KEEPER
Cybersecurity Starts Here™

DATASHEET

Automated Provisioning

Automated Provisioning with Keeper Enterprise

Keeper Security transforms the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and increase online productivity. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach.

Migration Towards Unified Directory Services

Identity and access teams strive to build and maintain a unified corporate directory structure that can be utilized across both on-prem and cloud-based infrastructure. Active Directory has been traditionally used in Microsoft-centric environments to control access to resources. As more enterprises move to the cloud, migrations from on-prem AD to Azure AD or a replication between the two environments has been taking place. Directory-As-A-Service (DaaS) products have emerged which unify diverse requirements into a single unified directory.

IT Admins don't want to maintain multiple directory services because it introduces operational complexity, inefficiencies and security vulnerabilities. Controlling access to corporate resources and removing access in an efficient and timely manner is critical for compliance and protecting against data breaches.

Keeper's Automated Provisioning

One of the most important ways to ensure compliance and simplify the rollout and onboarding of Keeper Enterprise is through the use of automated provisioning methods. Keeper Enterprise integrates with both on-premise and cloud-based directory services for the automated deployment and provisioning of password vaults. With Keeper's automated provisioning methods, IT Admins can deploy end-user vaults without having to manage yet another directory of users.

Auto-Provisioning Features

- User onboarding and offboarding
- User authentication through SAML 2.0
- Integration with SCIM
- Team creation and management
- Role enforcement policy management
- Access to shared team folders

SCIM (System for Cross-Domain Identity Management)

Keeper supports SCIM 2.0, a REST-based API using JSON message structure. The Keeper SCIM endpoint supports Users and Groups resources, and the below message types:

Base Product	Teams
Retrieve user information	Retrieve user information
Add a user	Add a team
Update a user profile	Add users to a team
Delete a user	Delete a team

SAML (Security Assertion Markup Language)

Keeper supports SAML 2.0 for provisioning and authenticating users with our proprietary Keeper® SSO Connect software. Keeper SSO Connect is a SAML 2.0 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 supports the following features:

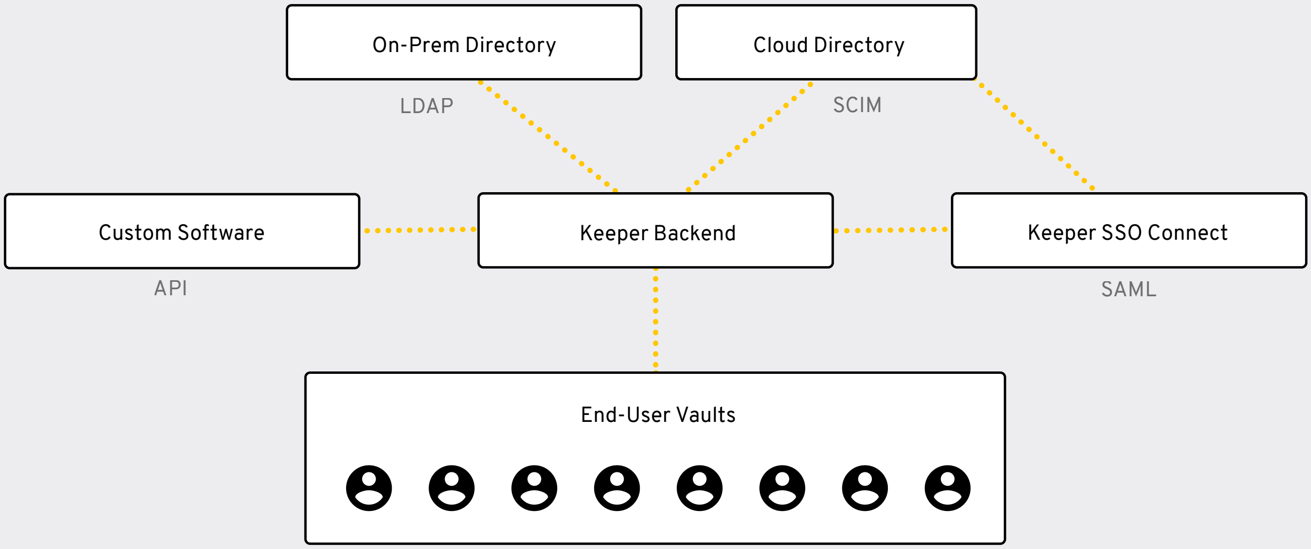
- Seamless authentication with any SAML 2.0 compliant identity provider
- Just-in-time (JIT) provisioning of users
- Access on any platform including desktop, mobile and tablet devices
- Segmentation of SAML-based users and non-SAML user

Exemplary Integrations with Keeper Enterprise*

- On-prem Active Directory sync using the Keeper AD Bridge software
- Microsoft Azure AD integration with SAML 2.0 and SCIM
- G Suite integration through SAML 2.0 and Auto Provisioning through SCIM
- Okta integration through SAML 2.0 and Auto Provisioning through SCIM
- Email-based Provisioning through self service and email verification
- API Provisioning using the Keeper Commander CLI and SDK platform
- Any SAML 2.0 compliant identity provider
- Any SCIM 2.0 compliant directory service or identity provider

*Additional integrations are available based on the customer's provisioning environment.

System Architecture


On-Prem Directory
Cloud Directory
LDAP
SCIM
Custom Software
Keeper Backend
Keeper SSO Connect
API
SAML
End-User Vaults