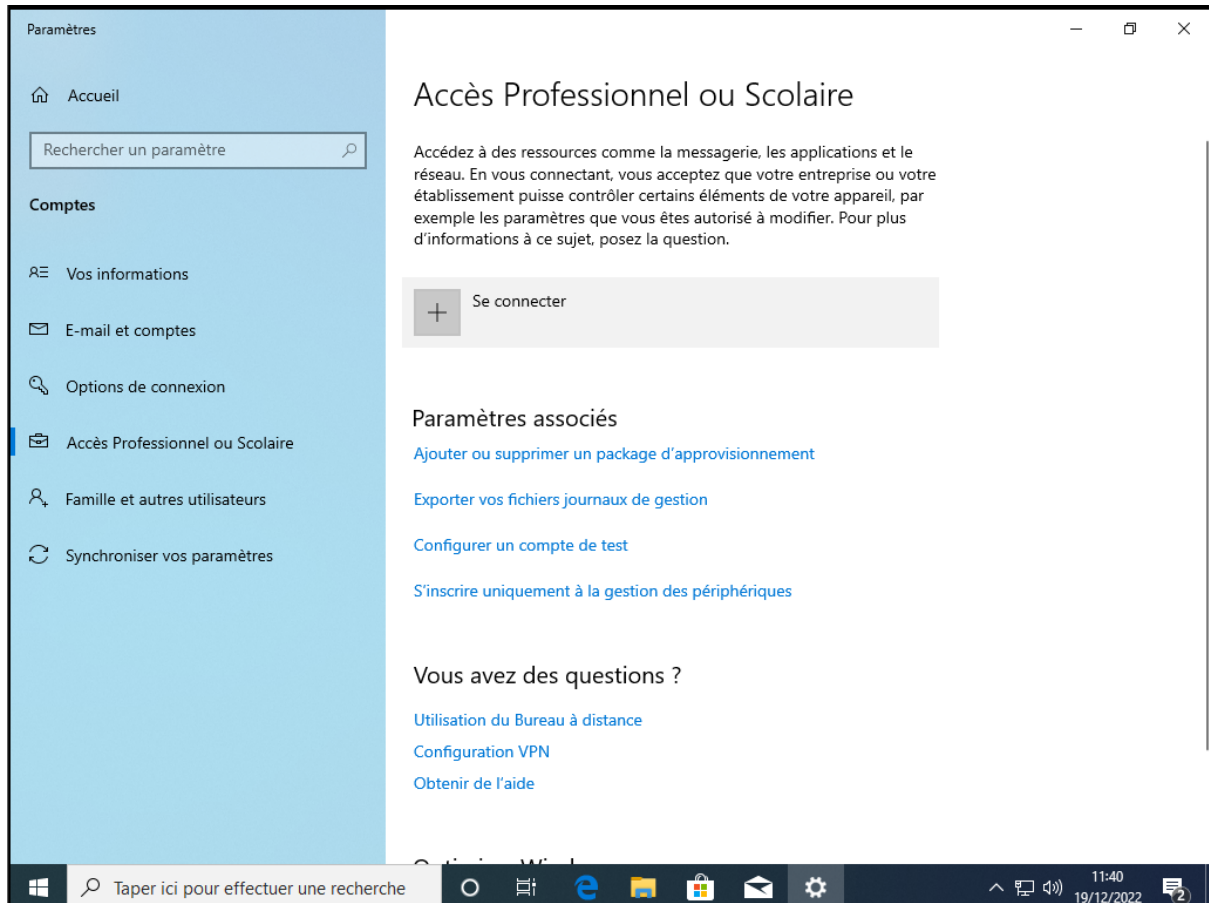
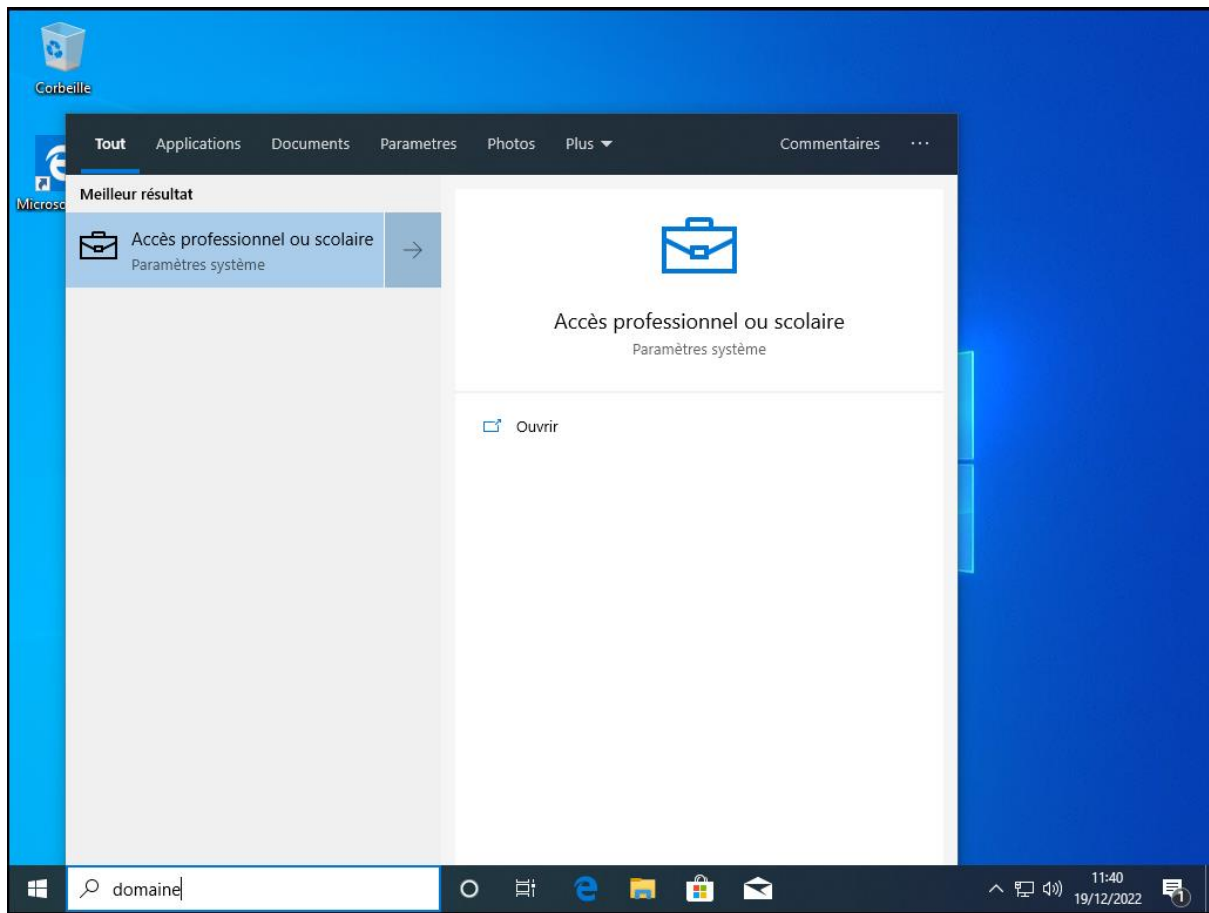
Ignorer pour le moment

Liaison au domaine Azure Active Directory / Ajout du compte principal  
si compte local déjà existant

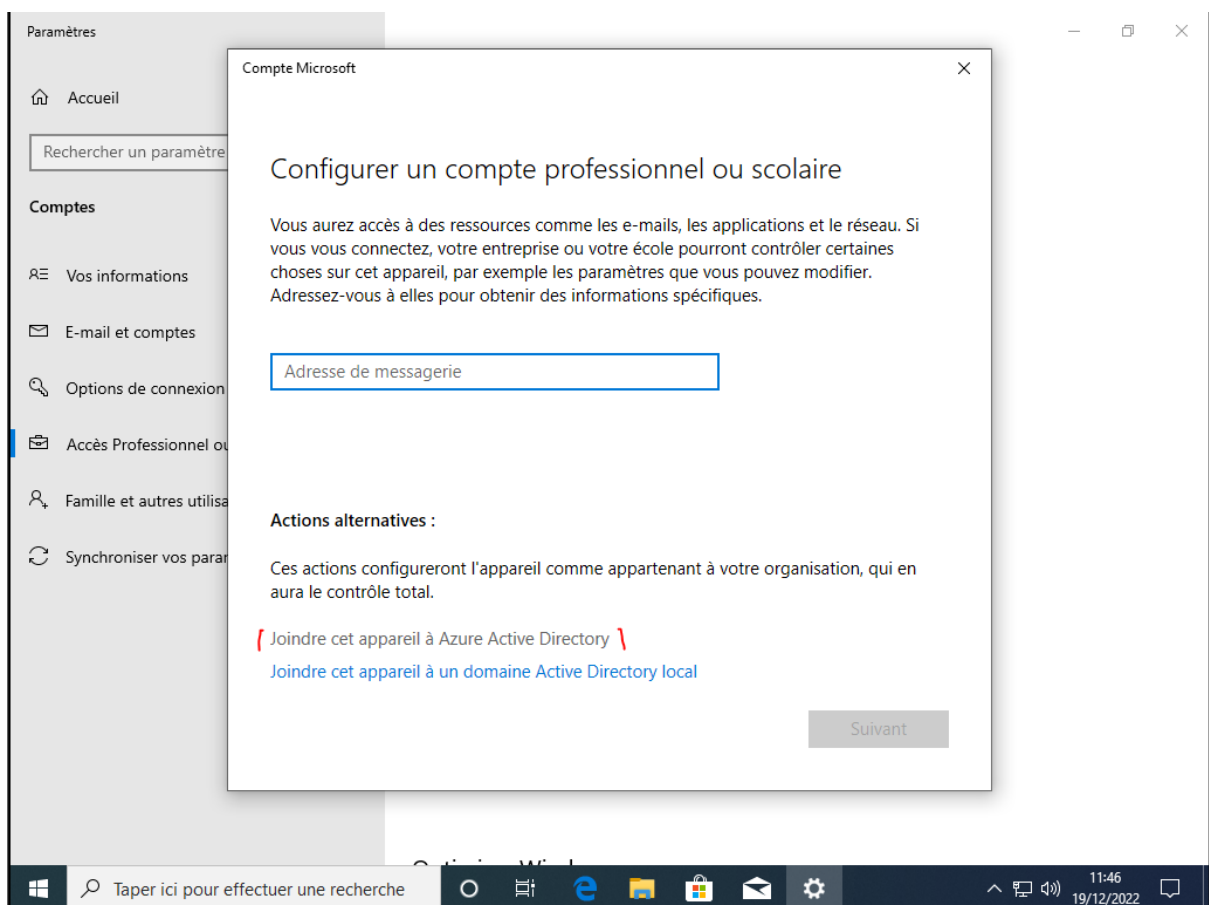


Depuis la barre de recherche intégrée au bureau, taper domaine et ouvrir Accès professionnel ou scolaire.

Le menu est également accessible depuis les *Paramètres*, section *Compte*.

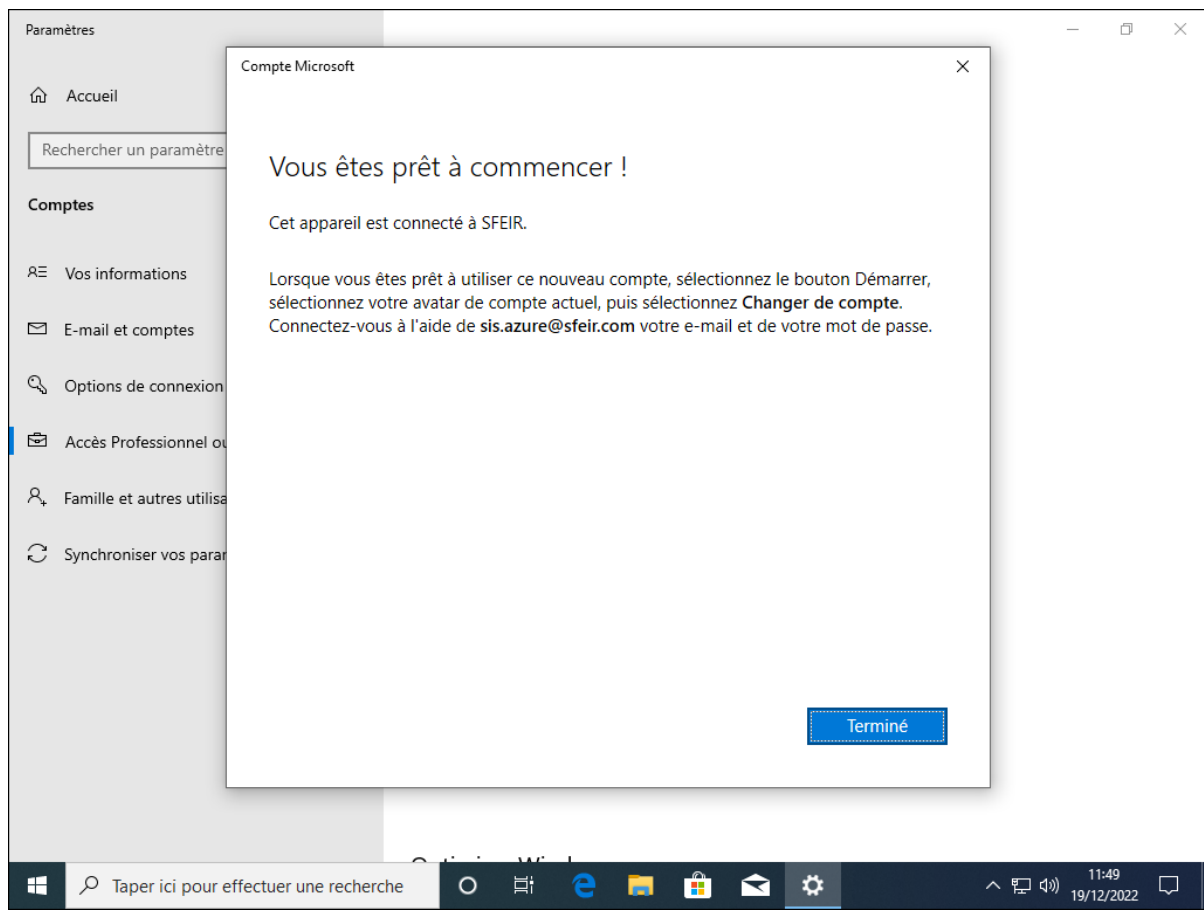


Se connecter désormais depuis l'espace afin de joindre l'appareil à l'annuaire de l'entreprise.



Entrer les informations de connexion, adresse mail et mot de passe.

Vérifier qu'il s'agit bien du domaine à rejoindre, ici sfeir.com



Le poste a rejoint le domaine de l'entreprise SFEIR et désormais il est possible d'ajouter des comptes pour les autres collaborateurs.

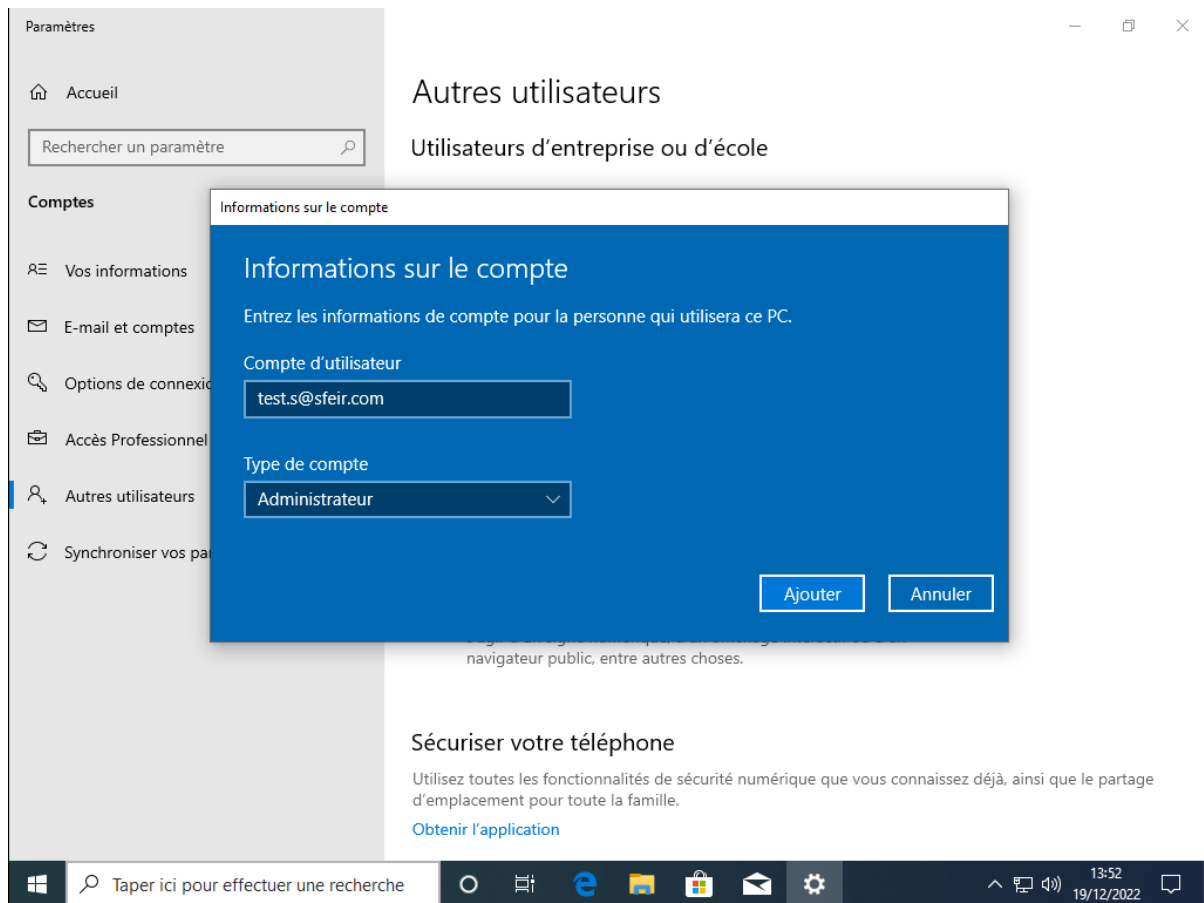


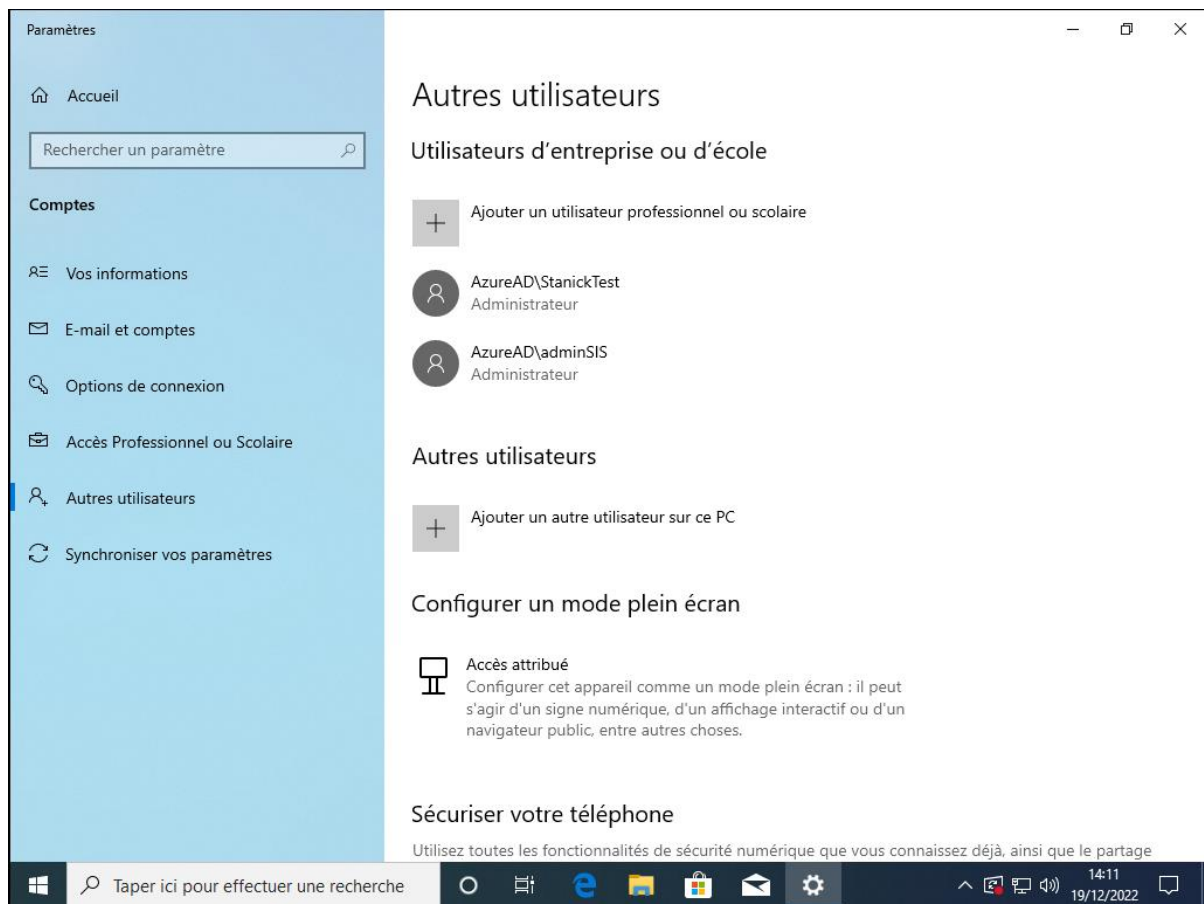
## Ajout d'un compte utilisateur/collaborateur

Dans la partie autres utilisateurs, il est possible d'ajouter des comptes avec des accès restreints (compte standard) ou sans restriction (compte Administrateur).

En raison des besoins spécifiques de développement, d'accès à des répertoires protégés, le type de compte Administrateur est attribué à chaque collaborateur.

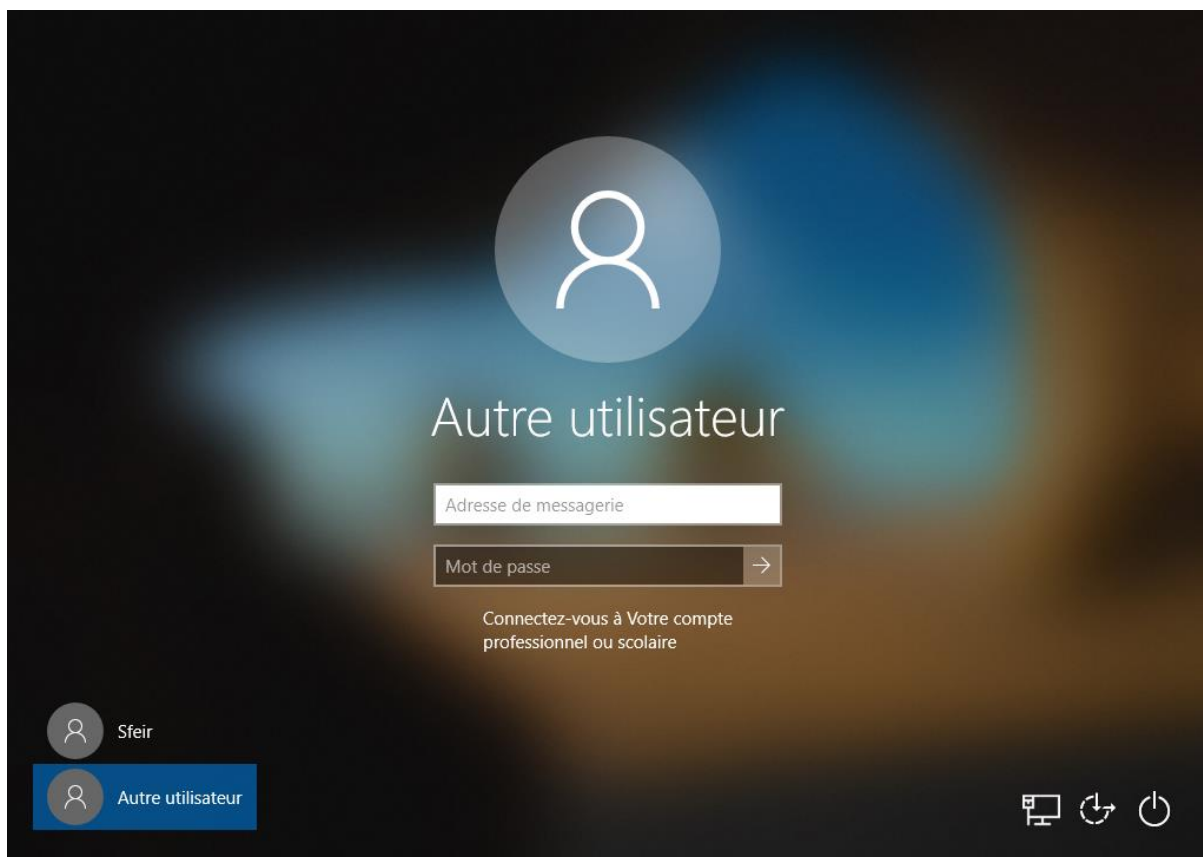
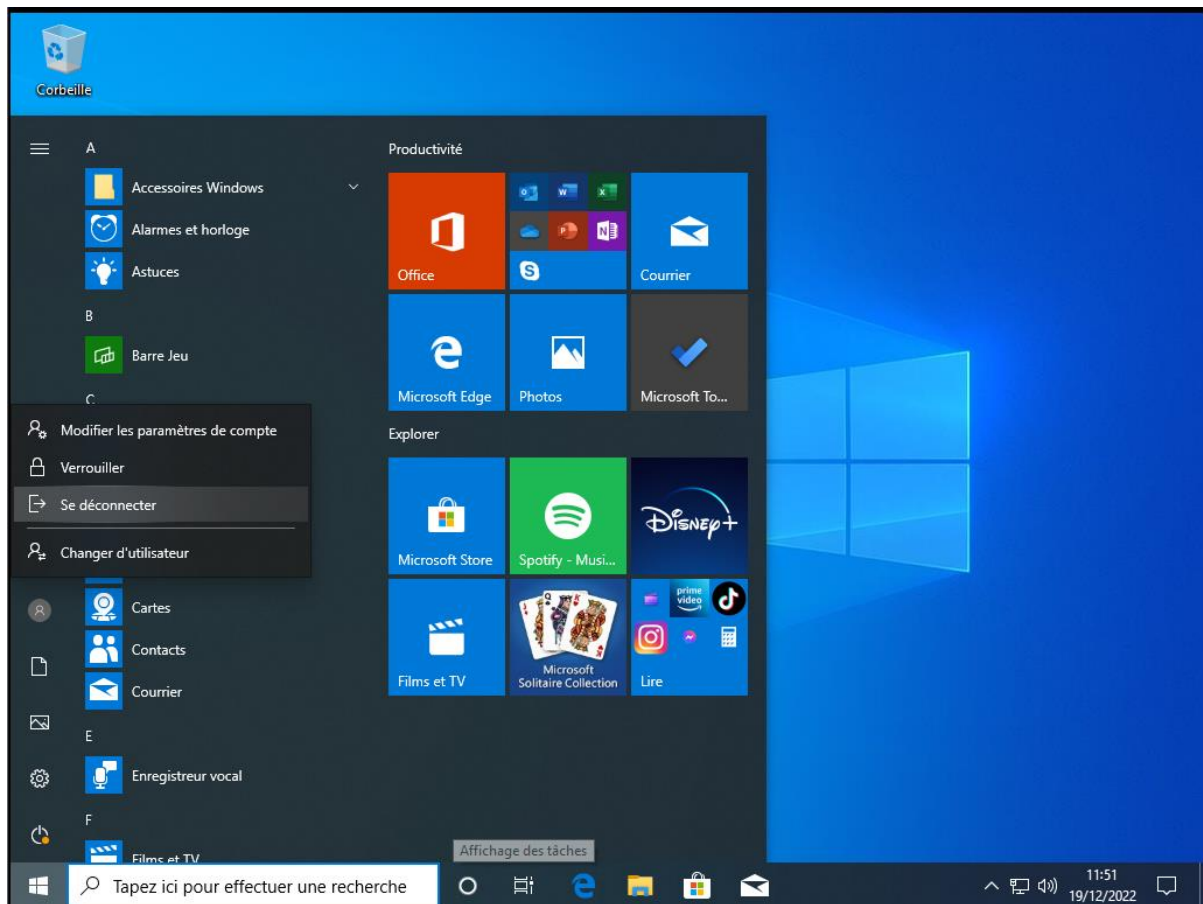
Pour des utilisations brèves ou peu poussées, un compte standard est suffisant.

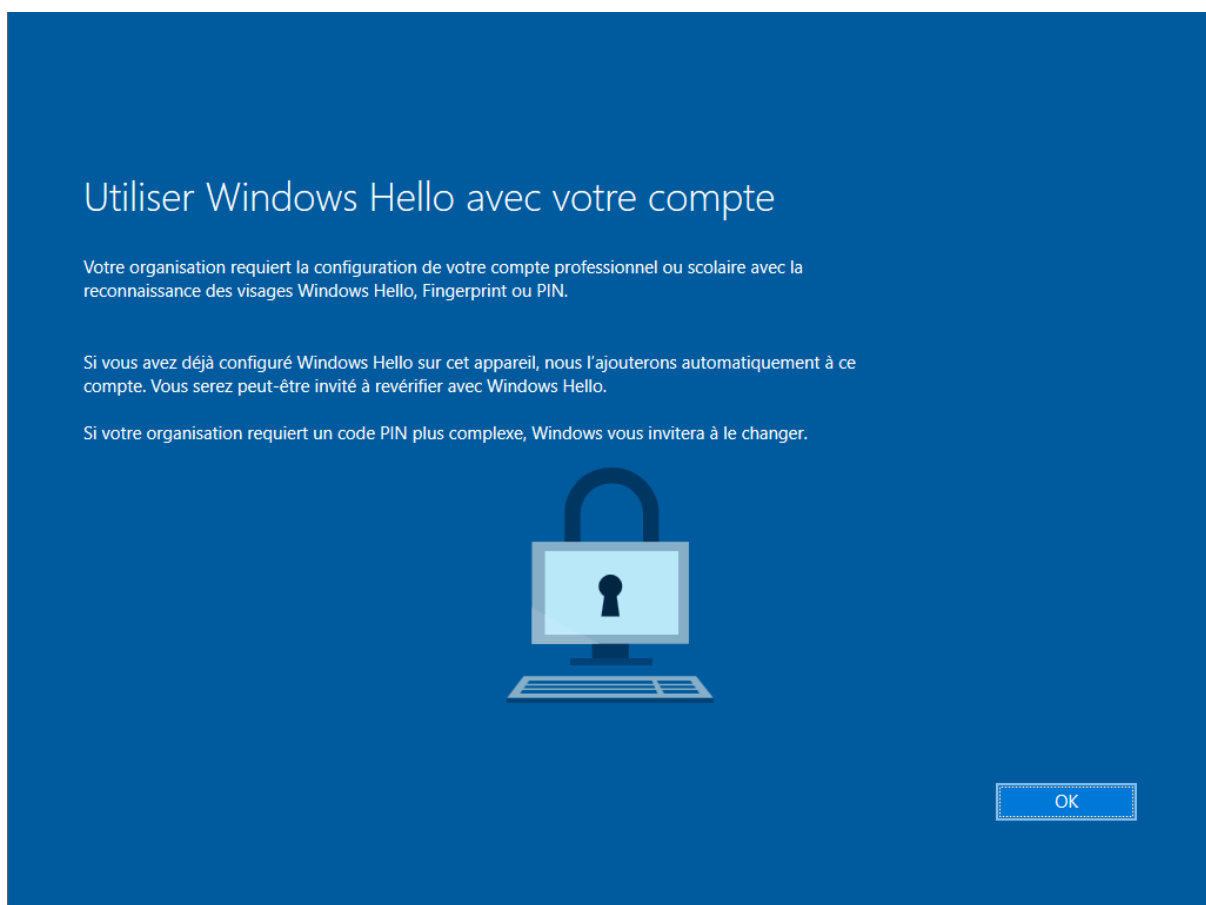
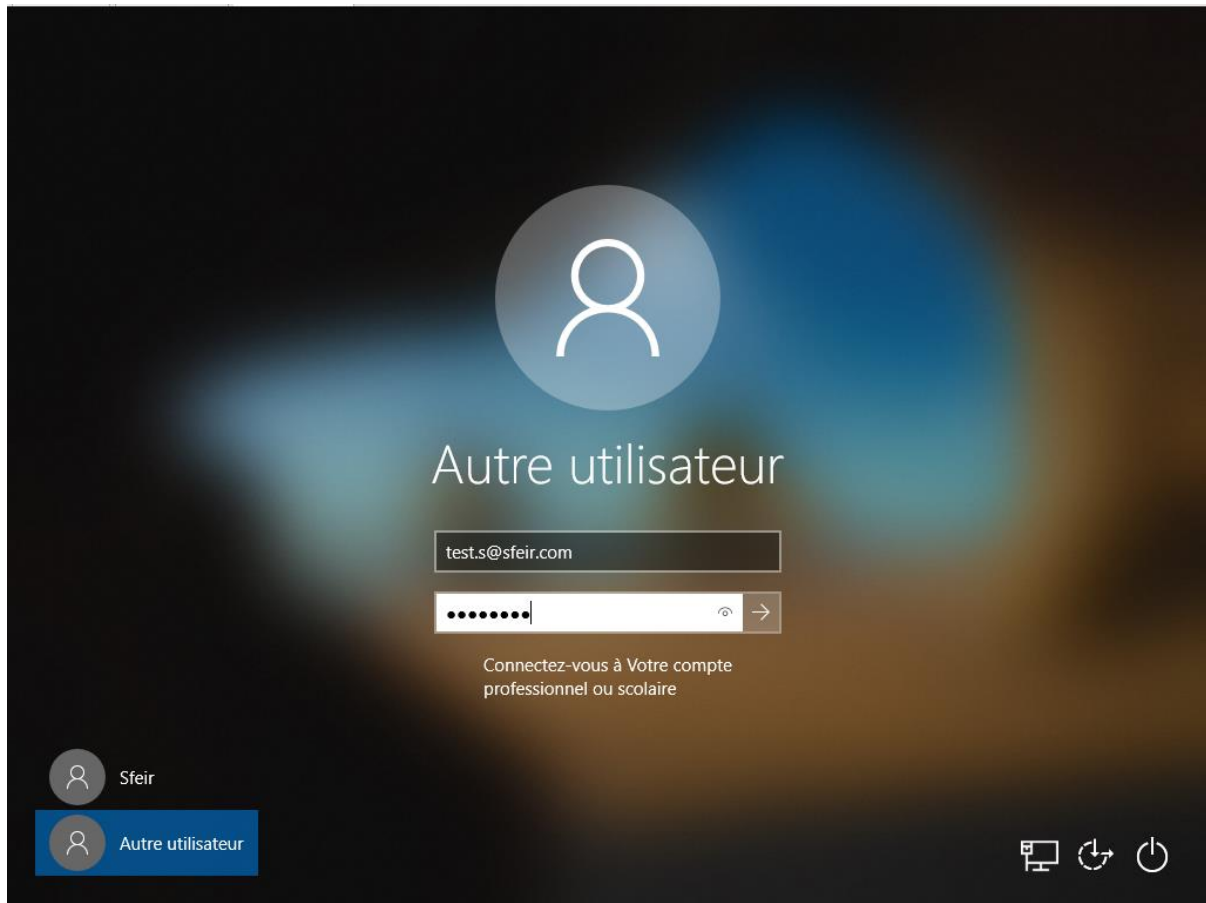





## Connexion au compte collaborateur

Les informations fournies au préalable, le collaborateur pourra se connecter et sécuriser l'accès à son compte, en changeant à nouveau son mot de passe, ajoutant un deuxième facteur d'authentification (téléphone ou QR code via l'application de Microsoft), définir un code PIN pour faciliter le démarrage du poste.





×



test.s@sfeir.com

## Entrez le mot de passe

Mot de passe


[J'ai oublié mon mot de passe](#)

[Se connecter avec un autre compte](#)

[Se connecter](#)

Conditions d'utilisation Confidentialité et cookies Accessibilité : partiellement conforme ...

×



test.s@sfeir.com

## Plus d'informations requises

Votre organisation a besoin de plus d'informations pour préserver la sécurité de votre compte

[Utiliser un autre compte](#)

[Suivant](#)

Conditions d'utilisation Confidentialité et cookies Accessibilité : partiellement conforme ...


SFEIR

?

## Protéger votre compte

Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.

### Microsoft Authenticator



#### Commencer par obtenir l'application

Sur votre téléphone, installez l'application Microsoft Authenticator.  
[Télécharger maintenant](#)

Après avoir installé l'application Microsoft Authenticator sur votre appareil, cliquez sur « Suivant ».

[Je souhaite utiliser une autre application d'authentification](#)

Suivant

[Je veux configurer une autre méthode](#)

Microsoft

test.s@sfeir.com

## Mettre à jour votre mot de passe

Vous devez mettre à jour votre mot de passe, car vous vous connectez pour la première fois ou votre mot de passe a expiré.

Mot de passe actuel

Nouveau mot de passe

Confirmer le mot de passe

Se connecter

Conditions d'utilisation

Confidentialité et cookies


Accessibilité : partiellement conforme

...

Sécurité Windows

### Configurer un code confidentiel

Créez un code confidentiel utilisable à la place des mots de passe. La définition d'un code confidentiel simplifie la procédure de connexion à votre appareil, à vos applications et à vos services.



☐ Inclure des lettre et des symboles

