



KEEPER
Cybersecurity Starts Here™

Keeper Enterprise White Paper and Use Cases

March 12, 2019



Table of Contents

End-User Vault

- 1 Deploy Zero-Knowledge Vault to Employees
- 2 Generate Strong Passwords
- 3 Protect All Platforms and Devices
- 4 Autofill Website Passwords with KeeperFill[®]
- 5 Change Passwords and Increase Security with KeeperFill
- 6 Autofill a Native Desktop Application with KeeperFill for Apps
- 7 Stay Organized and Efficient with Keeper's Advanced User Interface Features
- 8 Protecting Confidential Files, Photos and Videos
- 9 Protect Secure Certificates and SSH Keys
- 10 Share a Password With a Colleague or Team
- 11 Separate Business and Personal Info
- 12 Log In with Existing Identity Providers

Administration and Onboarding

- 13 Monitor the Security Score of the Company
- 14 Manage and Onboard Users
- 15 Enforce Role-based Permissions
- 16 Transfer Vaults When Employees Leave
- 17 Audit Event Logs and Perform Forensic Analysis
- 18 Protect against Account Takeover with BreachWatch[®] Dark Web Monitoring

Overview

Passwords represent the greatest security risk to businesses today. With Keeper, your employees have on-demand access to encrypted passwords, websites and applications, increasing their productivity while protecting them with best-in-class security. This document covers the most common use cases of the Keeper Enterprise product.

End-User Vault

Every user is provided a secure and private vault. 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 and mobile devices.
- Share confidential information between users and teams.

1. Deploy a Zero-Knowledge Vault to Employees

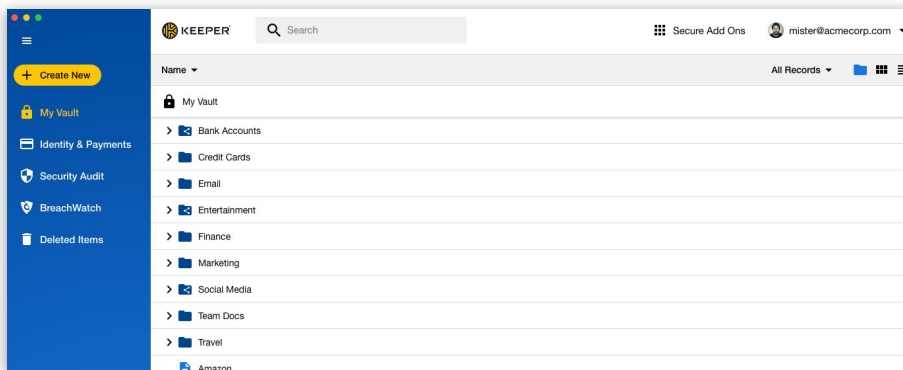
Keeper is a Zero-Knowledge vault that is protected with multiple layers of encryption. Each user's vault is protected by a Master Password which is used to encrypt and decrypt data on the local device. Two-Factor Authentication protects cloud access.

Security Note 1: The Master Password is used to derive an encryption key using PBKDF2, which is used to encrypt and decrypt the vault.

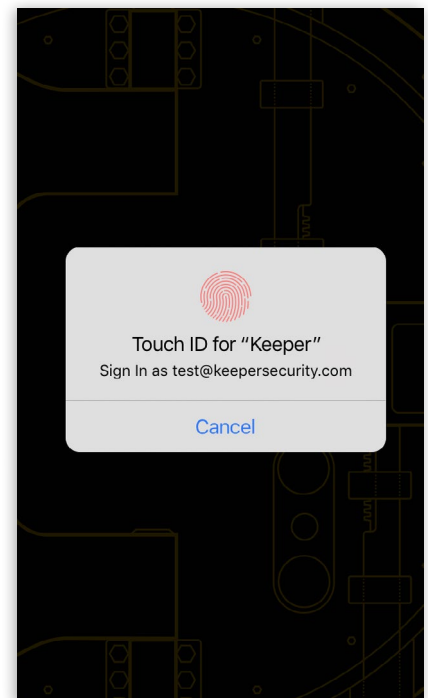
Security Note 2: Each password and file stored in the vault is protected with a separate strong 256-bit AES key.

Security Note 3: Users who login with Keeper SSO Connect integration don't require a master password, as the encryption keys are managed by the Enterprise. Biometrics (Face ID, Touch ID, Windows Hello, etc.) can be permitted as a convenience factor.

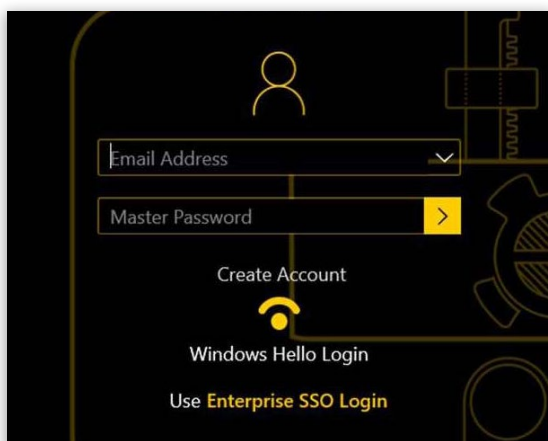
Web Vault / Desktop App for Mac, Windows



iOS Touch ID Login



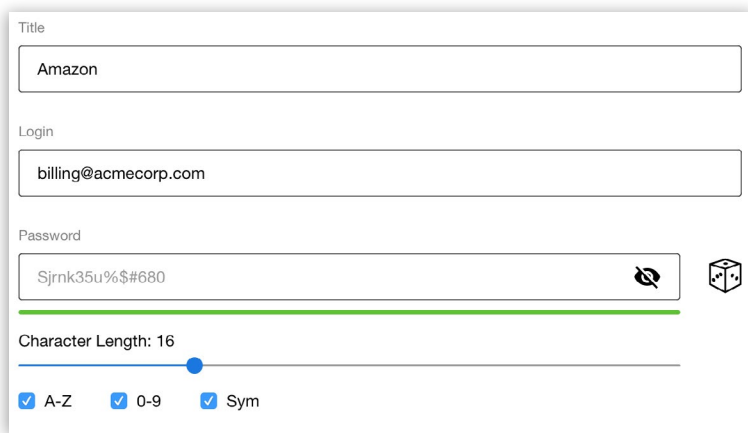
Windows 10 with Windows Hello Biometric Login



2. Generate Strong Passwords

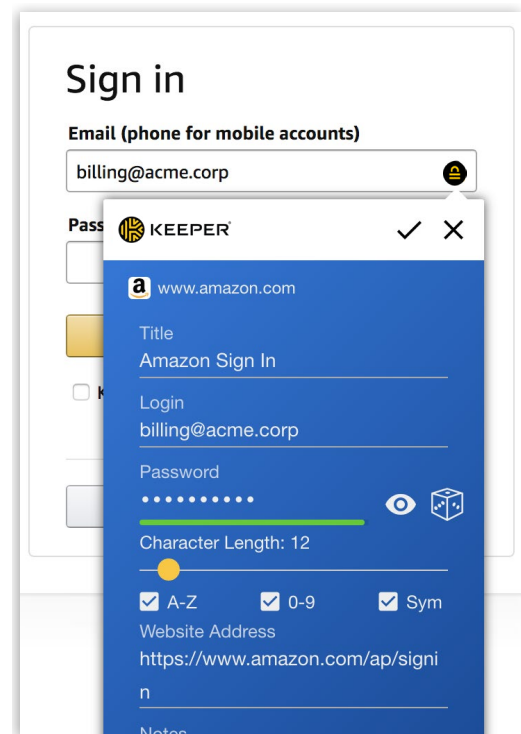
Creating unique and strong randomly generated passwords for each website and service is critical to protecting against a data breach, password stuffing and password spraying attacks. Keeper's password generator and auditing capabilities ensure compliance company-wide.

Web Vault Password Generator



The screenshot shows the 'Web Vault Password Generator' interface. It features three input fields: 'Title' with the value 'Amazon', 'Login' with the value 'billing@acmecorp.com', and 'Password' with the value 'Sjrnk35u%\$#680'. Below the password field is a green progress bar and a 'Character Length: 16' label. At the bottom, there are three checked checkboxes: 'A-Z', '0-9', and 'Sym'. There are also icons for a password strength indicator and a copy function.

Browser Extension – New Record Creation



The screenshot shows the 'Browser Extension – New Record Creation' interface. It features a 'Sign in' form with fields for 'Email (phone for mobile accounts)' containing 'billing@acme.corp' and 'Password'. A blue overlay window is shown in the foreground, displaying the generated record details: 'Title: Amazon Sign In', 'Login: billing@acme.corp', 'Password: [masked]', 'Character Length: 12', and 'Website Address: https://www.amazon.com/ap/signin'. The overlay also shows checked checkboxes for 'A-Z', '0-9', and 'Sym'.

3. Generate Strong Passwords

Keeper protects passwords and private information on all devices and operating systems. Deployment options are available through the Keeper Security website and every popular App Store. SCCM deployments and virtual environments (e.g. Citrix) are fully supported.

Keeper® Desktop App: Fully-featured desktop application for fast and secure access to your Keeper vault.



Mac



Windows



Linux

KeeperFill®: A browser extension that lets you autofill your login credentials in your favorite websites.



Chrome



Firefox



Safari



IE



Edge



Opera

Keeper® Mobile App: Fully-featured mobile application for fast and secure access to your Keeper vault.



iOS



Android



Windows
Store

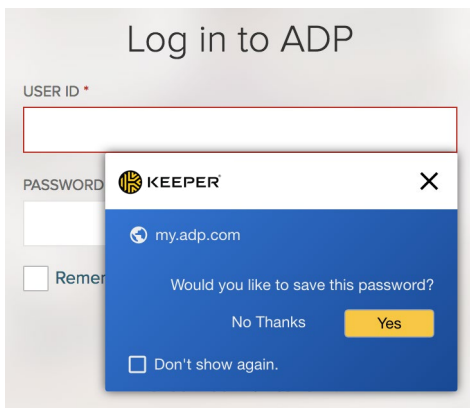
4. Generate Strong Passwords

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:

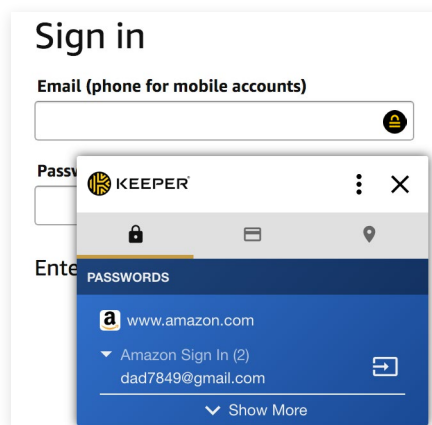
- Filling a login and password
- Selecting from multiple passwords on the same website
- Automatically filling a password (optional)
- Prompting to fill or manual click to fill
- Saving new passwords to the vault as you type

The ability to customize the behavior of the browser extension is covered in the Settings screen of the extension.

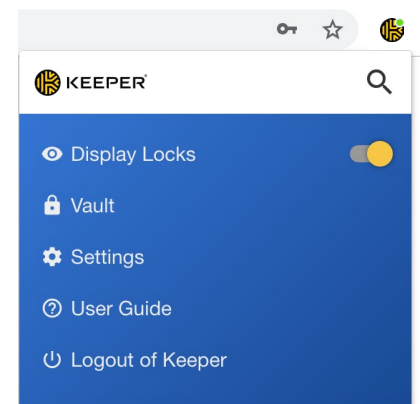
Browser Extension – Autofill Prompt



Browser Extension – Multiple Account Fill

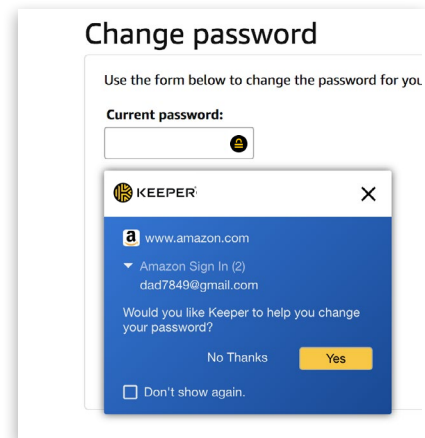
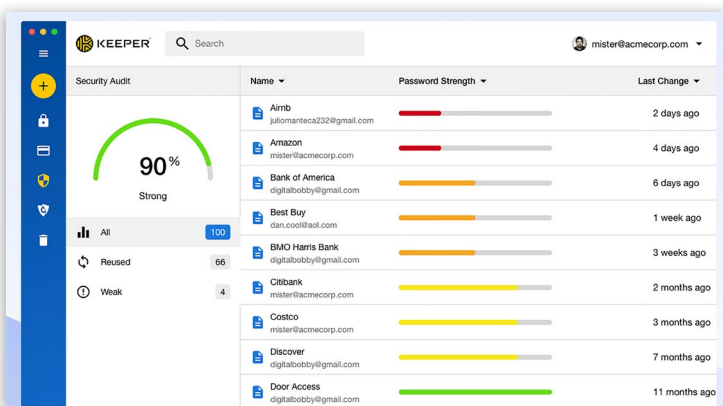


Browser Extension – Options



5. Change Passwords and Increase Security with KeeperFill

Keeper automatically detects password change forms on websites and can rotate your password to a strong auto-generated password with a single click. By using Keeper’s Security Audit screen, you can identify which accounts require an update. On the “Change Password” screen of the website, Keeper will automatically prompt you to update your password.



6. Autofill a Native Desktop Application with KeeperFill for Apps

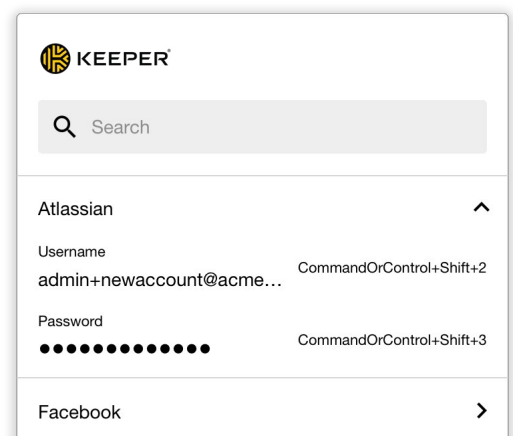
Keeper Desktop provides a unique and powerful native app form fill capability using a simple keyboard hotkey. IT admins who are accessing remote services can make use of this capability without having to resort to “copy” and “paste”. By storing all passwords in the vault and using KeeperFill for Apps, you can be assured that your application passwords are not stored anywhere in plaintext.

KeeperFill for Apps works across Mac and PC platforms with popular native applications such as:

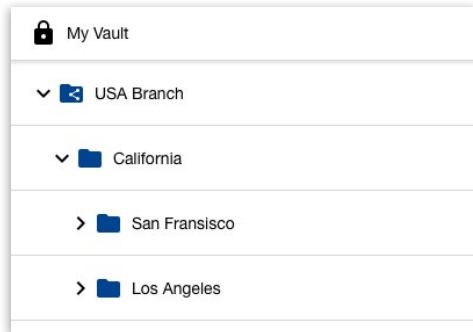
- Skype, Slack, Evernote and other productivity apps
- Custom and/or proprietary applications
- Remote Desktop, VNC, Terminal and other command-line utilities

KeeperFill for Apps is available in the “Settings” screen inside Keeper Desktop.

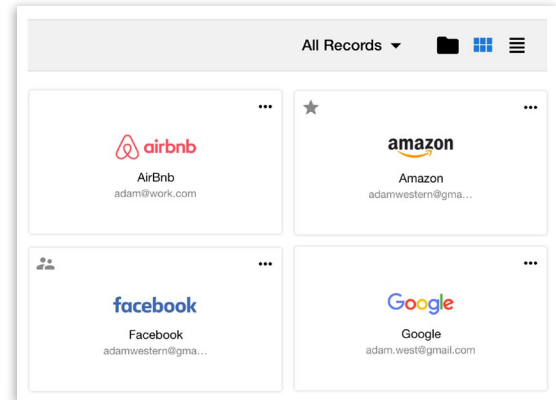
KeeperFill for Apps using Microsoft Remote Desktop on Mac OS



7. Stay Organized and Efficient with Keeper’s Advanced User Interface Features



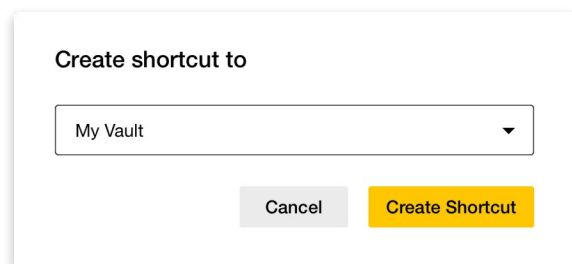
Sub-folders: Sub-folders (or folders within folders) provide greater control and organization over your private Keeper records and files. They increase organization across teams and accounts types.



Grid view layout: Grid view allows you to view your records in a graphical, tile format which displays beautiful, curated logos for popular websites. To enter Grid view, simply click on the grid icon.

Record History	Version
Last Modified Jan 3, 2019 at 5:10 PM CDT	V.5
Last Modified Jan 1, 2019 at 5:10 PM CDT	V.4
Last Modified Dec 31, 2018 at 3:10 PM CDT	V.3
Last Modified Dec 31, 2018 at 2:03 PM CDT	V.2

Record History: Every change made to a record creates a backup version that can be viewed and restored at any time. Deleted records can also be recovered. There is no limit to the number of versions stored.



Creating Shortcuts: A record can exist outside of a folder, inside a folder or inside a shared folder. A record can also be linked into multiple folders or shared folders. A linked record is also referred to as a “shortcut”.

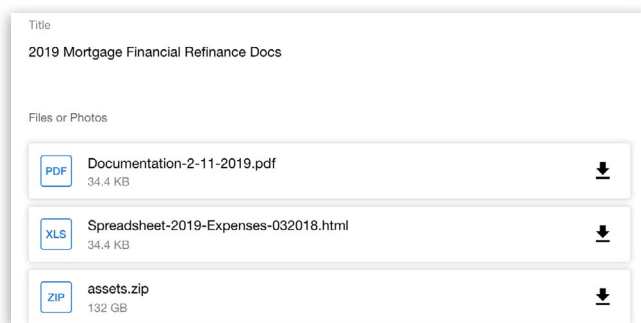
8. Protecting Confidential Files, Photos and Videos

Keeper protects confidential files with 256-bit AES encryption using record-level keys, just like our password encryption technology. You can drag-and-drop files into your vault or take pictures & videos directly from your mobile devices.

Examples of files that might be stored in the vault include:

- Customer information
- Financial & Banking Documents
- Tax Returns
- Medical photos and videos

Example of Financial Documents Stored in the Vault

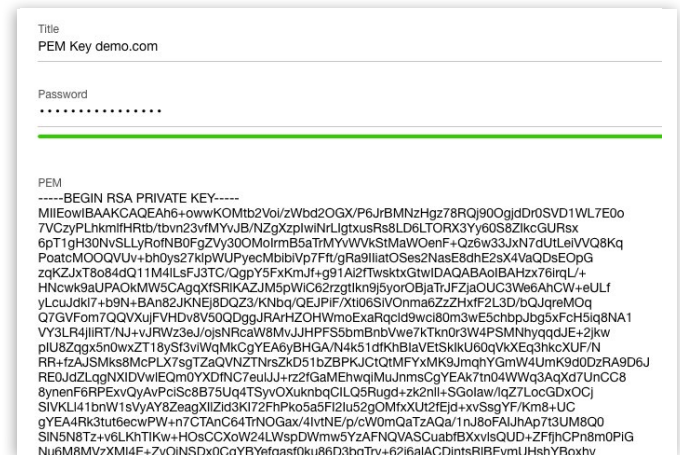


9. Protect Secure Certificates and SSH Keys

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

Example of a Private RSA Key Inside the Vault



10. Share a Password With a Colleague or Team

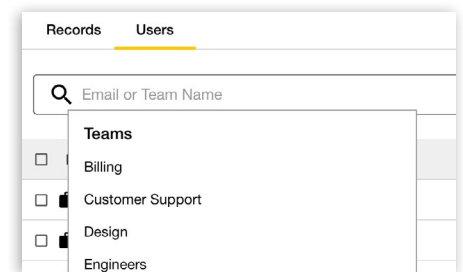
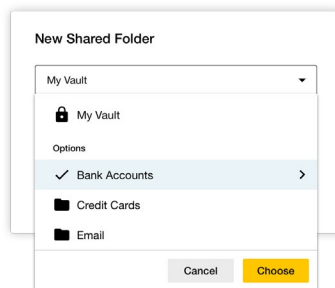
Keeper uses RSA encryption to share passwords and files. You can share passwords or files directly with another Keeper user or with a team. Behind the scenes, information is encrypted with the recipient's public key and decrypted with their private key.

Permissions can be assigned to individual users, or teams of users.

Individual Record Sharing Permissions

Name	User Permissions
dad345@gmail.com (you) Owner	Can Edit & Share
adam@acmecorp.com	Can Manage Records
brian@acmecorp.com	Can Manage Users
danny@acmecorp.com	Can Manage Users
elliott@acmecorp.com	No User Permissions

Sharing a Folder With a Team



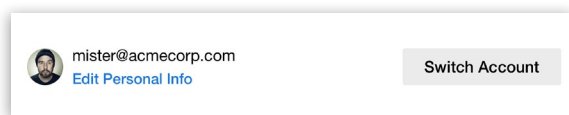
View, edit and share permission sets can be applied to individual users. Shared folder permissions can provide control over the management of the folder, users and records.

Teams are created and managed in the Keeper Admin Console. Teams can also be provisioned automatically using our Active Directory Bridge software, SCIM protocols or the Keeper Commander SDK.

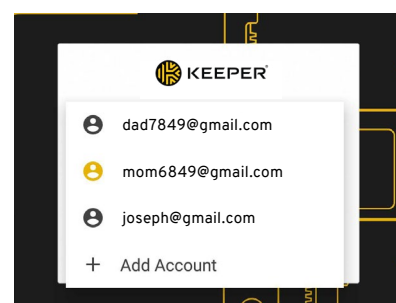
11. Separate Business and Personal Info

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.

Switching Accounts on the Web Vault / Desktop App



Switching Accounts on Mobile Devices



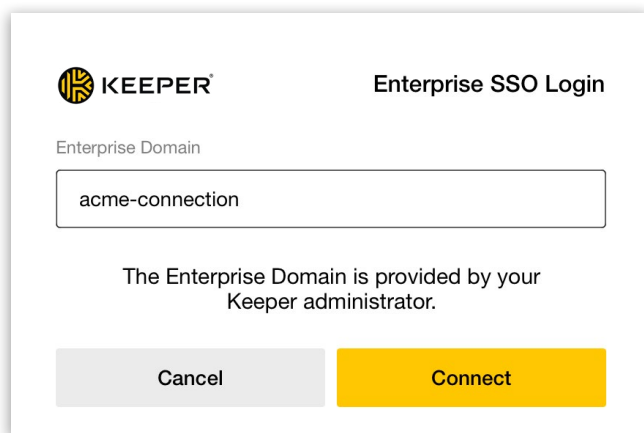
12. Log In with Existing Identity Providers

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 identity provider such as Okta, Centrify, Microsoft AD FS / 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 identify the provider and then launch their Keeper Vault.

User Signs Into Keeper With Enterprise SSO Login



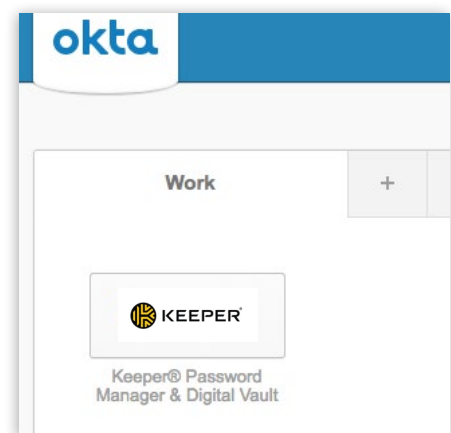
KEEPER Enterprise SSO Login

Enterprise Domain

The Enterprise Domain is provided by your Keeper administrator.

Cancel Connect

Okta End-User Login Flow



Administration and Onboarding

Keeper Enterprise provides a web-based Admin Console application. The Admin Console allows administrators to:

- Onboard and offboard users
- Apply role-based enforcement policies
- Manage two-factor authentication
- Monitor the security score of the organization
- Customize end-user experience

13. 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.

Security Audit Overview of Key Metrics



Security Audit Report Details

Record Password Strength

Search Users Export

User	Weak	Medium	Strong
Ethan King	333	102	221
Brandon Fuller	707	707	177
Sara Graham	755	587	221
Linda Bishop	232	103	177
Linda Wheeler	655	29	221

14. Manage and Onboard Users

Keeper Admin Console provides several solutions to onboard users based on the size of the organization. Users can be provisioned through one of the following methods:

- Active Directory or LDAP sync via AD Bridge
- Single Sign-On (SAML 2.0)
- SCIM and Azure AD
- Email Auto-Provisioning
- CSV File upload
- Manual entry via the web interface
- Command Line Provisioning via Keeper Commander SDK

Different organization units (nodes) can be provisioned in different ways. For example, end-users within one organizational unit can onboard via Active Directory and another group of users can be provisioned with an identity platform like Microsoft Azure or Okta.

User-Provisioning

Add Provisioning Method ✕

Node

- Active Directory or LDAP Sync**
 Provision user accounts through Active Directory or LDAP-based directory services. Keeper Bridge™ software automatically onboard users, assign users to roles and teams.
- Single Sign-On (SAML 2.0)**
 Provision and authenticate users into their Keeper vault using any SAML 2.0 compatible Identity Provider. Keeper SSO Connect™ is an on-premise or cloud based service that seamlessly authenticates users into their Keeper vault and dynamically provisions accounts.
- SCIM and Azure AD**
 Automatically provision users from your Azure Active Directory (AD) account by establishing a SCIM connection.
- Email Auto-Provisioning**
 Automatically provision users based on your organization's domain name.
- Command Line Provisioning**
 Automatically provision users on the command line with Keeper Commander SDK™, our API toolkit.

[Next](#)

Active Directory or LDAP sync via AD Bridge

KEEPER LDAP and Active Directory Interface ✕

Connections LDAP / AD Options

LDAP Connection

Domain Name: LDAP Port: SSL

User Name: Password:

[Test Connection](#)

Keeper Bridge

Users: Registration: Lurey Test, Inc. Active Directory

[Admin Login](#) [Register](#)

Connection Status

Keeper Service	Started
Directory Services	Online
Keeper Cloud	Online
Admin Login	Login Required

[Reset](#) [Publish](#)

Add User ✕

Node

Full Name

Email Address

Import Users
 Quickly import multiple users via CSV format.

Drag and Drop CSV File
or [Choose CSV](#)

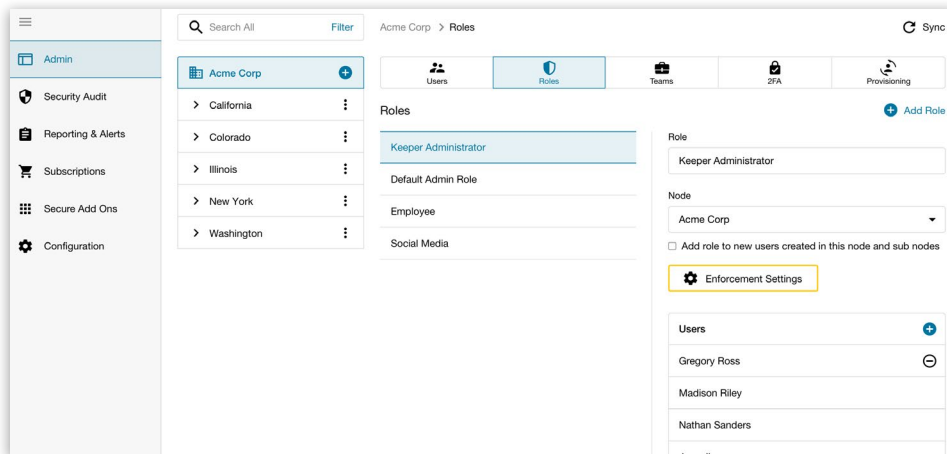
15. Enforce Role-based Permissions

Keeper’s role-based enforcement policies provide organizations with the most flexibility to customize their solution to meet the needs of internal controls. This includes:

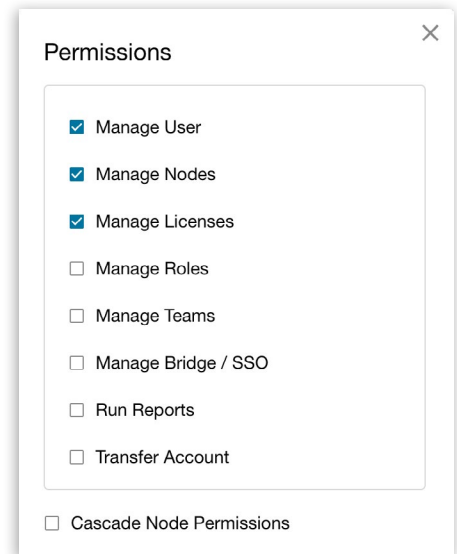
- Onboard and offboard users
- Apply role-based enforcement policies
- Manage two-factor authentication
- Monitor the security score of the organization
- Customize end-user experience

Administrative permissions are also applied at the role level. Any role with administrative permission can log in to the Keeper Admin Console and perform specific job functions.

Role-based Permissions are Fully Customizable



Admin Permissions Settings



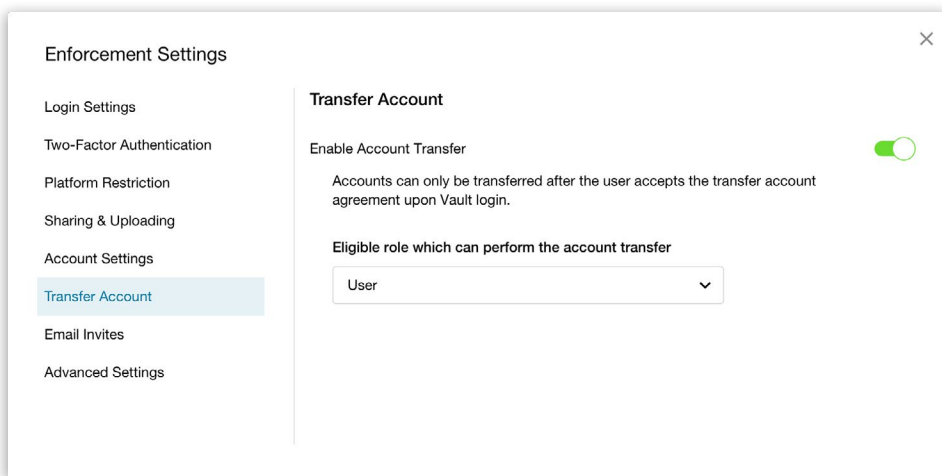
16. Transfer Vaults When Employees Leave

Retaining critical and confidential information is important when employees leave the organization, especially users that are in some administrative or management capacity.

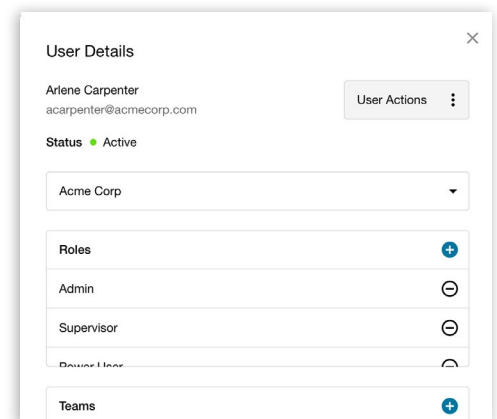
Through the use of Keeper's secure "Account Transfer" feature, a user's vault can be locked and then transferred to another user within the organization. The process of account transfer remains fully zero-knowledge, and the responsibility of performing the account transfers can be limited based on roles within the organization. For example, only the Engineering Manager can transfer the vault of an Engineer. Or the Marketing Manager can transfer the vault of the Marketing Coordinator.

Keeper's security model is based on the least privileged access model. Administration of groups can be delegated and restricted based on job function or any other criteria.

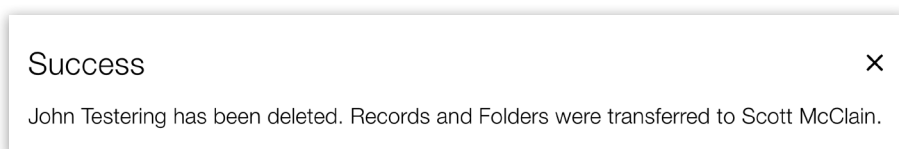
Enabling Account Transfer From the Role Enforcements Screen



Transferring a User's Vault



Account Transfers are a one-directional action. The source account is deleted and the vault records are transferred to another user account.

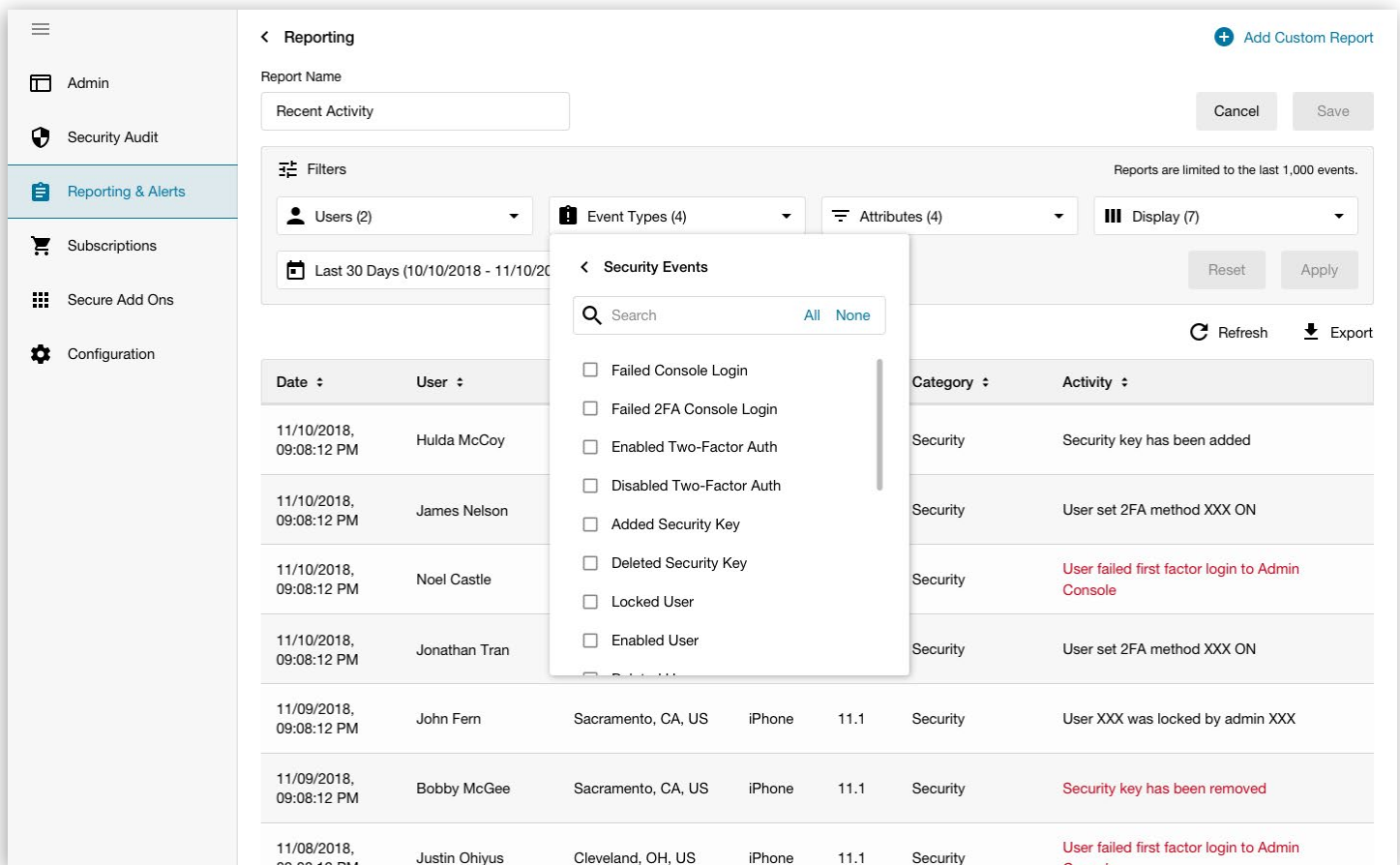


17. Audit Event Logs and Perform Forensic Analysis

Recent Activity

Keeper’s “Recent Activity” section provides event logging and forensic analysis capabilities to comply with corporate governance and audit requirements. Events are tracked throughout the system while maintaining zero-knowledge. Only privileged users with sharing or ownership rights to decrypt individual vault records are capable of viewing the stored vault information.

Recent Activity Report



The screenshot displays the 'Reporting & Alerts' section of the Keeper interface. The main area is titled 'Recent Activity Report' and includes a search bar for the report name (currently 'Recent Activity'), a 'Cancel' button, and a 'Save' button. Below this is a 'Filters' section with dropdown menus for 'Users (2)', 'Event Types (4)', 'Attributes (4)', and 'Display (7)'. A date range filter is set to 'Last 30 Days (10/10/2018 - 11/10/2018)'. A note states 'Reports are limited to the last 1,000 events.' There are 'Reset' and 'Apply' buttons for the filters, and 'Refresh' and 'Export' buttons for the data.

A 'Security Events' dropdown menu is open, listing the following event types:

- Failed Console Login
- Failed 2FA Console Login
- Enabled Two-Factor Auth
- Disabled Two-Factor Auth
- Added Security Key
- Deleted Security Key
- Locked User
- Enabled User

The main table displays a list of events with columns for Date, User, Location, Device, IP, Category, and Activity. The activity column contains details such as 'Security key has been added', 'User set 2FA method XXX ON', 'User failed first factor login to Admin Console', and 'User XXX was locked by admin XXX'.

Date	User	Location	Device	IP	Category	Activity
11/10/2018, 09:08:12 PM	Hulda McCoy				Security	Security key has been added
11/10/2018, 09:08:12 PM	James Nelson				Security	User set 2FA method XXX ON
11/10/2018, 09:08:12 PM	Noel Castle				Security	User failed first factor login to Admin Console
11/10/2018, 09:08:12 PM	Jonathan Tran				Security	User set 2FA method XXX ON
11/09/2018, 09:08:12 PM	John Fern	Sacramento, CA, US	iPhone	11.1	Security	User XXX was locked by admin XXX
11/09/2018, 09:08:12 PM	Bobby McGee	Sacramento, CA, US	iPhone	11.1	Security	Security key has been removed
11/08/2018, 09:08:12 PM	Justin Ohiyus	Cleveland, OH, US	iPhone	11.1	Security	User failed first factor login to Admin Console

Advanced Reporting & Alerts Module

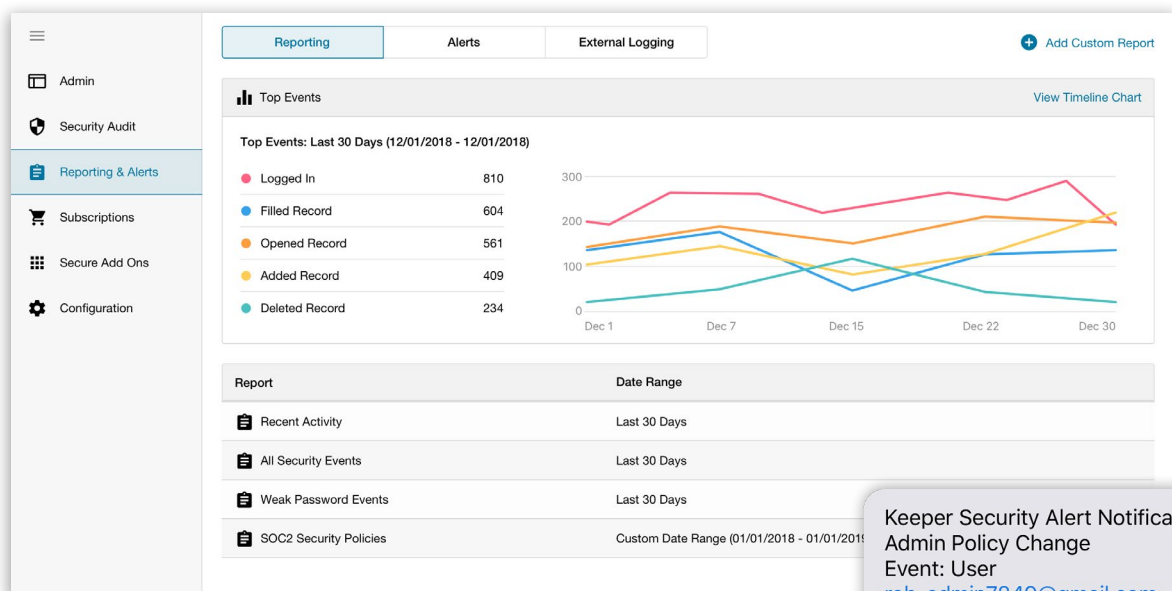
Keeper’s Advanced Reporting & Alerts Module (ARA Module) provides event logging and log event tracking for over 75 event types, the ability to send event based alerts and the capability to log events to an external system. Create customized reports by specifying what criteria to filter and present in each column. Reports can now be filtered and saved based on Event types (Policy Changes, Sharing, Logins, etc), Users, and Attributes (Nodes, Devices, Location, etc).

ARA Module integrates with 3rd party Security Information and Event Management (SIEM) tools for external logging. Integrations include the following:

- Onboard and offboard users
- Apply role-based enforcement policies
- Manage two-factor authentication
- Monitor the security score of the organization
- Customize end-user experience

The ARA Module supports over 75 event types (e.g. Expired Master Password, Changed Master Password, Shared Record, Disabled Two-Factor Authentication etc.) that can be automatically pushed to popular SIEM products such as Splunk, Sumo and QRadar.

Reporting



Alerts

Keeper Security Alert Notification:
 Admin Policy Change
 Event: User rob-admin7849@gmail.com
 changed enforcement REQUIRE_ACCOUNT_FOLDER to OFF
 for role 47377784242320
 Occurred: 3/11/2019, 7:54:34 PM UTC

18. Protect against Account Takeover with BreachWatch® Dark Web Monitoring

Keeper’s “Recent Activity” section provides event logging and forensic analysis capabilities to comply with corporate governance and audit requirements. Events are tracked throughout the system while maintaining zero-knowledge. Only privileged users with sharing or ownership rights to decrypt individual vault records are capable of viewing the stored vault information.

BreachWatch®

