CONFIGURATION – WINDOWS HELLO FOR BUSINESS

Content

I.PURPOSE

The purpose of this document is to detail the current configuration standards of Ciena Healthcare's Windows Hello for Business environment.

II. SCOPE

The configuration is only applied to IT department and some other users currently.

III. AUDIENCE

This document is intended for Ciena IT Administrators and those with elevated privileges to configure and manage the Windows Hello for Business environment.

IV. DEPLOYMENT PREREQUISITES

- Azure AD Multifactor Authentication
- Windows 10 21H2, Windows 11 or later
- Windows Server 2016 or later domain controllers
- Microsoft Intune or another modern device management platform for deploying the Cloud Kerberos trust policy settings
- all devices have a TPM 2.0 module that complies with Federal Information Processing Standards (FIPS). All devices should be on Windows 10 version 1709 (or later) or Windows 11. Preferably, all devices should be Windows 10 version 1903 or later.
- Devices are equipped with an infrared camera or fingerprint reader for biometric authentication.

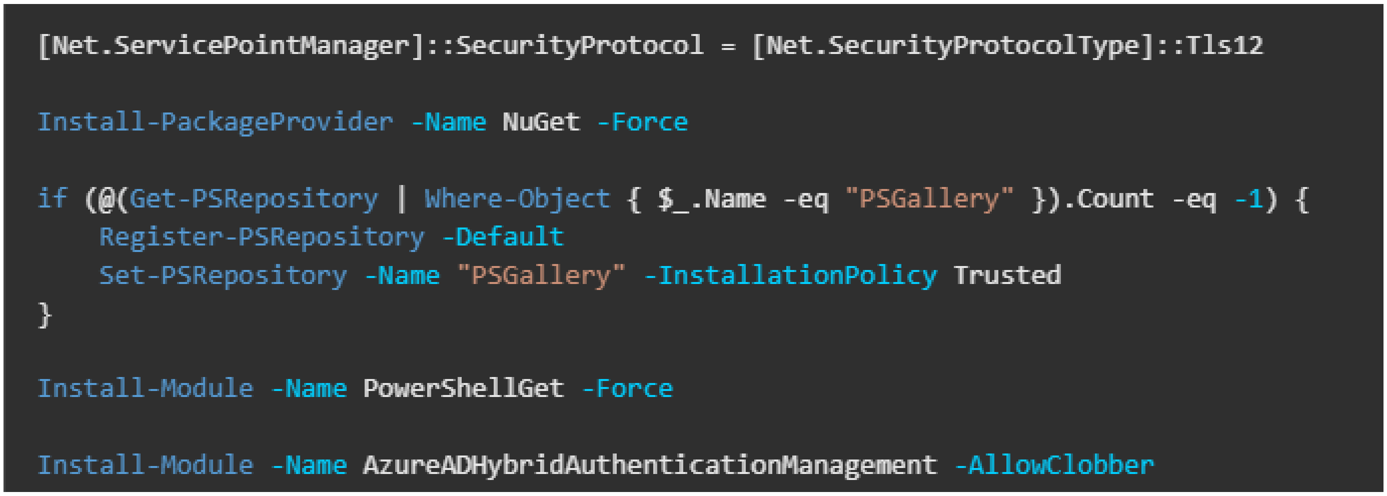
Install the Azure AD Hybrid Authentication Management PowerShell module

You'll use the *Azure AD Hybrid Authentication Management PowerShell module* to configure a Trusted Domain Object in the on-premises AD and register the trust with Microsoft Entra ID, establishing an inbound trust.

1. Start a Windows PowerShell session with **Run as administrator**
2. Install the Azure AD Hybrid Authentication Management PowerShell module using the following script

To install Azure AD Kerberos, we are going to use PowerShell. Make sure that you have a Global Administrator account for Azure AD and a Domain Admin account for your on-premises AD.

Note: TLS 1.2 is required to access the PowerShell Gallery. Run the following command if it is not enabled.



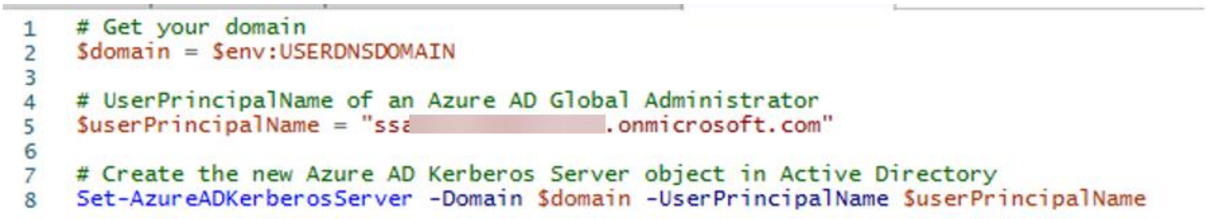
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

Install-PackageProvider -Name NuGet -Force

if (@(Get-PSRepository | Where-Object { $_.Name -eq "PSGallery" }).Count -eq -1) {
    Register-PSRepository -Default
    Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
}

Install-Module -Name PowerShellGet -Force

Install-Module -Name AzureADHybridAuthenticationManagement -AllowClobber
```

V. IMPLEMENT HYBRID CLOUD TRUST

We are going to create the Kerberos Server object. For this, we will need to an administrator account, so we create the object in the Active Directory and verify our tenant.

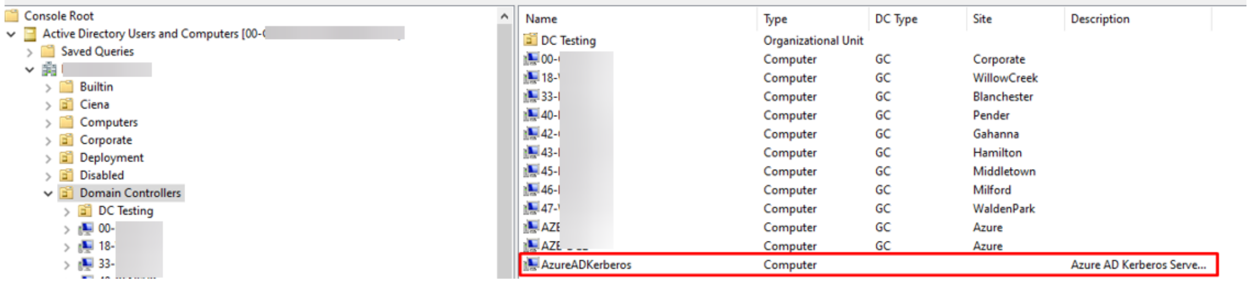
- AzureADKerbrosServer object has been install on these domains
    - South.MoMotecho.com
    - Columbus.MoMoTecho.com

1. Run the script below on the domain controller.



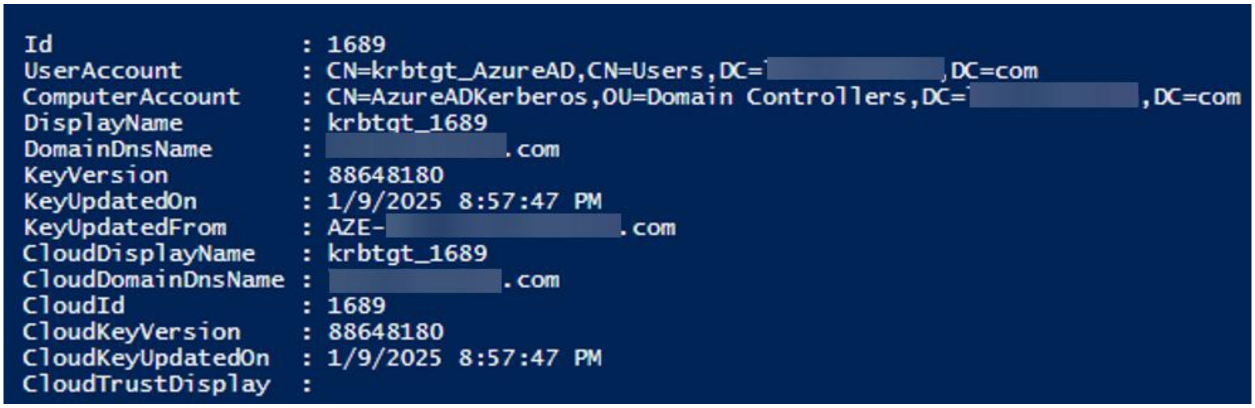
```
# Get your domain
$domain = $env:USERDNSDOMAIN

# UserPrincipalName of an Azure AD Global Administrator
$userPrincipalName = "ssa[redacted].onmicrosoft.com"

# Create the new Azure AD Kerberos Server object in Active Directory
Set-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName
```

2. Once completed, you will find the AzureADKerberos computer object in your Active Directory in the domain controller OU as shown below.

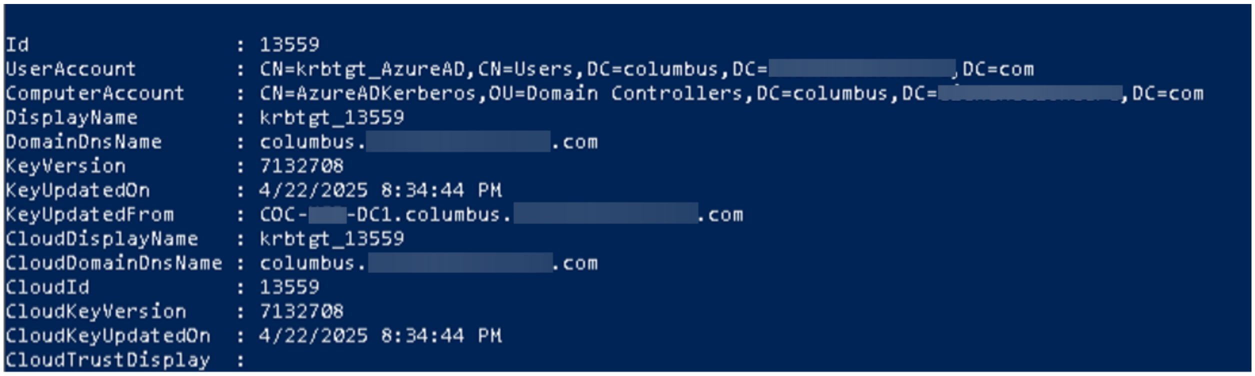


Name	Type	DC Type	Site	Description
DC Testing	Organizational Unit			
00-[redacted]	Computer	GC	Corporate	
18-[redacted]	Computer	GC	WillowCreek	
33-[redacted]	Computer	GC	Blanchester	
40-[redacted]	Computer	GC	Pender	
42-[redacted]	Computer	GC	Gahanna	
43-[redacted]	Computer	GC	Hamilton	
45-[redacted]	Computer	GC	Middletown	
46-[redacted]	Computer	GC	Milford	
47-[redacted]	Computer	GC	WaldenPark	
AZE[redacted]	Computer	GC	Azure	
AZE[redacted]	Computer	GC	Azure	
AzureADKerberos	Computer			Azure AD Kerberos Serve...

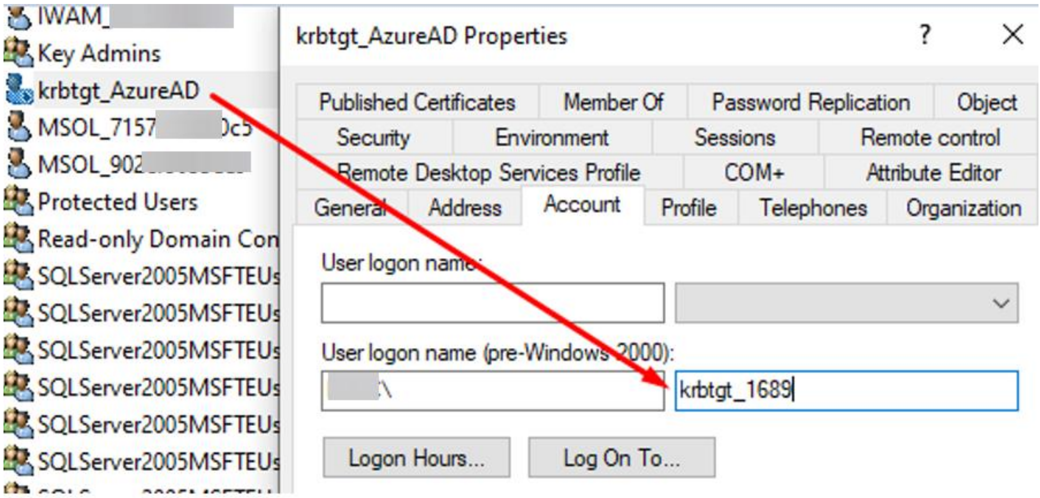
3. Verify that the Kerberos server RODC object was created successfully (intentionally disable)
    - Open PowerShell and run as Admin. Type the script below:
    - *Get-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName*



```
Id                    : 1689
UserAccount           : CN=krbtgt_AzureAD,CN=Users,DC=[redacted],DC=com
ComputerAccount       : CN=AzureADKerberos,OU=Domain Controllers,DC=[redacted],DC=com
DisplayName           : krbtgt_1689
DomainDnsName         : [redacted].com
KeyVersion            : 88648180
KeyUpdatedOn          : 1/9/2025 8:57:47 PM
KeyUpdatedFrom        : AZE-[redacted].com
CloudDisplayName      : krbtgt_1689
CloudDomainDnsName    : [redacted].com
CloudId               : 1689
CloudKeyVersion       : 88648180
CloudKeyUpdatedOn     : 1/9/2025 8:57:47 PM
CloudTrustDisplay     :
```



```
Id                 : 13559
UserAccount        : CN=krbtgt_AzureAD,CN=Users,DC=columbus,DC=[redacted],DC=com
ComputerAccount    : CN=AzureADKerberos,OU=Domain Controllers,DC=columbus,DC=[redacted],DC=com
DisplayName        : krbtgt_13559
DomainDnsName      : columbus.[redacted].com
KeyVersion         : 7132708
KeyUpdatedOn       : 4/22/2025 8:34:44 PM
KeyUpdatedFrom     : COC-[redacted]-DC1.columbus.[redacted].com
CloudDisplayName   : krbtgt_13559
CloudDomainDnsName : columbus.[redacted].com
CloudId            : 13559
CloudKeyVersion    : 7132708
CloudKeyUpdatedOn  : 4/22/2025 8:34:44 PM
CloudTrustDisplay  :
```



User logon name:

User logon name (pre-Windows 2000): [redacted]\ krbtgt_1689

VI. CONFIGURE WINDOWS HELLO FOR BUSINESS WITH POLICY

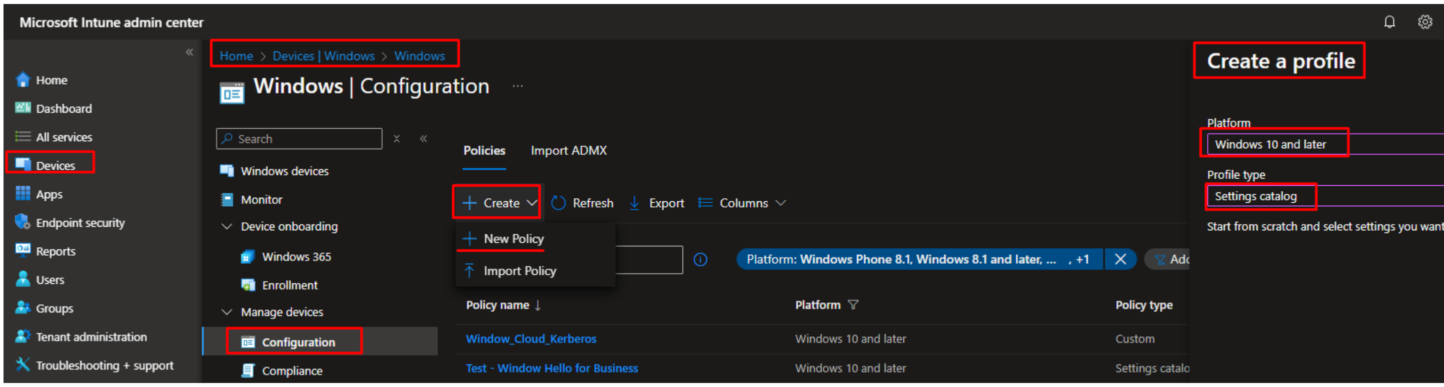
INTUNE POLICY SETTINGS

WINDOW HELLO FOR BUSINESS POLICY CONFIGURATION

In a hybrid environment, we can configure Windows Hello for Business group policy through Microsoft Intune. Below is the configuration for Windows Hello for business.

1. Open the Microsoft Intune admin center portal and navigate to **Devices > Windows > Configuration**

2. On the **Windows | Configuration profiles**, click “**Create Profiles**”
3. On the **Create a profile**, provide the following information and click **Create**
    - Platform: Select Windows 10 and later create a profile for Windows 10 and Windows 11 devices
    - Profile: Select Settings Catalog to select the required setting from the catalog



Platform: Windows Phone 8.1, Windows 8.1 and later, ... , +1

Policy name ↓	Platform	Policy type
Window_Cloud_Kerberos	Windows 10 and later	Custom
Test - Window Hello for Business	Windows 10 and later	Settings catalo

Platform: Windows 10 and later

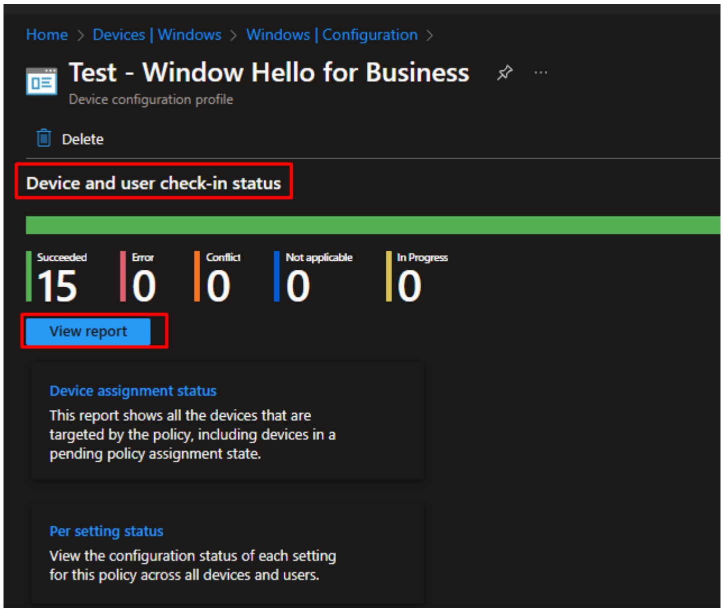
Profile type: Settings catalog

4. On the **Basics** page, provide the following information and click Next
5. On the Configuration settings page, perform the following actions
    - Click **Add settings** and perform the following in Settings picker
    - Select **Windows Hello for Business** as category (Select any settings as you desire)
    - Select Use **Cloud Trust for On Prem Auth** as settings
6. On the **Scope tags** page, configure the required scope tags and click Next
7. On the **Assignments** page, select the group that you want the policy to apply
8. On the **Review + create page**, verify the configuration and click **Create**

Our current configuration settings for “Windows Hello for Business” are:

- Allow Use of Biometrics: (Enabled)
- Facial Features Use Enhanced Anti Spoofing: (true)
- Require Security Device: (true)
- PIN History: (5) - the number of past PINs that can be stored in history that can’t be used
- Enable Pin Recovery: (true)
- Minimum PIN Length: (7)
- Maximum PIN Length: (127)
- Use Cloud Trust For On Prem Auth: (Enabled)
- Use Windows Hello For Business (Device): (true)
- Special Characters (Device): Require the use of at least one special character in PIN

You can check the status of the policy as shown in the picture below.



Test - Window Hello for Business

Device configuration profile

Device and user check-in status

Succeeded	Error	Conflict	Not applicable	In Progress
15	0	0	0	0

Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

Per setting status

View the configuration status of each setting for this policy across all devices and users.

CLOUD KERBEROS TRUST SETTINGS

We will now need to deploy additional Cloud Kerberos trust policy settings to clients via modern device management policy deployment and OMA-URI settings.

1. Open Microsoft Intune admin center portal and navigate to **Device > Windows > Configuration**
2. On the **Windows | Configuration profiles**, click “**Create Profiles**”
3. On the **Create a profile**, provide the following information and click **Create**
    - Platform: choose “Windows 10 and later”
    - Profile Type: choose “**Templates**” and under “**Template Name**” select “**Custom**” and click “**Create**”
4. Provide the profile with a name and description, then click **Next**
5. On the configuration settings page, add a new configuration with the following values”

   OMA-URI settings for “**Windows Hello for Business Cloud Kerberos Trust”**

    - Name**: Windows Hello for Business Cloud Kerberos Trust**
    - Description: **Enable Windows Hello for Business cloud Kerberos trust for sign-in**
    - OMA-URI: **./Device/Vendor/MSFT/PassportForWork/2fd31256-778e-49eb-84ff-28e677d2d88c/Policies/UseCloudTrustForOnPremAuth**
    - Data Type: **Boolean**
    - Value**: True**

   OMA-URI settings for “**Cloud Kerberos Ticket Retrieval”**

    - Name**: Cloud Kerberos Ticket Retrieval**
    - Description: **Cloud Kerberos Ticket Retrieval**
    - OMA-URI: **./Device/Vendor/MSFT/Policy/Config/Kerberos /CloudKerberos**

TicketRetrievalEnabled

- Data Type**: Integer**
- Value: **1**

<u>OMA-URI settings for “**Enable PIN Reset”**</u>

- Name**: Enable PIN Reset**
- Description: **Enable PIN Reset**
- OMA-URI: **./Device/Vendor/MSFT/Policy/Config/Kerberos /CloudKerberos TicketRetrievalEnabled**
- Data Type**: Boolean**
- Value: **True**

VII. USER EXPERIENCE

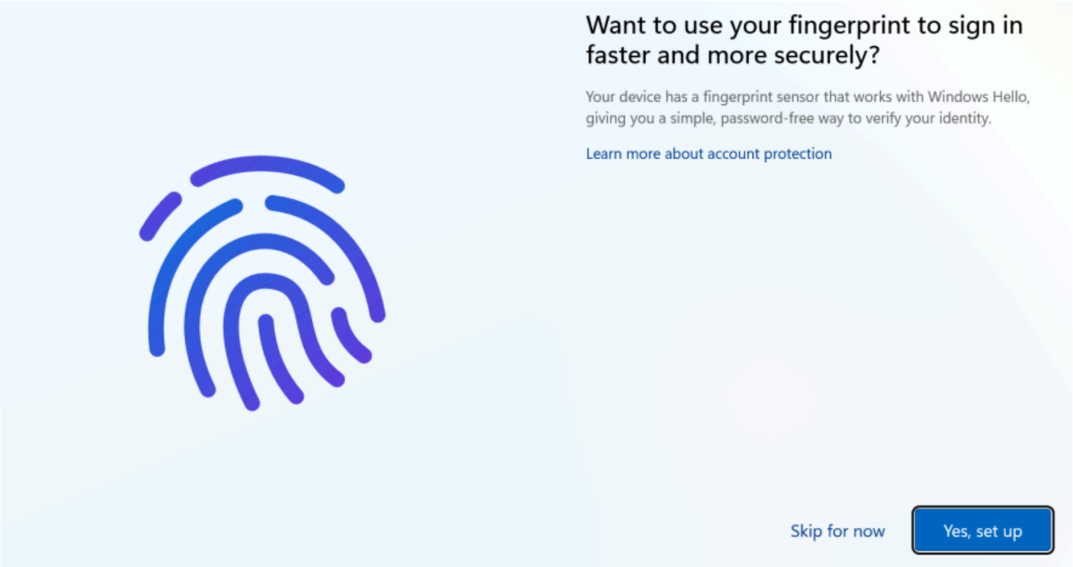
SETTING UP WINDOWS HELLO FOR BUSINESS

When setting up your new Windows computer, you may see a screen instructing you to set up Windows Hello before the first sign-in completes.

There are 2 methods that will be prompted on the initial set up. The first one is ***facial recognition***, second is ***fingerprint***. The computer will prompt you to be based on what your computer is compatible with.

Below is an example of a fingerprint set up for Windows Hello for business.

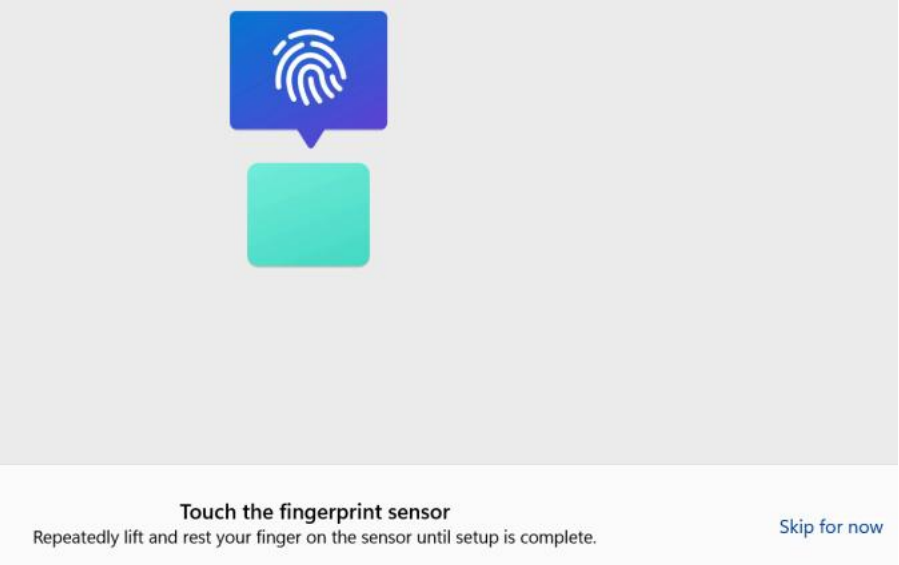
1. At the introduction, click “Set Up” to begin Windows Hello setup.



Want to use your fingerprint to sign in faster and more securely?

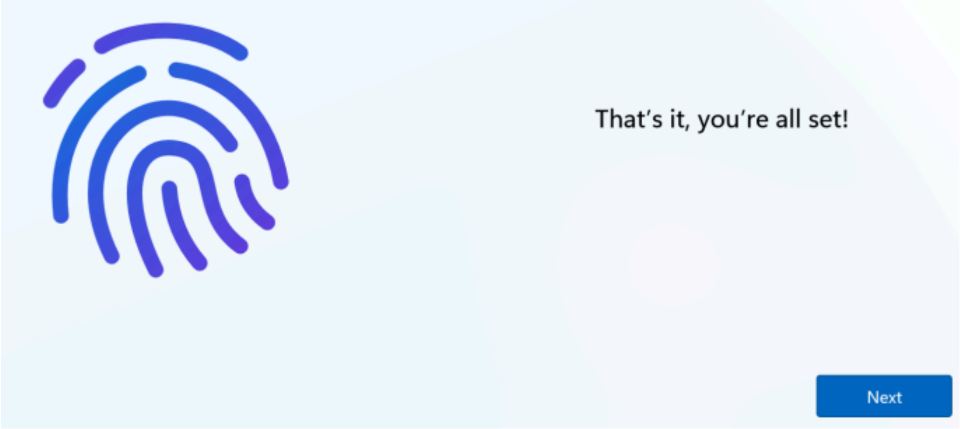
Your device has a fingerprint sensor that works with Windows Hello, giving you a simple, password-free way to verify your identity.

Learn more about account protection



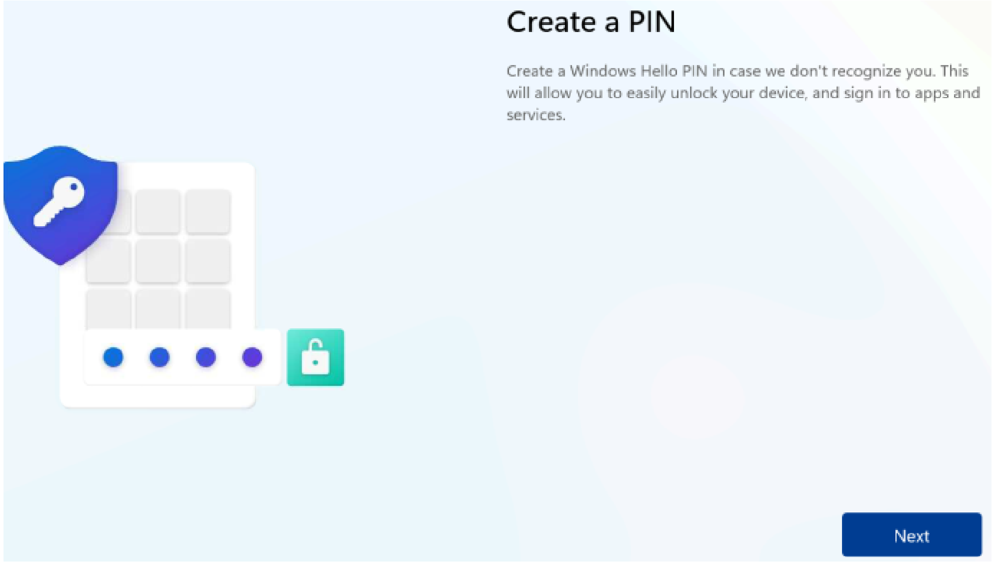
Touch the fingerprint sensor

Repeatedly lift and rest your finger on the sensor until setup is complete.



That's it, you're all set!

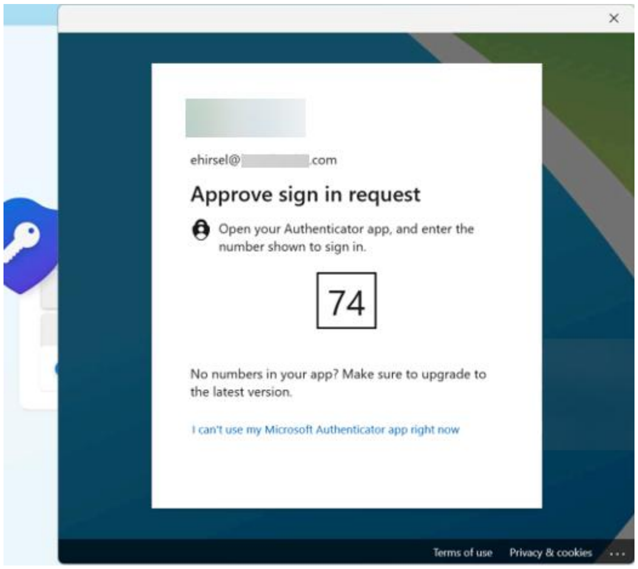
2. Windows Hello for Business requires MFA. Therefore, it requires approval through Microsoft Authenticator app or another app you have configured.



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.

3. Once you finish authenticating your MFA with MS authenticator, you will be prompted to set up a PIN as a backup sign in method. Requirements for PIN is:
    - Minimum of 7 digits
    - You can check the box to add letters or special characters



[redacted]

ehirsel@[redacted].com

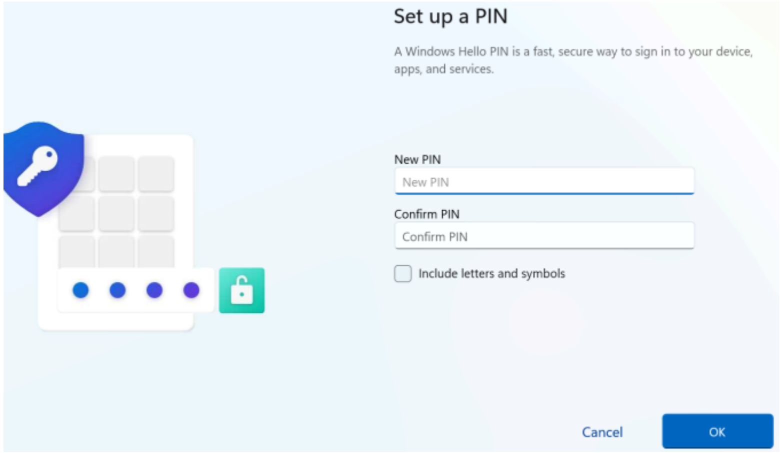
Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

74

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now



Set up a PIN

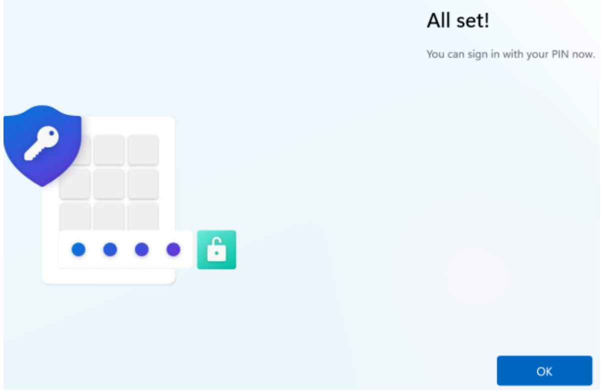
A Windows Hello PIN is a fast, secure way to sign in to your device, apps, and services.

New PIN: New PIN

Confirm PIN: Confirm PIN

□ Include letters and symbols

4. After your finish setting up your PIN. Just click “OK”, and you’ll be signing into your computer.

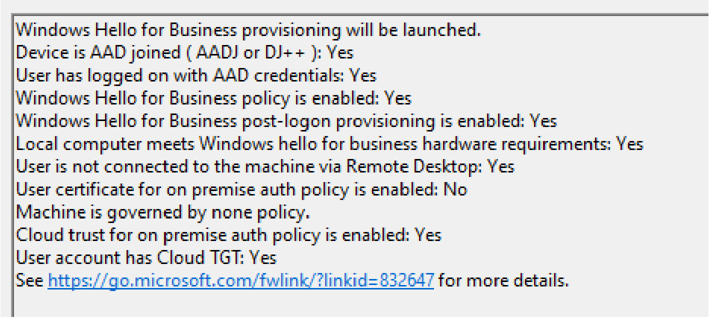


All set!

You can sign in with your PIN now.

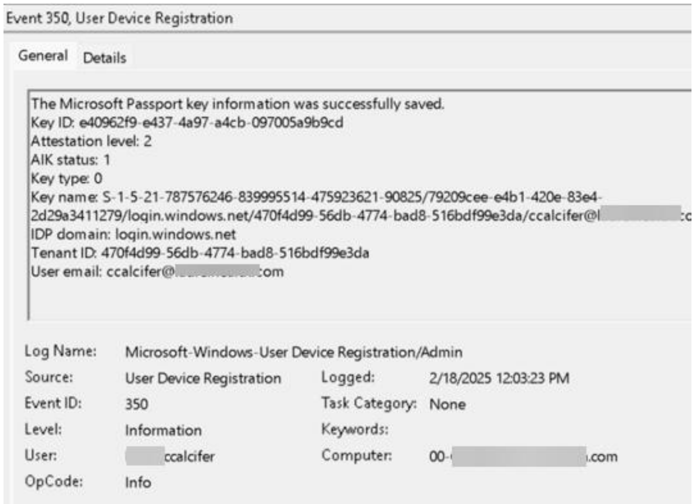
To verify that WHfB has been set up successfully, launch Event View.

- Navigate to **Applications and Services Logs** > **Microsoft** > **Windows** > **User Device Registration > Admin**



```
Windows Hello for Business provisioning will be launched.
Device is AAD joined ( AADJ or DJ++ ): Yes
User has logged on with AAD credentials: Yes
Windows Hello for Business policy is enabled: Yes
Windows Hello for Business post-logon provisioning is enabled: Yes
Local computer meets Windows hello for business hardware requirements: Yes
User is not connected to the machine via Remote Desktop: Yes
User certificate for on premise auth policy is enabled: No
Machine is governed by none policy.
Cloud trust for on premise auth policy is enabled: Yes
User account has Cloud TGT: Yes
See https://go.microsoft.com/fwlink/?linkid=832647 for more details.
```

This clearly showed that WHFB will be launched as all prerequisites were met including hardware requirements.



Event 350, User Device Registration

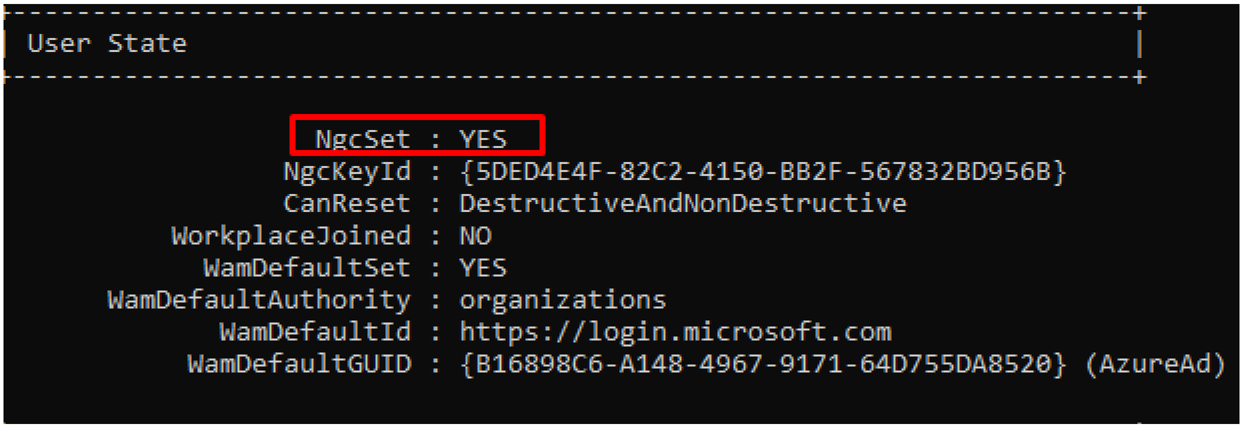
```
The Microsoft Passport key information was successfully saved.
Key ID: e40962f9-e437-4a97-a4cb-097005a9b9cd
Attestation level: 2
AIK status: 1
Key type: 0
Key name: S-1-5-21-787576246-839995514-475923621-90825/79209cee-e4b1-420e-83e4-
2d29a3411279/login.windows.net/470f4d99-56db-4774-bad8-516bdf99e3da/ccalcifer@l[redacted]:c
IDP domain: login.windows.net
Tenant ID: 470f4d99-56db-4774-bad8-516bdf99e3da
User email: ccalcifer@[redacted]com
```

```
Log Name:   Microsoft-Windows-User Device Registration/Admin
Source:     User Device Registration     Logged:         2/18/2025 12:03:23 PM
Event ID:   350                          Task Category:  None
Level:      Information                  Keywords:
User:       [redacted]ccalcifer          Computer:       00-[redacted].com
OpCode:     Info
```

- Above, you can see Microsoft Passport key information was saved which was related to PIN info saved.

Note: Microsoft Passport is a two-factor authentication (2FA) system that combines a PIN or biometrics (via Windows Hello) with encrypted keys from a user's device to provide two-factor authentication.

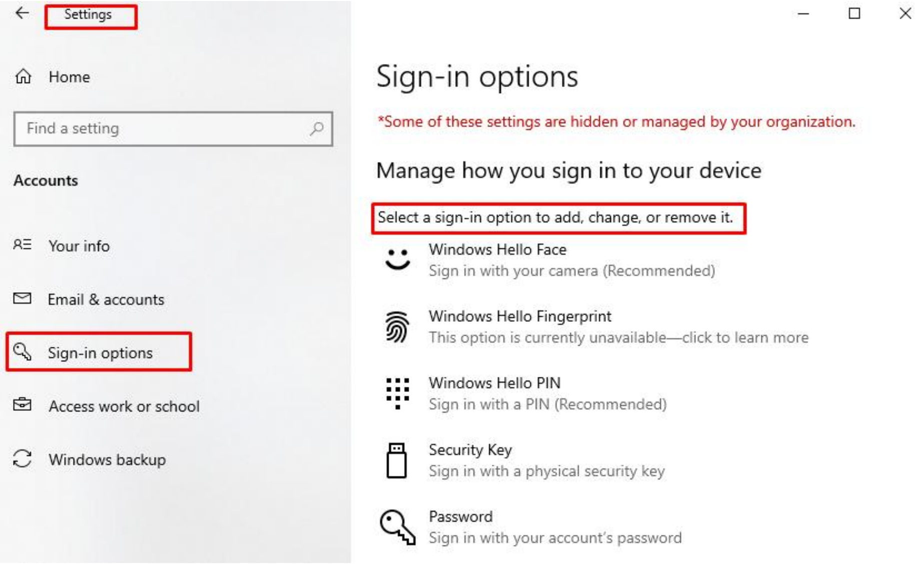
- You can verify whether if the user has Windows Hello configured and whether a workspace account is configured on the computer is:
- Navigate to **CMD** > type **DSREGCMD /STATUS:**
    - NgcSet: If a Windows Hello key is assigned to the currently logged-in user, the flag is set to **YES.**



```
+----------------------------------------------------------------------+
| User State                                                           |
+----------------------------------------------------------------------+

                    NgcSet : YES
                  NgcKeyId : {5DED4E4F-82C2-4150-BB2F-567832BD956B}
                  CanReset : DestructiveAndNonDestructive
           WorkplaceJoined : NO
             WamDefaultSet : YES
       WamDefaultAuthority : organizations
              WamDefaultId : https://login.microsoft.com
            WamDefaultGUID : {B16898C6-A148-4967-9171-64D755DA8520} (AzureAd)
```

ADDING SIGN-IN METHOD FOR WINDOWS HELLO

1. Go to Start > Settings > Account > Sign-in Options and follow the on-screen instructions to set up Windows Hello
2. Select one of the options below as you desire. You can add or remove those options. (Ex. Facial recognition, fingerprint or PIN)



Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.

Windows Hello Face
Sign in with your camera (Recommended)

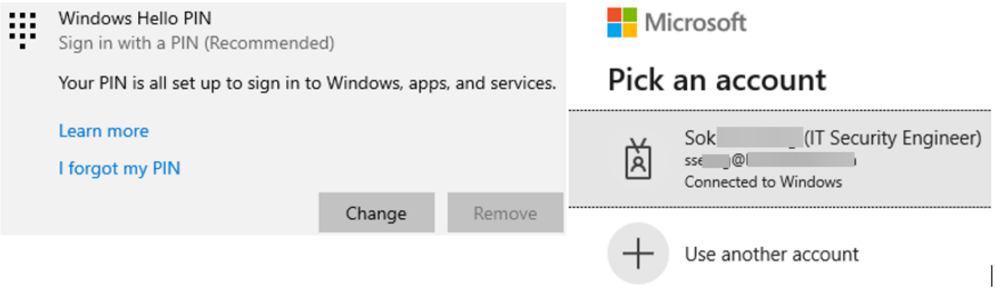
Windows Hello Fingerprint
This option is currently unavailable—click to learn more

Windows Hello PIN
Sign in with a PIN (Recommended)

Security Key
Sign in with a physical security key

Password
Sign in with your account's password

3. You can click on "Forget your PIN" and you will be prompt with MFA challenging

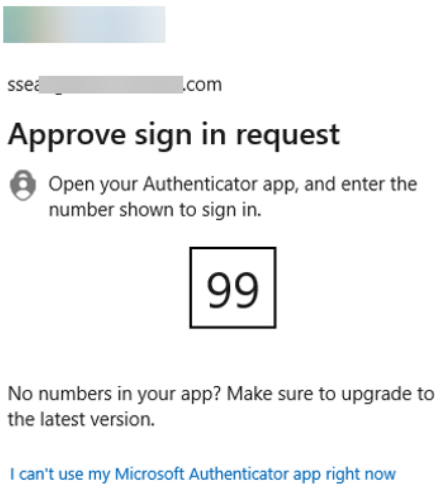


Windows Hello PIN
Sign in with a PIN (Recommended)

Your PIN is all set up to sign in to Windows, apps, and services.

Pick an account

Sok[redacted](IT Security Engineer)
sse[redacted]@[redacted]
Connected to Windows



sse[redacted].com

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

99

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

4. Just authenticate your account and then you will be able to change your PIN.

Frequent Questions:

1. How does WHfB determine how many users are logged in the device if the maximum per device is 10 users?
   Answer:

- Windows Hello determines the number of active users by tracking unique biometric profiles or PINs registered on the device and comparing them to the user's current attempt to authenticate.
- When a user enrolls in Windows Hello, the system creates a unique biometric profile (facial recognition, fingerprint, or iris scan) or PIN, which is stored locally on the device.
- During sign-in, Windows Hello uses the device's camera (for facial recognition) or fingerprint sensor to capture the user's biometric data or prompts for the PIN.
- The captured biometric data or entered PIN is then compared to the stored profile or PIN.
- If a match is found, Windows Hello verifies the user's identity and grants access to the device.
- By tracking the number of unique biometric profiles or PINs registered on the device and comparing them to the current authentication attempts, Windows Hello can determine the number of active users.

2. Where does the user's Windows Hello configuration locate in the local drive?

Answer: C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Ngc

C:\Windows\System32\WinBioDatabase

3. How many attempts do I get if I don't remember my PIN?

Answer: You have 3-4 attempts. If you enter the PIN wrong 3 times, we suggest doing the "Forgot PIN".

<u>Suggestion</u>: When you fail to type in your PIN several times, Windows Hello will ask you to type in the default Phrase (A1B2C3). Then, you should be able to enter your PIN again.

Revision

1.0	03/19/2025	Soklim Seang		Initial document creation.
1.1	05/16/2025	Soklim Seang		Modified PIN requirement and special characters
1.2	05/19/2025	Soklim Seang		Added available methods - WHfB