Rolling out KeeperMSP to your Clients
Introduction

Thank you for purchasing KeeperMSP!

• Now that you are using Keeper’s password manager internally, you know how helpful it is. Keeper is here to help you extend this great capability to your clients (“Managed Customers” or “MC’s”).

• Rolling out to clients is a straightforward process which allows you to increase your revenue at a variety of service levels, from simply reselling it as a passthrough or with full “white glove” administrative service.

• We will walk you through the implementation process along with some best practice recommendations.

Let’s take it to the vault!
Checklist Steps

1. Set up MC’s in the Admin Console
   - Purchase licenses
   - Add the company

2. Admin set up for the MC
   - Set up role enforcements in the console
   - Designate at least one “local” admin

3. Setting up MC users
   - Announce Keeper password vaults are coming and briefly explain why they are important
   - Provision users for each MC (via email)
   - Track user’s accepted invite
   - Track creation of vault records & password via the console’s Security Audit
Step 1: Add a Managed Company (MC)

- “NewCo” wants Keeper Enterprise base license
  - Needs 10 seats

- Review your licenses, do you have enough to allocate?
  - If not, purchase more to cover their needs

- Add “NewCo” as a Managed Company
Purchase Licenses for MC’s in Bulk

• Monthly basis

• Purchase a mix of SKU bundles (Business Base, Business Pro, etc) which go into pool

• Then can assign bundle licenses in the pool to each company
NewCo is now a Managed Company with 10 licenses

To administer NewCo, click here

<table>
<thead>
<tr>
<th>Company</th>
<th>Plan</th>
<th>Allocated</th>
<th>Active</th>
<th>Launch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flintstone Rock &amp; Garden</td>
<td>Keeper Business</td>
<td>9</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Sierra Adventures</td>
<td>Keeper Business Plus</td>
<td>14</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Claimstake Brewing</td>
<td>Keeper Enterprise Plus</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Dunder Mifflin</td>
<td>Keeper Enterprise</td>
<td>25</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>NewCo</td>
<td>Keeper Enterprise</td>
<td>10</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Step 2: Set Up MC Administration

- Keeper allows for granular control of how users can access their vaults
- Multiple enforcement settings can be placed on roles for different classes of users
Setting Up Enforcements

Enforcement Settings

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

Master Password Complexity

Allow users who login with SSO to create a Master Password.

Length: 12
Digits: 2
Special Characters: 1
Uppercase Letters: 0
Lowercase Letters: 0

Master Password Expiration

Master password expires every 30 days.
Step 3: Setting Up Users

Dashboard
Admin
Security Audit
Configurations

NewCo > Users

Add User

Node
NewCo

Full Name
Bill Adminiudo

Email Address
tjineveworf1@keepersecurity.com

Import Users
Simply drag and drop a comma-separated value (CSV) file using this format:
Email Address,Name,Role e.g. joe@test.com,Joe Smith,Manager

Drag and Drop CSV File
Browse Files

Cancel Add
User invited via Email

Inform users to check email and accept invitation.
User Sets Up Vault

A member of your organization's security team, bill+msp@keepersecurity.com, has provisioned a Keeper Security account for you. Keeper is the leading password security and management software for protecting organizations against password-related data breaches and cyberthreats.

Setting up your account is easy and takes less than a minute. Please create your Keeper account using the email address bill+newco1@keepersecurity.com.

Verification Code: 9276076454

Set Up Your Account Now

Please contact your Keeper Administrator, bill+msp@keepersecurity.com if you have any questions or need assistance.

Thank you,
Keeper Security
User Added First Record to Vault

- Name: Newco HR System
  - bill@newco.com
Verify User Compliance with Security Audit

Security Audit Score

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.

Record Password Strength

- Strong: 100%
- Medium: 0%
- Weak: 0%

Unique Record Passwords

- Unique: 100%
- Reused: 0%

Two-Factor Authentication

- On: 0%
- Off: 100%

<table>
<thead>
<tr>
<th>User</th>
<th>Record Password</th>
<th>Unique Record Passwords</th>
<th>2FA</th>
<th>Security Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill Adminidue</td>
<td>Weak 0</td>
<td>Medium 0</td>
<td>Strong 1</td>
<td>Reused 0</td>
</tr>
</tbody>
</table>
Thank You!