KEEPER
Cybersecurity Starts Here™

Turbocharge Your Single Sign-On Solution with a Major Security Boost

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

Table of Contents

Introduction

Many mid-to-large sized organizations and a fast-growing segment of SMBs have embraced and deployed one of the many single sign-on (SSO) solutions available. In simplest terms, SSO is a session and user authentication solution allowing an employee to use just one login credential (Active Directory credentials or email/password) to access any number of web-based sites and services. SSO authenticates that the user has specific access rights and also obviates the need for further prompts when the user switches from one application to another in the same session.

SSO solutions also help simplify the otherwise complex task of administration of user access by allowing administrators to quickly revoke or authorize access to specific users for specific services. In organizations that have to manage scores if not hundreds of internal and external services, SSO is a valuable tool.

Not surprisingly given the cybersecurity threat environment today and the intrinsic link between weak or stolen passwords and the incidence of breaches, the **SSO market is growing briskly** at a nearly 15% compound annual growth rate.

The Benefits of SSO

1. **Rapid Provisioning for Cloud Applications**

   For organizations who have adopted SSO, deployment of cloud-based applications (which support the SAML 2.0 protocol) can usually be completed quickly. If an application or service connecting to an SSO supports SAML 2.0, the application 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.

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

The Limitations and Challenges of SSO Solutions

When adopting an SSO solution, it's important to understand its limitations. First, there is one important feature that SSO solutions today do not have, and that is the ability to support all accounts and services that employees use, both for work and personal use while at work. For example, SSO works only with a set list of cloud services and cloud applications that support SAML (Security Assertion Markup Language) protocols. Without this, business users are left to find some way of keeping track of all the passwords they use for all unsupported systems. Often these employees are privileged or high-end users, meaning they have access to sensitive data on various systems.

Also for applications that do not support SAML, most SSO solutions lack the flexibility to store a variety of sensitive information beyond simple username and password. An SSO solution is not an encrypted digital vault. They cannot accommodate login credentials for native applications, bank account numbers, digital certificates, SSH keys, PINs, employee census data, confidential images, documents and video files. By contrast a digital vault inherent in the better password management solutions available today can securely hold much more information, including encryption keys and digital certificates.

As stated, there are many positive benefits of using an SSO product for cloud applications. But there are several gaps in the technology which have created difficult situations for many IT admins, including the following:

1. **Limited Application Coverage**

   In order to deploy a service or application with an SSO provider, the service must fully support SAML 2.0 technology. There are various levels of SAML support. For example, some apps can dynamically provision a user account but some apps don't support this ability. The SSO administrator must then be responsible for manually provisioning specific applications to users.

2. **Insufficient Support for Native Applications**

   SAML was created to primarily focus on web browser-based applications. The protocol depends on web browsers for many of the protocol exchanges that take place, such as redirects and form posts. As cited in **Wikipedia**,

> “The single most important use case that SAML addresses is web browser single sign-on (SSO).”

   The fact that SAML was created as a solution for web browser SSO is the reason that Single Sign-On products do not work well for native applications. A software developer who would like their product to work with SAML is forced to embed web-based forms into their applications, mimic the behavior of a web browser, perform parsing of XML and HTML and deal with the complexities of the user interface during the process.

The emergence of App Stores for distribution of native applications to devices and computers increases the complexity of developing SAML integration, since often times the same app is deployed to both SSO and non-SSO users. Many products in the app stores were designed for mass market users, not necessarily for Enterprise. Therefore, major rewrites of the applications must take place to support both login flows. New and emerging software companies don’t always prioritize the development of SAML features. It takes significant effort to build, deploy and test this functionality.

3. Insufficient Support for Legacy Applications

Many enterprises utilize legacy applications that simply do not support SAML-based authentication for various reasons. IT organizations need to be able to roll out an SSO solution with full coverage of these applications and in many cases it could take months or years to implement the necessary software changes to a legacy platform - not to mention the risk in causing other bugs or unforeseen issues.

4. Limited Use Cases for IT and Non-Password Based Data

For the aforementioned reasons, there are many services and applications that companies use which do not support SAML or will never support it based on the architecture and use case. IT departments and employees with access to IT-related products and services often require the use of passwords or other credentials.
A few examples of this include:

- Logging into a server or a network appliance
- Storing SSH and other private keys
- API access keys and cloud credentials
- Bank account / financial information
- Private customer information
- Confidential photos and videos
- Social media accounts
- Shared passwords
- Custom applications

When an application falls outside of the SSO scope, the end result is that the employee typically resorts to bad password management habits.

As written by Forrester in a recent Best Practices report (December 2017):

> **“While technologies such as two-factor authentication (2FA), web single sign-on (SSO), and privileged identity management are helping to reduce reliance on static, easy-to-hack passwords, security teams still require passwords and use them to authenticate employees into a range of commercial and custom applications.”**

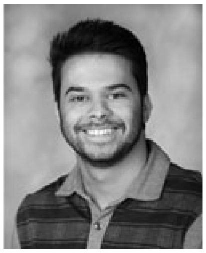
While SSO solutions continue to grow and do indeed provide invaluable security services to organizations, many SSO users also supplement and further bolster their security profile by adding a comprehensive password management solution to their portfolio. Password management solutions with secure password generators and auto-fill capabilities provide the same type of single sign-on functionality for sites and services that don’t support SAML-based login. They also give IT significant visibility into the overall password practices of every employee, and provide the tools to enforce good habits.

The better password managers include separate digital vaults for business and personal passwords, which is vital given the BYOD nature of business users today. Employees can take their personal passwords with them if they leave the company while the business passwords stay behind.

5. **Inherent and Significant Security Gaps**

   Due to the limited coverage of SSO solutions, significant security gaps exist. A plethora of native and cloud applications are not covered by SSO solutions and thus, cannot be integrated as an SSO service. Further, SSO solutions are not digital vaults – they cannot manage, encrypt or store files, photos, videos, notes, codes, keys, certificates and other sensitive digital assets that can result in a data breach. The outlier passwords and assets not covered by SSO represent a major security threat to an organization. The protection of every password and sensitive digital assets counts because these assets are primary attack vectors for hackers.

Case Study: MRA Associates boosts its SSO profile



A good example of this strategy of pairing an SSO solution with a comprehensive password manager is given by the experience gained at MRA Associates. This Phoenix-based, fully independent investment adviser differentiates itself from the constellation of wealth management and advisory firms by being 100% partner-owned and managed, boasting absolutely no influence from banks, shareholders, or corporate overlords. MRA has about 60 employees in three locations.

According to Zack Feldman, MRA's Technology Associate, the company's employees are continuously accessing various online services and resources, including email, financial products, HR resources, and various Web-based SaaS services, to name a few. All these and other resources require separate logins. It is imperative at MRA that employees have ubiquitous access from their smartphones, laptops and tablets. Some of these devices are employee-owned, complying with MRA's BYOD policies.

Reaping the Benefits of SSO

About two years ago MRA began using ADFS Server from Microsoft. With its integration with MS Active Directory, this solution is designed to bring benefits for business applications such that users can have easy and quick access to a high trust key and digital certificates held within ADFS Server. These can be used to create digital signatures on business documents and data. ADFS server has proven a boon to employees that use just one login and user name to access any sites or services supporting ADFS. For IT, Feldman said security has gotten a great boost from the SSO's centralized management. As an example, if an employee leaves, it is a simple matter for IT to disable his or her access to all sites immediately, Feldman notes.

However, this single point of failure feature is a double-edged sword. Should the server fail for any reason, employees have no site and services access unless you set up multiple ADFS servers, which is often beyond the reach of smaller organizations.

Filling the Gaps

Feldman noted there is one other shortcoming of the SSO solution. Not all vendors and products support ADFS and SSO solutions in general, as previously discussed. As Feldman says with respect to certain sites and services, "There are always outliers." Outliers must be protected noting they represent digital assets that are often more sensitive than web-based sites and applications.

Thus, MRA needed a comprehensive password management solution to remedy these shortcomings with SSO without overburdening employees or interfering with seamless access to services. Without such a solution, Feldman says, passwords for these sites and services not supporting SSO may well be kept on an Excel spreadsheet, which is hardly a secure solution. Also if an employee who may have securely shared passwords with others leaves the company, then all passwords must be manually changed. Finally the very small Operations team at MRA can easily be overburdened by password-related helpdesk requests, such as password resets or forgotten passwords, in the absence of a comprehensive password manager.

Feldman and MRA turned to Keeper Security and its Password Manager & Digital Vault. Keeper's integration with current Active Directory and SSO systems (Keeper® SSO Connect) was a big selling point, along with Keeper's proprietary, zero-knowledge security architecture. Keeper's 'zero-knowledge' digital vault insures that IT has complete visibility into employees' use of strong (or weak) passwords, but no one at the MRA or at Keeper can ever access the actual passwords in use. Keeper SSO Connect is an application that runs on-prem at the client. It is a service provider to all SSO systems that allows users to directly access their Keeper Vault using their SSO credentials. It takes any SSO solution and turbocharges it with a ubiquitous digital vault. Keeper SSO Connect enables every SSO solution to provision and govern access to any type of system, website or application (native and web) and secure any type of digital asset (files, photos, videos, notes, lists, codes, digital certificates, SSH keys, etc.). It protects every password and sensitive digital asset in an organization.

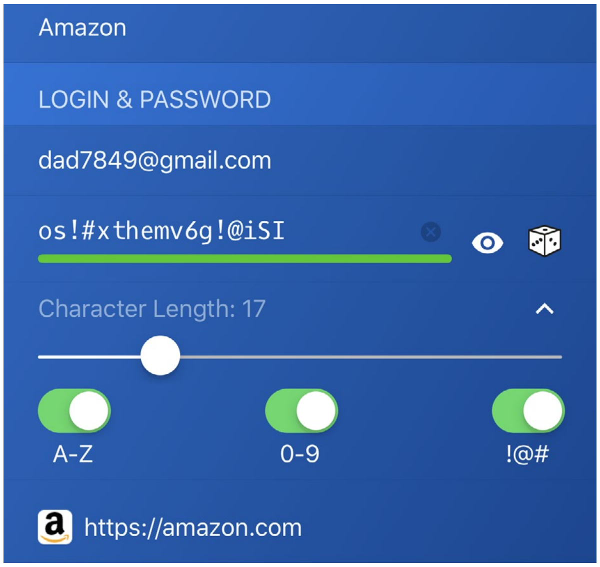
Now, with just one single sign-on, employees access the Keeper solution, which auto-fills every site and service with a highly secure, machine generated password. Feldman says that once these passwords were imported into the Keeper solution, the rest 'was very easy', adding that employees eagerly embraced it, such as the operations team which was an early user.

The Keeper Advantage

Zero-Knowledge Digital Vault

Every user 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.


Amazon

LOGIN & PASSWORD

dad7849@gmail.com

os!#xthemv6g!@iSI

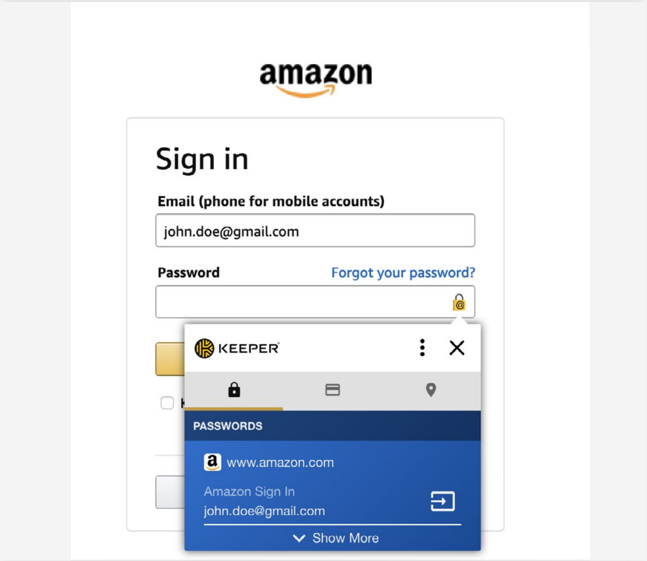
Character Length: 17

A-Z 0-9 !@#

https://amazon.com

Generate Strong Passwords

Creating unique and strong randomly generated passwords for each website is critical to limiting the risk of a data breach and improving the overall security posture of an organization. Keeper's secure password generator is available across every platform and device type.



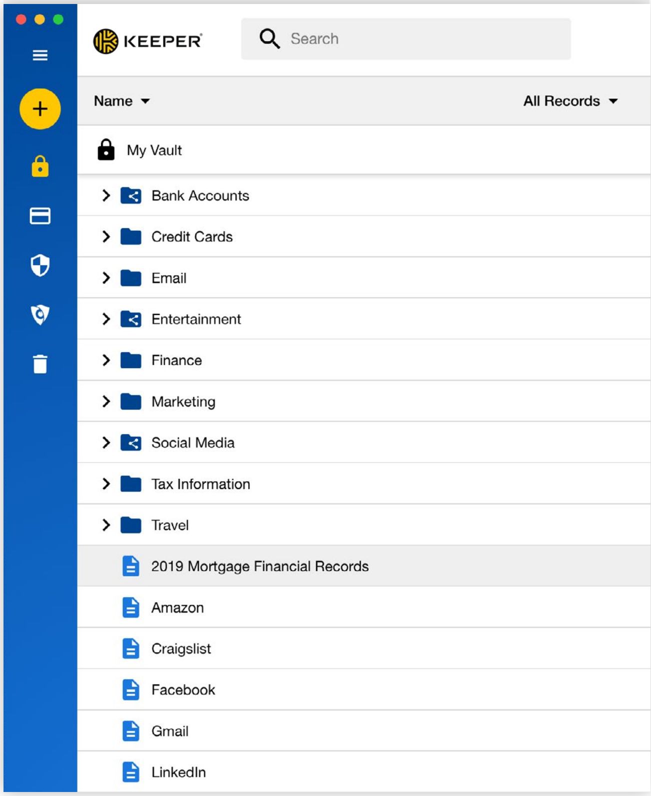
Email (phone for mobile accounts): john.doe@gmail.com

Password:

www.amazon.com
Amazon Sign In
john.doe@gmail.com

KeeperFill for web browsers provides a powerful and easy-to-use autofill feature. Various paths and scenarios are covered by the browser extensions, including the following:

- Filling a login and password
- Selecting from multiple passwords on the same website
- Automatically filling a password
- Prompting to fill or manual click to fill
- Saving new passwords to the vault as you type

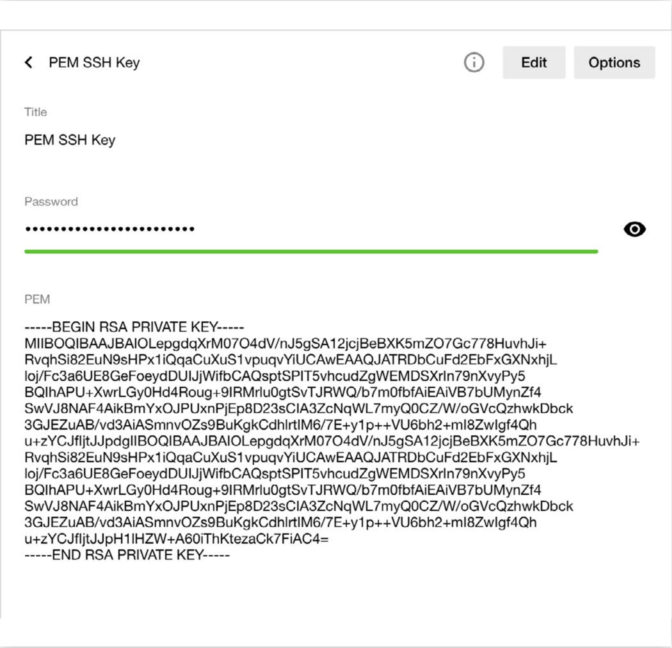


My Vault
- Bank Accounts
- Credit Cards
- Email
- Entertainment
- Finance
- Marketing
- Social Media
- Tax Information
- Travel
- 2019 Mortgage Financial Records
- Amazon
- Craigslist
- Facebook
- Gmail
- LinkedIn

Protecting Confidential Files, Photos and Videos

Keeper protects confidential files with 256-bit AES encryption using record-level keys, just like its password encryption technology. Users can drag-and-drop files into the vault or take pictures & videos directly from mobile devices. Examples of files that might be stored in the vault include:

- Customer information
- Employee census data
- Financial statements
- Banking information
- Tax returns
- Medical photos and videos
- Personal identifiable information



Title
PEM SSH Key

Password
••••••••••••••••••••••••

PEM

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOQIBAAJBAIOLepgdqXrM07O4dV/nJ5gSA12jcjBeBXK5mZO7Gc778HuvhJi+
RvqhSi82EuN9sHPx1iQqaCuXuS1vpuqvYiUCAwEAAQJATRDbCuFd2EbFxGXNxhjL
loj/Fc3a6UE8GeFoeydDUIJjWifbCAQsptSPIT5vhcudZgWEMDSXrIn79nXvyPy5
BQIhAPU+XwrLGy0Hd4Roug+9IRMrlu0gtSvTJRWQ/b7m0fbfAiEAiVB7bUMynZf4
SwVJ8NAF4AikBmYxOJPUxnPjEp8D23sCIA3ZcNqWL7myQ0CZ/W/oGVcQzhwkDbck
3GJEZuAB/vd3AiASmnvOZs9BuKgkCdhlrtIM6/7E+y1p++VU6bh2+mI8ZwIgf4Qh
u+zYCJfljtJJpdgIIBOQIBAAJBAIOLepgdqXrM07O4dV/nJ5gSA12jcjBeBXK5mZO7Gc778HuvhJi+
RvqhSi82EuN9sHPx1iQqaCuXuS1vpuqvYiUCAwEAAQJATRDbCuFd2EbFxGXNxhjL
loj/Fc3a6UE8GeFoeydDUIJjWifbCAQsptSPIT5vhcudZgWEMDSXrIn79nXvyPy5
BQIhAPU+XwrLGy0Hd4Roug+9IRMrlu0gtSvTJRWQ/b7m0fbfAiEAiVB7bUMynZf4
SwVJ8NAF4AikBmYxOJPUxnPjEp8D23sCIA3ZcNqWL7myQ0CZ/W/oGVcQzhwkDbck
3GJEZuAB/vd3AiASmnvOZs9BuKgkCdhlrtIM6/7E+y1p++VU6bh2+mI8ZwIgf4Qh
u+zYCJfljtJJpH1lHZW+A60iThKtezaCk7FiAC4=
-----END RSA PRIVATE KEY-----
```

Protect Secure Certificates and SSH Keys

The growing threat of trust-based attacks is opening security risks for IT organizations who rely heavily on access to critical systems via digital certificates and keys. Keeper protects certificates and keys with 256-bit AES zero-knowledge encryption. Examples of the types of certificates that can be stored include:

- SSL Certificates
- SSH Keys
- RSA Key Pairs
- Code Signing Certificates
- API Keys

Share a Password With a Colleague or Team

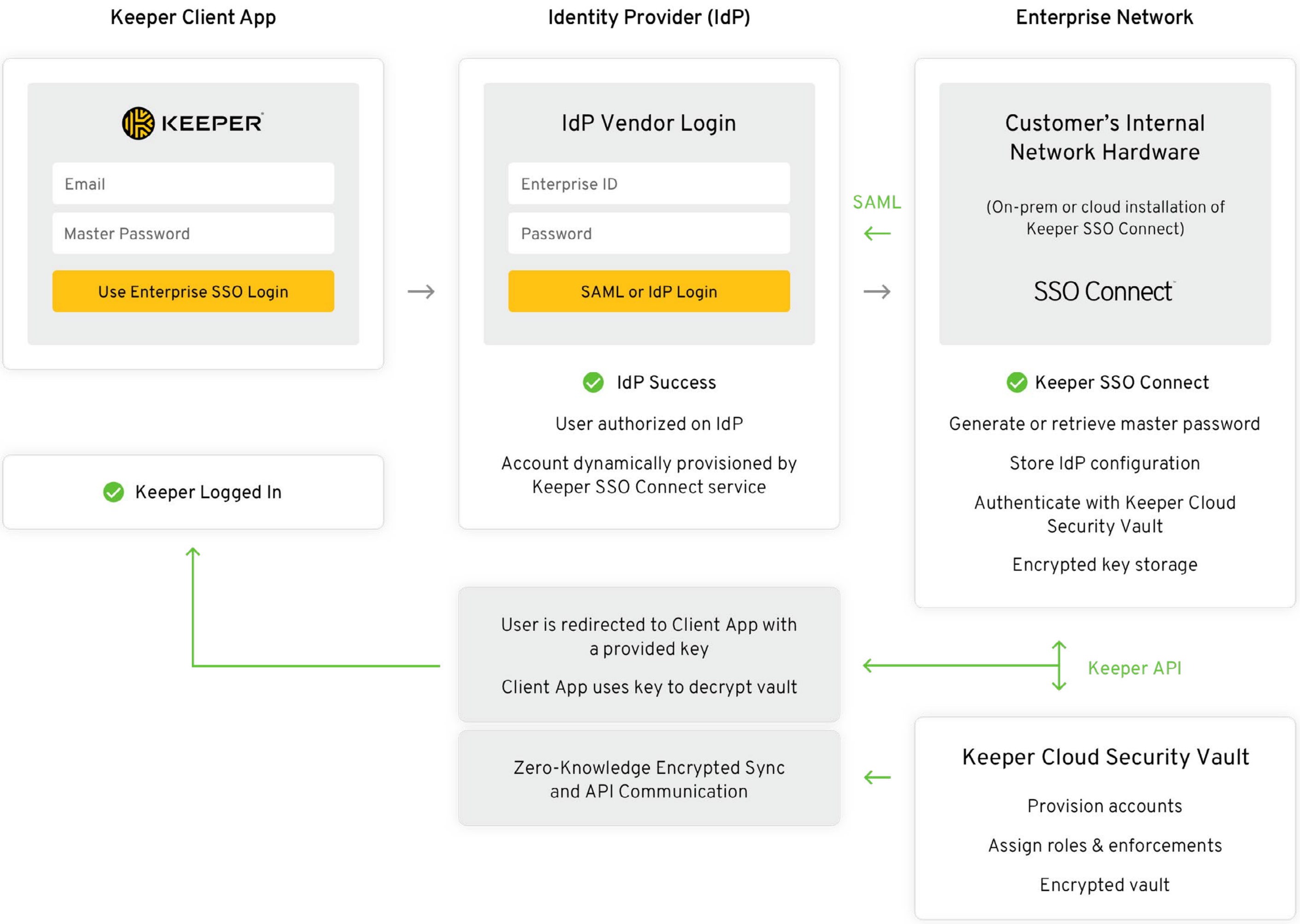
Keeper uses RSA encryption to share passwords and files. If permitted by the enterprise, users on the Keeper platform can share passwords or files directly with another Keeper user or with a team. Behind the scenes, information is encrypted with the recipient's public key and decrypted with their private key. Permissions can be assigned to individual users, or to teams of users.

Separate Business and Personal Info

Since Keeper Enterprise provides a mechanism for Administrators to suspend and transfer end-user vaults, Keeper Security recommends that end-users keep business and personal vaults separate. This can be done easily using Keeper's Account Switching features. Every platform supports the ability to easily switch between business and personal vaults.

Monitor the Security Score of the Company

The overall security score can be monitored by delegated Keeper administrators to ensure compliance with password policies. Detailed reports identify users who need to take corrective action. The record password strength, master password strength and two-factor authentication usage is monitored.



Keeper Client App

KEEPER

Email

Master Password

Use Enterprise SSO Login

Keeper Logged In

Identity Provider (IdP)

IdP Vendor Login

Enterprise ID

Password

SAML or IdP Login

IdP Success

User authorized on IdP

Account dynamically provisioned by Keeper SSO Connect service

User is redirected to Client App with a provided key

Client App uses key to decrypt vault

Zero-Knowledge Encrypted Sync and API Communication

SAML

Enterprise Network

Customer's Internal Network Hardware

(On-prem or cloud installation of Keeper SSO Connect)

SSO Connect

Keeper SSO Connect

Generate or retrieve master password

Store IdP configuration

Authenticate with Keeper Cloud Security Vault

Encrypted key storage

Keeper API

Keeper Cloud Security Vault

Provision accounts

Assign roles & enforcements

Encrypted vault

Integration With Existing Identity 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.

Keeper SSO Connect is an SAML application that leverages Keeper's zero-knowledge security architecture to securely and easily authenticate users into their personal Keeper Vault. Users can be dynamically provisioned to their Keeper Business account upon their first successful authentication on SSO.

Businesses require a password manager and digital vault solution in a zero-knowledge environment that stores not only a login and password, but also proprietary customer data, access credentials to restricted systems and sensitive documents.

Summary and Comparison of Capabilities

Enterprise Single Sign-On

- Eliminates repetitive logins for cloud-based web applications
- Provides fast access to a pre-defined set of applications
- Relies on SAML or screen scraping technology which can be costly to manage
- Potentially requires insecure storage of credentials
- Does not address the need for different levels of secure access
- Lacks seamless support for multiple user interfaces (client, web, mobile, etc.)
- A single point of failure in the event of downtime
- Potentially cost-prohibitive based on the size of your organization

Keeper Enterprise

- Cost effective – fraction of the cost of deploying SSO
- Quick and easy to scale and deploy
- Works across all platforms, operating systems and mobile devices
- Provides admin console with security enforcements, role based access and delegated admin
- Protects passwords, files or any other type of information with zero knowledge architecture
- Reduces both problems with passwords and helpdesk load
- Contains Self-Destruct feature to protect against brute force attacks
- Integrates with multi-factor authentication and biometric solutions
- Automates the storage and collection of user credentials
- Simplifies the creation of unique and secure passwords

Benefits of combining Keeper Enterprise with Single Sign-On

- Secure and seamless login for any application or service across all devices
- Secure, digital vault storage of other critical data
  (e.g. server credentials, certificates and highly confidential documents)
- No need for user to remember passwords – it is stored and randomized in the Keeper Vault
  using zero-knowledge encryption technology

Conclusion

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 (Enterprise Password Management) 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.

To learn more about how Keeper EPM and Keeper SSO Connect can help your organization, please contact sales@keepersecurity.com.

Business Sales

Americas & APAC
+1 312 829 2680

United Kingdom
+44 20 3405 8853

Germany & DACH
+49 89 143772993

Ireland
+353 21 229 6020

EMEA
+353 21 229 6011

Netherlands
+31 20 262 0932

Iberia & Italy
+34 919 01 65 13

Sweden & Nordics
+46 8 403 049 28

Support

Consumer
+1 312 971 5702

Business (Americas & APAC)
+1 312 226 4782

Business (EMEA)
+353 21 229 6019