



Keeper MSP Technical Whitepaper

Table of Contents

Introduction	3
System Architecture	3
Zero-Knowledge Architecture	3
Master Password	4
Encrypted Vault	4
Ubiquitous access to password vaults from any device	6
Fully-Managed SaaS Platform	6
Isolation of Managed Companies	7
Industry Certifications	8
Certified SOC 2 Compliant	9
ISO 27001 Certified (Information Security Management System)	9
GDPR Compliance	9
Key Functionality	10
Roles & Enforcements	10
Administrative Permissions	10
Two Factor Authentication (2FA)	11
Two Factor code generator in user's vault	12
MSP Remote Administration & Permissions	12
Teams & Shared Folders	13
License Pool	14
Logging license transactions for Billing purposes	14
Reporting	15
SIEM Integration	16
Versatile provisioning	16
Import / Email	16
AD Bridge	16
SSO	16
Account Transfer	16
Deploying KeeperMSP	17
Full Service model	17
Reseller model	17
Hybrid model	17
Summary	17

Introduction

KeeperMSP is a natural extension of Keeper's Enterprise Password Management solution which allows an MSP to manage multiple independent tenants (a.k.a. "Managed Companies" or "MC's") from a central console.

Keeper began as a mobile-first, consumer-focused product. As a result, our application is easy and enjoyable to use. This is evidenced by our 15M+ downloads, very high renewal rates, and positive reviews. Keeper's solutions are also used heavily by Small and Medium Businesses (SMB's) given these firms are often highly vulnerable to cyber security crimes. It is estimated that 39% of SMB's use an MSP in some capacity as they typically not staffed with all the IT specialists they need to function in today's digital world.¹

Keeper has also expanded into the Enterprise space and honed the product by meeting the needs of demanding administrators in mission critical environments with complex deployments and use cases. The enterprise version of the product has been architected to scale and has the core features and functionality that MSP's require, including: organizational roles; robust enforcement policies; multiple provisioning mechanisms, full support for 2FA methods; and robust auditing and reporting capabilities.

To better service the MSP market, Keeper now offers this highly scalable, purpose-built solution so that our password management solution can be more easily offered and managed by MSP's.

System Architecture

Zero-Knowledge Architecture

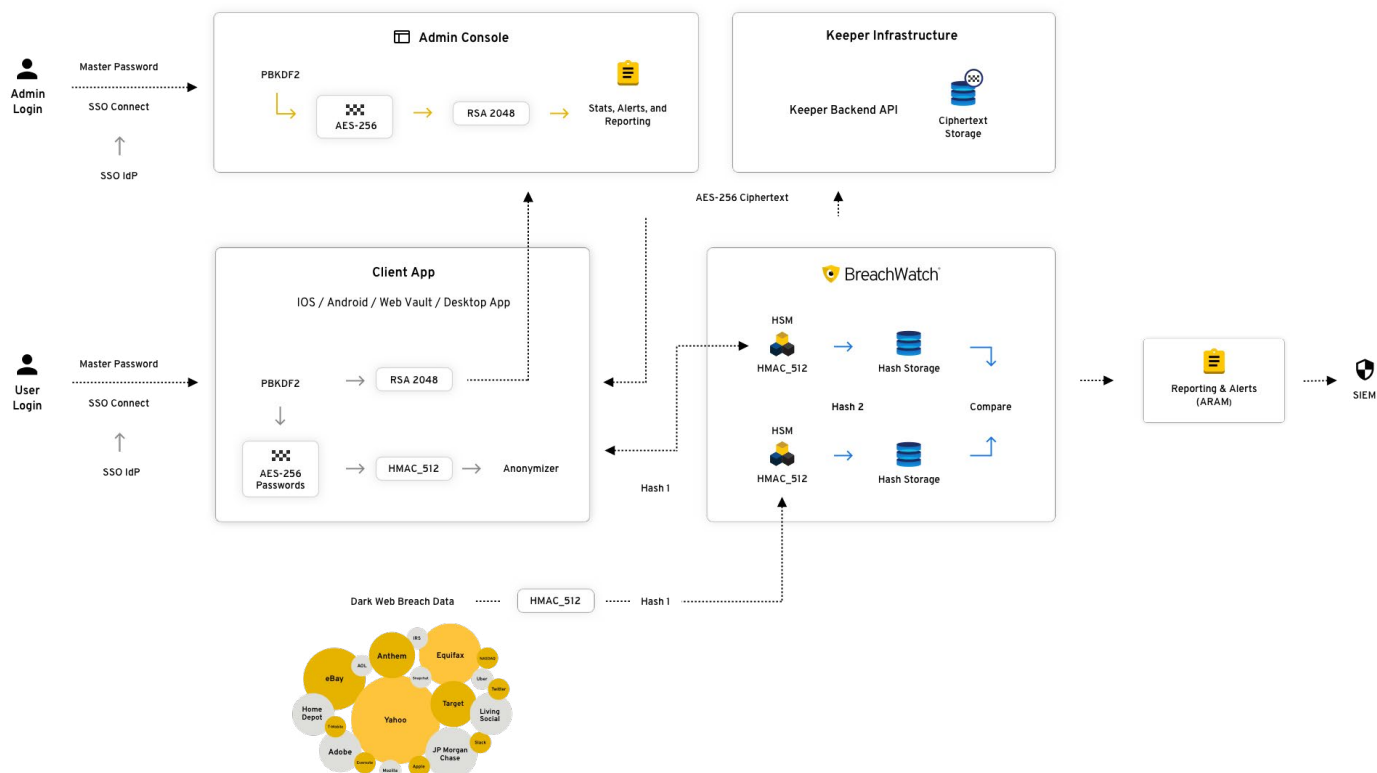
Keeper is a Zero Knowledge security provider. Zero Knowledge is a system architecture that guarantees the highest levels of security and privacy by adhering to the following principles:

1. Data is encrypted and decrypted at the device level (not on the server)
2. The application never stores plain text (human readable) data
3. The server never receives data in plain text
4. No Keeper employee or 3rd party can view the unencrypted data
5. The keys to decrypt and encrypt data are derived from the user's master password
6. Multi-Layer encryption provides access control at the user, group and admin level
7. Sharing of data uses Public Key Cryptography for secure key distribution

Data is encrypted locally on the user's device before it is transmitted and stored in Keeper's Cloud Security Vault. When data is synchronized to another device, the data remains encrypted until it is decrypted on the other device.

Keeper is the most secure, certified, tested and audited password security platform in the world. We are the only SOC 2 and ISO 27001 certified password management solution in the industry and Privacy Shield Compliant with the U.S. Department of Commerce's EU-U.S. Privacy Shield program, meeting the European Commission's Directive on Data Protection. Not only do we implement the most secure levels of encryption, we also adhere to very strict internal practices that are continually audited by third parties to help ensure that we continue to develop secure software and provide the world's most secure cybersecurity platform.

To learn more about the Keeper zero-knowledge architecture please see our [encryption model documentation](#).



Master Password

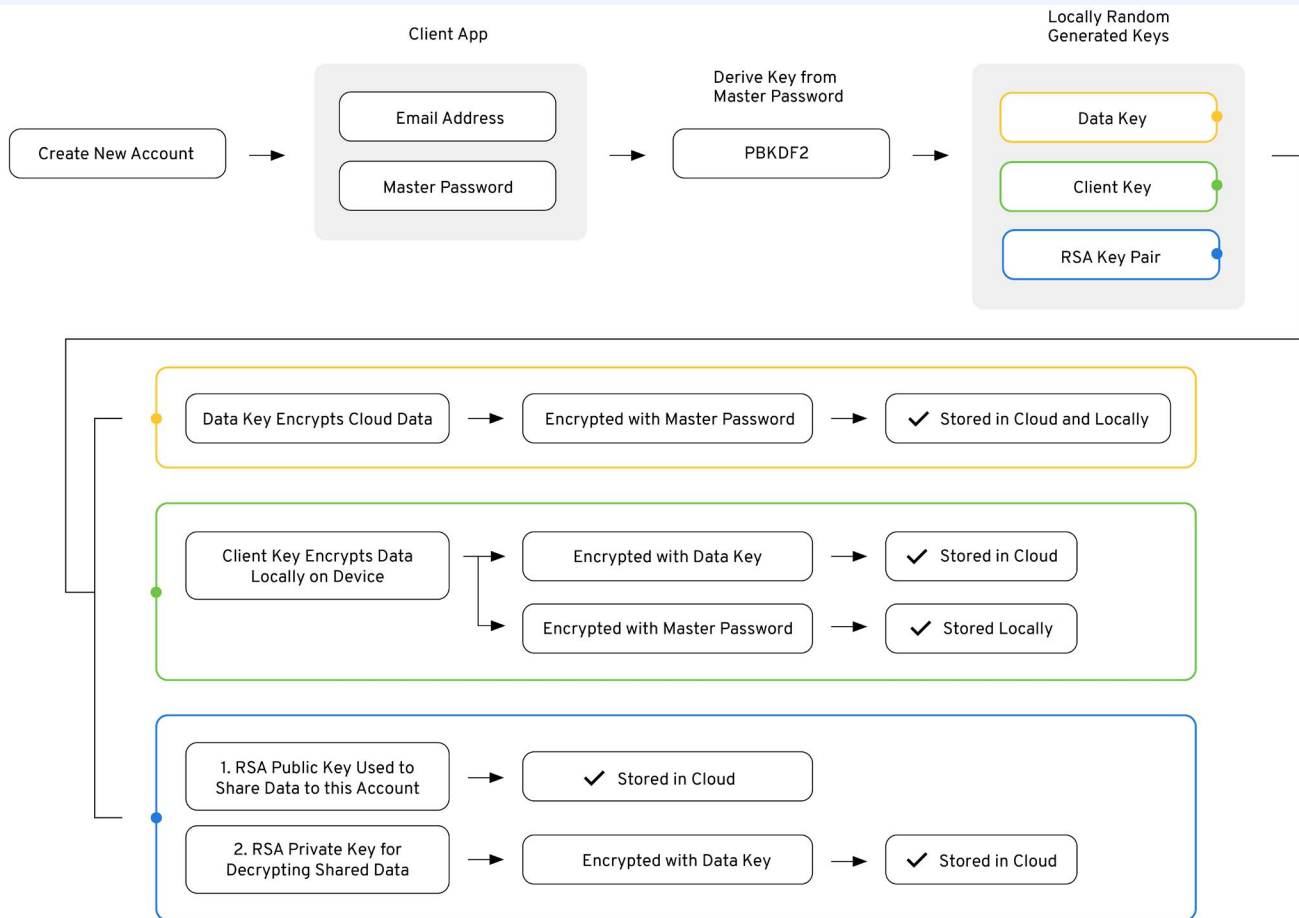
Each Keeper user must choose a “Master Password” which is only used for Keeper and not used for any other service. Keeper’s Zero Knowledge architecture ensures that no one – not even the administrator, MSP or Keeper employees – have access to a user’s master password.

The Master Password must adhere to the guidelines enforced by the Keeper Administrator and can be applied to users via role enforcement policies. In the case of lost Master Password, users can recover their account through a zero-knowledge recovery process by answering a security question, email verification and two-factor verification.

Encrypted Vault

Numerous government and regulatory guidelines, including the National Institute of Standards and Technology and the European Union’s General Data Protection Regulations recommend encryption as the most effective form of data protection. Keeper’s implementation of symmetric encryption in the vault represents the most advanced and secure solution available in the market.

All passwords in Keeper are stored in encrypted records which reside in a digital vault. The encryption key to decrypt the vault is first derived from the user’s Master Password, which then unpacks other private keys such as the “Data Key” and “RSA Private Key” which are unique to the user. The Data Key unpacks additional keys called “Record Keys” and “Folder Keys” which are used to decrypt the user’s stored records.



Keeper Encryption Model

All top tier password managers encrypt data at some level, but not all encryption is implemented the same. Keeper supports 256-bit AES encryption and PBKDF2 for key derivation, which are widely accepted as the strongest forms of protection available. We also provide multiple layers of encryption at the record, folder and team level. By implementing record-level encryption, records can be shared among privileged users without risking unauthorized or elevated access.

Protection of “data in motion” has been an issue in the past with products that may briefly decrypt data during transmission, or while stored on cloud servers for their own convenience. For Keeper any Data in transit is protected by 256-bit TLS/SSL encryption and the application itself is protected with Key Pinning and layers of encryption that cannot be defeated with MITM (man-in-the-middle) attacks.

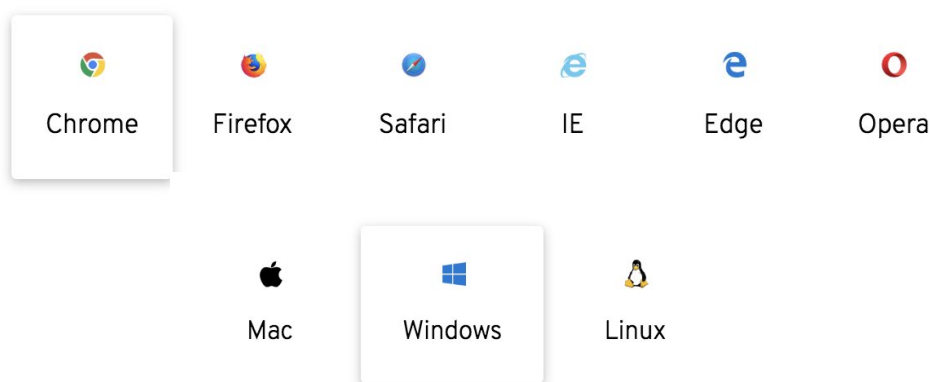
The encrypted vault resides in the cloud to ensure synchronization, but can also be used in an offline mode. Users can login offline and decrypt stored data on mobile and desktop devices. Offline access can be restricted on a role enforcement basis by the Keeper Administrator.

Ubiquitous access to password vaults from any device

We live in a multi-device world, but that shouldn't inconvenience people who need access to valuable information no matter where they are. Keeper supports the major types of mobile devices (iOS and Android), as well as the most popular browsers, both on the desktop and the phone or tablet. Data is automatically synchronized across these devices so a user can gain access wherever they need to, from any device they have access to, without fear of losing their credentials if any one device is lost, stolen, or left behind.

As of October, 2019 Keeper's native client applications include: Windows 7/8/10, Mac OS, Linux/Unix, iOS 8+, Android 4.4+, Windows Phone 8+. In addition Keeper offers internet browser add-ons (called KeeperFill) for Edge, Internet Explorer, Chrome, Safari, Firefox and Opera. Download [here](#).

For additional information on deploying Keeper to end-users, go [here](#).



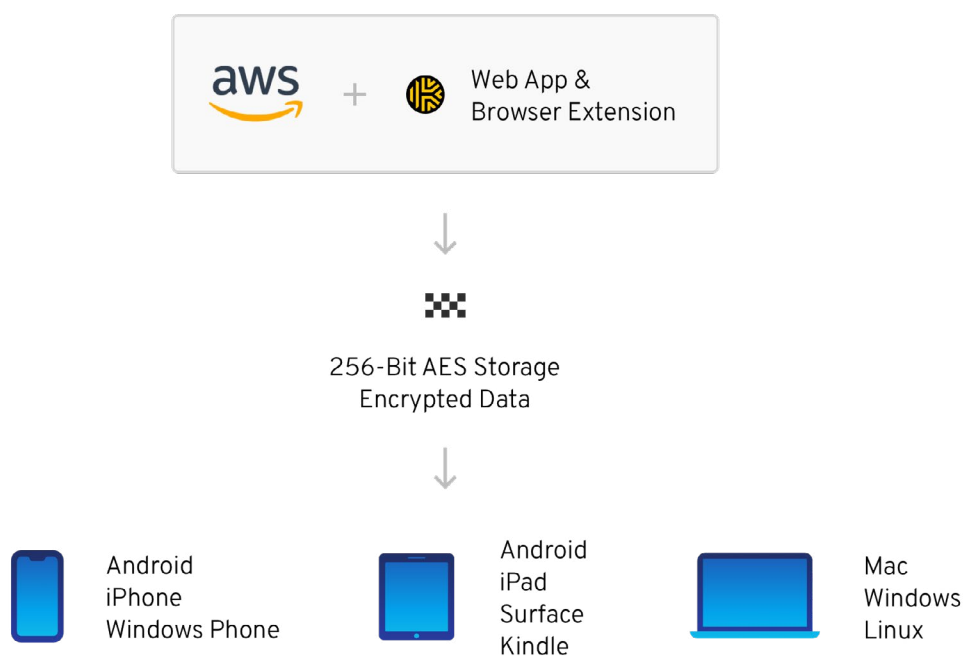
Fully-Managed SaaS Platform

Keeper is a fully managed hybrid SaaS solution. All the encryption/decryption of vault records occurs on the user's device. This encrypted vault data is then stored in the cloud for browser access, synchronization across devices, and backup.

All of Keeper's user-facing applications contain on-device local encrypted storage. The applications can be locked down to only run within the customer's network environment through role-based enforcement policies. The MSP can also enforce the use of 2FA and other security policies through the Keeper Admin Console.

The Keeper Cloud Security Vault is hosted with Amazon AWS in North America and Europe, for localized data privacy and geographic segregation to host and operate the Keeper solution and architecture. Utilizing Amazon AWS allows Keeper to seamlessly scale resources on-demand and provide customers with the fastest and safest cloud storage environment. Keeper Security operates both multi-zone and multi-region environments to maximize uptime and provide the fastest response time to customers.

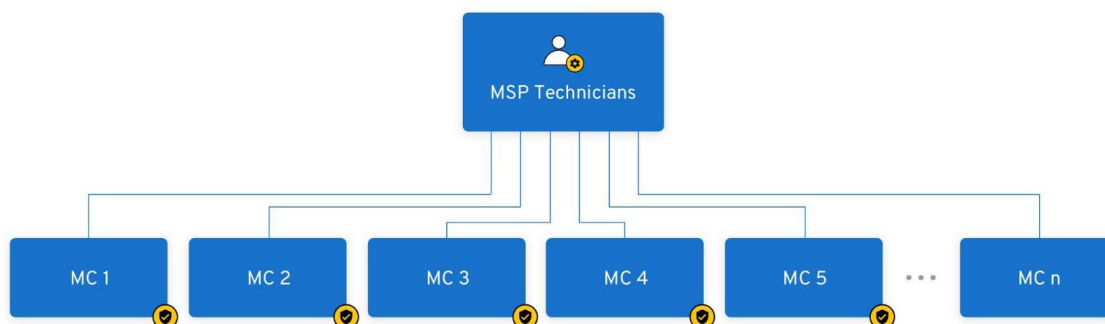
New MSP and MC accounts are created either in the US or EU regions. Once the region has been established, the data center region cannot be changed without re-creating the environment.



Isolation of Managed Companies

Keeper MSP provides full data isolation between each MC, at both the logical and encryption layer. For preservation of zero knowledge security architecture, each MC's data is completely separated and encrypted with key derivation architecture that is specific to each MC. Therefore, no inadvertent sharing of MC-related data such as emails, admins, teams, roles or vault data is possible.

MSP Technicians exist in the root level of the MSP's system and have ability to cross-over to each MC instance for administrative purposes. Any "local" admins set up in the MC's do not have that root level access to the MSP's console or any of the MSP's data.



KEEPER

msp

Nodes, Roles, Teams, Users

Schedule Demo

bill+m1@keepersecurity.com

X

Dashboard

Admin

Managed Companies

Security Audit

BreachWatch

Reporting & Alerts

Subscriptions

Configurations

Managed Companies

+ Add Managed Company

License Usage by Plan

Keeper Business

100 of 100 licenses available

Keeper Business Plus

75 of 100 licenses available

Keeper Enterprise

62 of 100 licenses available

Keeper Enterprise Plus

55 of 100 licenses available

License Allocation History

Company	Plan	Allocated	Active	Launch
Darren Rock Supply	Keeper Business Plus	25	2	
Sierra Adventures	Keeper Enterprise Plus	45	1	
El Dorado Construction	Keeper Enterprise	38	0	

License pool with list of Managed Companies

Industry Certifications

MSPs serve many industries which maintain strict regulatory compliance. Password Management is a key component of compliance requirements within the MC environments. As a Zero-Knowledge platform, Keeper solves critical compliance needs in regards to stored data, password policies and access controls.

Certified SOC 2 Compliant

Customer vault records are protected using stringent and tightly monitored internal control practices. Keeper is certified as SOC 2 Type 2 compliant in accordance with the AICPA Service Organization Control framework. SOC 2 certification helps ensure that your vault is kept secure through the implementation of standardized controls as defined in the AICPA Trust Service Principles framework.

ISO 27001 Certified (Information Security Management System)

Keeper is ISO 27001 certified, covering the Keeper Security Information Management System which supports the Keeper Enterprise Platform. Keeper's ISO 27001 certification is scoped to include the management and operation of the digital vault and cloud services, software and application development, and protection of digital assets for the digital vault and cloud services.

GDPR Compliance

Keeper is GDPR compliant and we are committed to ensuring our business processes and products continue to maintain compliance for our customers in the European Union. [Click here](#) to learn more about Keeper's GDPR compliance and download data processing agreements.

The Keeper website and cloud storage runs on secure Amazon Web Services (AWS) cloud computing infrastructure. The AWS cloud infrastructure which hosts Keeper's system architecture has been certified to meet the following third-party attestations, reports and certifications:



SOC 1 / SSAE 16 / ISAE 3402
(SAS70)



SOC 2



SOC 3



PCI DSS Level 1



ISO 27001



FedRamp



DIACAP



FISMA



ITAC



FIPS 140-2



CSA



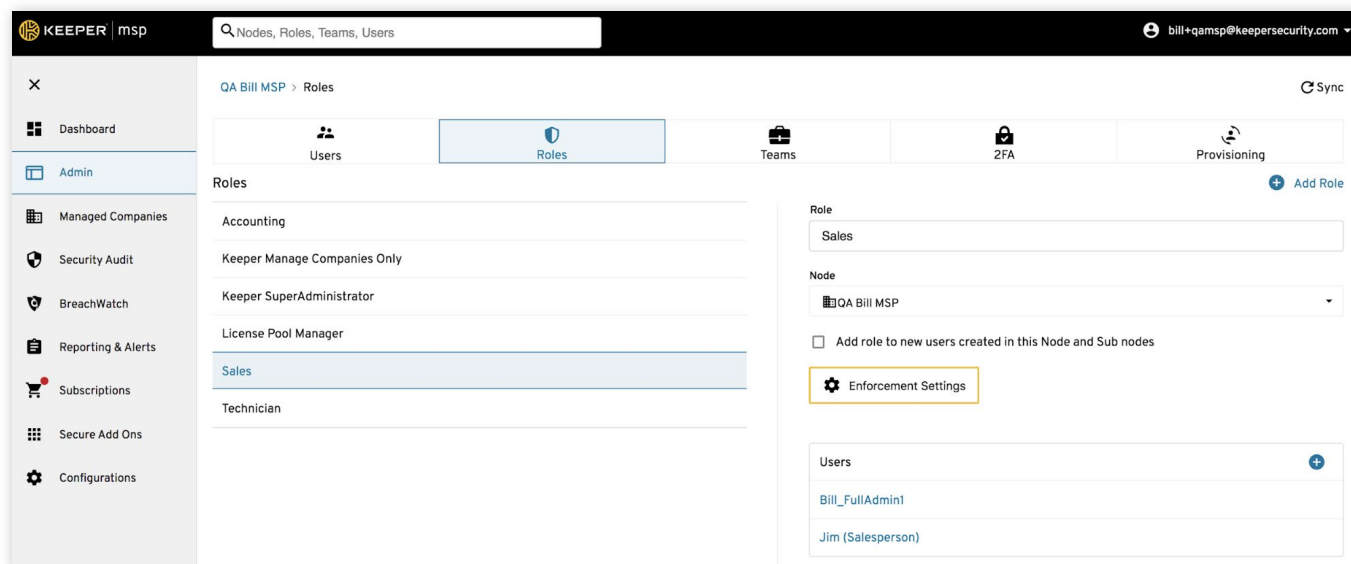
MPAA

Key Functionality

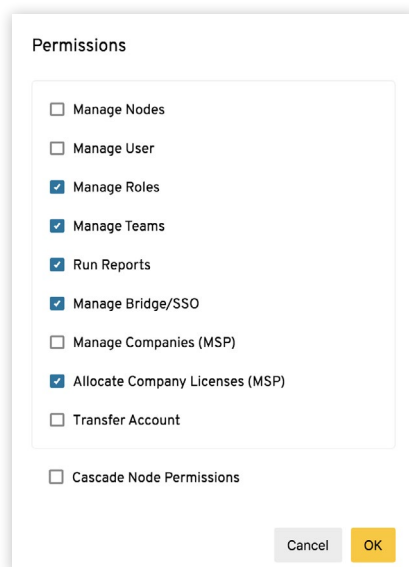
Roles & Enforcements

Roles enable login enforcements to be set for users who are assigned to that role. A robust variety of enforcements are possible, including those limiting platforms, requiring strong passwords, and more. Roles with elevated permissions are also assignable for administrative staff, and allow a variety of actions like managing teams, roles, running reports and more.

Roles are set up in a hierarchical “tree” structure with visibility and inheritance of permissions limited to nodes below the current node, but not sideways to sibling nodes.



Administrative Permissions



Two Factor Authentication (2FA)

Role policies that are enforced across all devices and computers can require the use of several popular two-factor authentication methods such as Duo, RSA SecurID, Text Message (SMS), Google Authenticator and Microsoft Authenticator.

Users of mobile devices may require an extra layer of protection via 2FA both to access their Keeper vault, as well as when accessing important sites or applications. Keeper supports all the native biometric features of the user's preferred device, including fingerprint and facial identification. In addition Keeper has the ability to generate and store Two-Factor Codes in vault records for a more convenient and secure access method when logging into websites and/or applications.

Keeper enables synchronization of a fully encrypted local copy of the user's password vault for offline access. Any changes to the vault are instantly replicated across all devices for consistency and security.






For using 2FA during login to sites or applications Keeper has built in an authenticator capability which will generate a TOTP code when logging in, and which will fill that code into the appropriate field on the site being accessed. This dramatically improves security and convenience, so even if a user's username and password are compromised, access is still off-limits until the 2FA code is provided as well.

Enforcement Settings

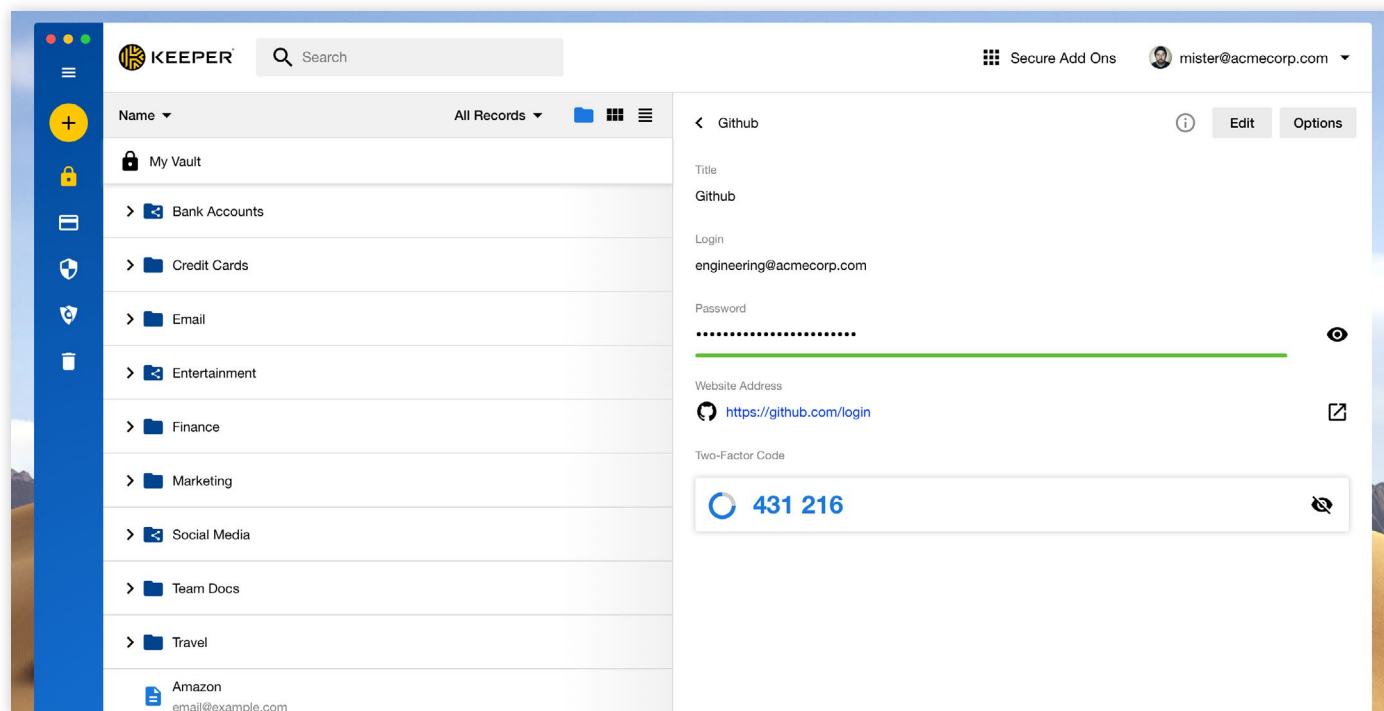
- Login Settings
- Two-Factor Authentication**
- Platform Restriction
- Vault Features
- Sharing & Uploading
- KeeperFill
- Account Settings
- IP Whitelisting
- Transfer Account

Two-Factor Authentication

Require the use of Two-Factor Authentication ☐

Available 2FA Methods	Enable
 Text Message	<input checked="" type="checkbox"/>
 Google and Microsoft Authenticator (TOTP)	<input checked="" type="checkbox"/>
 Smartwatch	<input checked="" type="checkbox"/>
Advanced	
 RSA SecurID	<input checked="" type="checkbox"/>
 Duo Security	<input checked="" type="checkbox"/>

Two Factor code generator in user's vault



MSP Remote Administration & Permissions

- An MSP technician who has the “Manage Companies” permission enabled is able to launch into a MC’s Admin Console with a single click. A separate tab for that MC will open and now the technician has full administrative rights to set up roles, teams, users, etc. for that MC.

- A separate permissions exist to allow an MSP administrator to add/reduce licenses via the MSP's central license pool to an MC. This permission provides the ability to limit who has the “checkbook” for providing licenses to a MC, without restricting their right to act their administrator.

Managed Company

Managed Company Name

Example Medical Clinic, LLC

Active

Options ▾

Plan

Keeper Business

Available for allocation: 100 ▾

License Status

Total Allocated	Reduce Allocation	500
Active		347
License Utilization		69.4%

Additional Licenses

0

Add

[View License History](#)

Cancel

Update


Teams & Shared Folders

Teams can be defined that allow groups of users to share login credentials which are stored as a collection of records in a folder. This functionality can be leveraged by MSP's to set up passwords for use by their MC client. For instance, a series of records with the URL, username, and an initial password could be setup by the MSP technician as the initial “owner”, and then that folder could be shared with a user, or users at the client. Once done, the MSP could relinquish ownership and visibility of that folder so that it is effectively transferred to the MC user and completely private.

Reporting

Keeper’s Advanced Reporting and Alerts Module (“ARAM”) provides filtered views and real time alerts on over 90 different types of events driven by user and administrative activity. These event types have been expanded to include MSP-specific operations:

- ☒ Registered Managed Company
- ☒ Attached to node
- ☒ Increased number of seats
- ☒ Decreased number of seats
- ☒ Changed Plan
- ☒ Renamed Managed Company
- ☒ Paused Managed Company
- ☒ Resumed Managed Company
- ☒ Removed Managed Company



bill+qamp@keepersecurity.com

×

Dashboard

Admin

Managed Companies

Security Audit

BreachWatch

Reporting & Alerts

Subscriptions

Secure Add Ons

Configurations

← Reporting

Report Name

MSP_Events

Cancel

Save

Filters

Users

Event Types (10)

Attributes

Display (7)

Last 30 Days (9/14/2019 - 10/15/2019)

Reset

Apply

Reload

Export

Date	User	Location	Device	Version	Category	Activity
10/15/2019 3:51:17 PM	Bill_FullAdmin1	Mount Laurel, NJ, US	EMConsole	14.3.0	MSP	User bill+qamp@keepersecurity.com resumed enterprise Sergey Financial, premium enterprise, 12 seats
10/15/2019 2:47:51 PM	Bill_FullAdmin1	Mount Laurel, NJ, US	EMConsole	14.3.0	MSP	User bill+qamp@keepersecurity.com increased number of seats for enterprise Sergey Financial by 2
10/14/2019 5:25:01 PM	Bill_FullAdmin1	Mount Laurel, NJ, US	EMConsole	14.3.0	MSP	User bill+qamp@keepersecurity.com renamed enterprise MichelleTrainingCo to Michelle Training Co
10/14/2019 5:24:57 PM	Bill_FullAdmin1	Mount Laurel, NJ, US	EMConsole	14.3.0	MSP	User bill+qamp@keepersecurity.com renamed enterprise RainerMicroBrew Inc, to Rainer MicroBrew Inc,

© 2019 Keeper Security, Inc.

15

SIEM Integration

This module also supports integration with 3rd party Security Information and Event Management (SIEM) tools to support external logging of all events with a simple setup flow for Splunk, Sumo, Amazon S3, IBM QRadar and any other syslog-compatible product.

Versatile provisioning

Import / Email

Users can be invited to the system manually, each time they are created. In addition they can be created in bulk when imported from an email list.

AD Bridge

Keeper Bridge allows businesses running Microsoft Active Directory or Open LDAP to integrate Keeper password management software within their current systems, automatically adding any number of Nodes (a.k.a. Organizational Units), Users, Roles and Teams. Once connected, Keeper enables role-based access control at any Node.

These controls include master password strength, masking, rotation, 2FA, IP whitelisting, biometrics, platforms, sharing and account transfers. Those controls can be cascaded to all lower Nodes if desired. Teams may be provisioned for sharing credentials. As the people move throughout the organization, Keeper keeps their roles updated through AD. This includes locking an account when an employee leaves and the ability to transfer those credentials to a trusted admin.

SSO

Keeper's Single Sign-On solution provides a secure password manager that stores not only login credentials and passwords, but also proprietary customer data, access credentials to restricted systems and sensitive documents.

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.

SSO Connect works with popular SSO IdP platforms such as Okta, Centrify, AWS, OneLogin, Ping Identity, F5 BIG-IP APM, GSuite, Microsoft ADFS/Azure AD and JumpCloud to provide businesses the utmost in authentication flexibility.

Account Transfer

Organizations can enable the Account Transfer feature, which provides a break glass recovery of all records stored in a user's vault if a user was to leave an organization and they find themselves in the position of not knowing that user's master password for accessing critical data in their vault (or security answer for account recovery).

Deploying KeeperMSP

KeeperMSP can support a wide spectrum of deployment models, from full service (“white glove”) MSP’s who manage everything for their users all the way to pure resellers who do little or no administration for their clients.

Full Service model

MSP Technicians have access to a MC’s admin console and thus have full rights to provision end users, set up MC-specific roles, login enforcements, and teams for sharing credentials. These technicians may also choose to set-up a login credentials for users which can be done by sharing records from their personal vaults to those of an MC. This allows an MSP to offer a fully integrated set of services that included a set of pre-configured logins that they can keep updated if needed.

Reseller model

Resellers may simply want to act as distributors and for Keeper and sell the solution to customers who can manage themselves. In his case the MC may can designate a user at MC to handle all management of the system for self-administration. The resellers role would be limited to license management for the MC which can be handled in the KeeperMSP console.

Hybrid model

Both the MSP Technician and the MC Administrator can share responsibilities to manage the system. For instance, for frequently changing or highly specific settings (e.g. which employees are in a team folder) the “local” MC administrator may be able to handle that most efficiently. For large scale initial provisioning and configuration the MSP may be better equipped to facilitate this with Keeper’s Active Directory bridge.

Summary

KeeperMSP combines proven password management functionality with a flexible new capabilities to enable MSP’s to manage a large portfolio of MC’s secure and efficiently.

Business Sales

Americas & APAC +1 312 829 2680	Ireland +353 21 229 6020	Iberia & Italy +34 919 01 65 13
United Kingdom +44 20 3405 8853	EMEA +353 21 229 6011	Sweden & Nordics +46 8 403 049 28
Germany & DACH +49 89 143772993	Netherlands +31 20 262 0932	

Support

Consumer +1 312 971 5702
Business (Americas & APAC) +1 312 226 4782
Business (EMEA) +353 21 229 6019