EXECUTIVE BRIEF

Swift and Seamless Sign-In with Microsoft Hello & HID Global

Windows Hello for Business is a new credential for Microsoft's Windows 10, designed to help increase security when accessing corporate resources. This feature offers a streamlined user sign-in experience—it replaces passwords with strong two-factor authentication by combining an enrolled device with a PIN or biometric user input for sign-in. Windows Hello is easy to implement within Microsoft's existing identity infrastructure and is compatible for use within the Microsoft remote access solution. Windows Hello for Business conveniently lets users authenticate to an Active Directory or Azure Active Directory account.

Solving the Problem with Passwords

Data leaks and hacks are more frequent and damaging than ever, putting an increased emphasis on strong authentication. The weak points are often passwords—even the most complex password requirements can result in vulnerable systems.

Windows Hello addresses the following problems with passwords:

- Strong passwords can be difficult to remember and can be compromised since users often reuse the same password for multiple sites.
- Server breaches can expose symmetric network credentials (passwords).
- Passwords are subject to replay attacks.
- Users can inadvertently expose their passwords due to phishing attacks.

Windows Hello provides reliable, fully integrated biometric authentication based on facial recognition or fingerprint matching and uses a combination of special infrared (IR) cameras and software to increase accuracy and guard against spoofing. Major hardware vendors are shipping devices that have integrated Windows Hello-compatible cameras. Fingerprint reader hardware can be used as installed or added to devices that don't currently have it. On devices that support Windows Hello, an easy biometric gesture like facial recognition unlocks users' credentials.

Windows Hello and Fingerprint Recognition

Fingerprint readers have been available for Windows computers for years, but the current generation of sensors is significantly more reliable and less error prone. Most existing fingerprint readers, whether external or integrated into laptops or USB keyboards, work with Windows 10.

Windows stores biometric data that is used to implement Windows Hello securely on the local device only. The biometric data doesn't roam and is never sent to external devices or servers. Because Windows Hello only stores biometric identification data on the device, there's no single collection point an attacker can compromise to steal that data.

HID Global supports Windows Hello for Business with the EikonTouch TC510 and EikonTouch TC710 capacitive fingerprint USB readers.

The EikonTouch TC510 USB capacitive fingerprint reader provides quick and reliable biometric authentication.

Key Features

- Steelcoat® for durability (> 4 million touches)
- Small form factor
- Works well with dry, moist or rough fingerprints
- High-quality fingerprint image
- Multiple cable lengths and connectors
- Match-on-device, OTP options

EXECUTIVE BRIEF

The EikonTouch TC710 capacitive fingerprint reader provides strong, fast biometric authentication—it's also the only touch silicon FIPS 201 PIV certified single fingerprint reader on the market.

Key Features

- FIPS 201 PIV certified
- Small form factor
- Works well with dry, moist or rough fingerprints
- Highly durable (> 2 milion touches)
- High-quality fingerprint image
- Multiple cable lengths and connectors

The EikonTouch TC710 and TC510 both utilize patented HID Global technology to capture a wide range of fingerprints and fine print details with superior image quality for a broad range of use cases.

HID Global fingerprint readers are certified by Microsoft and support the Windows Biometric Framework (WBF), which comprises of a set of services and interfaces supporting the consistent development and management of biometric devices. The WBF also enhances the reliability and compatibility with biometric services and drivers and allows device developers to interact with the client side of the framework that supports each biometric solution.

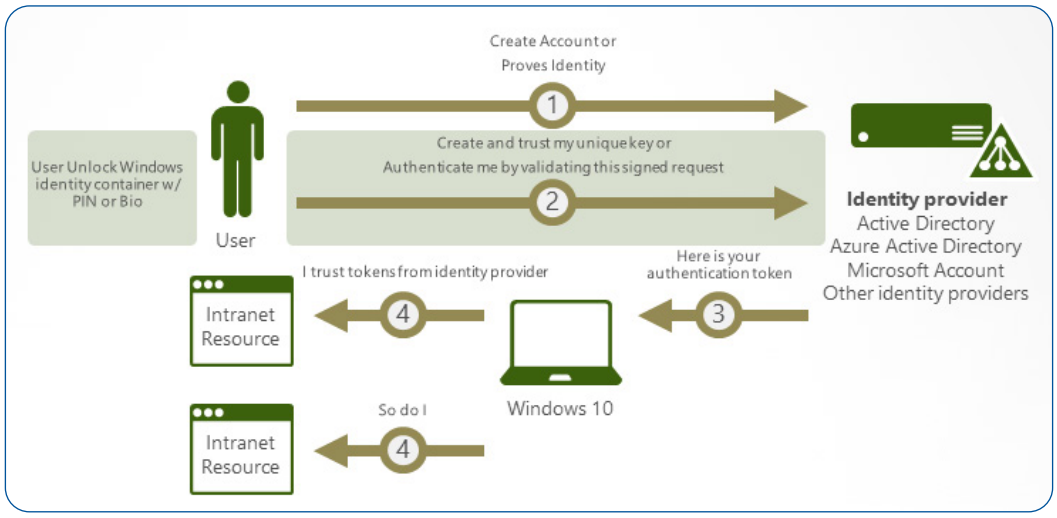
The Windows Biometric Service is an essential part of the WBF. The Windows Biometric Service enables client applications to capture, compare, manipulate and store biometric data without direct access to the biometric hardware or samples. It runs in the security context of the local system and is hosted in a privileged SVCHOST process.

Windows Hello vs Windows Hello for Business

With Windows Hello, individuals can create a PIN or biometric gesture unique to a personal device for convenient sign-in. This configuration is referred to as Windows Hello convenience PIN and it is not backed by asymmetric (public/private key) or certificate-based authentication. It can also use a simple password hash depending on an individual's account type.

Windows Hello for Business, however, is configured by Group Policy or mobile device management (MDM) policy, and always uses key-based or certificate-based authentication. This makes it much more secure than Windows Hello convenience PIN.

Windows Hello and Windows Hello for Business work with HID Global fingerprint readers to provide significantly stronger data access protection than passwords alone. Importantly, this increased authentication security is also easy to implement. For information on how to set up your Windows Hello system with EikonTouch readers, contact us at https://www.hidglobal.com/products/readers/single-finger-readers.



2021-11-12-eat-sign-in-microsoft-hello-eb-en PLT-04759