1Password | Partner Portal

Reference Card

Technician EPM Setup Checklist

MSP - Internal Company Setup

This checklist is a handy reference sheet to help guide you in the setup of 1Password Enterprise Password Manager and decisions needed as you set up 1Password for your organization. We recommend using this checklist to ensure all the bases are covered and your organization is set up for success.

✅ Checklist for a MSP Setting up 1Password Internally

- ☐ Best Practices for a Business account
- ☐ Manage the Emergency Kit for non-SSO users
- ☐ Signing-in to 1Password with SSO on multiple devices and how to trust devices
- ☐ Get the apps on a desktop and mobile device
- ☐ Import data from other applications into 1Password
- ☐ If passwords are stored in Chrome and have them synced with their Google account, you may need to visit passwords.google.com and turn off auto sign-in there as well
- ☐ Turn off the built-in password manager in their browser
- ☐ Implement a recovery plan for your team
- ☐ Create and manage custom groups to organize your team
- ☐ Create new vaults to give people access to the items needed
- ☐ Set up 1Password Team Policies for your organization
- ☐ Turn on two-factor authentication for the 1Password account, and consider if you want to enforce two-factor authentication for everyone
- ☐ Securely share 1Password items with anyone and manage how they can shares items
- ☐ Invite your team when the account is set up
- ☐ Share Get started with 1Password and applicable training resources (administrators and end-users) to set team members up for success in using their password management solution
- ☐ Show users how to redeem their free 1Password Families membership from My Profile
- ☐ Off boarding team members

Decisions Needed Before Inviting Users

How are users being invited?

When inviting specific users, manual invitations or auto-provisioning will be the best options. For a more passive enrollment, consider using the sign-up link option.

- For auto-provisioning; reference the SCIM bridge pre-deployment checklist
- For a detailed implementation and best practice plan for SSO; reference the MSP Admin: SSO Adoption Kit, Admin FAQs and End User FAQs.

Who will be able to create a vault?

By default, all users will be able to create vaults. This can be changed by managing permissions.

Is anyone supporting account recoveries outside of owners and admins?

By default, owners and administrators will have the permission to recover users who have lost their Emergency Kit or forgotten their password. You can create custom groups with granular permissions in case you want others outside of owners and administrators to complete this task as well.

What would you like the account password policy to be?

You can set a password policy on employee account passwords – the one password they need to remember to unlock 1Password. 1Password will not prompt users to change their password if the policy is changed, so set the password policy prior to inviting the team.

Would you like to enable or enforce two factor authentication?

You can opt to enable or leave two-factor authentication off. You can also select which two-factor authentication methods are allowed, and/or enforce two-factor authentication for the entire team.

Do you intend on allowing users to share information outside of 1Password?

1Password helps to securely share copies of passwords and other items that have been saved in 1Password with anyone, even if they don't use 1Password. You can manage permissions for item sharing and change who the team can share items with outside the account and how long item links can be shared.