Keeper Enterprise
White Paper and Use Cases
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 facts.
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](image1)

![Browser Extension – New Record Creation](image2)
3. Protect All Platforms and Devices

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.

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

KeeperFill®: A browser extension that lets you autofill your login credentials in your favorite websites.
4. Autofill Website Passwords with KeeperFill®

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.
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.

![Keeper Security Audit Screen](image1)

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 on Mac OS](image2)
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: 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”.

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Vault</td>
<td>V.5</td>
</tr>
<tr>
<td>USA Branch</td>
<td>V.4</td>
</tr>
<tr>
<td>California</td>
<td>V.3</td>
</tr>
<tr>
<td>Los Angeles</td>
<td>V.2</td>
</tr>
<tr>
<td>San Francisco</td>
<td></td>
</tr>
</tbody>
</table>
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 & videos

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
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.

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.
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 identity the provider and then launch their Keeper Vault.
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

<table>
<thead>
<tr>
<th>Security Audit Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Security Score</td>
</tr>
<tr>
<td>76%</td>
</tr>
</tbody>
</table>

This is your organization's overall security audit score based on the factors below. Please notify users for any scores that fall below your acceptable internal control policies.

<table>
<thead>
<tr>
<th>Record Password Strength</th>
<th>Unique Record Passwords</th>
<th>Master Password Strength</th>
<th>Two-Factor Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>98%</td>
<td>76%</td>
<td>50%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User</th>
<th>Record Password</th>
<th>Unique Record Password</th>
<th>Master Password</th>
<th>2FA</th>
<th>Security Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sara Graham</td>
<td>378 587 221</td>
<td>23 12</td>
<td>100%</td>
<td>Google</td>
<td>98%</td>
</tr>
<tr>
<td>Brandon Fuller</td>
<td>707 707 177</td>
<td>820 459</td>
<td>77%</td>
<td>Text Message</td>
<td>53%</td>
</tr>
<tr>
<td>Bruce Pearson</td>
<td>745 221 981</td>
<td>169 140</td>
<td>45%</td>
<td>Off</td>
<td>53%</td>
</tr>
<tr>
<td>Katherine Collins</td>
<td>721 117 924</td>
<td>494 693</td>
<td>53%</td>
<td>Text Message</td>
<td>100%</td>
</tr>
<tr>
<td>Julia Garcia</td>
<td>412 48 841</td>
<td>649 542</td>
<td>72%</td>
<td>Text Message</td>
<td>35%</td>
</tr>
</tbody>
</table>
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.
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.
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.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>User</th>
<th>Category</th>
<th>Activity</th>
<th>User Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/10/2018, 09:08:12 PM</td>
<td>Hulde McCoy</td>
<td>Security</td>
<td>Security key has been added</td>
<td></td>
</tr>
<tr>
<td>11/10/2018, 09:08:12 PM</td>
<td>James Nelson</td>
<td>Security</td>
<td>User set 2FA method XXX ON</td>
<td></td>
</tr>
<tr>
<td>11/10/2018, 09:08:12 PM</td>
<td>Noel Castle</td>
<td>Security</td>
<td>User failed first factor login to Admin Console</td>
<td></td>
</tr>
<tr>
<td>11/10/2018, 09:08:12 PM</td>
<td>Jonathan Tran</td>
<td>Security</td>
<td>User set 2FA method XXX ON</td>
<td></td>
</tr>
<tr>
<td>11/09/2018, 09:08:12 PM</td>
<td>John Fern</td>
<td>Security</td>
<td>User XXX was locked by admin XXX</td>
<td></td>
</tr>
<tr>
<td>11/09/2018, 09:08:12 PM</td>
<td>Bobby McGee</td>
<td>Security</td>
<td>Security key has been removed</td>
<td></td>
</tr>
<tr>
<td>11/08/2018, 09:08:12 PM</td>
<td>Justin Ohius</td>
<td>Security</td>
<td>User failed first factor login to Admin Console</td>
<td></td>
</tr>
</tbody>
</table>
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 and Alerts Module](image)

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®

<table>
<thead>
<tr>
<th>BreachWatch</th>
<th>View Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,093</td>
<td>Records at Risk</td>
</tr>
<tr>
<td>Passwords Scanned</td>
<td>10,730</td>
</tr>
<tr>
<td>Passed</td>
<td>6,430</td>
</tr>
<tr>
<td>Ignored</td>
<td>1,207</td>
</tr>
</tbody>
</table>