KEEPER®

Datasheet

Keeper SSO Connect™

# Enhance & Extend Your SSO Deployment

## SSO Doesn't Secure All of Your Apps

Organizations are embracing single sign-on (SSO) because it reduces password fatigue, minimizes help desk tickets for lost passwords, and enhances efficiency. In theory, instead of having to remember multiple passwords, users memorize only one. However, this isn't how SSO works in reality. The average organization uses nearly 1,200 cloud apps and services; the exact number varies from a few hundred in a small business to over 3,000 in a large enterprise[1]. Many of these apps and services do not support SSO, or they support different and incompatible SSO protocols.

For example, an organization's identity provider (IdP) may use the SAML protocol, but some of the apps that employees need to do their jobs use OAuth. Additionally, most organizations remain dependent on line-of-business (LOB) legacy apps. These old apps don't support SSO at all, but they contain essential data or perform critical business functions, so employees must continue to use them. Not all modern apps support SSO, either.

So much for having to memorize only one password! Employees must keep track of passwords for these sites and apps on their own, leaving companies open to data breaches.

## SSO Has Security Shortcomings

SSO has other shortcomings, especially if it's not paired with multi-factor authentication (2FA) and role-based access control (RBAC). These include:

- SSO controls only access to system and not the individual user access levels which is why administrators must deploy a separate solution to enforce RBAC and least-privilege
- If a user forgets their password, they're locked out of multiple sites and apps instead of just one
- If a cybercriminal steals a user's password, they can access multiple systems instead of just one
- SSO doesn't provide administrators with any visibility into user password habits, so they can't prevent employees from engaging in poor password habits, such as using weak passwords, reusing passwords across accounts, or not enabling 2FA on all accounts that support it

## Keeper SSO Connect Enables End-to-End Password Protection Across Your Entire Data Environment

Keeper SSO Connect is a SAML 2.0 application that seamlessly joins your existing SSO deployment with Keeper's Password Management System. This enhances and extends SSO with zero-knowledge password management, enforced RBAC to applications, and visibility to users' password security practices. Since Keeper offers multiple layers of data security, it provides a much stronger defense against attackers than SSO alone.

Keeper SSO Connect seamlessly integrates with Keeper's zero-knowledge vault provides a secure password, sensitive data, and file storage, along with sharing and advanced security capabilities.

## Keeper + SSO = 100% Coverage

| Use Case | Keeper Enterprise | SSO Identity Provider |
|---|---|---|
| Password-Based Apps | ✓ | ✗ |
| Shared Passwords & Secrets | ✓ | ✗ |
| Encrypted Data Storage | ✓ | ✗ |
| Social Media Sites | ✓ | ✗ |
| Native Apps | ✓ | ✗ |
| Offline Access | ✓ | ✗ |
| SSH Keys & SSL Certs | ✓ | ✗ |
| API Credentials | ✓ | ✗ |
| Encrypted Private Files | ✓ | ✗ |
| Zero-Knowledge Encryption | ✓ | ✗ |
| SAML-Based Apps | ✓<br>via Keeper SSO Connect | ✗ |

### Works With Your Existing Identity Provider

Some password managers either don't support SSO at all or don't support zero-knowledge encryption. Keeper SSO Connect easily and seamlessly integrates with all popular SSO IdP platforms, including Microsoft 365, Azure, ADFS, Okta, Ping, JumpCloud, Centrify, OneLogin, and F5 BIG-IP APM.

Microsoft | DUO | Google Workspace | aws
Centrify | f5 | okta | onelogin
Ping Identity | CAS | jumpcloud | IBM Security

### Extend Your SSO While Deploying Keeper's Password Security & Encryption Platform to Everyone

Keeper SSO Connect enhances any SSO solution by seamlessly and easily integrating it with a zero-knowledge password manager and digital vault that can be used to store and encrypt not only login credentials but also proprietary customer data, access credentials to restricted systems, and sensitive documents.

Simply by authenticating through your existing IdP, your employees gain access to all of the capabilities of the top-rated Keeper password management platform, including:

- A secure digital vault that can be accessed from any device, running any OS
- Automatic password generator
- Login credential autofill that works on any website or app
- Secure storage for sensitive files, documents, photos, and videos on unlimited devices

IT administrators gain complete visibility and control into employee password practices, enabling them to enforce the use of strong, unique passwords, multi-factor authentication (2FA), and other password and security policies.

- Exclusive, patented zero-knowledge security model
- Rapid deployment on all devices with no upfront equipment or installation costs
- Personalized onboarding and 24/7 support and training from a dedicated support specialist
- Support for RBAC, 2FA, auditing, event reporting, and multiple compliance standards, including HIPAA, DPA, FINRA, and GDPR
- Provision secure shared folders, subfolders, and passwords for teams
- Provision users for either SSO or Master Password authentication
- Enable offline vault access when SSO is not available
- Dynamically provision vaults through SCIM
- Configure for High Availability (HA)

### Single Cloud, Multi-Cloud & Hybrid Deployment Options

Keeper SSO Connect is a fully managed SaaS solution that can be deployed on or in any Windows, Mac OS, or Linux environment, in the cloud or on-prem.

### Zero-Knowledge Architecture

User encryption keys are generated dynamically by Keeper SSO Connect, and all encryption and decryption is done on the user's device. PBKDF2 with 100,000 rounds is used for deriving a key from the user's master password. Each record is encrypted using AES-256, with a different and unique key that is randomly generated client-side. RSA encryption is used for secure record sharing between users and teams. Keeper's infrastructure syncs encrypted ciphertext between devices. Key pinning is enforced between client and server. All data in transit and at rest is always encrypted; it cannot be viewed by Keeper Security employees or any outside party.

### About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the market-leading, top-rated cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity, and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice, and is the winner of four G2 Best Software Awards. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM).

Learn more at https://keepersecurity.com.

[1] Dark Reading