

Keeper Security Launches Innovative Biometric Login with Passkeys

New update enables native passwordless vault access on the browser extension and Commander CLI

LONDON, UNITED KINGDOM, August 20, 2025 /EINPresswire.com/ -- [Keeper Security](#), the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords and passkeys, privileged accounts, secrets and remote connections, announces the release of biometric login using FIDO2/WebAuthn passkeys on the Chrome/Edge browser extension and Keeper Commander CLI. This update, the first of its kind in the industry, enables users to securely access their Keeper Vault with passkeys protected by biometrics or PINs across multiple platforms, including Windows devices via Windows Hello and Mac devices using Touch ID – replacing the need to type passwords. Biometric information never leaves the user's device and is never transmitted to or accessible by Keeper, ensuring complete privacy. Customers are not required to install a companion application, simplifying the user experience and retaining zero-knowledge end-to-end encryption.

A passkey is a FIDO authentication credential, based on FIDO standards, that allows a user to sign in to apps and websites with the same process they use to unlock their device, such as biometrics. The cryptographically unique, device-bound credentials are designed to replace traditional passwords with phishing-resistant, passwordless authentication. Passkeys are both more secure and easier to use, as the user no longer needs to enter their username, password or additional factors.

The UK government and National Cyber Security Centre (NCSC) are increasingly moving towards more widespread passkey adoption across public services and have advised private UK organisations and citizens to do likewise. This latest update from Keeper aligns with the NCSC's position on passkey adoption being vital for transforming the UK's cyber resilience at a national scale. By supporting the widely adopted FIDO2/WebAuthn protocols, Keeper offers a secure and convenient login experience for its browser extension as well as Keeper Commander, its command-line and SDK interface, across all compatible devices and browsers.

"Security is shifting from passwords alone to stronger, more reliable methods," said Craig Lurey, CTO and Co-founder of Keeper Security. "This industry-leading update lets users unlock their vaults using trusted, device-based credentials such as biometrics or PINs, reducing reliance on passwords that can be stolen or phished. Keeper is proud to be the first to provide this functionality to individuals and organisations."

Windows Hello offers native biometric and PIN authentication on Windows 11 devices, while Apple's Touch ID enables similar capabilities on macOS. Keeper's implementation of FIDO2/WebAuthn supports passkey-based login on Chromium-based browsers, providing a secure and seamless experience across a broad range of supported platforms and devices.

Keeper is a proud member of the [FIDO Alliance](#), supporting its mission to move the industry beyond passwords. Through its work developing open standards like FIDO2 and WebAuthn, the Alliance is helping organisations adopt secure, phishing-resistant authentication that's built into the devices people already use. This update reflects that shift – simplifying sign-in while strengthening protection and making it easier for IT teams to support passwordless access at scale.

In addition to enabling passkey login, Keeper supports the creation, secure storage and autofill [of passkeys](#) across devices, browsers and operating systems. Keeper's cross-platform passkey management is available through its browser extension, mobile apps, web and desktop vault, as well as Keeper Commander CLI, enabling users to leverage passkeys without compromising usability or security. Whether accessing their Keeper Vault or signing in to supported websites and applications, users can store and autofill passkeys seamlessly – no password or second factor required.

Keeper's passkey login functionality aligns with the growing adoption of passkeys within organisations. According to Keeper's Insight Report: Navigating a Hybrid Authentication Landscape (1), 80% of organisations are currently using or plan to adopt passkeys to reduce the risk of threats like phishing and credential stuffing. However, many face challenges managing hybrid systems that combine passwords with passwordless methods. Keeper makes it easy to adopt passkeys at scale by supporting FIDO2 standards across devices, platforms and browsers, eliminating complexity for users and IT teams alike.

The Keeper Browser Extension is available now for download from Keeper's website (2), the Chrome Web Store and the Microsoft Edge Add-ons Store. The Keeper Commander CLI is available from Keeper's open source Github repository (3). For additional information, visit Keeper's documentation portal (4).

###

About Keeper Security

Keeper Security is transforming cybersecurity for millions of individuals and thousands of organisations globally. Built with end-to-end encryption, Keeper's intuitive cybersecurity platform is trusted by Fortune 100 companies to protect every user, on every device, in every location. Our patented zero-trust and zero-knowledge privileged access management solution unifies enterprise password, secrets and connections management with zero-trust network access and remote browser isolation. By combining these critical identity and access management

components into a single cloud-based solution, Keeper delivers unparalleled visibility, security and control while ensuring compliance and audit requirements are met. Learn how Keeper can defend your organisation against today's cyber threats at KeeperSecurity.com.

Learn more: KeeperSecurity.com

- (1) <https://www.keepersecurity.com/navigating-hybrid-authentication-landscape-insight-report/>
- (2) <https://www.keepersecurity.com/>
- (3) <https://github.com/keeper-Security/commander/>
- (4) <https://docs.keeper.io/en/release-notes/browser-extensions/browser-extension/browser-extension-version-17.2>

Media Contact

Charley Nash, Account Manager

Eskenzi PR

charley@eskenzipr.com

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/841226790>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.