KEEPER
Cybersecurity Starts Here

DATASHEET
Keeper® SSO Connect

Turbocharge Your Single Sign-On (SSO) Solution with Keeper

A comprehensive privileged password manager fills the SSO gaps and boosts overall data security

Many organizations have embraced and deployed an SSO solution, which is a session and user authentication solution allowing employees to use one login credential to access any number of websites and services. SSO authenticates the user with specific access rights and also obviates the need for further prompts when the user switches between applications in the same session.

SSO Provides Businesses Some Key Benefits

1. Rapid Provisioning for Cloud Applications

For organizations who have adopted SSO, SAML 2.0 compliant applications and services can be quickly provisioned by the SSO administrator and made available to employees.

2. Increased Security

By enforcing the use of Two-Factor Authentication with the SSO solution, organizations can protect accounts with a unified 2FA method that works across a linked application.

3. Increased Productivity

Productivity is increased and IT help desk password resets are drastically minimized since employees do not need to manage or remember their passwords for the applications connected through the SSO platform.

However, SSO is Not a Silver Bullet

When adopting an SSO solution, it's important to understand its limitations.

1. Limited Application Coverage

SSO works only with cloud services and applications that support SAML protocols. Non-SAML compliant services and applications (e.g. legacy applications) are unable to authenticate against the Identity Provider.

2. Only Authentication, Not Encryption

Most SSO solutions lack the flexibility to store a variety of sensitive information beyond username and password. By contrast, a digital vault with enterprise password management solutions can securely hold sensitive information, including encryption keys and digital certificates.

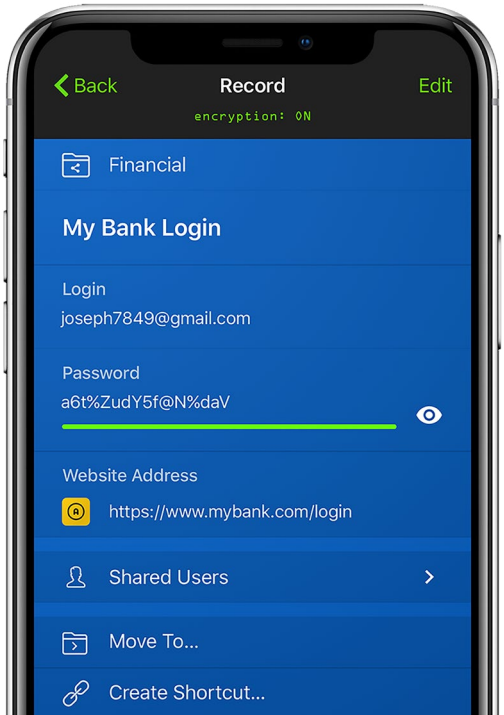
Keeper is an Enterprise Password Management (EPM) Solution that Fills the Security Gaps of SSO

SSO does not solve all security and productivity issues with passwords. Keeper adds the following to SAML-based SSO solutions:

- Client-side encryption and zero-knowledge security architecture
- Ubiquitous digital vaults on all employee devices
- Authentication for all non-SAML cloud applications, native apps and systems

With Keeper, every employee is provided with a secure and private vault for all their devices. Keeper works on all device types, platforms and operating systems to allow users to:

- Create and manage strong passwords across all device types
- Securely store files and other secret information
- Autofill passwords across web browsers, apps, mobile devices and computers
- Share confidential information between users and teams



Factors and Use Cases	Keeper	SSO
Authentication for SAML-compliant cloud applications	●	●
Authentication for non-SAML-compliant cloud applications	●	○
Authentication for native applications and systems	●	○
Encrypted vaults for storing access credentials, metadata, documents and media files - for all employees on all devices	●	○
Offline, secure access	●	○
Cost and time to integrate and provision	Low	High
Performs client-side encryption	●	○
Zero-knowledge security architecture	●	○

Keeper Integrates with Leading SSO Providers

Through the use of Keeper SSO Connect technology, end-users can seamlessly log in to their Keeper vault with any existing SAML 2.0 compatible SSO identity provider such as Okta, Centrify, Microsoft Azure, G-Suite, JumpCloud and F5 BIG-IP APN. Once this capability is activated by the Keeper Administrator, logging in is seamless across all device types and platforms Alternatively, users can first log in to identity the provider and then launch their Keeper Vault.

ADFS · Microsoft Azure · okta · G Suite · JumpCloud · amazon web services · CAS · IBM Security · Ping Identity · onelogin · Centrify · f5

Turbocharge Your SSO with Keeper

Without question, SSO solutions are here to stay. The value they provide an organization is significant. But simply put, SSO solutions can't accommodate the full range of data security, access and device flexibility challenges that organizations face today. Thus, organizations should supplement their SSO strategy with an EPM solution that can cover the many additional use cases and protect all sensitive digital assets. Keeper SSO Connect transforms SSO into an essential, ubiquitous application.