10ZiG Introduces Multi-Environment Support for YubiKey (FIDO2) Authentication to Strengthen Passwordless Security

New FIDO2-based authentication capability enhances Zero Trust aligned identity protection for hybrid environments including AVD, Citrix and Omnissa.

PHOENIX, AZ, UNITED STATES, December 10, 2025 /EINPresswire.com/ -- 10ZiG® Technology, a global leader in thin and zero client endpoint solutions for VDI, DaaS and SaaS workspaces, today announced new support for YubiKey (FIDO2) authentication for Microsoft Azure Virtual Desktop (AVD), Citrix and Omnissa Horizon and Workspace ONE. This capability enables organizations to deliver phishing resistant, passwordless authentication across 10ZiG endpoints and improves identity security for hybrid workers who move between multiple devices throughout the day.

> "With our new FIDO2 WebAuthn authentication support, we are giving customers a highly secure, low friction way to protect user access across thin clients, laptops and BYOD devices."
>
> *Kevin Greenway, CTO, 10ZiG Technology*

The new FIDO2 authentication workflow is supported from the latest version of 10ZiG Linux operating systems, including 10ZiG NOS™, PeakOS™ and RepurpOS™, and through the [10ZiG Secure Browser](#) (a secure browsing solution built on the Chromium Embedded Framework). Users can authenticate by tapping a hardware security key, providing a stronger and more convenient alternative to passwords, authenticator apps or mobile device-based MFA.

"With our new FIDO2 WebAuthn authentication support, we are giving customers a highly secure, low friction way to protect user access across thin clients, laptops and BYOD devices," said Kevin Greenway, CTO of [10ZiG Technology](#). "FIDO2 keys offer true phishing resistant multi-factor authentication (MFA) at a very low cost, and by integrating this natively through our Secure Browser, we are making it easy for organizations to adopt modern passwordless access without additional tools or agents."

Purpose Built Passwordless Authentication for AVD and Hybrid Work

As organizations continue shifting toward cloud hosted desktops, browser-based applications

and hybrid work strategies, secure identity access has become a central requirement of modern IT architecture. Native FIDO2 authentication support for AVD, Citrix and Omnissa-powered workspaces allows IT teams to deliver consistent, hardware-backed identity verification across 10ZiG endpoints, corporate laptops and personal devices.

The new support delivers a predictable, passwordless login experience no matter where users work or what device they are using. This approach provides strong protection against credential theft because it removes passwords entirely. No secrets are stored or transmitted during login and the private key never leaves the hardware token, which protects against phishing, MFA fatigue, credential replay and other identity attacks.

User Experience, Operational Efficiency and Strategic Alignment

FIDO2 authentication simplifies the user journey for workers who frequently move between thin clients, Windows devices, macOS systems and BYOD hardware. A single tap on the key provides fast, secure access to supported VDI and DaaS platforms, without the need for mobile phones, authenticator apps or SMS codes. This significantly reduces daily friction and removes concerns related to personal device use for work authentication.

From an operational standpoint, organizations adopting FIDO2 typically experience fewer password reset tickets and fewer MFA re-enrollment issues, which lowers help desk workloads and improves overall support efficiency. Extending passwordless authentication across multiple workspace delivery platforms helps unified identity workflows and further simplifies administration. FIDO2 authentication also supports compliance requirements for organizations seeking stronger identity controls. This approach is aligned with the industry's move toward passwordless identity and cloud-first authentication and allows customers to modernize their security posture without the need for additional licensing, agents or third party authentication tools.

Support for YubiKey FIDO2 authentication is available now through the latest 10ZiG firmware update version 16.5.39.4 or above on devices using 10ZiG NOS, PeakOS and RepurpOS operating systems. All new 10ZiG devices and OS subscriptions will include Secure Browser and FIDO2 WebAuthn support at no additional cost. For more information about 10ZiG secure operating systems, visit www.10zig.com/10zig-operating-systems.

About 10ZiG Technology

10ZiG Technology is a leading Thin and Zero Client hardware and software provider delivering a modernized and secure user experience for VDI, DaaS or web based environments. With more than 22 years in the thin client market, no hassle repurposing software and easy to use free management, 10ZiG supports a single vendor strategy for endpoint modernization. The company offers a wide range of TAA compliant devices including desktop clients, laptops and all in ones along with features such as fiber, wireless support, quad screen options and more.

Through a broad ecosystem of technology partners including Microsoft, Citrix and Omnissa, 10ZiG provides secure, high performance solutions for today's diverse IT requirements. Learn more at www.10zig.com.

Erin Jones
Avista PR for 10ZiG
10ZiG@avistapr.com
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
[X](X)