digicert®

DigiCert® Enterprise PKI Platforms: Support for Windows Hello for Business

Going Passwordless?

Passwordless authentication is gaining attention as a way to improve security at the point of access while simplifying the user sign-in experience. Even strong passwords are subject to replay and phishing attacks, may be exposed by server breaches, or can be difficult for users to remember. And, as companies turn to Zero Trust security models that require verification of each access request, access security becomes an increasingly important IT concern for protecting against attacks and enabling a corporate workforce. With passwordless authentication, end users no longer need to create or remember passwords and employ more secure methods for verifying identity.

> **"89%**
>
> **of web application breaches involved some sort of credential abuse (either use of stolen credentials or brute force)."**
>
> --Verizon 2021 Data Breach Investigation Report

Windows Hello for Business: The Certificate Trust Model

Windows Hello for Business (WHfB) is a passwordless authentication solution from Microsoft to verify sign-in/login, using strong authentication (multi-factor) on PCs and mobile devices using biometric or PIN identity credentials.

The certificate trust model for WHfB uses digital certificates underpinned by a Public Key Infrastructure (PKI) to authenticate to Active Directory (AD) with certificates issued by a Certificate Authority (CA).

The key trust model authenticates to AD with a key and requires self-signed certificates.

Of the two main trust models employed by WHfB, key trust and certificate trust, certificate trust may be preferred by companies concerned with:

- Use Cases: With the certificate trust model, a WHfB certificate can be used in the same way as smart card certificates with Windows logon.
- Identity and access technology: Enterprises that already use PKI for issuing and managing end user certificates can also leverage their PKI in combination with Windows Hello for Business.

digicert®

DigiCert® Enterprise PKI Platforms & Windows Hello For Business

DigiCert enterprise PKI platforms provide support for the WHfB certificate trust model, delivering the use cases, and convenience that customers require with passwordless authentication initiatives, which:

- **Simplifies** WHfB certificate administration with pre-configured certificate templates and corresponding enrollment methods.
- **Accelerates** on-boarding with automated workflows and zero-touch provisioning of client-authenticated certificates required by WHfB to Windows domain-joined workstations.
- **Delivers** the convenience of managing WHfB digital certificates with the same platform used for managing other enterprise use-cases.

Support for WHfB is one of the many features in DigiCert enterprise PKI platforms that provide organizations with a simplified digital certificate provisioning and administration experience based on automated workflows, preconfigured templates, multiple enrollment methods, and third-party integration capabilities.

For administrators of Windows Hello for Business, this means:

PKI Platform Features	Benefits
Predefined certificate templates for WHfB	Facilitates rapid on-boarding of users and devices via DigiCert Auto-Enrollment Server (client-less) with predefined certificate templates for WHfB Domain Controller, Enrollment Agent and User Authentication
Zero-touch certificate lifecycle management	Increases user productivity and security with automated certificate renewal, re-issuance, expiration and re-provisioning capabilities
Strong key protection and policy enforcement	Provides options for key generation and protection using Trusted Platform Module (TPM), and policy enforcement to use TPM
Seamless integration with WHfB third-party systems and applications	Eases integration by leveraging support for REST API, SCEP and EST as well as SAML for federated and distributed services
Centralized administration & management for WHfB and other digital certificates	Enables visibility and control of enterprise-wide certificate landscape with complete certificate lifecycle management, tracking, audit logs and reporting on one central platform
Rapid platform deployment	Drives rapid deployment and online CA creation for both software and HSM-based CAs
Highly flexible and scalable PKI platform	Supports multiple PKI platform deployment options including cloud, on-premises, and hybrid models with proven scalability
Multiple language support	Supports multiple languages on all web interfaces, administration consoles, and end-user enrollment web pages.

Technical Requirements

DigiCert® enterprise PKI platforms:	• PKI Platform 8 with Autoenrollment Server on domain-joined Windows Server* or • Enterprise PKI Manager with Autoenrollment Server on domain-joined Windows Server (availability Q1 2022)
Windows Server Operating Systems (OS):	2019, 2016 or 2012
Directory Service:	Windows Active Directory (AD)*, Azure AD
Single Sign-on Solution:	Microsoft Active Directory Federation Services (ADFS)
Identity Data Synchronization Solution:	Azure AD Connect
Client Machine OS:	Windows 10

*Components must be running on the same supported Windows Server OS

For more information or to request a free trial, call 1.801.770.1736,
email **pki_info@digicert.com**, or visit **digicert.com/pki/enterprise-pki-manager**