New Windows 10 features enhance security and productivity at Microsoft

Microsoft IT enabled Azure Active Directory Join and other Windows 10 features that enhance security and productivity, including Windows Hello for Business, Credential Guard, and Enterprise State Roaming.

Enhanced security
The Windows 10 November update offers two new features for improving security. A combination of cryptographic keys that are uniquely tied to a user and device, and facial or fingerprint recognition, provide a more convenient way to sign in with strong authentication.

Windows Hello for Business
The Windows Hello for Business (formerly known as Microsoft Passport for Work) feature for Windows 10 helps Microsoft employees and other corporate network users to securely sign in to their PCs. Windows Hello for Business simplifies signing in to on-premises and cloud resources without using a password. Using Windows Hello, our network users can sign in to their Windows 10 devices with just a look or a touch if the device is equipped with compatible hardware.

Windows Hello for Business creates a certificate-based credential on a device, which is unlocked by a PIN or biometric (fingerprint or facial recognition). This is more secure than a password, because the PIN is tied to the device, and only the user knows the PIN. With Windows Hello for Business, we have a convenient and secure authentication method. Other benefits include:

- **Easy certificate renewal.** Microsoft corporate network users receive a prompt to verify their PIN when their certificate needs renewal. The certificate is renewed in the background rather than the cumbersome certificate renewal process that existed before.
- **Single sign-on.** Windows Hello for Business reduces the number of requests for credentials and gives users a single sign-on experience. Microsoft users saw a significant decrease in the number of times they had to sign in during their daily work.
- **Simplified remote access.** When Microsoft network users use their PIN, they can connect remotely using the Microsoft IT VPN client without the need for a smart card.
- **Biometric sign in.** With compatible biometric hardware, Microsoft corporate network users can set up Windows Hello and sign in with only a swipe of their finger or a quick look at the device’s camera. This enterprise-grade security meets the requirements of Microsoft IT.

Before Microsoft IT deployed Windows Hello for Business, users who accessed the corporate network remotely had a user name and password to sign in. Every time they needed access to resources such as Microsoft SharePoint or Visual Studio, users had to provide a smart card or username and password again.

Credential Guard
Credential threat attacks are one of the biggest security threats to an organization. In 2014, a number of major companies were victims of an attacker gaining unauthorized access to user credentials. According to the Verizon 2015 Data Breach Investigations Report, participating partners confirmed over 2,000 data breaches worldwide. This report estimated the average loss to an organization, for a breach of 1,000 records, was between $52,000 and $87,000.

Credential Guard increases the security of derived domain credentials by using platform security features, including Secure Boot and virtualization. Securing derived domain credentials with virtualization-based security blocks the credential theft attack techniques and tools used in many targeted attacks. Credential Guard uses Virtual Secure Mode to store hashes and tokens in a way that makes unauthorized access difficult. At Microsoft, we added
Credential Guard to take advantage of this additional security protection and deployed it using a phased approach. After testing it in our hardware lab to ensure compatibility, the feature was enabled globally using group policy. There were no related help desk calls, validating a seamless adoption. More details about Credential Guard are described in Protect derived domain credentials with Credential Guard.

We enjoy the simple manageability of Credential Guard using group policy, but you can also use Windows PowerShell or Windows Management Instrumentation. Credential Guard has a very transparent installation and deployment is simple: go to Group Policy, enable Credential Guard, and push to the domains. Credential Guard is enabled the next time a corporate network user restarts their machine. We continue to monitor the state of Credential Guard with System Center Configuration Manager, visualized in our Power BI dashboard and are on track for 100 percent adoption for all compatible machines.

Improved productivity

In addition to protecting the enterprise, Windows 10 helps Microsoft network users work the way that they want to work. Now you can achieve greater productivity in your organization. When you prepared for Windows 7 and Internet Explorer 11, you already did most of the heavy lifting for your migration to Windows 10 and these great features.

Azure Active Directory Join

We have enabled Azure Active Directory (AD) Join for Windows 10 because it brings significant flexibility to our users and offers benefits such as single sign-on to our users.

Our corporate network users are able to automatically join Azure AD during the initial startup. Azure AD Join will register their device in our directory and enroll it in the Mobile Device Management (MDM) solution and Microsoft Intune, which is part of the Enterprise Mobility Suite. In addition to PCs and Windows devices, any mobile device can be joined, allowing users to work on the device of their choice. With the combination of Azure AD Join and Microsoft Intune, we have more control over corporate data on the device, and user data is no longer controlled by us. This has reduced resistance by users and encouraged wider adoption.

As an example of the benefits of Windows 10 integration with Azure AD Join, we rolled out virtual private network (VPN) settings. For non-domain-joined PCs to access corporate resources, the process is greatly simplified. With Windows 10 and Azure AD Join, the PC is enrolled automatically with Microsoft Intune in a matter of seconds and the user is presented with a number of configurations, including VPN settings. Previously, users had to install a VPN client from IT Manager, and then use a smart card or other device to do strong authentication and connect to VPN. Now, with Azure AD Join, users automatically get a VPN connection along with Windows Hello for Business and security settings.

Data geolocation and privacy concerns are addressed through points of presence in data centers around the world using MDM and Microsoft Intune. An added benefit of enabling Azure AD Join is the ability to use Enterprise State Roaming.

Enterprise State Roaming

With the Windows 10 November update on Azure AD Premium, we wanted to take advantage of the Enterprise State Roaming (ESR) feature, which synchronizes our users’ corporate Windows and application data settings to Microsoft Azure. With this feature, their settings roam across all Windows devices, reducing the time needed for configuring a new device. And it provides a separation between personal and corporate user settings, protecting user privacy. In addition, Azure Rights Management Services (RMS) encrypts settings on the Windows 10 device and stays encrypted in the cloud providing added security.

We worked closely with the product group during deployment. The initial rollout was limited to a self-host pilot, which was expanded later with a group policy rollout. This early interaction with the product group provided helpful feedback and uncovered a number of issues that were rectified before general release.
ESR is deployed with roaming turned on as the default, and users can turn roaming on or off. Every setting is not automatically set as default roaming, and these are easily configured from Settings > Accounts > Sync as shown in Figure 1.

The Windows settings categories that synchronize include:

- Theme (desktop theme, taskbar settings, etc.)
- Internet Explorer settings (recently opened tabs, favorites, etc.)
- Passwords (Internet passwords, Wi-Fi profiles, etc.)
- Language preferences (keyboard layouts, system language, date and time, etc.)
- Ease of access (high contrast theme, narrator, magnifier, etc.)
- Other Windows settings (notification settings, spelling dictionary, etc.)

Figure 1. Settings for Enterprise State Roaming.

Deployment is a simple matter of enabling the feature at the tenant admin level. From then on, everything is backed up automatically. Management and monitoring services are available in the Azure AD portal with menu-based settings. Applications that have their own sync solutions are not affected.

Employee productivity increases because they don’t have to reset settings and there is less IT administration and support, with seamless manageability. It’s a win-win!

For more information

Microsoft IT Showcase
microsoft.com/itsshowcase

© 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.