

DIGIPASS[®] FX

for Google Workspace



Phishing-resistant and passwordless authentication with Google Workspace

Integrating FIDO2 hardware keys with Google Workspace significantly enhances your organization's security posture while simplifying the authentication process. Traditional legacy multi-factor authentication (MFA) methods are increasingly vulnerable as social engineering attacks become more sophisticated. Hardware passkeys, such as DIGIPASS FX, provide a robust and frictionless solution to meet modern security needs in Google Workspace.

Google Account Logon with Username and Password

Username and password authentication, while familiar, presents inherent security risks. Weak or reused passwords are highly susceptible to phishing attacks, credential theft, and brute-force attempts. Moreover, frequent password resets create additional strain on IT support and disrupt workflows. This traditional method does not offer a passwordless experience, leading to additional challenges in terms of managing and remembering credentials.

Push Notifications via Mobile App

Push notifications delivered through a mobile authenticator app are often used for MFA, offering convenience but introducing certain risks. Users must manually approve login attempts on their devices, potentially disrupting their workflow. Furthermore, push notifications are vulnerable to phishing attacks where attackers could trick users into approving fraudulent requests. A growing threat in this space is push fatigue, where users, overwhelmed by frequent notifications, may inadvertently approve malicious access attempts.

Legacy One-time Passwords

One-time passwords (OTPs), often sent via SMS or email, remain a popular form

of MFA. While they add an extra layer of security, they are not immune to phishing attacks and can be intercepted by malicious actors. Additionally, retrieving and entering OTPs can slow down the login process, introducing friction to the user experience.

Improve your Security Posture with FIDO2 Passkeys

FIDO2 hardware keys, such as DIGIPASS FX, solve many of these challenges by providing a passwordless authentication experience. Leveraging strong cryptographic techniques, FIDO2 passkeys eliminate the need for passwords, significantly reducing risks associated with password management. By shifting the authentication process to the hardware key, users benefit from increased protection against phishing and credential theft, while enjoying a simplified login experience.

Passwordless, Phishing-resistant Authentication for Google Workspace

With FIDO2 passkeys, Google Workspace users can achieve a streamlined, secure login process, eliminating the need for passwords and reducing the associated risks of password-based attacks. DIGIPASS FX enhances the login experience by



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

enabling one-touch or tap authentication via hardware keys, mitigating phishing threats and eliminating the potential workflow disruptions caused by OTPs or push notifications.

DIGIPASS FX provides a consistent and portable authentication method across all devices. It allows users to authenticate from any device via USB, NFC, or Bluetooth. This expands both security and flexibility, making it ideal for environments with shared workstations or BYOD policies.

Additionally, DIGIPASS FX addresses the limitations of legacy MFA methods, like OTPs, by offering a seamless, phishing-resistant alternative. The authentication process is completed with a simple touch on the hardware key, bypassing the need to retrieve or enter time-sensitive codes. This streamlined process not only enhances security but also improves the user experience by reducing friction.

Superior Security and User Experience with Google Workspace

By integrating DIGIPASS FX passkeys with Google Workspace, your organization achieves a higher level of security and user convenience. Users can enjoy a fast, secure login experience without typing passwords, while sensitive credentials are safely stored within the device and cannot be extracted. This approach not only boosts security but also enhances the overall user experience, making passwordless authentication a practical and secure solution for modern work environments.



OneSpan helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

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

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



Copyright© 2024 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.