



Integrate Password Management and Zero-Knowledge Security Into Your Single Sign-on Solution With Keeper SSO Connect™



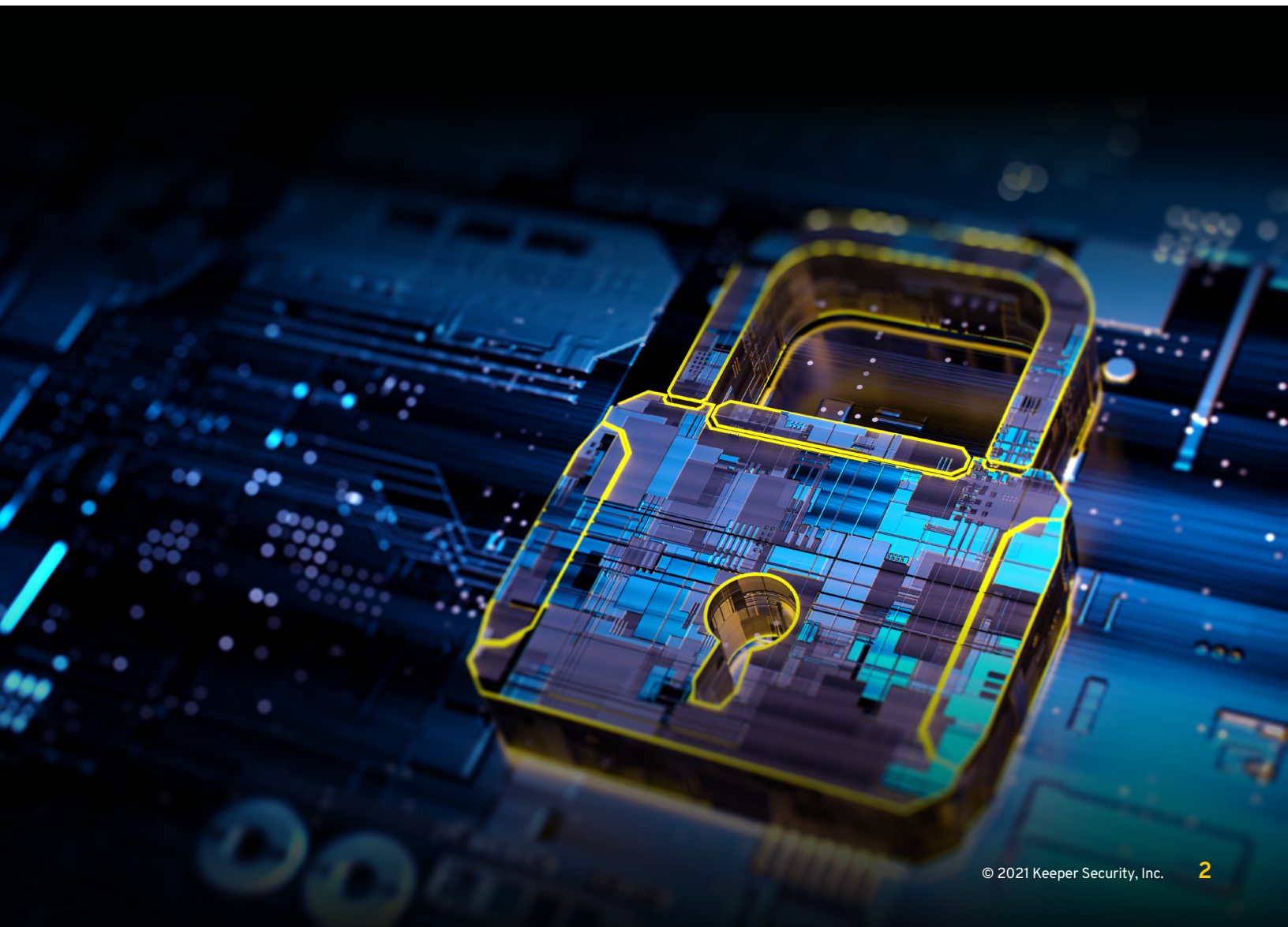
EXECUTIVE SUMMARY

Employees' inability to keep track of all the passwords they need to do their jobs harms productivity, wastes money, and complicates identity and access management (IAM) and security throughout the enterprise.

Single sign-on (SSO) solves some of these problems but still leaves organizations with significant logistical and security gaps. Keeper SSO Connect fills these gaps by extending SSO deployments with an integrated zero-knowledge password encryption system that provides advanced password management, sharing, and security capabilities.



Keeper SSO Connect fills IAM security gaps by extending SSO deployments with integrated zero-knowledge password encryption.



BENEFITS OF IMPLEMENTING SSO IN THE ENTERPRISE



Eliminating Password Fatigue

Instead of having to keep track of dozens of different passwords, employees have to memorize only one.



Enhancing Productivity

On average, employees devote nearly 11 hours every year to entering and resetting passwords. By simplifying access to resources, SSO helps keep users productive.



Minimizing Help Desk Tickets

The Gartner Group estimates that up to 50% of help desk support calls are for password resets, and the average labor cost to address one password reset is \$70. Greatly reducing or eliminating password reset tickets saves money and frees up help desk employees to focus on more complex support tasks.



Supporting Identity Access and Management (IAM)

SSO is a common component in enterprise IAM stacks. SSO simplifies and speeds up IAM deployment by enabling administrators to easily configure strong authentication and other access controls. Administrators also gain visibility into user access throughout the SSO deployment.



Supporting Zero-Trust Environments

By simplifying and speeding up IAM deployments, SSO supports zero-trust environments, which require strong authentication for all users.



Supporting Compliance Reporting

SSO systems are an easy way to extend audit and reporting capabilities to include user sign-on data, which is required by many compliance frameworks.

SSO SHORTCOMINGS

For all the benefits of SSO, it's not a panacea. SSO solutions leave significant security and functionality gaps. Ironically, these gaps involve the very problem that businesses seek to solve with SSO: **password management and security**.

A Single Point of Failure

One of the biggest shortcomings of SSO platforms is that they're a single point of failure. If a user forgets their password, they're locked out of multiple sites and apps instead of just one. Conversely, if a user's password is compromised, cybercriminals can access multiple systems instead of just one.

Incompatible Apps and Services

The typical organization uses anywhere from several hundred to several thousand cloud apps. In addition to business productivity applications that everyone in the company uses, specific departments and teams utilize their own subsets of job-specific applications. These frequently include legacy line-of-business (LOB) apps that don't support SSO but that aren't feasible to refactor or replace because they contain essential data or perform critical business functions.

No Visibility or Control Over User Password Habits

Left on their own to keep track of passwords for non-SSO accounts, individual users and teams come up with their own systems, such as storing passwords in text files or spreadsheets or writing them down on sticky notes. These "homemade" solutions are neither efficient nor secure. Users may also engage in poor password practices, such as using weak passwords, reusing passwords across accounts, sharing passwords without authorization, and not enabling multi-factor authentication (2FA).

As a result, despite having invested in an SSO deployment, organizations are left vulnerable to password-related data breaches -- especially since administrators have no visibility or control over password usage in these sections of the data environment. They're unable to enforce security policies such as using a strong, unique password for non-SSO accounts or enabling multi-factor authentication (2FA) on all accounts that support it.



KEEPER SSO CONNECT...



Easy to deploy and scale



Supports passwordless strategies















Extends to thousands of users and endpoints



Seamlessly Integrates with any IdP, in Any Data Environment

Keeper SSO Connect is a fully-managed SaaS solution that can be used without deploying any on-premise or customer-managed components. It is hosted and managed by Keeper Security while maintaining zero-knowledge architecture.

Keeper Integrates with All Major Identity Providers

 Azure AD and O365	 Active Directory Federated Services
 Microsoft 365	 Google Workspace
 Okta	 OneLogin
 Duo	 Centrify
 JumpCloud	 Ping
 F5 BIG-IP APM	 And More!

Two-Step Setup for Rapid Deployment

Keeper SSO Connect doesn't require any on-premises or customer cloud-hosted services, nor does it require any additional software or equipment. Setup is accomplished in two easy steps:

- > **Step 1:** Enable and configure the Keeper Application within the IdP
- > **Step 2:** Configure SSO Connect within the Keeper Admin Console

Streamlined Login Flow Promotes Efficiency & Enhances Security

Keeper SSO Connect's streamlined login flow promotes efficiency by simplifying end user login. If Keeper recognizes an end user's email domain as an SSO-enabled enterprise, the user will be automatically routed to their identity provider. When combined with SCIM auto-provisioning or Just-In-Time (JIT) provisioning, onboarding new users is fast and secure.

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	✓ via Keeper SSO Connect	✓

Proprietary Security Model Ensures No One Can Access User Login Credentials

Keeper SSO Connect utilizes client-side generated ECC (Elliptic Curve Cryptography) private/public key pairs for seamless, secure integration with SSO identity providers. By using device-level ECC keys to protect user vaults, Keeper maintains zero knowledge while offering a fully cloud-based SSO integration. All data in transit and at rest is encrypted and cannot be viewed by any outside party, not even Keeper Security employees.

Secure and Streamlined Device Approvals Support Zero-Trust Security

Device authorization is a core component of a zero-trust security model. With Keeper SSO Connect, every approved user device has a local, private, ECC key. With Keeper's advanced zero-knowledge encryption, keys are securely exchanged between the user's devices, or through Keeper administrator approvals. Device approvals can also be automated.

Organizations can configure push-based device approval to be performed one of two ways:



By an administrator who holds "Approve Device" permissions



Via an automated approval method (the Keeper Admin Console, the Keeper Commander CLI, or an Azure function)

End-to-End Password Management Across the Enterprise

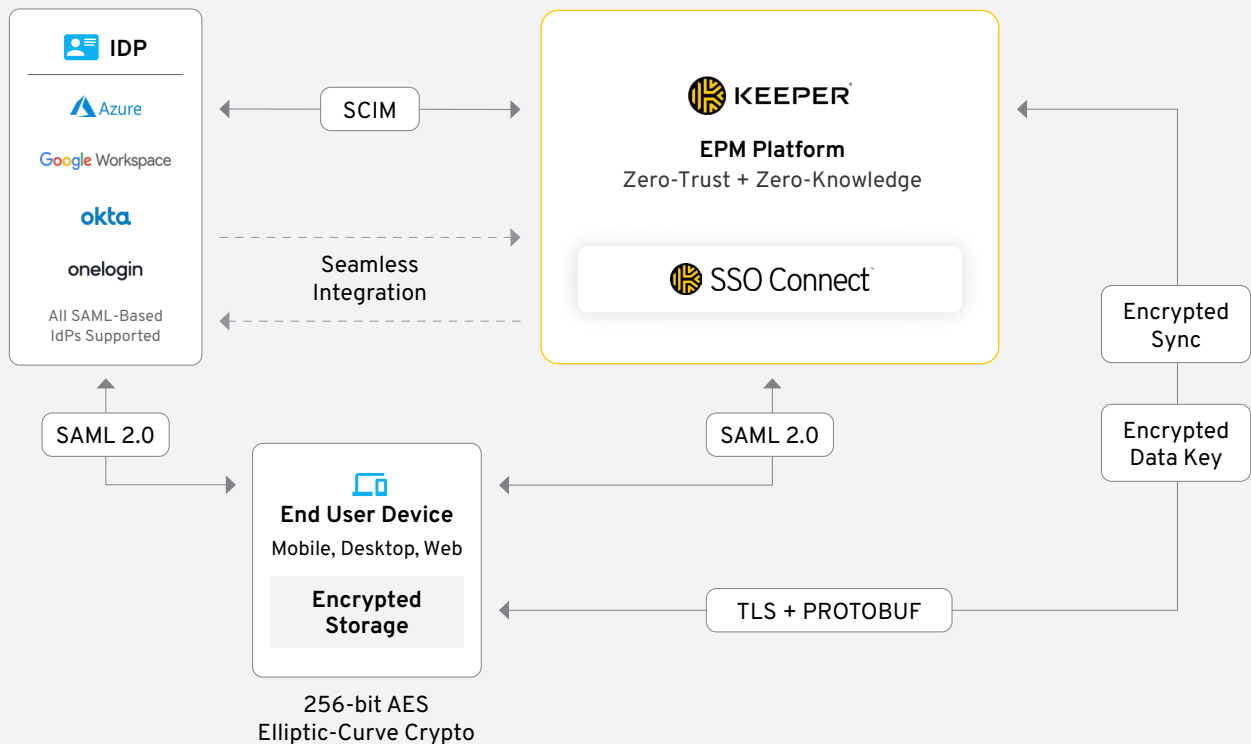
Keeper SSO Connect gives your administrators access to all of the capabilities of the top-rated Keeper password management platform, including:

- > 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
- > Specify password complexity requirements, such as maximum/minimum password lengths and include/exclude special characters
- > Provision secure shared folders, subfolders, and passwords for teams
- > Enable offline vault access when SSO is not available
- > Dynamically provision vaults through SCIM
- > Protect against the dark web and credential-stuffing attacks

Your end users benefit from features that help them optimize their workflows and improve their password security, 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

Seamlessly Provision Keeper Enterprise Across Your Entire Organization in a Few Hours



CONCLUSION

SSO platforms are designed to solve security and functionality problems related to user passwords, but unless organizations also invest in a password management solution, they are left with significant security and functionality gaps. Keeper SSO Connect bridges these gaps by extending SSO deployments with comprehensive password management and encryption through the top-rated Keeper password management platform.

Keeper SSO Connect works with any tech stack and seamlessly integrates with all popular IdP platforms. Deployment is simple and fast. The platform improves usability for end users, provides administrators with visibility and control over employee password practices, enhances employee efficiency, eliminates password-related help desk tickets, and helps organizations prevent password-related data breaches.

