Enabling remote access with Windows Hello for Business in Windows 10

With the Windows 10 November update, Microsoft IT enabled Windows Hello as an enterprise credential for our users. Our security policies already enforced secure remote sign in using multi-factor authentication, with smart card or phone verification as the second factor, to connect to corporate resources using VPN (virtual private network).

On any given weekday at Microsoft, there are roughly 35,000 to 45,000 users connected to the corporate network using VPN. There are 25,000 to 35,000 users connected on the weekends and during non-peak hours. We needed to easily incorporate Windows Hello for Business and enable:

- A single VPN solution to support our 180,000+ global users.
- A preferred credential backed by certificate-based authentication, providing a seamless sign in experience and connection to resources from outside the corporate network.
- The ability to “just work” with our existing VPN solution as machines upgrade to Windows 10 November update.
- Compliance with corporate policies using our preferred device management solution.

Windows Hello for Business is a private/public key or certificate-based authentication approach for organizations and consumers that goes beyond passwords. This form of authentication relies on key pair credentials that can replace passwords and are resistant to breaches, thefts, and phishing. With Windows Hello, biometric authentication and recognition is easy with a face or fingerprint. PCs with fingerprint readers are ready to use Windows Hello now, and more devices that can recognize faces are coming soon.

Microsoft IT integrated Windows Hello for Business with our existing VPN infrastructure and enabled secure remote access with certificate-backed credentials. In addition, Windows Hello provides a unified VPN connection experience for all modern devices, with fewer user touch points. It also sets the foundation for ongoing enforcement of corporate policies and enables AutoConnect for VPN.

For more information about how we enabled Windows Hello for Business as a credential, read [Implementing strong user authentication with Windows Hello for Business](#).

Supported authentication methods

We have a single VPN solution in place for use with all of the supported client operating systems in our environment. We support several strong authentication methods specific to the operating system that is being used. Our preferred credential is backed by certificate-based authentication (public key infrastructure, or PKI) and multi-factor authentication solutions.

Windows 10 November update with Windows Hello for Business

Windows 10 users that have installed the Windows 10 November update can use VPN with Windows Hello for Business. Windows Hello credentials address many of the inherent problems with passwords. Passwords can be difficult to remember, can be reused on multiple sites, and can sometimes be easy to guess. Server breaches can expose symmetric network credentials, or users can inadvertently divulge their passwords to phishing attacks. Because PINs are tied to the device and are stored locally, they are more secure than a password. The PIN is backed by a Trusted Platform Module chip, a requirement in our environment, and includes multiple physical security mechanisms to make it tamper resistant.
Windows 10 with multi-factor authentication

Windows 10 users that have installed the November update and have not set up Windows Hello for Business, or that are running an earlier version of Windows 10 can use VPN with multi-factor authentication with phone verification.

Multi-factor authentication with phone verification as a second form of strong authentication helped expand the types of devices that can access the corporate network through VPN. While cloud-based services can be accessed any time and from any device using federated identities and multi-factor authentication, VPN at Microsoft was limited to mostly domain-joined machines, which we manage using Microsoft System Center Configuration Manager. Before multi-factor authentication with phone verification and software-based certificates, VPN was cumbersome for users on non-domain joined machines. We can install the same policies that we use in Configuration Manager to provide client certificates to non-domain-joined devices that are managed through Microsoft Intune. Also note that multi-factor authentication with phone verification requires users to either join a Microsoft domain or enroll in Microsoft Intune to enable device management.

Remote access for earlier versions of Windows

Users that are running Windows 8.1, Windows 8, or Windows 7 and have installed the Microsoft IT VPN client can authenticate with a physical or virtual smart card or register and configure VPN to use multi-factor authentication with phone verification when connecting. We are still enforcing the Network Access Protection system health check and quarantine for these client machines.

Windows Mobile

On Windows Phone 8/8.1 and Windows Mobile 10, VPN profiles are deployed via Microsoft Intune. The VPN profiles are set to connect automatically using the Always On functionality and are configured to route only corporate data through the tunnel (using split tunneling). In Windows 10 Mobile, there is greater flexibility for secure authentication with new features such as Windows Hello for Business, and additional security features such as Conditional Access and Enterprise Data Protection.

VPN client connection manager application

The Microsoft IT VPN client, based on Connection Manager is required on all devices to connect using remote access. It is included as part of the corporate operating system deployment image, or is available for our users to download from the Microsoft IT remote access SharePoint portal. This allows a single client to be available for all devices and machines, which can connect remotely and access corporate resources.

Securely accessing corporate on managed devices

We use Configuration Manager to manage all of our domain-joined computers, and Microsoft Intune provides enterprise mobility management support for non-domain-joined computers and mobile devices that have enrolled in the service. In our hybrid configuration, VPN policies, including certificate issuance that we create in Configuration Manager for Windows 10 devices, are loaded into Microsoft Intune and applied to enrolled devices.

For more information about how we use Microsoft Intune as part of our mobile device management strategy, read Mobile device management at Microsoft.

Remote access infrastructure

The infrastructure for providing remote access to all of the supported operating systems at Microsoft is shared, with the exception of a few key pieces that were included to issue certificates and manage the non-domain-joined systems. We chose to make our certificates for Windows Hello for Business work the same as our smart card certificates so that we would have a seamless integration with our existing, geographically distributed Windows Server infrastructure.

- From the client side, we did not have to make any changes to the connection manager application that is used to connect to our VPN.
- From the server side, we only had to configure Windows Hello for Business as an accepted authentication credential on the Network Policy Server (NPS).
This illustration shows our remote access infrastructure.

Figure 1. Microsoft remote access

Certificate and device enrollment
Simple Certificate Enrollment Protocol (SCEP) and Network Device Enrollment Service (NDES) are the mechanisms we currently use to deploy certificates to our mobile devices via Microsoft Intune and Configuration Manager. NDES allows software on routers and other network devices running without domain credentials to obtain certificates based on the SCEP.

NDES performs the following functions:
1. Generates and provides one-time enrollment passwords to administrators.
2. Submits enrollment requests to the certificate authority (CA).
3. Retrieves enrolled certificates from the CA and forwards them to the network device.

For more information about deploying NDES, including best practices, see Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS). Also, see Securing and Hardening Network Device Enrollment Service for Microsoft Intune and System Center Configuration Manager.

RADIUS server
Remote Authentication Dial-In User Service (RADIUS) servers, or Network Policy Server, perform authentication, authorization, and accounting for RADIUS clients. A RADIUS client can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy. When NPS is used as a RADIUS server, it provides authentication, authorization, and accounting services for network access servers.

For more information, see Network Policy and Access Services Overview.
To enable Windows Hello for Business, the NPS server was configured to include a new condition in our network policy as shown in figure 2 EAP Types. Appropriate policies were set to ensure the new condition was processed before the auto-denial policies. The condition, in this case, was to accept a specific Windows Hello certificate.

![Network Policy Properties dialog box](image)

**Figure 2. Network Policy Properties dialog box**

**RRAS**

We use Routing and Remote Access Service (RRAS) to deploy VPN, dial-up remote access services, multiprotocol LAN-to-LAN, LAN-to-WAN, and network address translation (NAT) routing services.

For more information about deploying VPN using RRAS, see [Routing and Remote Access Service (RRAS)](microsoft.com/itshowcase).

**VPN tunnel types**

Our VPN solution supports the following tunnel types:

- **IKEv2**: This tunnel type is preferred and is set as the default. IKEv2 is more resilient to changing network connectivity, making it a good choice for mobile users who move between access points and even switch between wired and wireless connections.

- **SSTP**: The default tunnel fail-over strategy for Microsoft IT VPN. Secure Socket Tunneling Protocol (SSTP) provides firewall traversal capability. This means mobile users who are trying to access corporate network resources from behind customer firewalls, airport hotspots, hotels, and other public Wi-Fi hotspots can successfully use VPN.
Split tunneling
Split tunneling allows only the traffic destined for the Microsoft corporate network to be routed through the VPN tunnel, and all Internet traffic goes directly through the Internet without traversing the VPN tunnel. In Microsoft IT VPN, split tunneling is enabled by default.

Applying policies
We use Group Policy in Windows Server Active Directory to configure our Windows 10 domain-joined devices to provision Windows Hello credentials when a user signs in. We also use Group Policy Objects to define the complexity and length of the PIN that our users generate and to control Windows Hello use. For non-domain joined and mobile devices, the same policies are managed and applied by Microsoft Intune.

Policy enforcement
Configuration Manager and Intune handle policy enforcement as well as certificate enrollment and deployment on behalf of the client.

Providing exceptions
We have a process to provide time-bound exceptions for users if they are unable to connect. We give users time to troubleshoot and resolve their connection issue by giving them access for 24 hours—or 7 days in rare instances. Those exceptions are routed through the helpdesk and managed with certificates.

Compliance checks
Remote computers and devices that use VPN to connect to the corporate network have to be checked for compliance. For Windows 8.1 and earlier, we still use a separate compliance check that would quarantine a system, limiting its access to corporate resources while it performed a system health check and installed required updates.

We require certificates from Configuration Manager on Windows 10 domain-joined computers, or from Microsoft Intune for computers that are enrolled to be managed. That certificate implies that because the computer is managed, it should be able to pass a system health check. If a computer does not have all of the system and security requirements installed, Configuration Manager or Intune will install them—or the certificate that is needed to connect will not be issued.

Managing the service
We rolled out Windows 10 November update to a group of about 15,000 early adopters a few months before release. Early adopters validated the new credential functionality and used remote access connection scenarios to provide valuable feedback that we could take back to the product development team. Using early adopters helped validate and improve features and functionality, influenced how we prepared for the broader deployment across Microsoft, and helped us prepare support channels for the types of issues that users might experience.

Encouraging adoption
After enterprise release of Windows 10 November update, we required users to install the update on all domain-joined Windows 10 computers and to use the new connection methods when they connect using VPN. Users were notified that they had three weeks to 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 sign-in.

Most of our users on corporate-provisioned devices are running Windows 10 with November update. Our remote access infrastructure supports next-generation credentials as well as the multi-factor authentication methods used by earlier operating system versions and non-domain-joined running Windows 10.
Measuring service health
We measure connection rates as well as response times to monitor the service and report on the number of unique users that connect every month, the number of daily users, and the duration of connections. By measuring connection events, we know who has connected and who has failed to connect.

What’s next
Upcoming releases include new features that will improve both the service and the user experience.

- **Conditional access.** Conditional access is scheduled to be released in an upcoming update for Windows 10. Rather than just relying on the managed device certificate for a “pass” or “fail” for VPN connection, conditional access places machines in a quarantined state while checking for the latest required security updates and antivirus definitions to help ensure that the system is not introducing risk.

- **Auto-connect VPN client.** To enable mobile productivity and improve the user experience, users will have the option to stay connected to VPN without additional interaction after they sign in.

- **VPN profiles.** VPN profiles from Microsoft Intune and/or Configuration Manager will replace the Connection Manager client that we currently use. The profiles will automatically configure connection and authentication types.

Benefits
We saw benefits during the rollout of Windows Hello for Business when our users started using the new credential to connect. Specific benefits include:

- **Integration with existing infrastructure.** Our remote access infrastructure was set up to use smart cards and virtual smart card credentials and we already had a PKI infrastructure, which made it easy to enable Windows Hello for Business. The Network Policy Server updates enabled us to use the new credential for remote access as well.

- **Minimize user touch points.** When connecting via VPN, the user can input their PIN to gain a secure connection, with a consistent and simple connection experience.

- **No bandwidth or administration overhead.** Adding a new credential type did not affect our existing connectivity or bandwidth. Using existing infrastructure has also enabled us to extend our service monitoring capabilities to include Windows Hello for Business and provide a unified view of our service health.

- **Making IT future ready.** Our corporate policies require that devices must be compliant and enrolled in a device management service. With Windows 10, we can enforce ongoing compliance without additional scripts to connect remotely.

For more information
Microsoft IT Showcase
microsoft.com/ITShowcase

© 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.