Authentification sans mot de passe

L'authentification sans mot de passe est une méthode de sécurité qui vous permet d'accéder au réseau et aux systèmes de Suncor sans utiliser de mot de passe. Votre identité est vérifiée autrement qu'avec un mot de passe, ce qui signifie que vous n'avez pas besoin d'inscrire un mot de passe à l'ouverture d'une session Windows. Voici certaines des méthodes courantes (il est à noter que Suncor utilise déjà certaines d'entre elles) :

- les applications d'authentification tierces comme Microsoft Authenticator
- les numéros d'identification personnels (NIP), quatre ou même six chiffres (par souci de complexité accrue)
- la reconnaissance biométrique, c'est-à-dire les traits physiques comme les empreintes digitales ou les caractéristiques faciales
- l'utilisation d'un jeton ou d'un autre dispositif

En ce qui concerne les appareils qui appartiennent à Suncor ou qui sont gérés par cette dernière, l'utilisation de Windows Hello Entreprise, la reconnaissance faciale et l'utilisation d'un NIP à six chiffres deviennent les principales méthodes d'authentification. En éliminant l'emploi de noms d'utilisateur et de mots de passe de l'expérience d'ouverture de session, Suncor peut assurer une meilleure sécurité pendant que vous, l'utilisateur, bénéficiez d'un processus d'authentification plus rapide, plus simple et pratique.

AVANT DE COMMENCER

Veuillez lire la section **Foire aux questions** à la fin de ce document. Elle présente des renseignements utiles sur ce à quoi s'attendre ou non de Windows Hello, d'autres éléments de configuration et les changements en dehors de ce processus. Ces renseignements vous aideront à préparer et choisir la méthode qui vous convient.

Inscription à la sécurité de connexion améliorée

Objectif

Le présent Guide de référence rapide (GRR) décrit le processus d'inscription de l'appareil appartenant à Suncor ou géré par cette dernière à la sécurité de connexion améliorée à l'aide d'un NIP à six chiffres ou de la reconnaissance faciale (si cette technologie est compatible avec votre appareil) conjuguée à un NIP à six chiffres en guise de méthode auxiliaire.

Conditions préalables

- Windows 10, version 21H2 ou une version plus récente
- Configuration selon la politique de sécurité de connexion améliorée
- RF* seulement – le matériel doit être compatible
- Application MS Authenticator configurée comme méthode d'authentification par défaut

Utilisateurs visés

Les utilisateurs d'un appareil appartenant à Suncor ou géré par cette dernière, par exemple un ordinateur de bureau, un ordinateur portable ou une tablette, qui répond aux conditions préalables de Windows Hello.

Étapes à suivre

Connexion sûre au réseau de Suncor

1. Vous devez vous connecter au réseau de Suncor pour activer le processus d'inscription. Si vous êtes à une **installation**, passez à l'étape 9.

   Autrement, avant d'ouvrir une session, connectez-vous à l'aide du système **AnyConnect VPN**, comme il est indiqué ci-dessous.

2. À l'écran d'ouverture de session, cliquez sur l'**icône** affichant deux écrans dans le bas à droite.

   La boîte de dialogue **Cisco AnyConnect Secure Mobility Client** s'ouvre, effectue une analyse et indique si une connexion peut être établie.

   ***Remarque** : Si vous utilisez également d'autres connexions VPN de Suncor, vous devrez peut-être sélectionner AnyConnect.*

3. Dans la boîte de dialogue affichant « Suncor VPN », cliquez sur **Se Connecter**.

   (Il se peut que ce que vous voyez diffère de l'illustration.)

4. Entrez votre **Nom d'utilisateur** et votre **Mot de passe**, et cliquez ensuite sur **OK**.

5. Cliquez pour **Accepter** l'avis juridique.

6. **Bravo!** Vous vous êtes connecté en toute sécurité au réseau de Suncor à l'aide du VPN. Passez à la prochaine étape.

Mise à jour de la politique de groupe

Si votre ordinateur exige toujours le chargement de la politique de groupe, un courriel de notification est envoyé. Dès que vous accédez au réseau de Suncor, la politique est appliquée.

Vous ne recevrez pas de notification vous informant de son application. Cependant, si vous arrivez aux étapes d'inscription et que le système ne vous demande pas d'entamer le processus, redémarrez votre appareil. Il se peut que vous deviez effectuer deux redémarrages pour que les fonctions prennent effet. N'oubliez pas que vous devez toujours vous connecter au portail VPN.

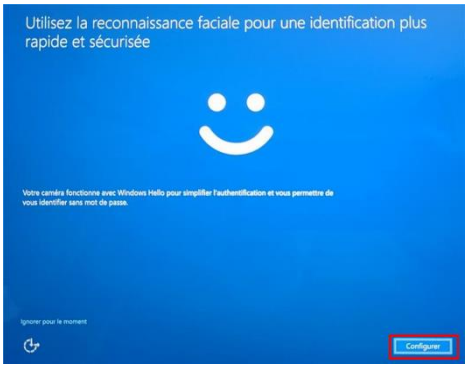
Passez aux étapes d'**inscription**.

L'inscription débute dès l'ouverture de session

Avant de commencer : Consultez les étapes 7 à 15 pour vous familiariser avec le processus. Quand vous êtes prêt, passez à la prochaine étape.

L'assistant à l'inscription à la sécurité de connexion améliorée est lancé.

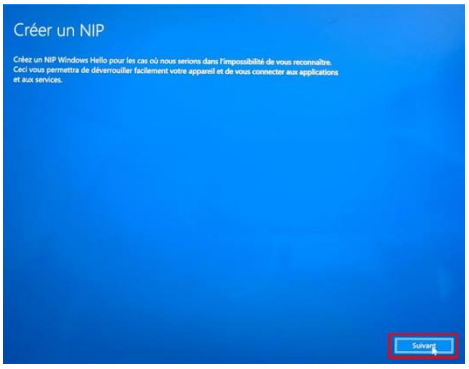
7. Si la page de **Créer un NIP** s'affiche, ou si vous souhaitez ignorer la reconnaissance faciale *(sélectionnez l'option **Skip for now** dans le coin inférieur gauche de l'écran),* rendez-vous à l'étape 10. Autrement, suivez les étapes de la reconnaissance faciale (présentées à droite).



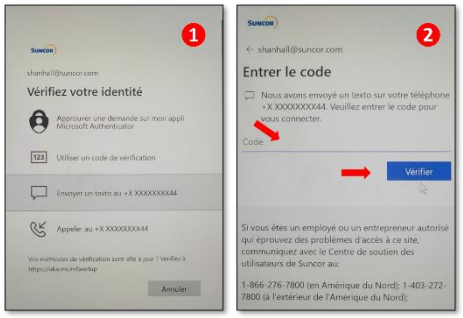
8. Cliquez sur **Set up**.
9. On vous demande de regarder directement la lentille de votre appareil. Soutenez le regard jusqu'à ce que le système vous demande de poursuivre en configurant le NIP.

10. À l'écran de **création d'un NIP**, cliquez sur **NEXT**.

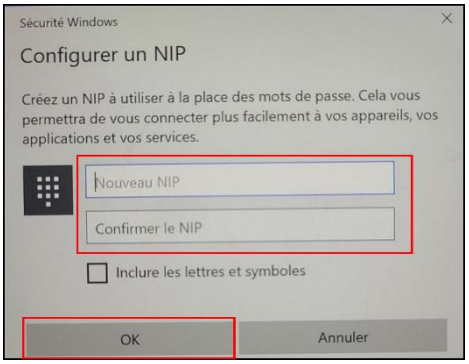
    On vous demande de confirmer votre identité.



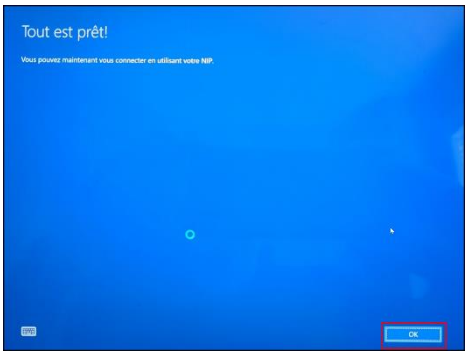
11. Sélectionnez la méthode d'authentification de votre choix, puis exécutez le processus de *confirmation* en cliquant sur **Verify**.



12. À la fenêtre de dialogue de **configuration d'un NIP**, entrez votre nouveau NIP dans la première zone de texte.
13. Confirmez votre nouveau NIP dans la deuxième zone de texte.
14. Cliquez sur **OK**.



15. Lorsque vous aurez terminé, la fenêtre **All set!** s'affichera. Cliquez sur **OK**.
16. L'écran d'ouverture de session s'ouvre. Poursuivez en utilisant vos nouvelles données d'identification à l'ouverture de session.



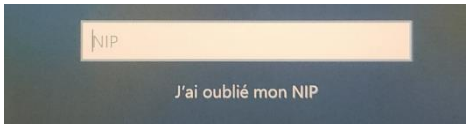
REMARQUE : *Si vous éprouvez des difficultés lors de l'inscription ou au moment d'ouvrir une session, vous pouvez annuler vos données biométriques et recommencer le processus. Document de référence :* ***GRR – Réinitialisation de l'inscription à la sécurité de connexion améliorée Windows Hello***

Après l'inscription

À la prochaine ouverture de session ou la prochaine fois que vous devrez déverrouiller Windows, les éléments suivants seront activés :

- La reconnaissance faciale (RF) améliorée, aussi appelée Reconnaissance faciale Windows Hello (si l'appareil est compatible). Regardez directement la lentille de l'appareil. Votre session s'ouvrira dès que la reconnaissance sera terminée. Le processus prend seulement quelques secondes.

- L'exigence relative au NIP à six chiffres. Il s'agit de votre principale méthode d'ouverture de session. La capture d'écran à droite indique où vous devez inscrire votre NIP.



Remarque : *Vous utiliserez aussi cette méthode si jamais l'authentification par reconnaissance faciale échoue.*

Foire aux questions (FAQ)

Q-1. Dois-je absolument utiliser les données biométriques sur mon appareil de Suncor?

Vous pouvez choisir la **reconnaissance faciale** (RF) ou le **NIP** comme principal moyen d'ouverture de session Windows Hello. À l'heure actuelle, aucun plan n'est prévu pour permettre l'authentification biométrique à l'aide des empreintes digitales, comme on peut le faire sur un cellulaire ou un appareil semblable.

Q-2. Mes données biométriques sont-elles sécurisées (et) ou sont-elles partagées?

Si vous choisissez d'activer la reconnaissance faciale, votre appareil prendra une série de mesures de vos traits faciaux pour créer une « carte numérique » (données biométriques) à votre image. Vos données biométriques sont ensuite cryptées, isolées et **conservées** sur votre appareil. Lorsque vous ouvrez une session en utilisant la reconnaissance faciale Windows Hello, les données biométriques enregistrées sont comparées à l'analyse actuelle et vérifiées localement. Lorsque vous vous connectez au réseau de Suncor, à l'une de nos installations ou ailleurs par voie du portail VPN, votre appareil envoie seulement une clé cryptée qui confirme au serveur authentifiant que c'est bien vous, afin que vous puissiez déverrouiller votre appareil.

Les détails de vos données biométriques ne sont jamais partagés ni envoyés à des appareils ou serveurs externes. De plus, même si un pirate arrivait à accéder aux données biométriques cryptées sur votre appareil, celles-ci ne pourraient pas faire l'objet d'une ingénierie inverse afin de créer votre image.

La fonction de reconnaissance faciale ne prend jamais de photo de votre image, n'enregistre pas de photos de vous et n'en partage pas non plus avec Suncor ou Microsoft.

Q-3. Quelle est la différence entre l'utilisation d'un NIP et l'utilisation d'un mot de passe?

Les mots de passe, ainsi que les noms d'utilisateur, sont mis en mémoire et authentifiés sur le serveur auquel vous vous connectez. Que vous tentiez d'accéder à un réseau ou à une application, au moment où vous ouvrez une session, votre mot de passe est transmis à un serveur qui confirme ensuite votre identité et vous accorde l'accès. En cas d'atteinte à la protection des données d'un serveur, les renseignements qui vous ont été volés peuvent être utilisés n'importe où aux fins d'accès si la combinaison (nom d'utilisateur et mot de passe) est la même.

Le NIP est associé à l'appareil	Comme c'est le cas pour les données biométriques, le NIP Hello est associé à l'appareil sur lequel vous avez configuré ce numéro. Si vous utilisez plus d'un appareil (p. ex., ordinateur de bureau et ordinateur portable), vous devez effectuer la configuration Hello sur chacun des appareils utilisés.
Le NIP est soutenu par le matériel informatique	Une puce du Module de plateforme sécurisée (TPM) est utilisée sur de nombreux appareils modernes. Il s'agit d'un cryptoprocesseur sécurisé qui comprend de multiples mécanismes de sécurité physique qui le

rendent inviolable, et ce, même face à des logiciels malveillants et des attaques par force brute contre le NIP. L'appareil sera verrouillé si trop de tentatives ont échoué.

Le NIP peut être complexe

Bien que les mêmes principes de gestion technologique puissent s'appliquer à un NIP et à un mot de passe, soit en matière de complexité, de longueur, d'expiration et d'histoire, Suncor a décidé de faire simple. Votre appareil géré nécessite un NIP composé de six chiffres seulement qui est configuré comme méthode de rechange en cas d'échec de la reconnaissance faciale ou comme principale méthode d'ouverture de session. Votre appareil sera verrouillé après un certain nombre de tentatives infructueuses.

Q-4. Qu'en est-il si quelqu'un vole mon appareil ou si je le perds?

Pour qu'une personne en possession de votre appareil arrive à en obtenir l'accès, elle doit arriver à déjouer la biométrie qui vous est propre ou à deviner votre NIP avant que votre appareil soit verrouillé. Le matériel spécial appelé le TPM possède une fonction limitant les attaques par force brute.

Q-5. Dois-je souscrire à la sécurité de connexion améliorée si je me connecte avec mon propre appareil?

Pour l'instant, seuls les appareils appartenant à Suncor ou gérés par cette dernière seront inscrits à la sécurité de connexion améliorée. Ces appareils doivent répondre aux conditions préalables, comme il est indiqué au début du présent document.

- Windows 10, version 21H2 ou une version plus récente
- Configuration selon la politique de sécurité de connexion améliorée
- RF* seulement – le matériel doit être compatible

Q-6. Mon appareil ne possède pas de caméra. Puis-je y brancher une caméra pour utiliser la reconnaissance faciale?

Les dispositions de mise en œuvre de la sécurité de connexion améliorée de Suncor ne sont pas adaptées aux modules de caméra externe et à l'utilisation de plus d'une caméra pour le moment.

Q-7. Puis-je désactiver la sécurité de connexion améliorée si je ne veux pas utiliser la reconnaissance faciale?

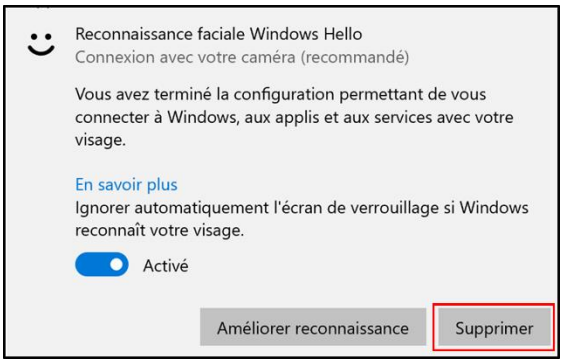
Il est impossible de modifier la politique de groupe de sécurité de connexion améliorée (Windows Hello). Cependant, si vous souhaitez simplement passer de la reconnaissance faciale au

NIP comme principale méthode d'authentification, vous pouvez retirer la Reconnaissance faciale Windows Hello des options d'ouverture de session sur votre compte.

Appuyez sur la touche Windows et la touche I, rendez-vous à la rubrique Comptes > Options de connexion > Reconnaissance faciale Windows Hello, puis sélectionnez Supprimer.

Vous pouvez aussi suivre les directives du document suivant : GRR **– Réinitialisation de l'inscription à la sécurité de connexion améliorée Windows Hello**. Ce document vous indiquera comment annuler vos données biométriques pour que vous puissiez réinscrire votre appareil à la sécurité de connexion améliorée. Une fois vos données biométriques effacées, le processus d'inscription est déclenché. Suivez les étapes présentées dans ce document afin de choisir l'option de **NIP** seulement plutôt que la combinaison **RF+NIP**. Il vous sera **IMPOSSIBLE** de retirer le NIP, car il est requis en cas d'échec de la Reconnaissance faciale Windows Hello.

***Remarque** : Ces étapes s'appliquent également si vous éprouvez des problèmes avec la reconnaissance faciale et devez procéder à une réinitialisation et une réinscription.*



Q-8. Puis-je opter temporairement pour l'utilisation du NIP si ma principale méthode d'authentification est la reconnaissance faciale?

Oui. Si vous couvrez la lentille de votre appareil à l'aide d'un papillon adhésif ou de votre main, la reconnaissance faciale échouera et le système vous demandera d'utiliser une autre méthode d'authentification. Sélectionnez l'icône NIP, entrez votre NIP et poursuivez vos activités comme d'habitude.

Q-9. Que se passe-t-il si mon appareil compte plus d'un écran et que je décide d'utiliser la reconnaissance faciale pour ouvrir une session?

La reconnaissance faciale fonctionne seulement sur l'appareil où se trouve la caméra.

Par exemple, si vous possédez actuellement trois écrans, soit un écran intégré à l'ordinateur portable et deux écrans externes, et que le premier écran externe est l'écran principal et affiche normalement la page d'ouverture de session / de verrouillage, la page d'ouverture de session s'affichera à l'écran de votre ordinateur portable. Lorsque la reconnaissance faciale aura confirmé votre identité, la configuration de vos écrans sera rétablie conformément à vos paramètres. Le processus est le même si vous fermez votre ordinateur portable, ouvrez votre ordinateur personnel et utilisez seulement les écrans externes.

Q-10. Que faire si j'oublie mon NIP?

À la page d'ouverture de session / de verrouillage Windows, juste en dessous du champ de saisie du NIP, se trouve le lien **J'ai oublié mon NIP**. Ce lien déclenche la fonction d'authentification multifacteur (AMF) qui confirme votre identité (comme il est indiqué aux étapes 10 à 14 dans le présent document). Suivez ces étapes pour réinitialiser votre NIP. Lorsque vous aurez terminé, déverrouillez votre ordinateur à l'aide de votre nouveau NIP.

Q-11. Que se passe-t-il si je change mon mot de passe?

Lorsque vous configurez Windows Hello Entreprise, le NIP ou le profil biométrique que vous utilisez est propre à l'appareil utilisé. Le changement du mot de passe du compte n'a pas d'incidence sur l'ouverture de session et le verrouillage sur ces appareils, car ils utilisent une clé pour l'authentification et non un mot de passe.

Q-12. Dois-je utiliser Windows Hello même si je ne suis pas connecté au réseau de Suncor?

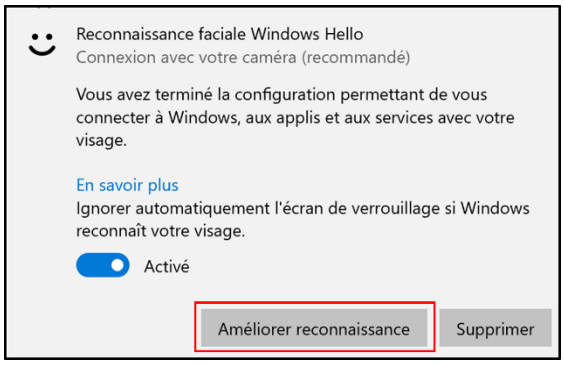
Votre méthode d'ouverture de session est associée à l'appareil, peu importe que vous soyez ou non connecté au réseau de Suncor. Après l'inscription, votre méthode d'ouverture de session demeurera la même, que vous soyez connecté au réseau ou que vous travailliez localement.

Q-13. Je porte des lunettes. Lors de l'inscription, dois-je les porter, les enlever ou combiner ces deux options?

Si vous portez toujours des lunettes, il serait alors mieux que vous portiez vos lunettes au moment de vous inscrire à la reconnaissance faciale. Si vous portez des lunettes à l'occasion seulement, ne les portez pas à l'inscription. Cependant, si vous portiez des lunettes lorsque vous vous êtes inscrit à la reconnaissance facile et que vous éprouvez des difficultés de reconnaissance, ou si vous portez des lunettes de façon irrégulière, vous devrez peut-être **améliorer la reconnaissance**. Il est toutefois à noter que ceux qui ont déjà adhéré à la reconnaissance faciale ont rarement éprouvé des difficultés.

Appuyez sur la touche Windows et la touche I, rendez-vous à la rubrique Comptes > Options de connexion > Reconnaissance faciale Windows Hello, puis sélectionnez l'option Améliorer reconnaissance.

Ce processus vous permet d'ajouter des possibilités d'inscription pour vos traits faciaux (avec lunettes, sans lunettes, éclairage différent, style capillaire différent et autre), ce qui aidera l'algorithme à vous identifier.



Q-14. Dois-je souscrire à la sécurité de connexion améliorée si je me connecte à Cloud PC ou à d'autres réseaux?

À l'heure actuelle, **Windows Hello Entreprise** n'est pas compatible avec Cloud PC (protocole RDP). **Ouvrez une session** Cloud PC comme vous le faites habituellement en utilisant votre compte et votre mot de passe.