Enterprise password and passkey management

Protect every employee's passwords, passkeys and sensitive information in an encrypted vault. IT teams gain centralized control over provisioning, authentication, sharing, security policies and reporting, while users get secure access across the devices and applications they use every day.

Keeper Password Manager capabilities

END USER

Passwords and passkeys	Securely store, manage and use passwords, passkeys, payment cards, SSH keys, certificates, identity documents and other sensitive information in the Keeper Vault.
Access across devices	Use the Keeper Web Vault, native desktop applications for Windows, macOS and Linux, iOS and Android applications, and the KeeperFill browser extension for Chrome, Firefox, Safari, Edge, Opera and Brave.
Offline access	Work from an encrypted local copy of the vault when you don't have a connection to Keeper or the identity provider. The device syncs online to cache the vault, and the user then unlocks it with a master password or biometrics.
Autofill	Fill passwords, passkeys, payment cards and other stored information in supported browsers, applications and websites across any device.
Password health	Generate strong passwords and passphrases, identify weak or reused credentials and help users improve password security across the organization.
Record organization	Organize credentials and sensitive information with folders, shared folders, custom record types, file attachments and record history.
Free family plan	Every licensed employee can claim a Keeper Family Plan for personal use, covering up to five family members with unlimited devices. Personal vaults stay separate from the business vault.

Secure sharing and collaboration

END USER

Secure sharing	Share passwords, passkeys, files and other records with authorized users while maintaining Keeper's zero-knowledge security model.
Shared folders and team folders	Give teams access to the credentials and records they need through role-based user and team permissions.
Bidirectional One-Time Share	Securely share passwords, passkeys, files and other records with people outside the organization, even if they do not have a Keeper account. Recipients can make permitted updates, and shares can be restricted by device and expiration date.
Vault transfer	Transfer a departing employee's vault to an authorized recipient when the feature has been configured in advance and the required consent and key-exchange setup are in place.

©2026 Keeper Security, Inc. | Rev. 10.2026

KEEPER

Administration and identity

ADMIN

Admin Console	Manage users, teams, roles, enforcement policies, delegated administration and security reporting from one centralized console.
Provisioning	Provision and deprovision users and teams through SCIM or synchronize users and groups from Active Directory and LDAP through Keeper Bridge. Authentication and provisioning are separate functions.
Single Sign-On (SSO)	Authenticate through SAML 2.0 using SSO Connect Cloud and leading identity providers, including Microsoft Entra ID, Okta, Google Workspace, Ping, JumpCloud, OneLogin and Duo.
Multi-Factor Authentication (MFA)	Support FIDO2 and WebAuthn security keys, authenticator applications, TOTP, Duo and RSA SecurID. Organizations can enforce MFA requirements through administrative policies.
Role-based enforcement	Apply enforcement policies by role across master password complexity, MFA methods, sharing and export, platform and device restrictions, offline access and vault features. Assign roles to teams to keep policy consistent across groups.
IP address allowlisting	Limit a role's users to approved IP address ranges. Keeper evaluates the external public address seen at login, so employees cannot reach the vault from unapproved networks.
Device approval	Use Keeper Automator to streamline device approval and key-exchange workflows while reducing manual administrative steps.

Security and governance

Zero-knowledge architecture	Vault data is encrypted and decrypted on the user's device. Keeper stores encrypted data and cannot access customers' plaintext vault contents. The master password is never sent to Keeper.
Centralized policy enforcement	Administrators can enforce password, authentication, sharing and security policies by user, role, team or organizational node.
Encryption and data protection	Keeper uses AES-256 encryption and layered protection for passwords, passkeys, files, payment cards and other sensitive vault data.
Certifications and authorizations	FedRAMP High Certified, GovRAMP High Authorized, FIPS 140-3 validated cryptography, SOC 2 Type 2, ISO 27001/27017/27018.

Secure add-ons

BreachWatch	Monitor the dark web for breached credentials that match records in employee vaults and alert users and administrators so they can respond. Passwords are hashed on the device before comparison, so Keeper never sees a plaintext password.
Compliance Reports	Run on-demand reports showing which users can access which credentials, at what permission level and through which share path. Reports support SOX and other access control audits and export to PDF, JSON or CSV. Report data is decrypted locally, and only administrators granted the Run Compliance Reports permission can run them.
Advanced Reporting & Alerts Module (ARAM)	Report on more than 300 event types, send alerts by email, SMS or webhook and push events to a SIEM. One external destination is active at a time, and ARAM is required for any destination beyond the built-in activity view.

©2026 Keeper Security, Inc. | Rev. 10.2026