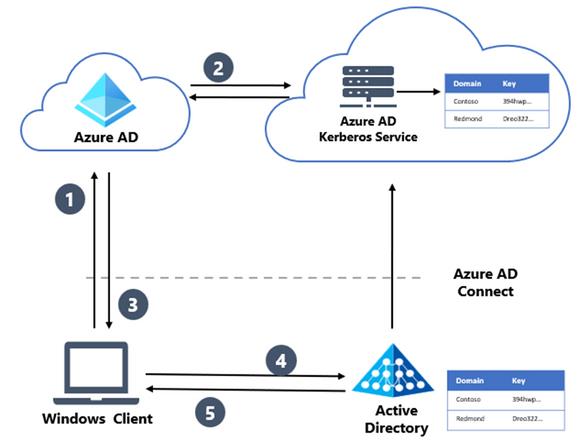
Who should do this?

Admins who need to set up WHFB for a hybrid environment but do not want or have ADFS. This does require Hybrid users therefore it will not work with cloud only or federated ADFS environments.

ALWAYS CHOOSE THIS IF YOU CAN. THE OVERHANG, SET UP AND KEEP UP IS FAR EASIER.

ARCHiTECTURE



Where to start.

Start by deploying the Kerberos Server. This needs to be done on an On-prem Joined Machine. It cannot be a hybrid joined machine! You will get an error.

If you run into errors running the provided Microsoft script then you should go to the AD Connect Server>Open Powershell as Admin> Navigate to the Aforementioned File path and run the script there. This file path already exists by default where AD Connect is set up and does not need to be created.

Instal the needed module:

# First, ensure TLS 1.2 for PowerShell gallery access.

[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor [Net.SecurityProtocolType]::Tls12

# Install the AzureADHybridAuthenticationManagement PowerShell module.

Install-Module -Name AzureADHybridAuthenticationManagement -AllowClobber

After that run the following

# Specify the on-premises Active Directory domain. A new Azure AD

# Kerberos Server object will be created in this Active Directory domain.

$domain = $env:USERDNSDOMAIN

# Enter a UPN of an Azure Active Directory global administrator

$userPrincipalName = "administrator@contoso.onmicrosoft.com"

# Enter a domain administrator username and password.

$domainCred = Get-Credential

# Create the new Azure AD Kerberos Server object in Active Directory

# and then publish it to Azure Active Directory.

# Open an interactive sign-in prompt with given username to access the Azure AD.

Set-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName -DomainCredential $domainCred

Sometimes this errors out the first time. So try running this at least twice.

Once it runs successfully, run the below to make sure that it was set up properly.

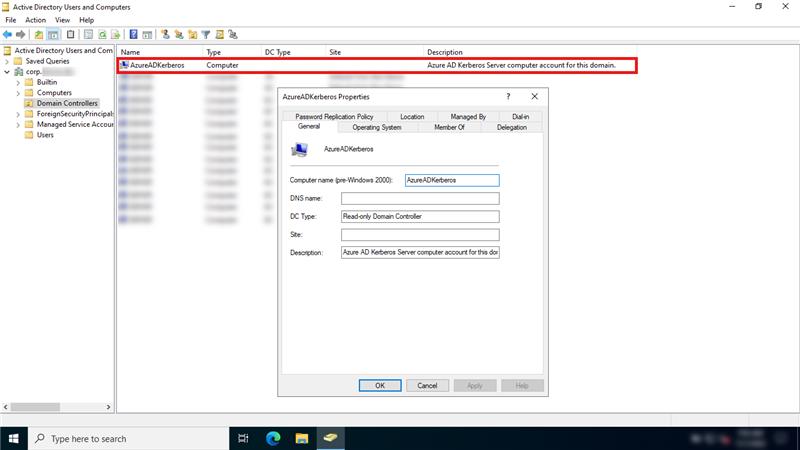
# When prompted to provide domain credentials use the userprincipalname format for the username instead of domain\username

Get-AzureADKerberosServer -Domain $domain -UserPrincipalName $userPrincipalName -DomainCredential (get-credential)

After this you need to set up the Intune Policies or GPO’s. It is up to you to decide which. However, GPO’s will take precedence in all on-prem joined machines unless you have rolled out a policy tthat states otherwise. This can cause some issues where Windows Hello is involved. So keep it in mind.

When Microsoft Entra Kerberos is enabled in an Active Directory domain, an AzureADKerberos computer object is created in the domain. This object:

* Appears as a Read Only Domain Controller (RODC) object, but isn't associated with any physical servers
* Is only used by Microsoft Entra ID to generate TGTs for the Active Directory domain



## **Configure Cloud Key Trust using Intune**

We can either use a GPO or push a configuration from Intune. If you are interested in using a GPO, read more [here](https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cloud-kerberos-trust?WT.mc_id=EM-MVP-5004117&tabs=gpo#tabpanel_1_gpo). In this post we will push the configuration from Intune (this is the way).

Ensure the client devices are a minimum of Windows 10 21H2 / Windows 11 Pro or Enterprise SKU. Perhaps consider using an [Intune Filter](https://learn.microsoft.com/en-us/mem/intune/fundamentals/filters) for targetting.

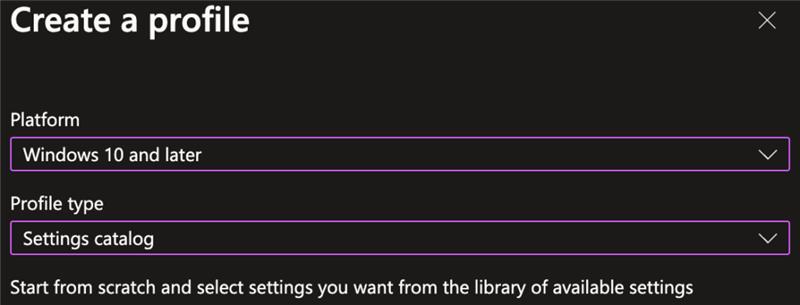
### **1. Create a configuration profile**

Assuming you don’t already have an existing policy for Windows Hello for Business, we will add it in it’s simplest form using the Settings Catalog.

### **2. Settings catalog profile**

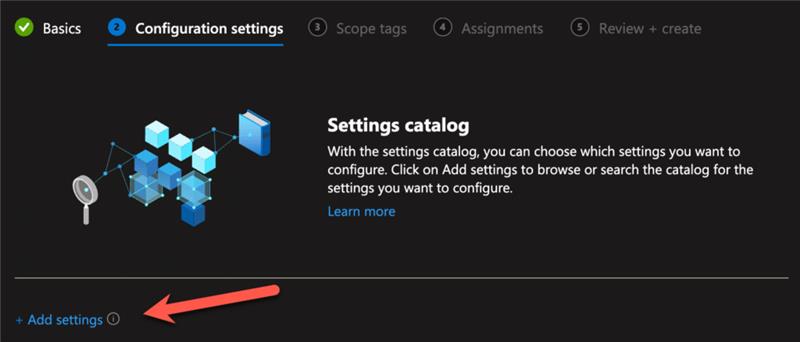
Go to the windows configuration profiles area and click “Create profile”

Select the “Windows 10 and later” platform along with the profile type “Settings catalog” and click “Create“

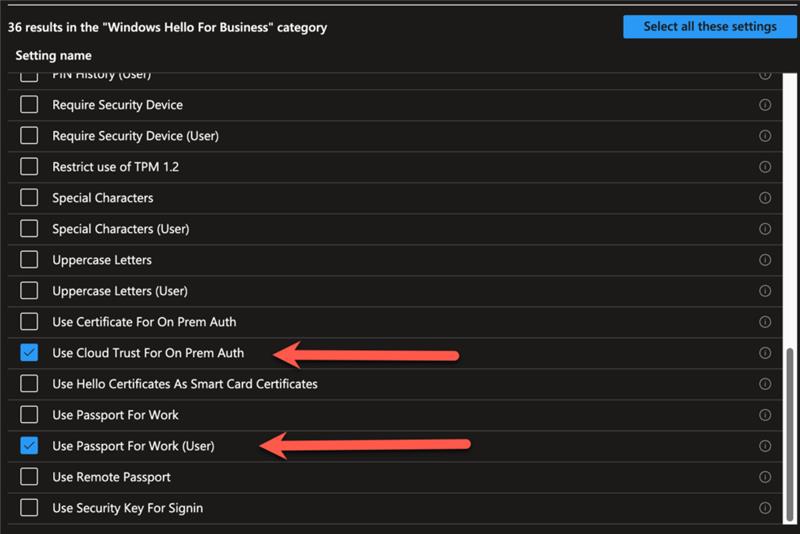


Give it an appropriate name and description and click “next“.

Now, start adding settings by clicking on the “Add settings button”.



The list of settings is LOOOONG, so, you want to do a search for “Windows Hello for Business” and click on the appearing category name “Windows Hello for Business” when it returns the result. Now we start by selecting the following settings (this is a minimum):

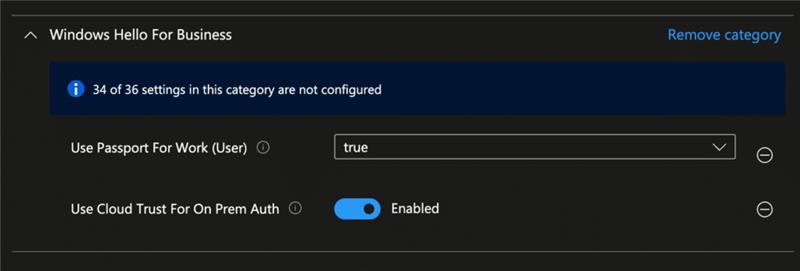


* Use Cloud Trust For On Prem Auth
* Use Passport for Work (User)

A few things to note here…

One is, that Passport for Work is the name in the CSP for “Windows Hello for Business”, it is a leftover form Microsoft rebranding. So, don’t get stuck on that. Speaking of rebranding, “Cloud Trust” and “Cloud Kerberos Trust” are the exact same thing, just another rebranding.

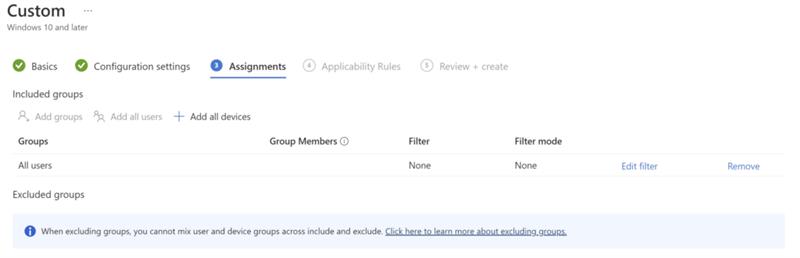
Second thing is that we selected a policy setting with the text “(User)” in it. This indicates that the user is the target. even if you assign to a device, this policy will be a user scoped policy on that device. This takes precedents over any other policies that might be targeted to the device. For Windows Hello for Business in Intune, the rules of precedents is “Tenant wide settings” over “User” and lastly “Device”.



Lastly we enable the settings and move on to the next part.

### **3. Assignments**

Assign the profile to your desired group. You can target either users or devices according to your own preference or policy in-house.

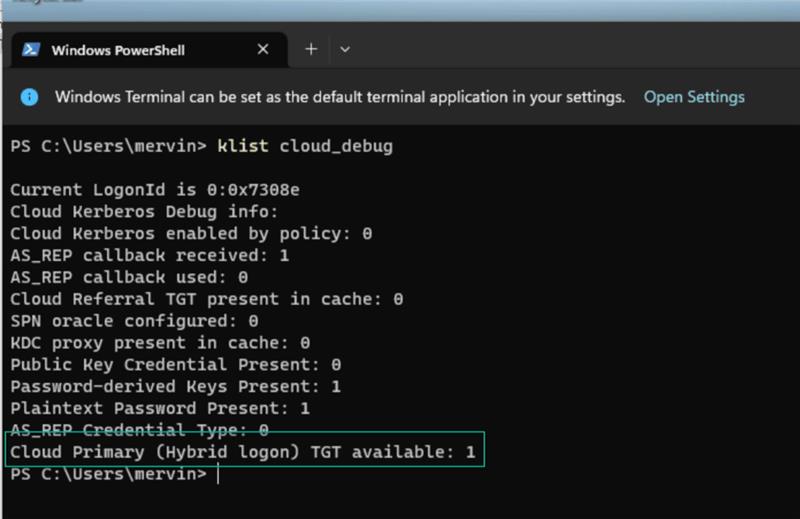


### **4. Test the policy worked**

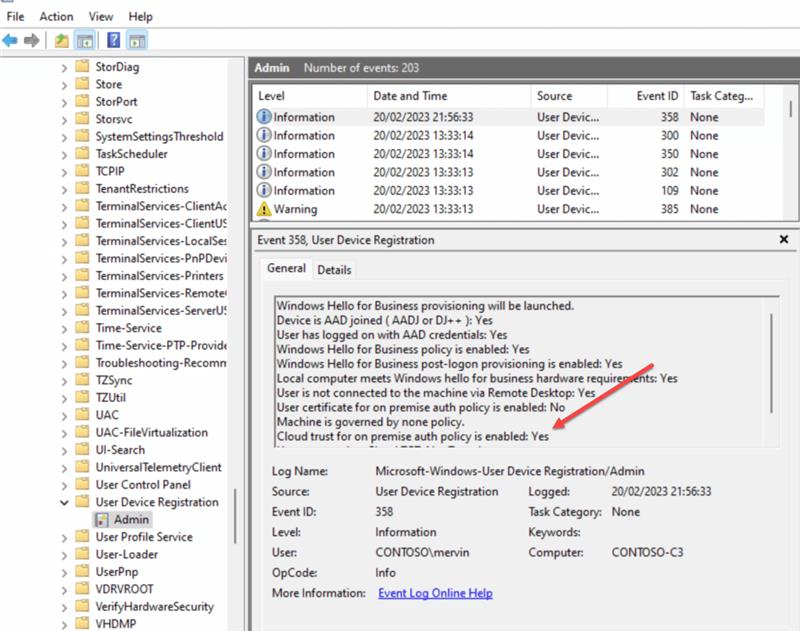
Now we are assuming that the policy has applied from Intune…

At this stage, after a synced user logs in using WHfB, verify that a partial TGT has been issued using the command:-

klist cloud\_debug



You can also be verify in the event log if the policy has been set successfully on the client.



If you don’t see the Cloud Primary TGT, then you might not have gotten a new token from Entra ID, and you can force that process by running the command line (as the user):

DSREGCMD /REFRESHPRT

Then wait a bit and issue the command:

DSREGCMD /STATUS

You should be able to see the “SSO” part has the following values set:

OnPremTgt : YES

CloudTgt : YES

GPO, you can do this below:

| **Group policy path** | **Group policy setting** | **Value** |
| --- | --- | --- |
| **Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business**  or  **User Configuration\Administrative Templates\Windows Components\Windows Hello for Business** | Use Windows Hello for Business | **Enabled** |
| **Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business** | Use cloud Kerberos trust for on-premises authentication | **Enabled** |
| **Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business** | Use a hardware security device | **Enabl** |

The Windows Hello for Business provisioning process begins immediately after a user signs in, if the prerequisite checks pass. Windows Hello for Business cloud Kerberos trust adds a prerequisite check for Microsoft Entra hybrid joined devices when cloud Kerberos trust is enabled by policy.

You can determine the status of the prerequisite check by viewing the User Device Registration admin log under Applications and Services Logs > Microsoft > Windows.

This information is also available using the dsregcmd.exe /status command in CMD

PLEASE BE AWARE

If you are migrating from another WHFB deployment, users must perform the first sign in with new credentials while having line of sight to a DC when signing in on hybrid joined devices,

GOOD DOCS TO HAVE

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/deploy/hybrid-cloud-kerberos-trust?tabs=intune#deploy-microsoft-entra-kerberos>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#cloud-kerberos-trust>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/configure#policy-conflicts-from-multiple-policy-sources>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/policy-settings>

<https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/configure#configure-windows-hello-for-business-using-microsoft-intune>