Keeper SSO Connect

Whitepaper
**What is Keeper SSO™ Connect?**

Keeper SSO Connect is a SAML 2.0 and OpenID Connect application which leverages Keeper’s zero-knowledge security architecture to securely and seamlessly authenticate users into their Keeper Vault and dynamically provision users to the platform. Keeper SSO Connect works with popular SSO IdP platforms such as Okta, OneLogin, Ping Identity, F5 BIG-IP APM, G Suite and Microsoft ADFS / Azure to provide businesses the utmost in authentication flexibility.

**What is the Use Case for Keeper SSO Connect?**

Many businesses use Single Sign-On (SSO) solutions that are already integrated into an Active Directory or LDAP environment. These solutions offer a unified login experience to proprietary or other business cloud applications. The administrator of the SSO solution selects specific applications (e.g. Service Provider "SP") from a set list of preconfigured apps and can provision those apps to users within the organization. The method of logging into one of these service providers depends primarily on the SP’s implementation of the SAML protocol and the ability to dynamically provision user accounts.

For applications that either don’t support SAML or are not accessed through a web browser authentication scheme, traditional SSO Identity solutions lack the flexibility to store a variety of sensitive information beyond a simple username and password record. More specifically, these solutions can’t accommodate login credentials for native applications, bank account numbers, personal identifiable information, employee census data, customer credentials and confidential images, documents and video files.

From a functional perspective, here are the general issues covering traditional SSO Identity solutions:

- Limited to authenticating a user into cloud-based applications
- Suboptimal user experience across mobile platforms and devices
- Unable to store anything besides a username and password
- Not zero-knowledge (Identity provider and admins can view stored data)
- Lack of administrative controls over password generation and usage
- No cross-platform syncing and management of passwords
- No ability to share credentials among users, teams and shared folders
- No password rotation capabilities
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.

System Requirements

Keeper SSO Connect is a software application that is installed on the enterprise customer’s on-premise, private or cloud servers. Users encryption keys are generated dynamically by Keeper SSO Connect, encrypted and stored locally on the installed server, providing the customer with full control over the encryption keys that are used to encrypt and decrypt their digital vaults.

The Keeper SSO Connect service application can be installed on a private on-premise or cloud-based server. Windows, Mac OS and Linux operating systems are supported.

System Architecture
Installation & Setup

The steps for setting up Keeper SSO Connect are as follows:

1. Enable SSO Connect from the Keeper Admin Console
2. Install Keeper SSO Connect on your server (supports Windows, Mac, Unix/Linux)
3. Configure Keeper as a SAML 2.0 service provider on your existing Identity Provider

Activating SSO Connect from the Admin Console

Visit the Keeper Admin Console at https://keepersecurity.com/console and login as the Keeper administrator.
Show Node Structure

SSO integration is applied to specific nodes (e.g. organizational units) within your Admin Console. To display the node structure, click on "Advanced Configuration" then "Show Node Structure".
Create SSO Node

Click on the "+" button to create a new node which will host the Keeper SSO Connect integration. The node can be anywhere in your organizational structure. In the below example, the node is called "SSO" and added beneath the root node.

Click "Create" then select the node.
Click on the "Bridge / SSO" tab.

<table>
<thead>
<tr>
<th>Users</th>
<th>Roles</th>
<th>Teams</th>
<th>2FA</th>
<th>Bridge / SSO</th>
<th>License</th>
</tr>
</thead>
</table>

**Keeper Bridge**

Keeper Bridge is a Windows application that communicates with Active Directory and LDAP-based Directory Services for automating the Keeper onboarding and role mapping process.

**Manage Bridge for SSO - OKTA**

**Keeper SSO Connect™**

Keeper SSO Connect is a SAML 2.0 compatible Service Provider (SP) application that allows Keeper Business customers to seamlessly login to their Keeper Vault using their existing identity provider (IdP). This application complies with Keeper's zero-knowledge security architecture while giving business customers the flexibility of providing seamless SSO login to their Keeper Vault.
Click on the "+ SSO Connection" link.

**SSO Connection**

Manage SSO Connect for Acme Corp

SSO Connect URL
190.123.123.445/880/sso-connect

Node
Acme Corp

Enterprise Domain
e.g. mycompanyssso

New User Provisioning
- Dynamically provision users upon successful login to SSO
- Invite manually or use Keeper Bridge

SSO Connection Node
Each SSO Connection can be associated with a node. Therefore, your organization is able to create multiple SSO connections assigned to different nodes. To move an existing SSO Connection to a different node, click on the pencil icon.

Dynamic User Provisioning
Users can be dynamically provisioned to your Keeper Business account upon their first successful authentication on SSO. For the best user experience, we recommend selecting this option.

You can also manually invite users through the Admin Console "Users" tab or invite users via the Keeper AD Bridge.
Enterprise Domain

Every SSO Connection must be uniquely identified through the use of a supplied "Enterprise Domain" alias. This alias should be named something that is easy for your users to remember because they may need to type the name into their mobile and apps (iOS, Android, Mac, Windows) upon first logging into a new device.

Install Keeper SSO Connect

Next, click on the "Download for Windows" or "Download for Mac" link on the "Bridge" tab in the Keeper Admin Console to download the service application.

Login to Keeper SSO Connect

After installation, login to Keeper SSO Connect with your Keeper Administrator email address and master password.
If you use a proxy server in your environment, click on the gear icon and select the proxy type and/or authentication.

The first time logging in, you will be prompted to select the SSO node from the admin console:
After selecting the SSO Connect endpoint, you will be taken to the Keeper SSO Connect configuration page:
By default, the Server Base URL is automatically assigned. It will default to the local IP address of the computer, with port 8443. If users will be accessing Keeper SSO Connect from outside of your internal network, the URL must be publicly accessible, and the port number must pass through your firewall to the service.
Identity Provider Setup

From your Identity Provider, download the "Identity Provider metadata" file. Upload this file into the Keeper SSO Connect interface by dragging and dropping the file into the Setup screen:

Click "Save" and your setup is complete.
Logging and Monitoring

The Keeper SSO Connect "Incident Log" screen contains all activity, such as new account creation and errors. This screen is helpful in the initial deployment and testing, to ensure that all system functions are performing optimally.
The Keeper SSO Connect application runs as a service. Closing out the user interface does not stop the service. To fully stop the service, exit the application from the system tray.

Windows:

Mac OS:
Logging into the Keeper Vault

Your users can access Keeper from the "Applications" screen of your Identity Provider. Or, they can access Keeper directly from our Web App, Mobile Apps or Desktop applications.

For example, from the Web App, visit https://keepersecurity.com/vault
Click on "Enterprise SSO Login"

Then enter the Enterprise Domain as provided by the Keeper Administrator, then click "Connect".

The user will be routed to Okta to authenticate, then logged into their Keeper vault.
Mobile app users can use the same flow by selecting "Enterprise SSO Login" during signup.
If you have any questions or require assistance in configuring this identity provider, please contact the Keeper Business Support team at: business.support@keepersecurity.com

Thank You!