Passwordless Authentication

Passwordless authentication is a security method that allows you to access the Suncor network and systems without the use of a password. Your identity is authenticated with something other than a password; which means you don't have to enter a password at Windows sign-in. Here are some common methods, some of which Suncor already employs:

- third-party authenticator apps such as Microsoft's Authenticator
- personal identification number (PIN) - 4 or even 6 (for enhanced complexity)
- biometric recognition - physical traits, like fingerprints or facial characteristics
- the use of a token or other device

For Suncor owned/managed devices using Windows Hello for Business, Facial recognition, or a 6-digit pin, is becoming the primary method for authentication. By reducing usernames and passwords from the user sign-in experience, Suncor can achieve enhanced security while you, the user, benefits from an authentication process that is faster, simpler and convenient.

BEFORE YOU BEGIN

Please read the **Frequently Asked Questions** section at the end of this document. It contains useful information on what Windows Hello is and isn't, other setup items or changes outside this process, that will help you prepare and decide what method to choose.

Enhanced Sign-in Security (ESS) Enrollment

Purpose	This Quick Reference Guide walks you through the process of enrolling your Suncor owned/managed device in ESS with either a 6-digit PIN, or Facial Recognition (should your device support) + 6-digit pin as backup.
Pre-requisites	• Window 10 version 21H2 or later; • configured with ESS security policy; • FR* only - H/W must be capable of supporting. • MS Authenticator app set as default method for authentication
Intended User	Users of a Suncor owned/managed device such as a desktop/laptop PC or tablet, whose device meets the pre-requisites for Windows Hello.

Procedure Steps

Connect securely to the Suncor network

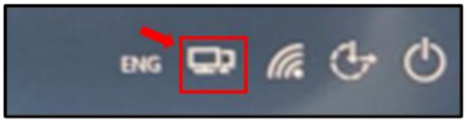
1. You must connect to the Suncor network to activate the enrollment process. If you are **on-site** go to Step 9.

   If you are not on-site, before you sign-in connect using **AnyConnect VPN**, as shown below.

2. On the sign-in screen, from the bottom right click the **icon** with the double-monitor.

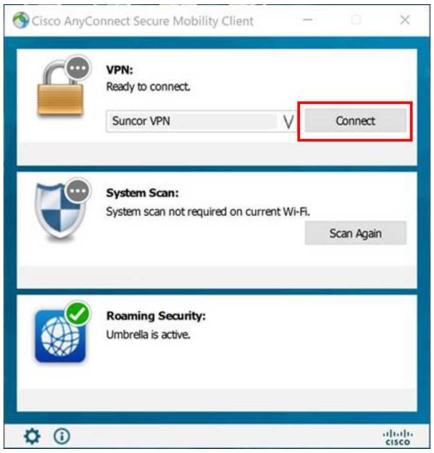
   The **Cisco AnyConnect Secure Mobility Client** dialog opens, performs a scan and advises if ready to connect.

   ***Note**: if you also use other Suncor VPN connections you may have to choose AnyConnect.*



3. In the dialog displaying the 'Suncor VPN', click **Connect**.

   (May not be exactly as shown)

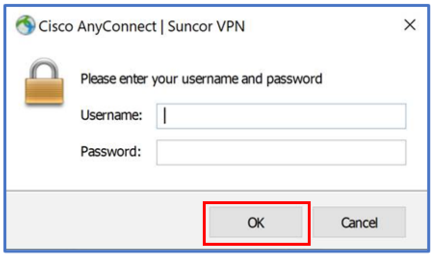


VPN:
Ready to connect.

System Scan:
System scan not required on current Wi-Fi.

Roaming Security:
Umbrella is active.

4. Enter your **username** and **password** then click **OK.**

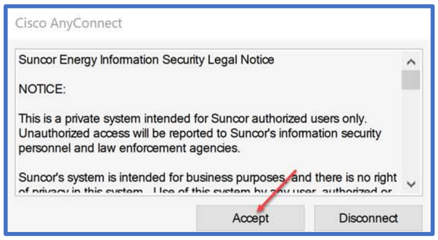


Please enter your username and password

Username:

Password:

5. **Accept** the legal notice



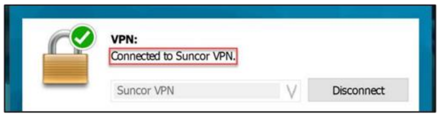
Suncor Energy Information Security Legal Notice

NOTICE:

This is a private system intended for Suncor authorized users only. Unauthorized access will be reported to Suncor's information security personnel and law enforcement agencies.

Suncor's system is intended for business purposes, and there is no right of privacy in this system. Use of this system by any user, authorized or

6. **Success!** You are securely connected to the Suncor network using VPN. **Advance** to the next step.



VPN:
Connected to Suncor VPN.

Updating the Group Policy

If your computer still requires the group policy loaded, an email notifying you of such is sent. As soon as you connect to the Suncor network the policy is applied.

You will not get a notification that this has occurred. However, if you advance to the Enrollment steps and you are not prompted to begin, then reboot your device. You may need to do this twice for the features to take effect. Remember to connect to VPN each time.

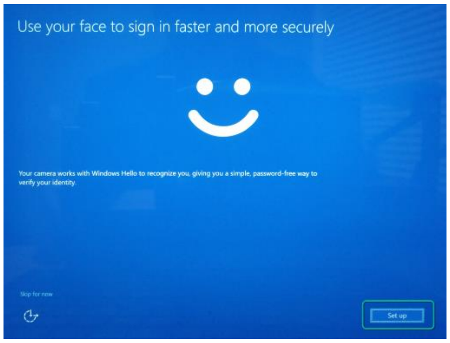
Continue to the **Enrollment** steps.

Enrollment begins at sign-in

Before you begin: Review steps 7 through 15, to familiarize yourself with the process. When you are ready, advance to the next step.

The ESS enrollment wizard begins

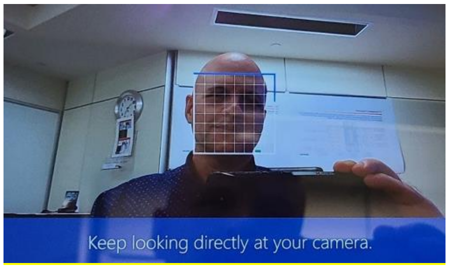
7. If the **Create a PIN** screen displays, or if you want to skip FR *(select **Skip for now** in the bottom left corner of screen)* go to Step 10, otherwise continue steps for facial recognition (shown on right).
8. Click **Set up**.



Use your face to sign in faster and more securely

Your camera works with Windows Hello to recognize you, giving you a simple, password-free way to verify your identity.

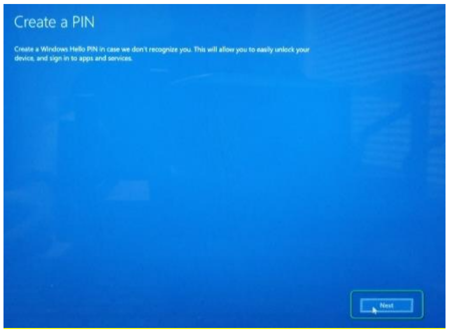
9. You are asked to look directly at your camera. Do so until prompted to continue with the PIN setup.



Keep looking directly at your camera.

10. At the **Create a PIN** screen, click **NEXT.**

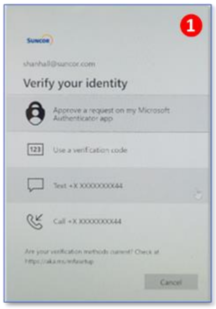
    You are prompted to **Verify your identity**.



Create a PIN

Create a Windows Hello PIN in case we don't recognize you. This will allow you to easily unlock your device, and sign in to apps and services.

11. Select your authentication method, then complete the '*Verify…'* process by clicking **Verify**.



1

shanhall@suncor.com

Verify your identity

Approve a request on my Microsoft Authenticator app

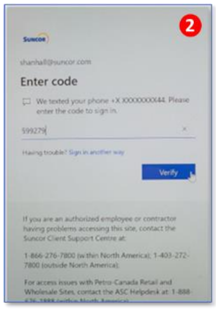
Use a verification code

Text +X XXXXXXXX44

Call +X XXXXXXXX44

Are your verification methods current? Check at https://aka.ms/mfasetup

Cancel



2

shanhall@suncor.com

Enter code

We texted your phone +X XXXXXXXX44. Please enter the code to sign in.

599279

Having trouble? Sign in another way

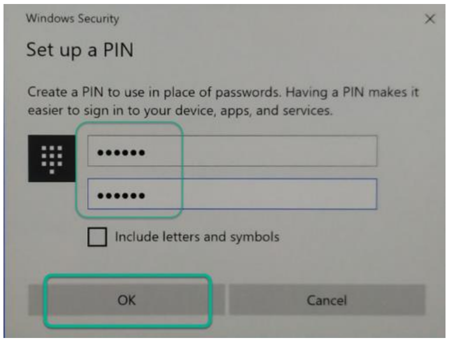
Verify

If you are an authorized employee or contractor having problems accessing this site, contact the Suncor Client Support Centre at:

1-866-276-7800 (within North America); 1-403-272-7800 (outside North America).

For access issues with Petro-Canada Retail and Wholesale Sites, contact the ASC Helpdesk at: 1-888-

12. At the **Set up a PIN** dialog, enter your new PIN in the first text box
13. Repeat your new PIN, in the second text box
14. Click **OK**



Windows Security

Set up a PIN

Create a PIN to use in place of passwords. Having a PIN makes it easier to sign in to your device, apps, and services.

••••••

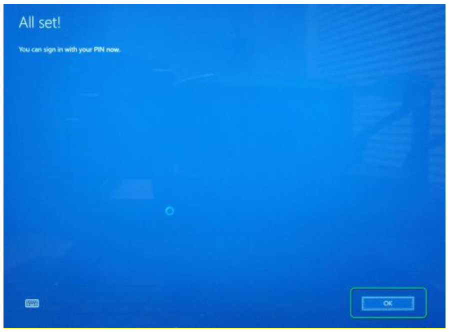
••••••

□ Include letters and symbols

OK Cancel

15. When complete, the **All set!** window displays. Click **OK**
16. The Sign in screen displays. Continue with your new sign-in credentials.

    NOTE: *If you encountered an issue completing enrollment or, when logging in, you can clear your biometric data and begin again. See the document:* ***QRG Resetting or Restarting ESS Windows Hello enrollment.***



All set!

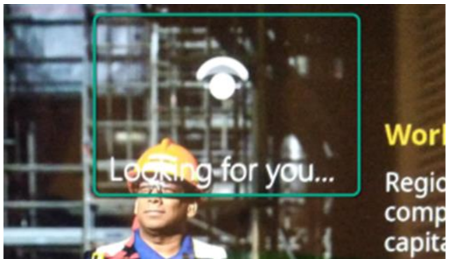
You can sign in with your PIN now.

OK

After enrollment is complete

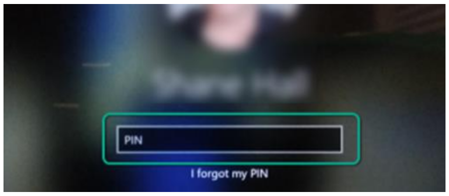
At your next sign-in or Windows unlock, the following is enabled:

- Enhanced Facial Recognition (FR) aka Windows Hello Face (if hardware supports). Look directly at the camera. You are logged in when recognition is complete. This should only take a few seconds.



- 6-digit PIN requirement.
  If this is your primary sign-in method, the screen to the right displays where you can enter your pin

  Note: *This is also your backup method should FR authentication fail.*



Frequently asked Questions (FAQ)

Q-1. Am I required to use biometric data on my Suncor Device?

You can choose either **Facial Recognition** (FR) or **PIN** as your primary means of Windows Hello sign-in. Currently, there are no plans to allow fingerprint biometrics, like you may use on your phone or similar devices.

Q-2. Is my biometric data secure and/or is it shared elsewhere?

If you choose to enable facial recognition, your device will take a series of measurements of your facial features to create a "digital map" (biometric data) of your likeness. Your biometric data is then encrypted, isolated and **kept** on your device. At sign in, using Windows Hello Face, the stored biometric data is compared to the current scan and verified locally. When you connect to the Suncor network, whether on-site or, off-site via VPN, your device only sends an encrypted key that tells the authenticating server that you are you, so you can unlock your device.

The specifics of your biometric data are never shared or sent to external devices or servers. Additionally, even if an attacker were able to access the encrypted biometric data on your device, it could not be reverse engineered to create your image.

The facial recognition feature never photographs your image, stores or shares photos of you with Suncor or Microsoft.

Q-3. What is the difference between using a PIN and using a password?

Passwords, along with user name, are stored and authenticated on the server to which you are connecting. Whether for network or application access, when you sign-in your password is sent to a server which then validates your identity and grants you access. In the event of a server’s data breach, your stolen information can be used anywhere to gain access if the combo (username/pw) is the same.

A PIN is tied to the device

Just as with biometric data, an Hello PIN is tied to the device you set it up on. If you use more than one device (i.e. desktop and laptop), you have to set up Hello on each device.

A PIN is backed by hardware

On many modern devices, the Trusted Platform Module (TPM) chip is used. It is a secure crypto-processor that includes multiple physical security mechanisms to make it tamper resistant even against malicious software and PIN brute-force attacks. Too many incorrect guesses and the device is locked.

A PIN can be complex

While the same IT management policies can be applied to a PIN as it can to a password – complexity, length, expiration and history, Suncor has kept it simple. Your managed device requires a 6-digit length, numbers only, pin to be set as either a backup to FR or a primary means of sign-in. It will be locked after a certain number of failed attempts.

Q-4. What if someone steals or I lose my device?

To gain access to your device, someone, in possession of your device, would need a way to spoof your biometrics or guess your PIN before your device gets locked. The special hardware, called the TPM module, has a feature that limits brute-force attacks.

Q-5. Do I need Enhanced Sign-in Security if I am connecting with my own device?

Currently, only Suncor owned/managed devices will be enrolled in ESS. Those devices must meet the pre-requisites as indicated at the beginning of this document.

- Window 10 version 21H2 or later;
- configured with ESS security policy;
- FR* only - H/W must be capable of supporting

Q-6. If my device does not have a camera can I use a pluggable camera if I want to use Facial Recognition.

Suncor's implementation of ESS does not support external camera modules or multiple cameras at this time..

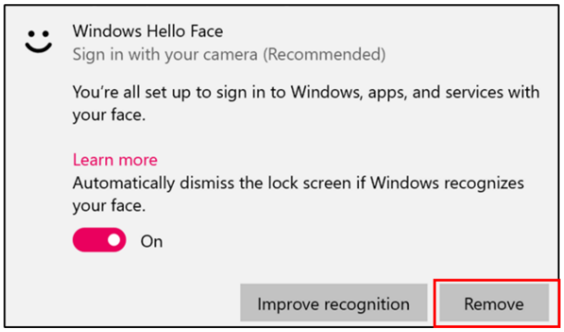
Q-7. Can I disable ESS if I don't want to use Facial Recognition (FR)?

The ESS (Windows Hello) group policy is not editable. However, if you just want to change from FR to PIN as your primary authentication method, you can remove Windows Hello Face from the sign-in options on your account.

Using **Windows key + I**, under **Accounts** > **Sign-in options** > **Windows Hello Face** > select **Remove**

Alternatively, you can follow the instructions in the document **QRG Resetting or Restarting ESS Windows Hello enrollment**. This document guides you through clearing your biometrics so you can re-enroll your device in ESS. After you have cleared your biometrics, enrollment is triggered. Follow the steps in this document to choose **PIN** only, rather than **FR+PIN**. You will **NOT** be able to remove the PIN as it is required as a back-up to Windows Hello Face.

__Note__: these steps also apply if you are having issues with FR and need to reset and re-enroll



Windows Hello Face

Sign in with your camera (Recommended)

You're all set up to sign in to Windows, apps, and services with your face.

Learn more

Automatically dismiss the lock screen if Windows recognizes your face.

On

Improve recognition

Remove

Q-8. Can I temporarily switch to using a PIN, if my primary method of authentication is currently FR.

Yes, if you cover your camera with a sticky-note or your hand, FR will fail and you will be prompted to use a different authentication method. Select the PIN icon, enter your PIN and continue as usual.

Q-9. What happens if I have multiple monitors and use FR to connect?

FR only works on the device where the camera resides.

For example, if you currently have three monitors – 1 built in to laptop, and 2 external –, with the first external monitor being primary and normally displaying the sign-in/lock screen, the sign-in screen displays on your laptop monitor. After FR has authenticated you, monitor order goes back to the configuration in your settings. This would be the same if you docked your PC, closed the laptop and only used the monitors.

Q-10. What happens if I forget my PIN?

At the Windows lock/sign-in screen, directly below the PIN entry field, is a link labeled **I forgot my PIN**. This triggers the Multi-Factor Authentication (MFA) function which validates your identity (as shown in steps 10-14 of this document). Follow those steps to reset your PIN. When finished unlock your desktop using your new PIN.

Q-11. What happens if I change my password?

When you set up Windows Hello for Business, the PIN or biometric gesture you use is specific to that device. Changing the account password does not impact sign-in/unlock on these devices because they use a key for authentication and not your password.

Q-12. Do I need to use Windows Hello even if I am not connected to Suncor’s network?

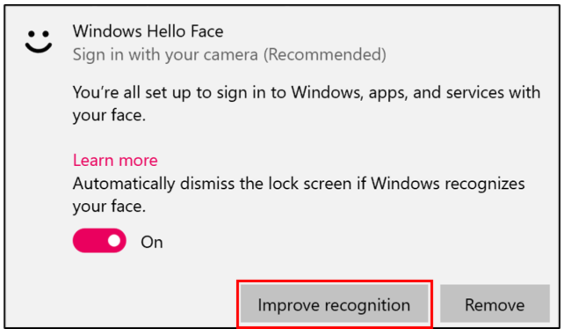
Your sign-in method is tied to the device regardless if you are connected to Suncor’s network or not. After enrollment is complete, whether you are connected or working locally, your sign-in method remains the same.

Q-13. I wear glasses. Do I need to enroll without them, with them, or both?

If you always wear glasses then enrolling facial recognition with your glasses on would be appropriate. If you only occasionally wear glasses then leave them off during facial recognition enrollment. However, if you had your glasses on when you enrolled in facial recognition, and you are currently having issues with recognition, or you wear/don’t wear glasses equally, then you may need to run ‘**Improve Recognition**’. Early adopters rarely ran into issues with FR.

Using **Windows key + I** , under **Accounts** > **Sign-in options** > **Windows Hello Face** > select **Improve recognition**.

This process lets you create additional enrollments of your facial features (w/ glasses, w/o glasses, different lighting, different hair style/cut et al), which then helps the algorithm to identify you.



Windows Hello Face

Sign in with your camera (Recommended)

You’re all set up to sign in to Windows, apps, and services with your face.

Learn more

Automatically dismiss the lock screen if Windows recognizes your face.

● On

Q-14. Do I need Enhanced Sign-in Security if I am connecting to my cloud PC or other networks?

Currently, **Windows Hello for Business** is not supported on cloud PCs (RDP). **Sign-in** to your cloud PC as you normally did with your account and password.