Implementing strong user authentication with Windows Hello for Business

In Windows 10, the Windows Hello for Business (formerly known as Microsoft Passport for Work) feature can replace passwords with strong two-factor authentication that combines an enrolled device with a PIN or biometric (fingerprint or facial recognition) user input to sign in. With the Windows 10 Anniversary Update, Core Services Engineering (CSE, formerly Microsoft IT) streamlined the deployment of this feature as an enterprise credential to improve the user sign-in experience and to increase the security of accessing corporate resources.

This feature lets users authenticate to a Microsoft account, an Active Directory account, or a Microsoft Azure Active Directory (Azure AD) Premium account.

The Windows Hello for Business feature is a public key or certificate-based authentication approach that goes beyond passwords. This form of authentication relies on key pairs that can replace passwords and are resistant to breaches, thefts, and phishing.

Other benefits of this feature include:

- **It uses existing infrastructure.** We configured Windows Hello to support smart card–like scenarios by using a certificate-based deployment. Our security policies already enforced secure access to corporate resources with two-factor authentication, including smart cards and Microsoft Azure Multi-Factor Authentication. Windows Hello is currently enabled, and we anticipate an increase in usage as more biometric-capable devices become available in the market.
- **It uses a PIN.** Replace passwords with a stronger authentication. Users can now sign-in to a device using a PIN that could be backed by a trusted platform module (TPM) chip.
- **It provides easy certificate renewal.** Certificate renewals occur automatically when a user signs in with their PIN before the lifetime threshold is reached.
- **It permits single sign on.** After a user signs in with their PIN, the user has access to email, SharePoint sites, when using the latest Office 365 versions, and business applications without being asked for credentials again.
- **It is compatible with remote access.** When using a certificate-based PIN, users can connect remotely using a CSE VPN without the need for multi-factor authentication with phone verification.
- **It supports Windows Hello.** If users have compatible biometric hardware, they can set up biometrics sign-in to swipe their finger or a take a quick look at the device camera.

Our deployment environment for the Windows Hello for Business feature include:

- **Server.** Azure AD subscription and Azure AD Connect to extend on-premises directory to Azure AD
  - **For Key-based.** Windows Server 2016 Technical Preview 4 domain controller or later
  - **For Certificate based.** Active Directory Certificate Services, Network Device Enrollment Service (NDES), Microsoft Intune and/or System Center Configuration Manager version 1606 or later. The experience defined in this document is based on System Center Configuration Manager version 1610.
- **Client.** A device, preferably with an initialized and owned TPM, running Windows 10 Anniversary Update

For more information about integrating on-premises identities with Azure AD, see [Integrating your on-premises identities with Azure Active Directory](#).

**Enrollment and setup**

Windows Hello for Business user enrollment steps vary, based on our deployed scenarios. For all scenarios, users will need to use their smart card or multi-factor authentication with a verification option—such as a phone call or verification on a mobile app, in addition to their user name and password—to complete the enrollment.
The Windows Hello for Business feature supports the following enrollment scenarios:

- **On-premises Active Directory domain-joined devices.** Users sign in with their domain account, the Group Policy is applied, the device is registered with Azure Active Directory, and then the user creates a PIN.

- **Azure AD-joined devices.** Users join and or sign in to Azure AD to begin PIN provisioning.

- **Microsoft Intune-joined devices, including non-domain devices.** Users must enroll in device management (or add a work account) through Microsoft Intune. After their device is enrolled and the policies are applied, the PIN credential provisioning process begins and users receive the prompt to create their PIN.

**Requirements**

- Two-factor authentication is required for PIN creation using one of the existing methods (virtual smart card, physical smart card, or multi-factor authentication with phone verification).

- A PIN that is at least six characters long.

- A connection to the internet or Microsoft corporate network.

**Physical architecture**

Our Windows 10 domain-joined devices were already synchronized with Azure AD through Azure AD Connect, and we already had a public key infrastructure (PKI) in place. Already having PKI reduced the amount of change required in our environment to enable the Windows Hello for Business feature.

To deploy user certificates based on Windows Hello keys, we used System Center Configuration Manager version 1511 or later. Note that the PKI must be extended to include the NDES servers and a Configuration Manager/Intune NDES module; not all on-premises environments will already have this implemented.

*Figure 1. Windows Hello for Business architecture*
Server roles and services
In our implementation, the following servers and roles work together to enable Windows Hello as a corporate credential:

- Azure AD subscription with Azure Active Directory Device Registration Service to register devices with Azure Active Directory.
- Microsoft System Center Configuration Manager, Certificate Registration Point (CRP), and Microsoft Intune infrastructure. Configuration Manager is used for domain-joined devices, and Microsoft Intune is used for non-domain joined devices, like Bring Your Own Device (BYOD) and Azure AD-joined. In addition to enrolling and deploying certificates on behalf of the client, they also handle policy enforcement.
- Azure AD Federated Services (AD FS) is used for federated identities and Azure AD Application Proxy for secure remote access of web applications hosted on-premises. Azure AD Application Proxy is used for internet-facing Network Device Enrollment Service (NDES) certificate issuance.
- PKI includes NDES servers (with policy module) and Certificate Authorities (with smart card EKU template), used for the issuance, renewal, and revocation of Windows Hello for Business certificates.

Service workflow
The following is our end-to-end service workflow:

- A device collection was created in Configuration Manager. Windows 10 machines were identified, based on Configuration Manager reports, and added to the device collection. This collection excluded virtual machines.
- Our domain-joined Windows 10 machines also had the latest Configuration Manager client installed, that deployed a configuration policy for certificate enrollment, PIN-enablement and notification tasks.
- After users sign out and sign in again, or selects the pop-up notification when displayed, a PIN creation workflow runs and they have to configure their new PIN.
- A policy has already been pushed to the device by the Configuration Manager/Intune service. This policy contains the URL of the NDES server and the challenge generated by Configuration Manager/Intune.
- The device contacts the internet-facing NDES server using the URL from the NDES server and provides the challenge response.
- The NDES server (using our Configuration Manager policy module) validates the challenge with the CRP. It is important to make sure that port 443 is open between the NDES server and the CRP for this validation to happen.
- The CRP responds to the NDES server over port 443 with a “true” or “false” to challenge verification.
- If the challenge response is “true,” the NDES server communicates with the certificate authority (CA) to get a certificate for the device. Appropriate ports need to be open between the NDES server and the CA for this to happen.
- The NDES server delivers the certificate to the computer.

Setting policies
CSE used Configuration Manager to push out policy-based settings to configure our Windows 10 domain-joined devices to provision Windows Hello user credentials when users sign in to Windows. Non-domain joined machines receive their policies from Intune. We also used these settings to define the complexity and length of the PIN that our users generate at registration and to control whether Windows Hello was enabled.

We had the option to configure whether we would accept certificate-based Windows Hello for Business with PIN as a software-backed credential. We chose to enable Windows Hello for Business with a hardware-required option, which means that keys are generated on TPM 1.2 or TPM 2.0.

To use the “Windows Hello/Windows Hello for Business” certificate-based sign-in, configure the certificate profile (Assets & Compliance > Compliance Settings > Company Resource Access > Certificate Profiles). Select a template that has smart card sign-in extended key usage. Note that this certificate template should be configured in
the SCEP Enrollment page to use the Windows Hello for Business and Certificate Properties page to set the minimum key size set to 2048.

To set up the desired policy, we also need to create a new Windows Hello for Business profile (Assets & Compliance > Compliance Settings > Company Resource Access > Windows Hello for Business profiles) and specify required options:

- Configure Hello for Business (enabled/disabled)
- Use a Trusted Platform Module (TPM) (preferred/required/not configured)
- Authentication method (certificate-based, key-based/not configured)
- Configure general PIN requirements—min/max length, use of uppercase/lowercase/special characters and digits (allow/required/not allowed/not configured), expiration, prevent reuse of previous PINs
- Enable biometric gestures/enhanced anti-spoofing/use phone sign in (yes/no/not configured)

**User enrollment experience**

Configuration Manager creates the scheduled task to domain-joined computers that are running Windows 10 Anniversary Update. The certificate enrollment and the Windows Hello for Business policies are visible from the Configuration Manager client on the Configurations tab (in Control Panel, search for "Configuration Manager").

**Scheduled task and notification for PIN provisioning**

The user receives the notification for PIN enablement and the task for certificate evaluation is triggered.

- Notification and PIN enablement. When all prerequisites are met, a toast notification informs users that a new type of credential is available with a PIN configuration message. When the user clicks the notification, PIN provisioning starts right from the desktop—the user doesn’t have to sign out and sign in.
- This scheduled task invokes Configuration Manager to trigger a certificate evaluation if there is no certificate installed.

**Client signs out and signs in (and unlocks) the device**

The user unlocks their device, and the certificate enrollment process is triggered.

**Certificate enrollment process**

After a PIN is successfully created, the scheduled task runs (triggered by Event ID 300, which is "Key registration was successful.") It checks for an existing certificate. If the user doesn’t have one, the task sends the requests for new challenge.

At this point, Windows 10 calls on the specified Configuration Manager server and requests a challenge with an expiration time. The challenge is encrypted by Configuration Manager server using the public key of the management point. The Configuration Manager client randomizes the NDES list and calls into the mobile device management (MDM) stack. If the PIN is cached, the certificate enrollment is triggered. If the PIN is not cached, a scheduled task is created under USERSID\EnterpriseMgmt and is triggered when the device is unlocked.

**Certificate renewal behavior**

We have configured PIN credential certificates to have a lifetime of 90 days from when they are issued. Renewals will happen approximately 30 days before they expire. When a user next enters their Windows Hello for Business PIN within the 30 days prior to its expiration, a new certificate will be automatically provisioned on their device.

A certificate policy in Configuration Manager gets triggered every 24 hours—or when the user unlocks the machine—that checks for certificate lifetime percentage that it compares against the renewal threshold. If it’s beyond the previously mentioned threshold, we start a new-certificate enrollment.

**Microsoft Intune specifics**

The Open Mobile Alliance Device Management client talks to the Microsoft Intune mobile device management server using SyncML. Policies are routed, and then the user receives the Simple Certificate Enrollment Protocol profile, as
configured in our hybrid environment, using Configuration Manager and deployed through Microsoft Intune. Within 10 minutes, the user should receive a certificate. If that fails, the user needs to manually sync.

Service management
We manage identity as a service at Microsoft and are responsible for deciding when to bring in new types of credentials and when to phase out others. When we were considering adding the Windows Hello for Business feature, we had to figure out how to introduce the new credential to our users, and to explain to them why they should use it. Windows Hello for Business is not replacing passwords at Microsoft, but it does allow our users to securely sign in to their device and provides them seamless access to both on-premises and cloud resources.

Driving adoption
Before the release of Windows 10 November update at Microsoft, it was rolled out to approximately 15,000 early adopters. These users validated the new credential functionality and user scenarios, and they provided valuable feedback that we shared with the product development team.

After the internal release of Windows 10 November update, we made it a requirement that users install the update on all domain-joined Windows 10 computers. Users were notified that they had three weeks in which they could voluntarily install the update and begin using the new credentials. We enforced this by using a version-check policy in Configuration Manager that installed the update in the background and prompted the user to create their Windows Hello for Business PIN. Of the 189,000 compatible user devices at Microsoft, so far 111,000 of the devices are enrolled in Windows Hello for Business.

One of the main challenges for adoption is that the users have multiple options, including old credentials, like virtual smart cards, they have been using for the last few years. We are addressing this in two ways—targeted user awareness and training on the benefits of using a PIN—this increased awareness and training is resulting in the increased use of a PIN as the sign-in method.

Measuring service health
We are in the process of creating end-to-end telemetry to measure the service health of Windows Hello for Business. For now, we are monitoring the performance and status of all of our servers. We are also expanding the service, so adoption and usage numbers are very important metrics that demonstrate the success of our service. We also track the number and types of help desk issues that we see.

We use custom reports created from certificate servers and custom telemetry service metrics to collect prerequisites, and key and certificate issuance times for troubleshooting. Detailed reports about other aspects of the service can also be generated from Microsoft Intune and Configuration Manager.

We configure a user’s certificate to expire, and certificate renewals are issued with the same key. When necessary, the certificates can be revoked directly though Microsoft Intune or Configuration Manager, which provides easier administration.

Lessons learned

TPM issues
OEM BIOS initialization instructions and TPM lockout policies are OEM-specific. We performed steps to identify and document the potential issues for each hardware provider. We also communicated to our users that clearing a TPM will cause their private key not to work in Windows Hello for Business.

Preventing PIN enrollment problems
Some of the common issues we saw with users creating their PINs could have been avoided with better communication. These issues include users not understanding the prerequisites, and not signing in and then signing
out with their user name and password. To help avoid this issue, we created a productivity guide to walk users through the steps.

**Limiting certificate issuance traffic**

NDES is a single-threaded app. To effectively funnel high volumes of traffic from clients enabling their PINs on busy days, we have limited the concurrent connections to 300 per NDES server for optimum performance. When the number of connections exceeds the limit, users receive a "service is busy" error, instead of performing automatic retries that cause performance issues.

**Monitoring end-to-end service health**

Windows Hello for Business relies on several underlying services: Azure AD, Configuration Manager, Microsoft Intune, NDES, and CA. All of these services need to be healthy and available. Certificate issuance delays can be hard to troubleshoot, but monitoring the health and performance of the supporting services can help.
For more information

Microsoft IT Showcase
microsoft.com/itshowcase

Microsoft Passport guide
Enable Microsoft Passport for Work in the organization
Implement Microsoft Passport in your organization

Active Directory and Azure Active Directory
Integrating your on-premises identities with Azure Active Directory
Connect domain-joined devices to Azure AD for Windows 10 experiences
Azure AD Join on Windows 10 devices

Management
Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)
PKI Certificate Requirements for Configuration Manager
PART 2 - SCEP certificate enrolling using ConfigMgr 2012, CRP, NDES and Windows Intune
Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority

Certificate profile management
Planning for Certificate Template Permissions for Certificate Profiles in Configuration Manager
Certificate Profiles in Configuration Manager
Configuring Certificate Profiles in Configuration Manager
How to Create Certificate Profiles in Configuration Manager

Policy Management
How to Configure the Policy Module to Use a New Client Certificate in Configuration Manager
Using a Policy Module with the Network Device Enrollment Service

© 2016 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.