Zero Sign-On: The Solution for Passwordless Authentication

Key Benefits of ZSO

Reduce the risk of data breaches

By eliminating passwords, ZSO reduces the risk of phishing and data breaches.

Provide frictionless access

ZSO eliminates the need for users to memorize, enter or reset complex passwords and enables them to access cloud-based apps and PM and Mac desktops/laptops quickly and easily.

Decrease helpdesk costs

ZSO's passwordless approach means no helpdesk resources are spent dealing with password resets and account lockouts.

Deploy scalable mobile-cloud security

ZSO is built on industry standards like FIDO2 and can be used to log into online and offline PC and Mac desktops/laptops, plus applications and enterprise cloud services on any managed or unmanaged device, anywhere in the world.

It's time to say goodbye to passwords

Everyone hates passwords. Not only are they hard to remember, time-consuming to enter, and annoying to reset, they are also a top source of enterprise cloud data breaches.[1] It's no surprise that 86% of security leaders want to get rid of passwords, preferably by using mobile devices as the enterprise ID.[2]

That's why Ivanti introduced Zero Sign-On (ZSO), a simple authentication capability that replaces passwords with secure mobile devices as the user identity. By leveraging our zero trust security framework, ZSO enables organizations in the Everywhere Workplace to:

- Transition towards a zero trust architecture by replacing passwords with multi-factor authentication (MFA) methods.
- Provide passwordless access to any business app or cloud service, including Microsoft 365.
- Deliver a consumer-like authentication experience to the enterprise through the use of strong biometrics.
- Eliminate the hassle and security risks of passwords.
- Ensure that only verified users, devices, apps and networks can access business resources.

Our unique approach

Ivanti ZSO – a component of the Ivanti Access platform – replaces passwords with mobile devices as the user's identity and primary factor for authentication. ZSO eliminates the need for passwords through its use of strong FIDO2 authentication protocols.

Ivanti Access is built for the Everywhere Workplace. It leverages unified endpoint management (UEM) as its foundation – whether Ivanti UEM or third-party UEM systems such as SCCM and Jamf – to provide a zero trust security approach that verifies every user, device, application and network before granting secure access to cloud resources.

Ivanti Access also integrates seamlessly with Ivanti Mobile Threat Defense (MTD) to provide companies with an added layer of security on user devices, along with context-aware, conditional access for the cloud. MTD can detect and remediate device, app and network threats before they can compromise business data.

Further, Ivanti Access and ZSO work with UEM and MTD to determine a device's health and whether it is free from mobile threats. If a threat is detected, Ivanti Access can revoke the end user's session token and block the device from accessing corporate resources until it returns to a compliant state, again free from mobile threats.

ZSO capabilities

Mobile device as user identity
Replace passwords with secure mobile devices as the primary factor for user authentication.

Adaptive authentication
Use our MFA capabilities to provide an additional layer of user verification for high-risk environments.

Secure any device – managed or not
ZSO works across all Android, iOS, macOS, and Windows 10 and 11 devices. Users are authenticated using public key credentials (certificates) on managed devices – whether managed via Ivanti UEM or third-party UEM solutions such as SCCM and Jamf – and with FIDO security keys or QR codes paired with biometrics on unmanaged devices.

Standards-based security
Ivanti ZSO supports FIDO2, SAML and WS-Fed protocols for simple and strong authentication for desktop/laptop and mobile login, and seamless SSO via certificates to SaaS-based and web-based applications.

Support for common business apps and IDPs
Ivanti Access secures any cloud or federated service including Microsoft 365, Google Workspace and Salesforce. It also integrates with many identity solutions including those from Okta, Ping and Microsoft.

Offline login
Users can log into desktops and laptops with mobile devices when offline using ZSO over Bluetooth.

Zero trust policy engine
Using a single console, you can define policies for all cloud apps that either block or limit access to unauthorized users, devices and apps over unsecure networks or when threats are detected. Intuitive remediation workflows help users self-remediate.

In-depth reporting
Our global authentication dashboard provides an in-depth view of users, apps and devices that connect to business services, alerts admins about policy violations, and much more.

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Verizon, "2021 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/
2. IDG Research, "Say Goodbye to Passwords," April 2019. www.mobileiron.com/sites/default/files/Whitepapers/Say-Goodbye-to-Passwords/Say-Goodbye-to-Passwords.pdf