

Plataformas DigiCert® Enterprise PKI: suporte para Windows Hello for Business

Quer adotar a autenticação passwordless?

A autenticação passwordless (sem senha) está atraindo atenção como uma forma de melhorar a segurança no ponto de acesso e, ao mesmo tempo, simplificar a experiência de login do usuário. Mesmo senhas fortes estão sujeitas a ataques de repetição e phishing e podem ser expostas por violações de servidor ou esquecidas pelos usuários. Além disso, conforme as empresas buscam modelos de segurança Zero Trust que exigem a verificação de cada solicitação de acesso, a segurança do acesso torna-se uma preocupação de TI cada vez mais importante para a proteção contra ataques e a capacitação da força de trabalho corporativa. Com a autenticação passwordless, os usuários finais não precisam mais criar ou lembrar senhas e utilizam métodos mais seguros para verificar a identidade.

“

89%

das violações de aplicativos web envolveram alguma forma de abuso de credenciais (uso de credenciais roubadas ou força bruta).

”

-- Relatório de investigação de violações de dados - Verizon 2021

Windows Hello for Business: o modelo de confiança de certificados

O Windows Hello for Business (WHfB) é uma solução de autenticação passwordless da Microsoft que verifica a entrada/login, usando a autenticação forte (multifator) em PCs e dispositivos móveis por meio de credenciais de identidade biométricas ou com PIN.

O modelo de confiança de certificados para WHfB usa certificados digitais vinculados a uma Infraestrutura de chave pública (PKI) para autenticação no Active Directory (AD) com certificados emitidos por uma Autoridade de Certificação (CA).

O modelo de confiança de chaves faz autenticação no AD com uma chave e exige certificados autoassinados.

Entre os dois principais modelos de confiança utilizados pelo WHfB (confiança de chaves e confiança de certificados), a confiança de certificado pode ser a preferida por empresas preocupadas com:

- Casos de uso: com o modelo de confiança de certificados, um certificado WHfB pode ser usado da mesma forma que certificados com smart card com logon do Windows.
- Tecnologia de identidade e acesso: empresas que já usam PKI para emitir e gerenciar certificados de usuário final também podem usar essa PKI com o Windows Hello for Business.

Plataformas DigiCert® Enterprise PKI e Windows Hello For Business

As plataformas DigiCert Enterprise PKI fornecem suporte para o modelo de confiança de certificados WHfB, apresentando os casos de uso e a conveniência que os clientes esperam de iniciativas de autenticação passwordless, que:

- **simplificam** a administração dos certificados WHfB com modelos de certificado pré-configurados e os métodos de registro correspondentes.
- **aceleram** a integração por meio de fluxos de trabalho automatizados e do provisionamento zero-touch de certificados autenticados pelo cliente exigidos pelo WHfB para estações de trabalho de domínios Windows.
- **fornecem** a conveniência de gerenciar certificados digitais WHfB com a mesma plataforma usada para gerenciar outros casos de uso empresariais.

O suporte para WHfB é um dos vários recursos das plataformas de PKI empresarial da DigiCert que fornecem às organizações uma experiência simplificada de administração e provisionamento de certificados digitais com base em fluxos de trabalho automatizados, vários métodos de registro e recursos de integração de terceiros.

Para administradores do Windows Hello for Business, isso significa:

Recursos da plataforma PKI	Benefícios
Modelos de certificados predefinidos para WHfB	Facilitam a rápida integração de usuários e dispositivos por meio do DigiCert Auto-Enrollment Server (client-less) com modelos de certificados predefinidos para Controlador de domínio, Agente de registro e Autenticação de usuários no WHfB
Gerenciamento zero touch do ciclo de vida dos certificados	Aumenta a segurança e a produtividade dos usuários por meio de recursos automatizados de renovação, reemissão, expiração e reprovisionamento de certificados
Proteção de chaves forte e aplicação de políticas de alto nível	Fornecem opções para geração e proteção de chaves por meio do Trusted Platform Module (TPM) e da aplicação de políticas para usar esse módulo
Integração otimizada com aplicativos e sistemas de terceiros para o WHfB	Facilita a integração utilizando o suporte para API REST, SCEP e EST, além de SAML para serviços federados e distribuídos
Administração e gerenciamento centralizados para WHfB e outros certificados digitais	Habilita visibilidade e controle do cenário de certificados de toda a empresa, com gerenciamento completo do ciclo de vida dos certificados, rastreamento, logs de auditoria e geração de relatórios, tudo em uma única plataforma
Implantação rápida da plataforma	Capacita a implantação rápida e a criação de CAs online tanto para CAs baseadas em software como HSM
Plataforma de PKI altamente flexível e escalável	Compatível com várias opções de implantação de plataformas de PKI, incluindo modelos no local, na nuvem e híbridos, com escalabilidade comprovada
Suporte para vários idiomas	Compatível com vários idiomas em todas as interfaces web, consoles de administração e páginas web de registro de usuários finais.

Requisitos técnicos

Plataformas DigiCert® Enterprise PKI:

- PKI Platform 8 com Autoenrollment Server no Windows Server* de domínio ou
- Enterprise PKI Manager com Autoenrollment Server no Windows Server de domínio (disponibilidade no 1º trimestre de 2022)

Sistemas operacionais Windows Server:

2019, 2016 ou 2012

Serviço de diretório:

Windows Active Directory (AD)*, Azure AD

Solução de Single Sign-on:

Microsoft Active Directory Federation Services (ADFS)

Solução de sincronização de dados de identidade:

Azure AD Connect

Sistema operacional de cliente:

Windows 10

*Os componentes precisam ser executados no mesmo sistema operacional Windows Server suportado

Entre em contato conosco usando o formulário da página <https://www.digicert.com/pt/> para obter mais detalhes.