1Password

Owners & Administrators Checklist

Welcome to 1Password! Now that training is complete, before you start inviting users, review this checklist to cover all your bases and set your team up for success.

Review all the key settings listed here for your preferred deployment, whether that's Secret Key or Single Sign-On, before you invite your team. We recommend that all steps outlined for your method be reviewed and completed before sending invites to end users.

01 Is anyone supporting account recoveries outside of your Owners and Administrators?

By default, Owners and Administrators will have the permission to recover users who have lost their Emergency Kit or forgotten their password. It's extremely important to have at least two users with Recover Accounts access, which can also be assigned to a custom group. You can create custom groups with granular permissions in case you want others outside of Owners and Administrators to complete this task as well.

02 How are your users being invited?

If you are inviting specific users, manual invitations or auto-provisioning will be your best options. Auto-provisioning through the SCIM Bridge saves time by auto-confirming new users and allows you to push group membership from your identity provider. If you were hoping for more passive enrollment, you should consider using the sign-up link option.

03 How do you want your team to unlock 1Password, with a Secret Key or SSO?

Choose your next step based on the method your team will be using to unlock and access 1Password.

Accounts unlocking with Traditional Unlock (with Emergency Kit/Secret Key)

Or

Accounts unlocking with Single Sign-On (SSO)

04 What would you like your account password policy to be?

For those unlocking 1Password with an Emergency Kit or Secret Key, you can set a password policy for 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 later, so set your password policy prior to inviting your team.

Note: If you're intending to use Single Sign-On, the account password policy does not apply to your organization. Those settings are controlled by your identity provider (IdP).

05 Would you like to enable or enforce two-factor authentication (2FA)?

For those unlocking 1Password with an Emergency Kit or Secret Key, you may leave two-factor authentication as optional or choose to enforce it for your entire team, including which 2FA methods are allowed.

Note: If you're intending to use Single Sign-On, the 2FA enforcement does not apply to your organization. Those settings are controlled by your identity provider (IdP).

04 Learn how to integrate 1Password with your identity provider.

Learn how to integrate 1Password with your identity provider so your team can unlock with Single Sign-On (SSO). You'll need to configure some settings on the Owners and Administrators side, along with giving your end users an overview of what will be changing. Each user will need to sign into their 1Password apps again with SSO, they will then receive a verification code the first time they sign in to confirm the trusted device.

Trusted devices help maintain security and it is recommended that end users sign in to 2 devices (if your security policy allows). This mitigates account recoveries from end users.

Use our SSO Adoption Kit (in our 1Password Launch Kit) to help make your transition to SSO a smooth process for you and your end users. *Note*: As a preventative security measure against account lockout, Owners group cannot use SSO.

05 Is there anything else I need to set up for SSO?

Once you have first signed up or switched to Unlock with SSO, you will need your one time verification code from a previous trusted device, to sign in on a new web browser or new device.

06 Would you like to provide your team Emergency Kits?

You can turn off Emergency Kits for your team to prevent team members from saving one. You can turn off Emergency Kits if you're an owner, administrator, or part of a group with the Manage Settings permission.

To turn off Emergency Kits for your team, you can turn off the option within the authentication policy page.

07 Would you like to set additional policies around how your team saves, accesses, and shares data in 1Password?

Manage and review your policies across authentication, app usage, and more. Manage whether you will allow your team to share information outside of 1Password and/or how long item links can be shared.

08 Who will be able to create vaults?

By default, all of your users will be able to create vaults. Change this by managing permissions for your Team Members Group. If you'd like to manage your vault structure, consider these best practices.

09 Will your team download the 1Password apps on their own or will you pre-install them on their managed devices?

We suggest automatically deploying the 1Password desktop application and browser extension for your team, for example with a mobile device management (MDM) system to help support stronger adoption and usage. Otherwise, you can direct your team to download the 1Password desktop application and browser extension as they set up their 1Password account.

10 Do you have any data from previous password managers or solutions that you would like to import to 1Password?

Import any shared data from previous solutions to 1Password and customize your groups and shared vaults for users based on your organization's sharing needs, while keeping in mind the principle of least privilege. Reference our groups and vaults setup videos and **Guide for Setting up 1Password for large organizations** in our 1Password Launch Kit.

Congratulations! You've now set up and customized your 1Password account based on your company's needs. Now you're ready to invite your team's users!