Passwordless Authentication with Windows Hello for Business

blog.netwrix.com/2022/09/08/passwordless-authentication-with-windows-hello-for-business

Jeff Warren

Passwords are everywhere — and nobody likes them. For users, they are a pain to remember and manage. For businesses, they continue to be a primary source of data breaches, both on premises and in the cloud. In fact, the 2022 Verizon DBIR reports that credential theft was involved in nearly half of all cyberattacks, including third-party breaches, phishing attacks and basic web application attacks.

Smartphones and tablets moved away from passwords long ago; today, most people sign into these devices with their face or fingerprint. But what options are available for corporate networks? Microsoft now offers Windows Hello for Business, which enables users to log in without a password. Instead, they provide two authentication two factors: something they have (their device), plus either something they know (a PIN) or something they are (biometrics). This approach is clearly far more secure than using passwords. With WHfB in place, in order to steal a user's identity, an adversary would have to obtain that user's laptop or phone. In contrast, a hacker has a number of far easier paths for stealing traditional user passwords, such as extracting the Ntds.dit file from any domain controller.

But how well does Windows Hello for Business actually work? To find out, I set up a lab in my hybrid environment and put WHfB through its paces. This article explains what I did — and the five key conclusions I was able to draw about its benefits and limitations.

Handpicked related content:

Password Policy Best Practices for Strong Security in AD

Testing Windows Hello for Business

Step 1. Set up a hybrid lab.

My goal was to be able to log into a device without a password and then access both an on-premises resource (a file share) and a cloud resource (SharePoint Online) without being prompted to enter a password. Accordingly, my lab consisted of:

- An on-premises domain controller and a file server running Windows Server 2016 and a member workstation running Windows 10, all joined to the same AD domain
- An Azure AD domain with Azure AD Premium licenses
- Azure AD Connect synchronizing users and hashes; no AD Federation Services
- Azure AD-joined devices through Intune with the Edge browser

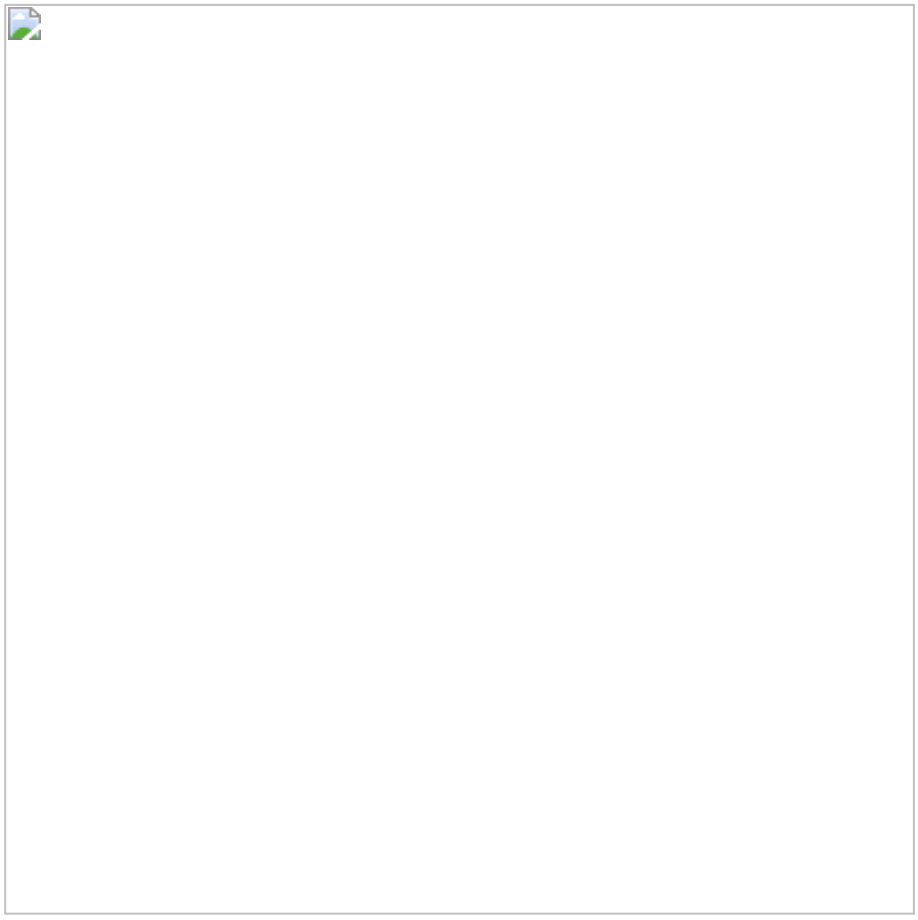
Step 2. Deploy Windows Hello for Business.

Windows Hello for Business offers multiple deployment models. The best option for you will depend on multiple factors, including whether you have an on-prem, cloud-only or hybrid environment, what operating system versions you're running, and whether you manage certificates on user devices.

I chose the Hybrid Azure AD Key Trust deployment model. (Note that this model does not support remote desktop connections, but that was not a concern for me since I use Netwrix Privilege Secure for that.)

This blog is not intended to be an in-depth guide on how to deploy Windows Hello for Business, but here are some tips for success:

- Set up your on-premises and Azure AD domains and connect them with Azure AD Connect. I enabled password-hash synchronization with single sign-on (SSO).
- Ensure Azure device registration is set up so you can auto-register your devices.
- Set up your certificates the right way on your DCs, including setting up a Certificate Revocation List (CRL).
- Configure your clients to enroll in Windows Hello for Business. This can be done through Intune if you are managing your devices there or through GPOs if you aren't.
- Users will be prompted to register their device and select a PIN:



Bonus tip: Get ready to run "dsregcmd /status /debug" at least 100 times as you work through what is and isn't working while trying to get your devices registered appropriately!

Once I finished the deployment, I could log into my device with a PIN and then access SharePoint Online and on-premises file shares without being prompted for logon.

Five thoughts on going passwordless with WHfB

Here are my top observations after using WHfB for passwordless authentication in a hybrid environment.

#1. Passwordless does not mean no more passwords.

Microsoft lists the elimination of passwords as Step 4 in their passwordless strategy, but that is not something that can be expected with WHfB in a hybrid AD environment. Still, users will have to type their passwords only once a week or once a month, rather than 10 times a day, so you might be able to require stronger passwords since your users don't have to use them often.

Ideally, you could get to the point where users don't know their passwords, but they will still be there, lurking in the shadows of your on-premises Active Directory environment.

#2. A lot depends on your needs

The value of Windows Hello for Business depends on the specifics of your environment. It worked great in my lab for connecting to Microsoft 365 and network file shares without any password prompt. If you have custom web apps and lots of cloud apps, start by getting them into Azure SSO; that's outside the scope of this research but it seems to have broad coverage and a web application proxy for custom on-prem web apps.

#3. Password attacks are still a thing.

Since WHfB does not eliminate passwords, it does not eliminate your risk from password-based attacks like password spraying. Therefore, you still need a good password security strategy for both human and non-human accounts. Netwrix Password Policy Enforcer can help by enabling you to:

- Create multiple password policies with powerful policy rules
- Block the use of leaked passwords
- Help users choose compliant passwords

#4. Lateral movement is still a thing.

Windows Hello for Business does not eliminate pass-the-hash, pass-the-ticket and other lateral movement attacks, nor does it block Golden Tickets and other privilege escalation techniques. Since those tactics take advantage of non-interactive logons, they are outside the scope of WHfB.

#5. Passwordless is a great way to go. Get there as soon as you reasonably can.

I definitely recommend evaluating WHfB if you are using Azure and already own licenses for the necessary components. It makes signing in easy, and you can improve your password security measures without user friction. In addition, users will start to find it weird when they are asked to enter their password, which will make them less likely to expose their credentials in attacks such as phishing scams.

Jeff Warren