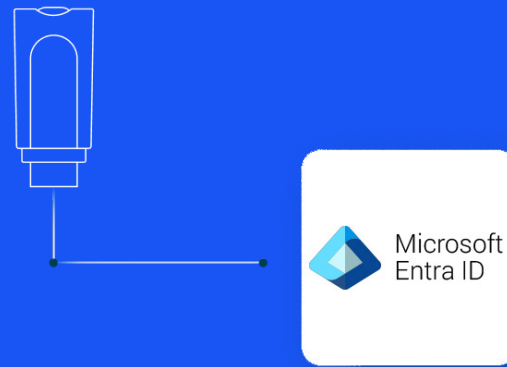




Phishing-resistant and passwordless authentication with Microsoft Entra ID

Integrating Digipass® FIDO2 security keys with Microsoft Entra ID significantly enhances your company's security posture while simplifying the authentication process. Traditional legacy multi-factor authentication methods often fall short as social engineering attacks become more sophisticated. Digipass FIDO2 security keys address these challenges and provide organizations with a robust and frictionless solution for modern security needs.

Windows logon with static password

Username and password authentication is a longstanding method but has inherent security vulnerabilities. Passwords are often weak or reused, making them susceptible to phishing attacks, credential theft, and brute force attempts. Frequent password resets further burden IT support teams and disrupt users. This traditional method is also not passwordless, forcing users to manage and remember credentials, which leads to a cumbersome experience.

Push notifications via mobile app

Push notifications for authentication via mobile apps offer convenience but introduce their own set of issues. Users must actively interact with their mobile devices to approve login attempts, which can disrupt workflow and introduce friction.

Push notifications are also vulnerable to phishing attacks, as attackers may trick users into approving fraudulent requests. Another emerging threat is push fatigue attacks, where users become desensitized to frequent notifications, increasing the risk of inadvertently approving malicious access attempts.

Windows Hello for Business

Windows Hello for Business offers strong

security through biometric authentication, such as facial recognition or fingerprint scanning. However, this method is restricted to the device on which the biometric data is stored, limiting flexibility and portability when users need to switch between different devices.

Legacy one-time passwords

One-time passwords (OTPs) most commonly sent via SMS text messages or e-mail are widely used for multi-factor authentication. Although OTPs add an extra layer of security, they are not resistant to phishing attacks and can be intercepted or tricked out of users. Additionally, the process of retrieving and entering OTPs within a limited time frame introduces friction, making the authentication experience cumbersome.

Digipass FIDO2 security keys

Digipass FIDO2 security keys overcome these challenges by providing a passwordless authentication method. Using strong cryptographic techniques, a Digipass FIDO2 security key eliminates the need for passwords, thereby significantly reducing the risks associated with password management. This shift not only enhances security by protecting against phishing and credential theft but also simplifies the user login experience.



Highlights

Secure and convenient

- Phishing-resistant authenticator protects against password-based attacks
- Frictionless login process with passwordless one-touch authentication
- Compatible with a wide range of devices and platforms
- Portable solution extending phishing-resistance to a wide range of devices enabling strong authentication for shared workstations and BYOD policies

With FIDO2, authentication occurs directly on the security key, removing the need for push notifications and the associated risks. This method simplifies the login process by allowing users to authenticate with a single touch or tap, eliminating the potential for phishing and reducing workflow interruptions.

Digipass FIDO2 security keys complement Windows Hello by providing a portable and consistent authentication method. While Windows Hello secures individual devices, Digipass FIDO2 security keys enable users to access their accounts securely from any device via USB, NFC and even Bluetooth. This combination enhances both security and flexibility, allowing seamless access across multiple devices.

Digipass FIDO2 security keys also address the limitations of OTPs by providing a seamless, phishing-resistant alternative. Authentication is completed with a single touch or tap on the hardware key, eliminating the need for OTP retrieval and entry. This streamlined process reduces user friction and enhances security, as Digipass FIDO2 security keys are

resistant to phishing and do not require time-sensitive code entry.

For BYOD environments, Digipass FIDO2 security keys provide a robust solution by ensuring consistent and secure authentication across all devices, regardless of their management status. Employees can use their personal devices without compromising security, as the security key handles the authentication process securely. This approach simplifies the implementation of security policies and ensures that sensitive data remains protected, even on personal devices.

Superior security and user experience

By integrating Digipass FIDO2 security keys with Microsoft Entra ID, your organization can achieve a superior level of security and user convenience. Users will enjoy a fast login experience without the need to type their credentials, while their secrets are securely stored within the device and cannot be extracted.

	Legacy MFA, OTP, push notifications	Windows Hello for Business	DIGIPASS FX
Passwordless & phishing-resistant	✗	✓	✓
Supports Windows login	✓	✓	✓
Supports SSO login	✓	✗	✓
Supports BYOD & shared workstations	✓	Max. 10 users	✓
Portable to other devices	✓	✗	✓
Works on macOS & Linux	✓	✗	✓

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
[OneSpan.com/security](https://onespan.com/security)

Contact us at
[OneSpan.com/contact-us](https://onespan.com/contact-us)



Copyright© 2025 OneSpan North America Inc., all rights reserved. OneSpan®, the "O" logo, Digipass®, Cronto® are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.