

Keeper Enterprise

White Paper and Use Cases

Table of Contents

End-User Vault

- 1 **Zero-Knowledge Digital Vault**
- 2 **Generate Strong Passwords**
- 3 **Autofill Website Passwords with KeeperFill®**
- 4 **Change Passwords and Increase Security with KeeperFill**
- 5 **Autofill a Native Desktop Application with KeeperFill for Apps**
- 6 **Protecting Confidential Files, Photos and Videos**
- 7 **Protect Secure Certificates and SSH Keys**
- 8 **Share a Password With a Colleague or Team**
- 9 **Separate Business and Personal Info**
- 10 **Log In with Existing Identity Providers**

Administration and Onboarding

- 11 **Monitor the Security Score of the Company**
- 12 **Manage and Onboard Users**
- 13 **Enforce Role-based Permissions**
- 14 **Transfer Vaults When Employees Leave**
- 15 **Audit Event Logs and Forensic Analysis**

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:

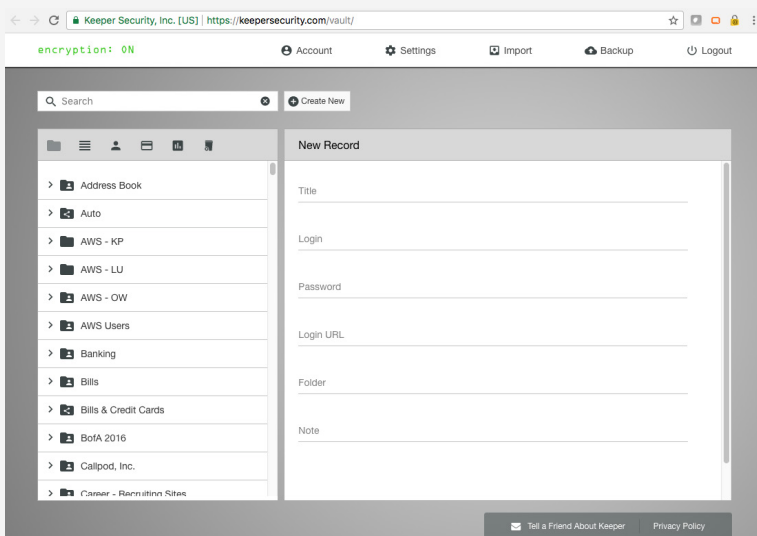
- > Create and manage strong passwords across all device types.
- > Securely store files and other secret information.
- > Autofill passwords across web browsers, apps and mobile devices.
- > Share confidential information between users and teams.

1 Zero-Knowledge Digital Vault

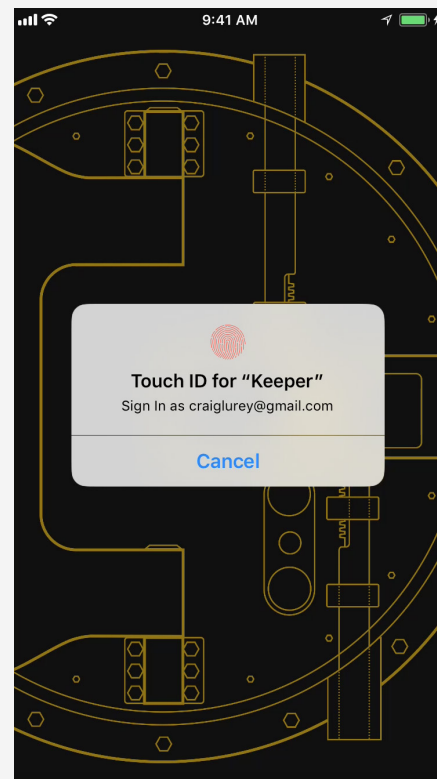
Keeper is a zero-knowledge vault that is protected with multiple levels of encryption. Each user's vault is protected by a Master Password which is used to decrypt data, and two-factor authentication system that protects cloud access to their account.

- * **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 use Keeper SSO Connect don't require a master password, as the encryption keys are then controlled by the Enterprise. Fingerprint (Windows Hello, Touch ID, etc.) can be permitted as a convenience factor.

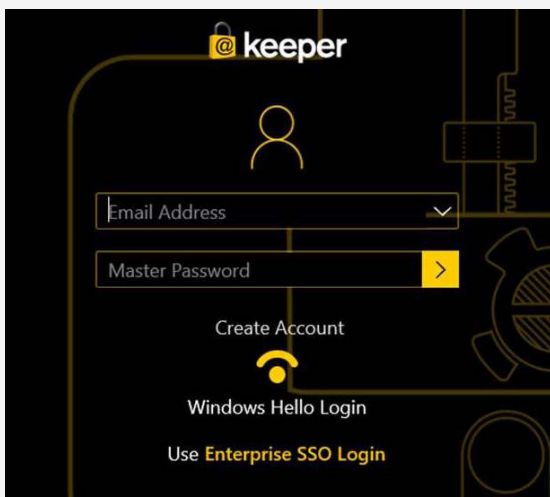
Web Vault / Desktop App for Mac, Windows



iOS Touch ID Login



Windows 10 with Windows Hello Biometric Login

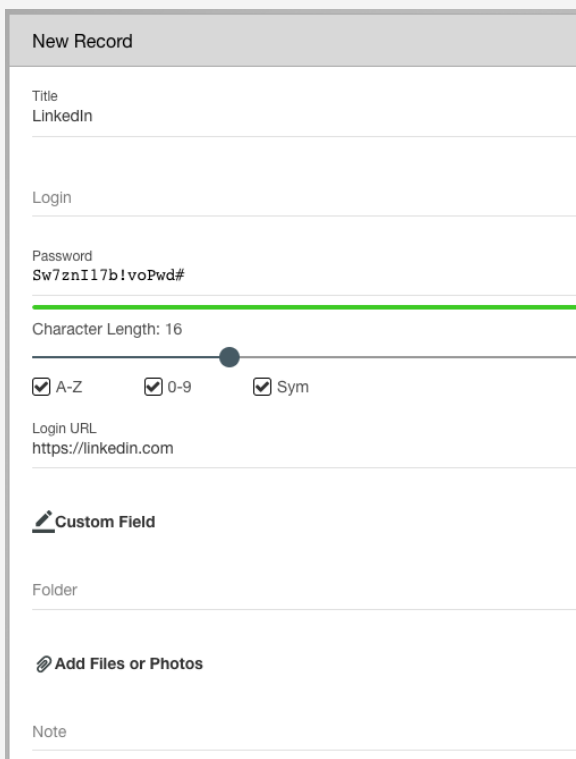


2 Generate Strong Passwords

Creating unique and strong randomly generated passwords for each website is critical to limiting the risk of a data breach and improving the overall security posture of an organization.

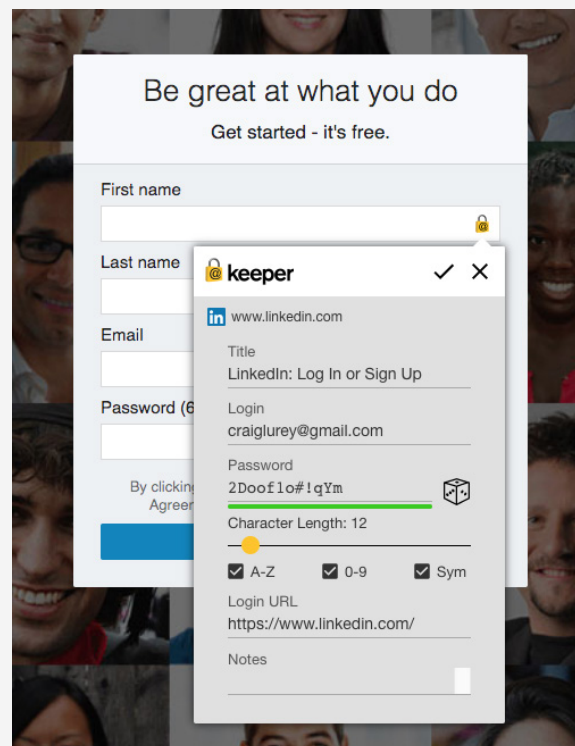
Keeper generates strong passwords inside the vault...

Web Vault Password Generator



The screenshot shows the 'New Record' form in the Web Vault Password Generator. The form includes fields for Title (LinkedIn), Login, Password (Sw7znI17b!voPwd#), Character Length (16), and Login URL (https://linkedin.com). There are checkboxes for A-Z, 0-9, and Sym. A 'Custom Field' section is also visible, along with a 'Folder' field and an 'Add Files or Photos' button. A 'Note' field is at the bottom.

Browser Extension — New Record Creation



The screenshot shows the 'New Record Creation' interface of the Browser Extension. It features a 'Be great at what you do' header and a 'Get started - it's free.' sub-header. The form includes fields for First name, Last name, Email, and Password (2Doo1o#!qYm). There are checkboxes for A-Z, 0-9, and Sym. A 'Login URL' field is also present, showing https://www.linkedin.com/. A 'Notes' field is at the bottom. The interface is overlaid on a background image of a group of people.

...and automatically suggests passwords when registering for accounts on the browser extension.

New passwords can be kept private to the user or shared to individuals or a team.

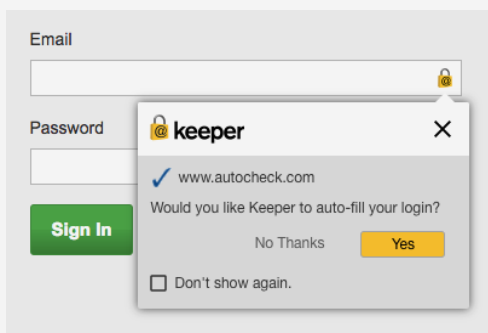
3 Autofill Website Passwords with KeeperFill®

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:

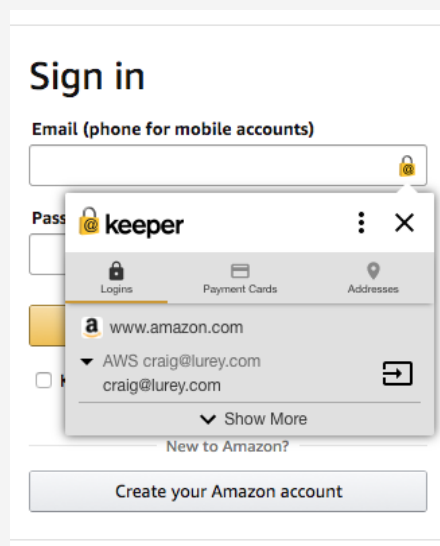
- > Filling a login and password
- > Selecting from multiple passwords on the same website
- > Automatically filling a password (optional)
- > Prompting to fill or manual click to fill
- > Saving new passwords to the vault as you type

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

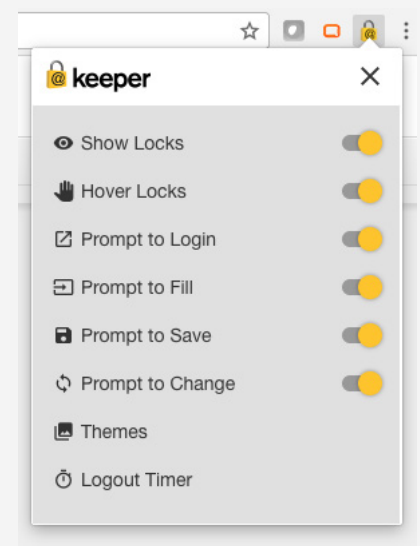
Browser Extension — Autofill Prompt



Browser Extension — Multiple Account Fill



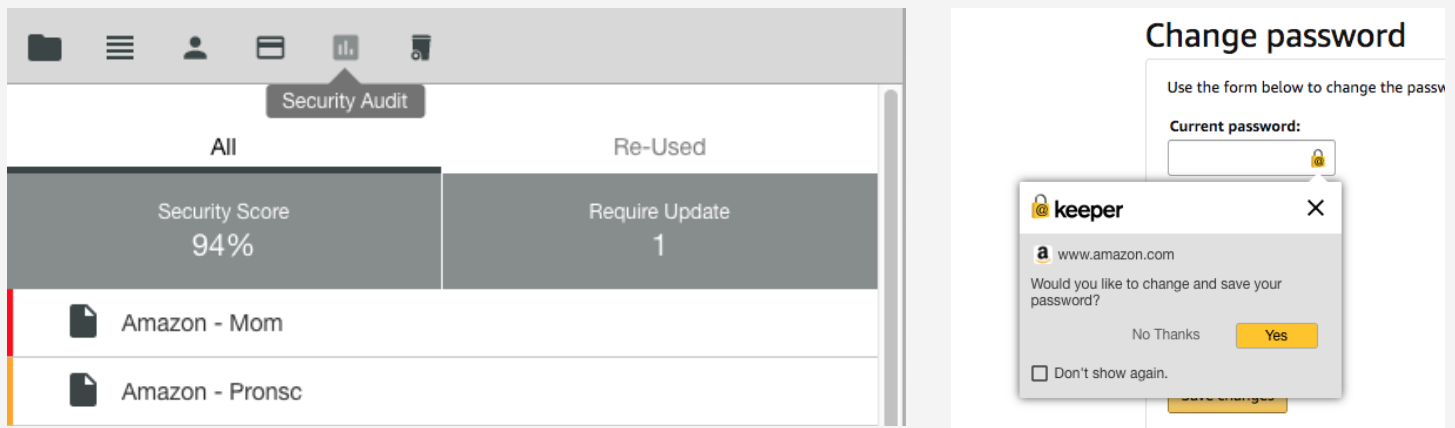
Browser Extension — Options



4 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.



5 Autofill a Native Desktop Application with KeeperFill for Apps

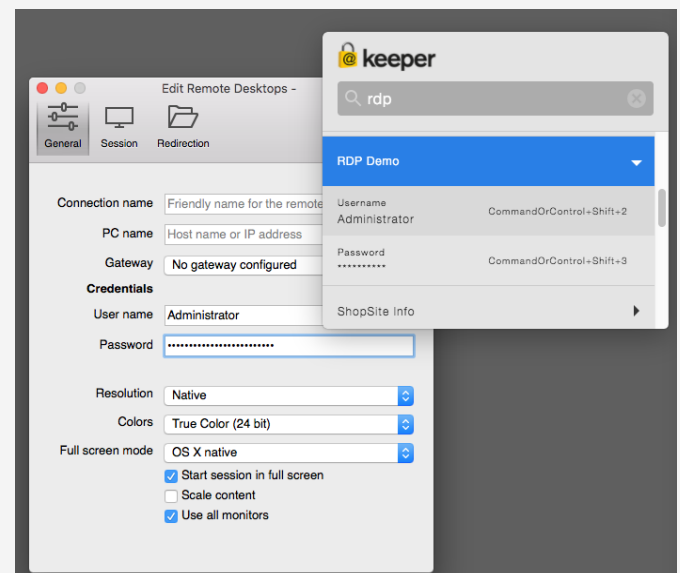
Keeper Desktop provides a unique and powerful native app form fill capability using a simple keyboard hotkey. IT admins who are accessing remote services can make use of this capability without having to resort to "copy" and "paste". By storing all passwords in the vault and using KeeperFill for Apps, 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



6 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

2014 Mortgage Refinance Docs ⓘ

Title

2014 Mortgage Refinance Docs

Shared Users

Folder

Financial

Files or Photos

20141015_0_6.pdf

47.18 KB

20141016_0_6.pdf

47.19 KB

Drivers License

3.40 MB

7 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

PEM Key demo.com ⓘ

Title

PEM Key demo.com

Password

.....

PEM

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAh6+owwKOMtb2Voi/zWbd2OGX/P6JrBMNzHg78RQj90QgdDr0SVD1WL7E0o
7VCzyPLhkmHFRb1bvb23vMYYJB/NZgKzplwNvLjgXusR5bLd6LTOFX3Yy0S8ZkC3UR8x
6pT1gH30NvSLyRoRNB0fgZ4y300MoImB5aTmYwWKSIMaW0enF+Q2wv33xkx7dULeVQ8Kq
PoatMOOQVUv+bn0ys27kipWUPYecMblbVp7Ft/gRa9llatOSes2NasE8dE2sX4VaQDsEOpG
zqKzT8o84dQ11M4ILsFJ3TC/QqpY5FxmJf+g91A2fTwsKtGtwIDAQABAoIBAHzx76irql/+
HNcwK9aUPAOKMW5CAgqJ5RIKAZJM5pWIC62zzgtikn9j5yorOBjaTrJFZJaOUC3We6AhCW+eULf
yLcJdki7+b9N+BA82JKN8DQZ3/KNbq/QEJPIF/Xt06SiVOnma6ZzZxHf2L3D/bQJqreMOQ
Q7GVFom7QQVXujFVHDv8V50QDggJRArH2OHWWmoExaRqcd9wci80m3wE5chbpJbg5xFcH5iq8NA1
VY3LR4jIR7/NJ+vJRW23eJ/ojsNRcaW8MvJHHPFS5bmBnbVwe/kTkn0r3W4PSMnhyqqdJE+2jkw
pIU8Zag5n0wZT18yS3vWwMqCgYEAb9HGA/N4k51dfkN8laEISkikU60qVXEC3thkXUJF/N
RR+faJSM8sMcPLX7sgTZAQVNZTnsZK051bZBPKJCT0IMFYxMK9JmghYGMW4UmK9d0DzRA9D6J
RE0JdZLqgNXIDVwEQm0YXDfNC7euJJ+rz2fGaMEhwgJMuJnmsCgYEAK7tn04WWq3AqX7UnCC8
8yrenF6RPEXvQyAvPcSc8B75Uq4TSYvOXuknbqCILQ5Rugd+zk2nli+SGolaw/lqZ7LocGDxOCJ
SIVKL41bnW1sVYAY8ZeagXILZid3KI72FhPko5a5FI2U52gOMfxXU12Ejd+xxSsgYF/Km8+UC
gYEA4Rk3ut6ecwPW+n7CTAnC64TrNOGax/4lvtNE/p/cW0mQaTzAQA/1nJ8oFAJhAp7I3UM8Q0
SIN5N8Tz+v6LKhTikw+HOsCCXoW24LWspDWmw5Y2AFNQVASCuabfBxxvlsQUd+ZFfjhCpN8m0PIG
Nu6M8MV2XMI4E+ZvOINSdXcGyBYefqasfku86D3bqTrv+626aIACDjntsRiBEvmUJhshYBoxhy
Drs9gPh8YQZ4VY8Y8Ph8hsWclJ8ccI4575yMcpHtB8pXDD9CATWTD9p+Otohs2QOQvCTZ7t
zrP5xCcT7PH+eEYP8aVDV8NtbOKDmPhnlahAOI9HJR/CQKBgG1g84byviBZY1uFNu11Vpwbpxpl
kKXxMIVeU95F0DJO1mUw1f1H9EdILZgCAdHplNB+Vntw4M7keqCd6SyyCdry5QwW97YUuziWR6
dTWrvRIBEXkm31lutWUKWlweAm1usU+39ogN6vyQMj+iac9txhTLJvQjQwFE9KZ8Fxl
-----END RSA PRIVATE KEY-----
```

Shared Users

Files or Photos

my_server_key.pem

1.63 KB

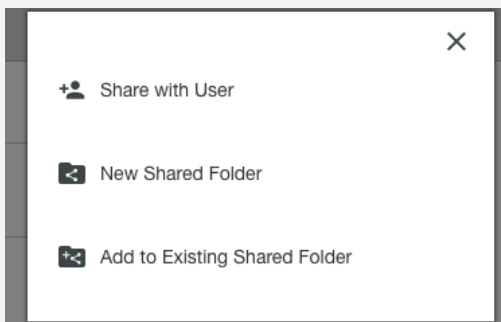
Note

Remember:
chmod +400 my_server_key.pem

8 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 to teams of users.



Individual Record Sharing Permissions

Add People

☐ Make Owner

☐ Can Edit ☒ Can View ☒ Can Share

Sharing a Folder With a Team

New Shared Folder

Users	Records
<input type="text" value="Add Users"/>	
<input type="checkbox"/> Sys Admin Team	
<input type="checkbox"/> Windows Team	

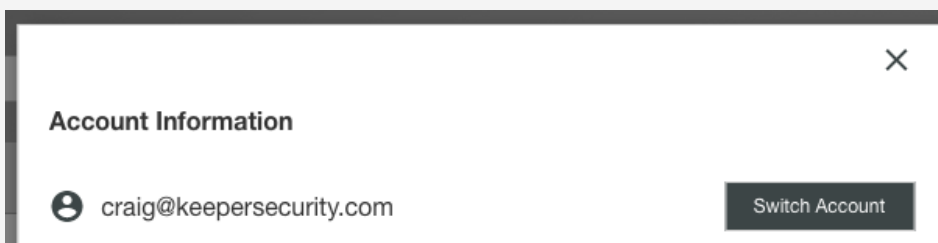
View, edit and share permission sets can be applied to individual users. Shared folder permissions can provide control over the management of the folder, users and records.

Teams are constructed in the Keeper Admin Console. They can be configured to prevent password viewing (called password masking) and can be automatically created by the existing Active Directory team structure.

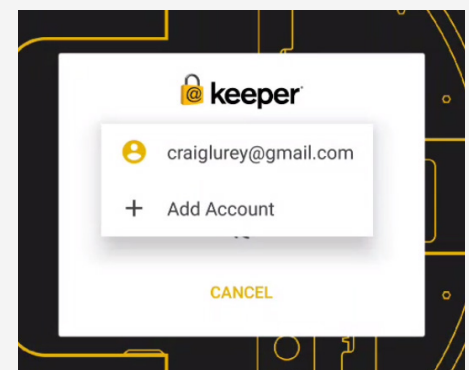
9 Separate Business and Personal Info

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



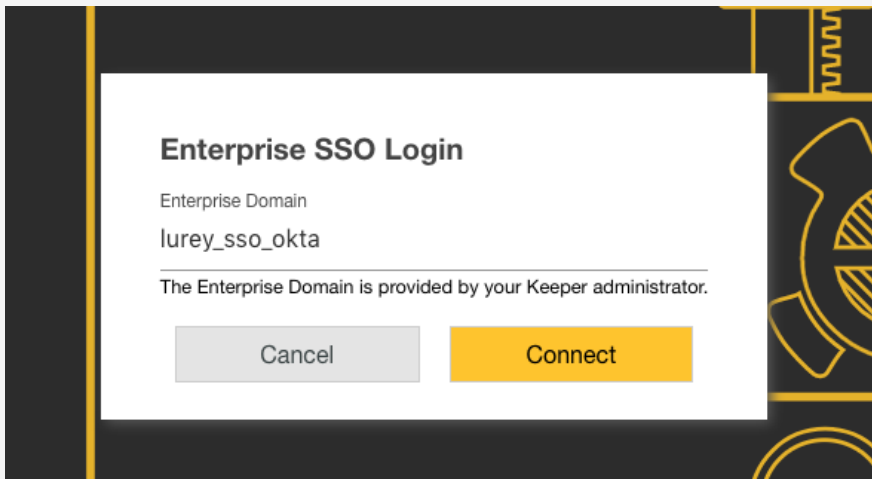
10 Log In With Existing Identity Providers

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 Azure, G-Suite, JumpCloud and F5 BIG-IP APN.

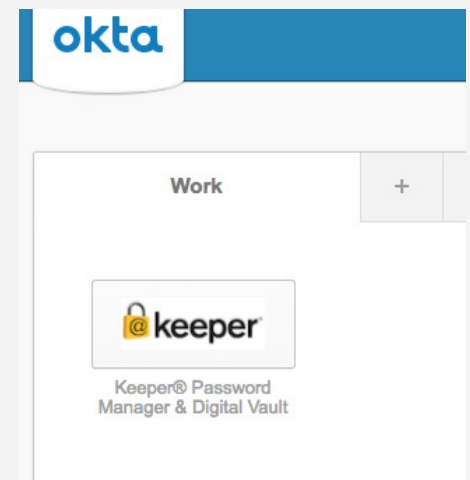
Once this capability is activated by the Keeper Administrator, logging in is seamless across all device types and platforms

Alternatively, users can first log in to identify the provider and then launch their Keeper Vault.

User Signs Into Keeper With Enterprise SSO Login



Okta End-User Login Flow



Administration and Onboarding

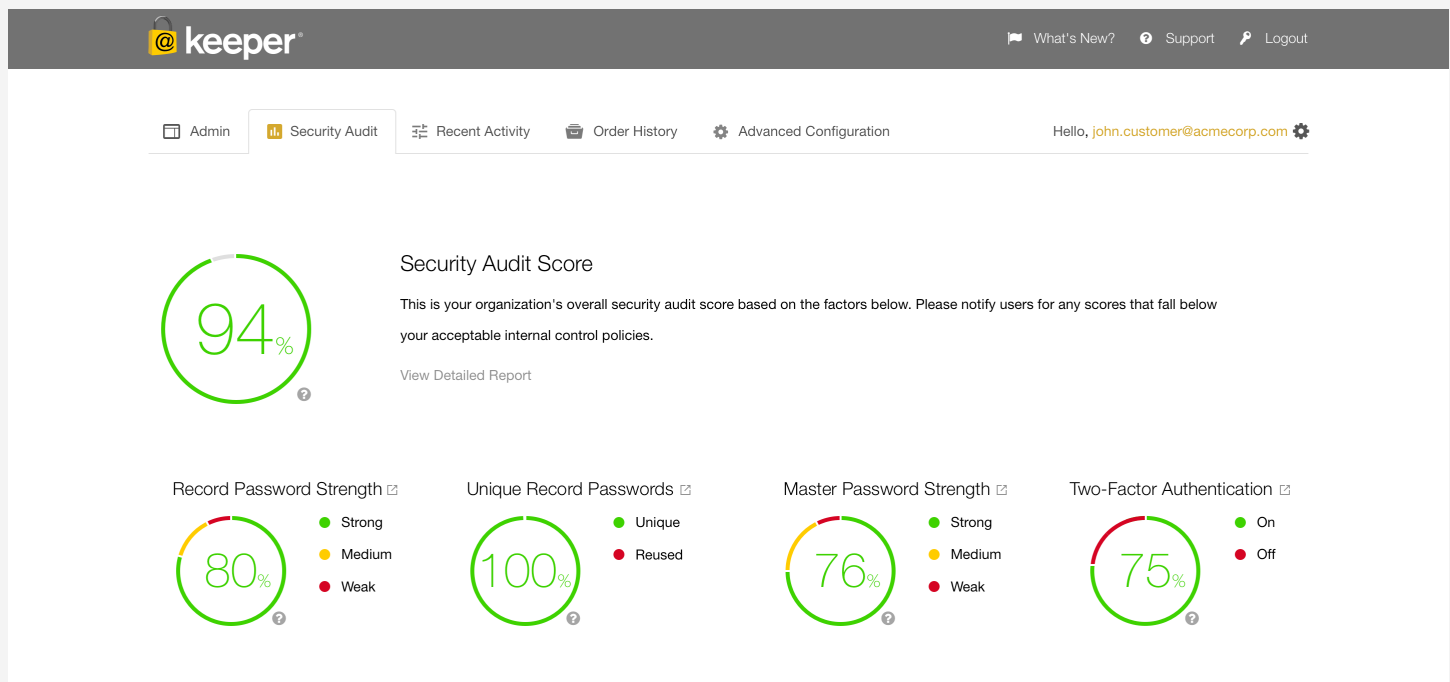
Keeper Enterprise provides a web-based Admin Console application. The Admin Console allows administrators to:

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

11 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			
<input type="text" value="Search Users"/>			Export
Users	Weak	Medium	Strong
Craig Lurey	1	2	21
Gene Dias	-	-	1
Paul Borghesi	-	-	1
Luise Jackson	-	1	-
Joe Smit	-	-	4
James Smitley	-	-	-

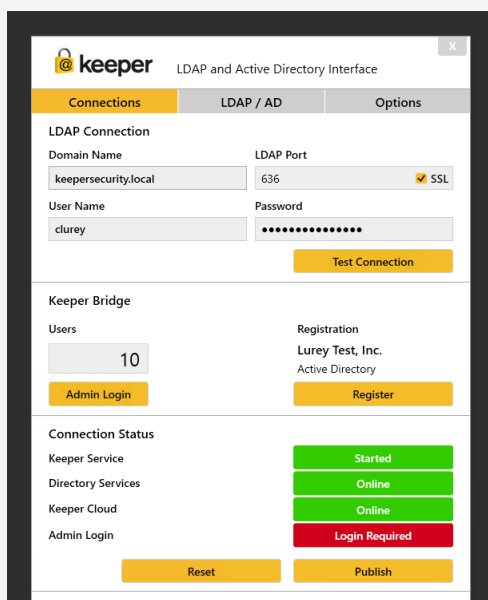
12 Manage and Onboard Users

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:

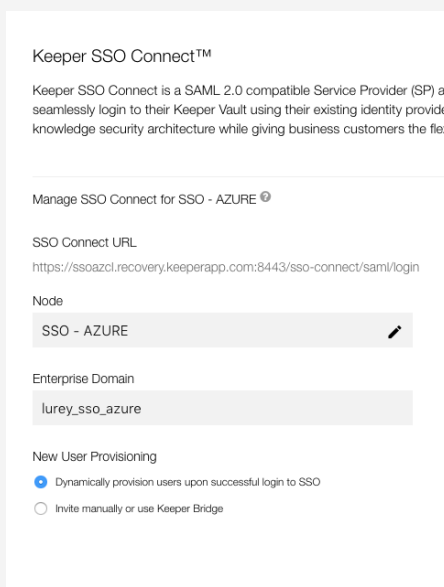
- > Active Directory through the Keeper AD Bridge
- > SAML 2.0 via the Keeper SSO Connect component
- > CSV File upload
- > Manual entry via the web interface

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.

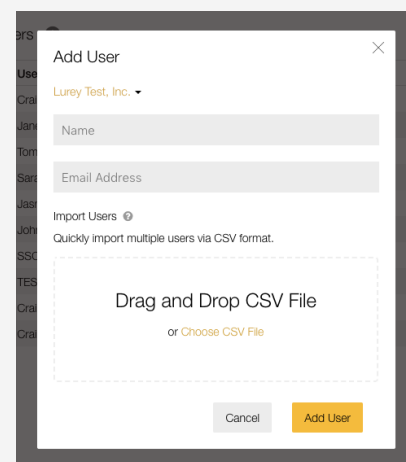
Onboarding Users via Active Directory Bridge Software



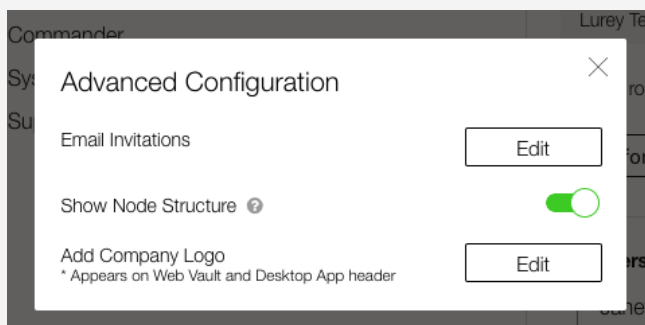
Onboarding Users Through SAML 2.0 / SSO Connection



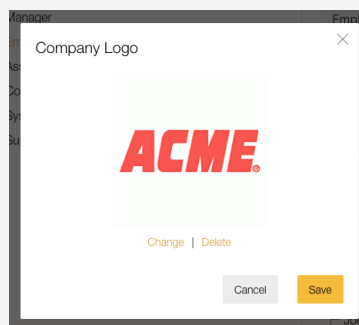
Adding Users Through CSV File or Manually



Email invitation and cobranding



Customized Vault Corporate Identity

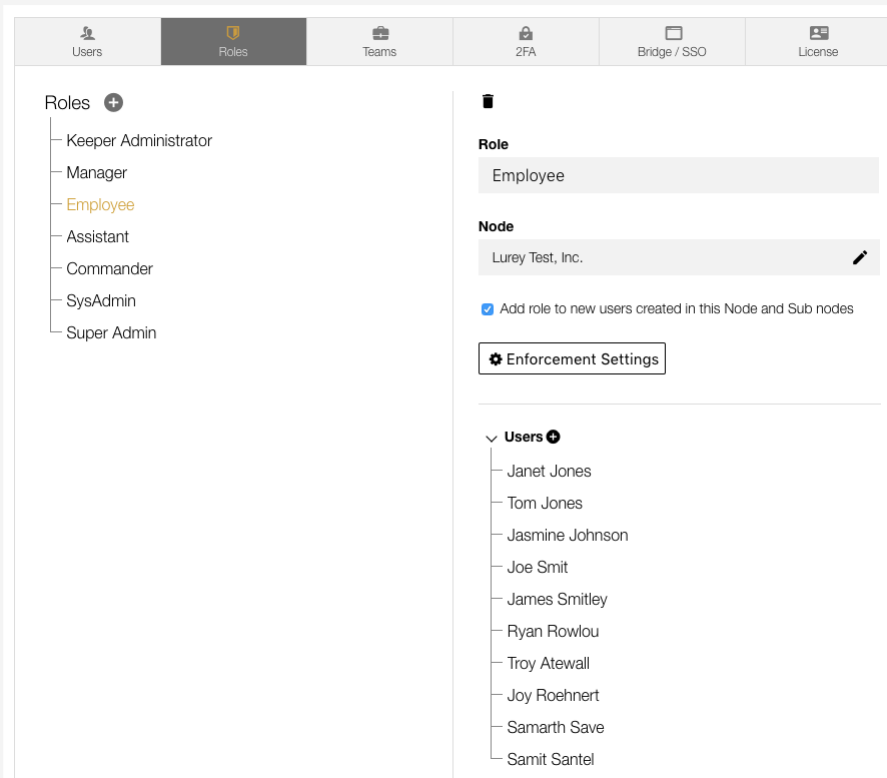


13 Enforce Role-based Permissions

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:

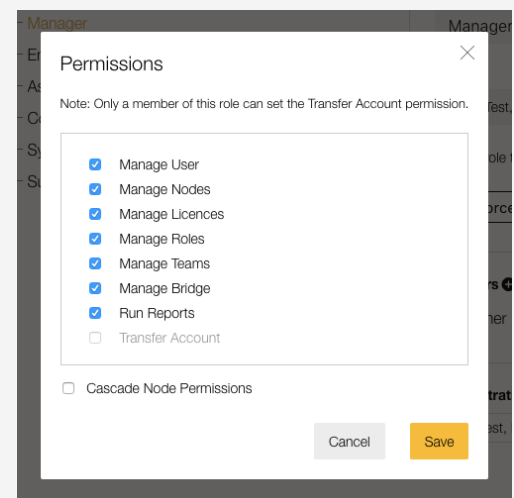
- > Master password complexity rules
- > Two-Factor Authentication channels
- > Physical location, IP addresses and device platforms
- > Sharing and data export rules
- > Device biometrics

Role-based Permissions are Fully Customizable



The screenshot shows the 'Roles' tab in the Keeper Admin Console. On the left, a list of roles includes Keeper Administrator, Manager, Employee (highlighted), Assistant, Commander, SysAdmin, and Super Admin. The main area displays the configuration for the 'Employee' role. It shows the role name, a list of nodes (currently 'Lurey Test, Inc.'), and a checkbox for 'Add role to new users created in this Node and Sub nodes'. Below this is an 'Enforcement Settings' button. At the bottom, a list of users is shown, including Janet Jones, Tom Jones, Jasmine Johnson, Joe Smit, James Smitley, Ryan Rowlou, Troy Atewall, Joy Roehnert, Samarth Save, and Samit Santel.

Admin Permissions Settings



The screenshot shows the 'Permissions' dialog box. It contains a note: 'Note: Only a member of this role can set the Transfer Account permission.' Below the note is a list of permissions with checkboxes: Manage User, Manage Nodes, Manage Licences, Manage Roles, Manage Teams, Manage Bridge, Run Reports, and Transfer Account. The 'Transfer Account' checkbox is unchecked. At the bottom, there is a 'Cascade Node Permissions' checkbox, which is also unchecked. 'Cancel' and 'Save' buttons are at the bottom right.

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.

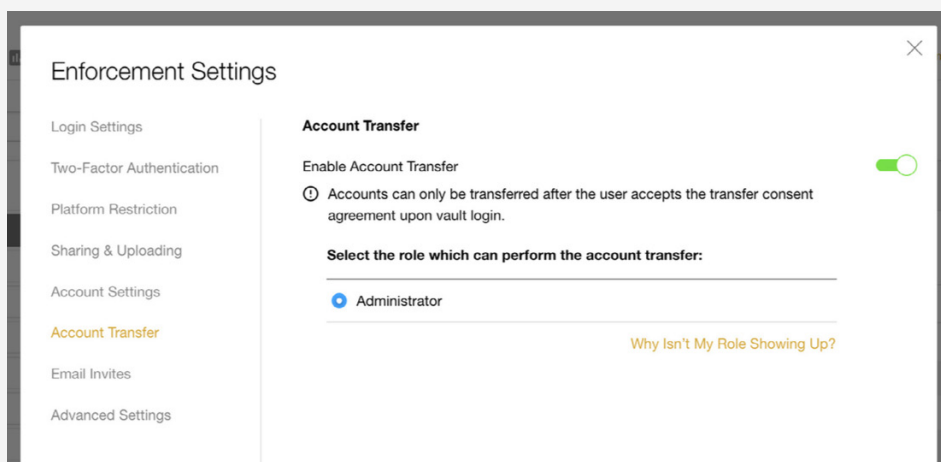
14 Transfer Vaults When Employees Leave

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

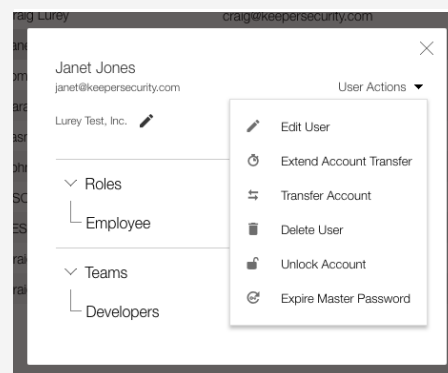
Through the use of Keeper's secure "Account Transfer" feature, a user's vault can be locked and then transferred to another user within the organization. The process of account transfer remains fully zero-knowledge, and the responsibility of performing the account transfers can be limited based on roles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

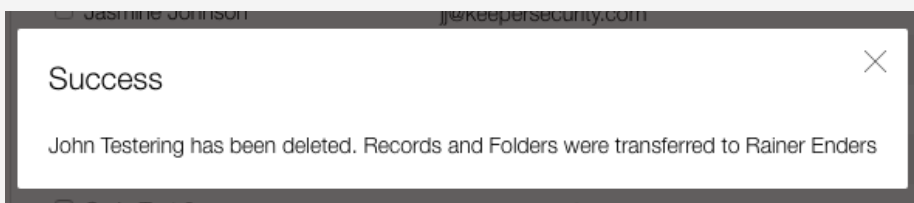
Enabling Account Transfer From the Role Enforcements Screen



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.



15 Audit Event Logs and Forensic Analysis

Keeper's "Recent Activity" section provides full event logging and forensic analysis capabilities to comply with corporate governance and audit requirements. Dozens of event types 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 Screen

Admin

Security Audit

Recent Activity

Order History

Advanced Configuration

Hello

Q Search

Filter Search

User	Event	Date	Time
Craig Lurey	Login	9/14/2017	5:38:06 PM
Deleted User ID: 11119554	Login	9/14/2017	5:16:21 PM
Deleted User ID: 11119554	Login Failure	9/14/2017	5:16:18 PM
Janet Jones	Login Failure	9/14/2017	5:14:14 PM
Janet Jones	Login Failure	9/14/2017	5:13:18 PM
Janet Jones	Login Failure	9/14/2017	5:12:33 PM
Janet Jones	Login Failure	9/14/2017	5:10:45 PM
Janet Jones	Login Failure	9/14/2017	5:10:27 PM
Janet Jones	Login Failure	9/14/2017	5:10:23 PM
Craig Lurey	Login	9/14/2017	5:02:45 PM
Craig Lurey	Login	9/14/2017	5:02:13 PM
Craig Lurey	Open Record	9/14/2017	4:44:19 PM
Craig Lurey	Open Record	9/14/2017	4:44:17 PM
Craig Lurey	Login	9/14/2017	4:44:17 PM
Craig Lurey	Login	9/14/2017	4:44:17 PM
Craig Lurey	Login	9/14/2017	3:44:46 PM
Craig Lurey	Login	9/14/2017	3:20:50 PM
Craig Lurey	Open Record	9/14/2017	2:49:54 PM
Craig Lurey	Open Record	9/14/2017	2:48:44 PM
Craig Lurey	Open Record	9/14/2017	2:48:40 PM

<

1 / 51

>

Activity Event Filters

Filter Search

☐ Change Master Password
 ☐ Change Role
 ☐ Change Security Question
 ☐ Change Status
 ☐ Change User
 ☐ Delete User
 ☐ Auto-Filled Credentials
 ☐ Login
 ☐ Login Failure
 ☐ Open Record
 ☐ Add Record
 ☐ Delete Record
 ☐ Remove Record
 ☐ Record Update
 ☐ Set Two Factor Auth
 ☐ Share

OK

Forensic Analysis of User Behavior and Record-Specific Activity.

Login Failure

Location

Sacramento, California

Version

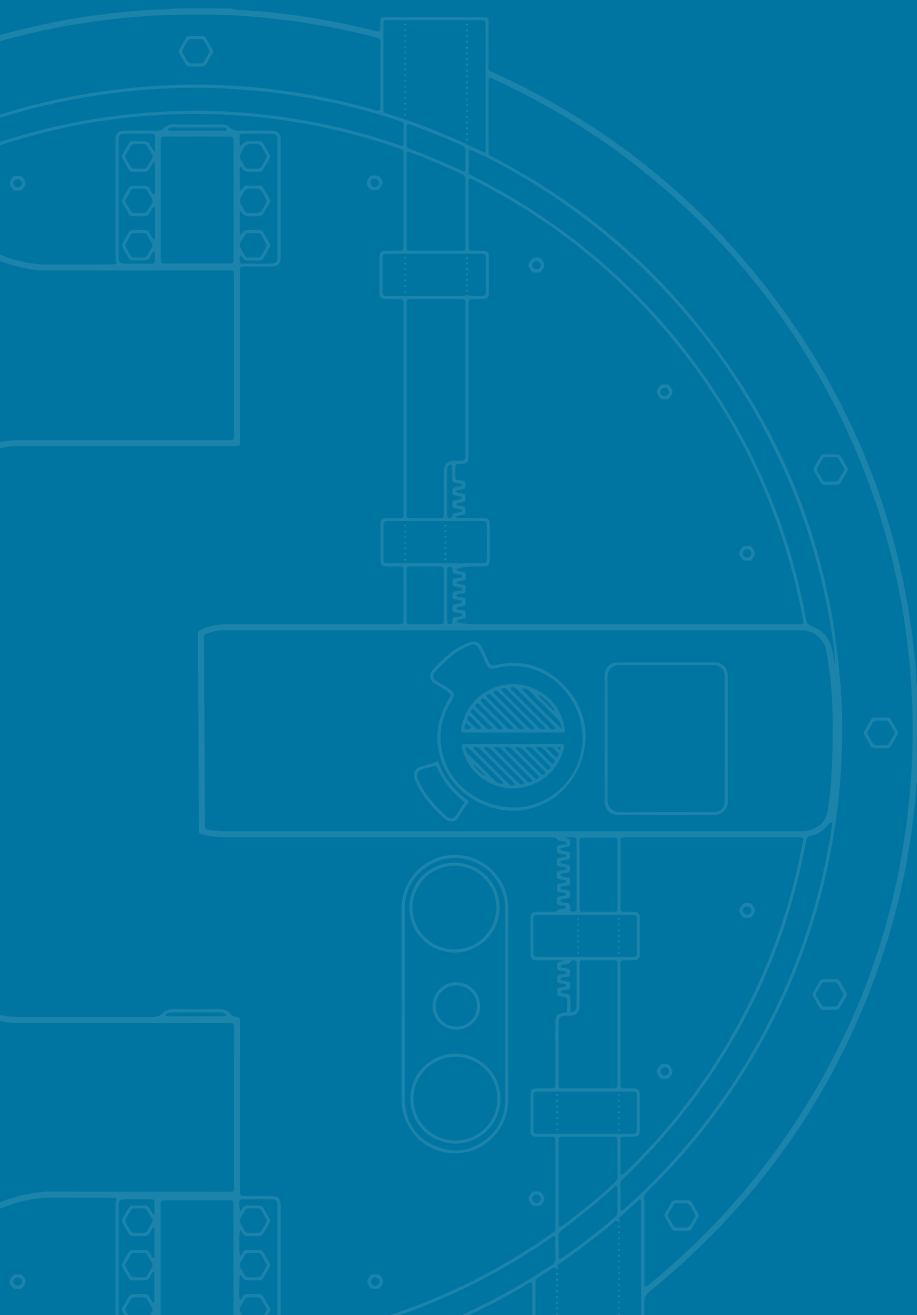
Web App 11.1.0

Detail

account_locked


IP Address

67.91.221.196



Contact

 keepersecurity.com

 312.829.2680

 sales@keepersecurity.com