1Password

Frequently Asked Questions

Unlock 1Password with SSO for End Users

What is Unlock with SSO?

Unlock 1Password with Single Sign-On (SSO) lets you sign in to your 1Password account using your identity provider credentials instead of an account password.

Without Unlock with SSO, you'll sign in to your 1Password account on any device using your account password and Secret Key.

With Unlock with SSO, you'll sign in to your 1Password account on your first trusted device using your identity provider credentials. Next, sign in to your 1Password account on a new device using your identity provider credentials and enter the verification code sent to your trusted device.

Where should I store my SSO password if I previously stored it in 1Password?

When Unlock with SSO is enabled by your administrator, your 1Password login is replaced by your identity provider login. While identity providers don't have Emergency Kits like 1Password does, a user can still store their identity provider password in ways similar to what we recommend for storing Emergency Kits.

We recommend users create a password for your identity provider that is random but memorable, and 1Password can help with that. Doing so eliminates the need to store the password anywhere other than in your memory. That password then becomes the only password you need to remember.

What is a trusted device?

When you set up Unlock with SSO, the device you initially use becomes your primary trusted device. Being trusted means this device has a unique key that encrypts your credentials, allowing it to sign you in securely.

When you sign in on a new device using SSO for the first time, that device undergoes an enrollment process. During this process, your credential bundle is securely transferred from your existing trusted device to the new one. This enables the new device to complete the sign-in process independently and decrypt your 1Password data, essentially becoming a trusted device itself.

Learn more about trusted device security.

What happens if my admin turns on Unlock with SSO?

If you're new to 1Password and signing up for the first time using Unlock with SSO, you'll receive a sign-up email that will prompt you to sign in to 1Password using your identity provider login. Once you sign in, your 1Password administrator will confirm your account and you're ready to start using 1Password.

The migration process when moving from account password and Secret Key to Unlock 1Password with SSO is just as simple. Once your admin configures Unlock 1Password with SSO, you'll see a pop-up in 1Password the next time you sign-in. You'll also receive an SSO migration email. The subject line of the email will look like "Set up 1Password with {Your identity provider} in X days".

Follow the sign-in flow steps, including signing in to your SSO identity provider and completing the migration. During migration, the first device and application you sign in on becomes your first trusted device. The next time you sign out and sign back in to 1Password, you will see the option to unlock with SSO rather than the account password. Watch the video tutorial for a step-by-step walkthrough.

What happens if I don't switch to SSO by the deadline?

If you don't switch to unlock with SSO before the grace period set by your 1Password administrator ends, you'll see a message that reads "User unable to sign in because grace period is expired." Your data will continue to be stored in 1Password, however you will not be able to access your account if you have not switched to SSO by the deadline.

If you see this message, contact your 1Password administrator for help recovering your account.

How do I log in to 1Password with SSO on another device?

When your team unlocks 1Password with SSO, the first time you sign up or switch to Unlock with SSO, you'll set up a trusted device. You can then use this device to verify other devices you want to add to your account. The verification process is an essential part of making sure the secrets you store in 1Password are safe and encrypted end-to-end.

You simply need to sign in to 1Password with your identity provider credentials on a new device or browser. You'll then be prompted to acknowledge the enrollment by unlocking 1Password on any of your existing trusted devices and entering a verification code.

Watch the video tutorial for a walkthrough, or review the support article on setting up trusted devices for more details.

Can I opt to continue using my account password and Secret Key instead of switching to SSO?

If your administrator mandates the use of the Unlock with SSO sign-in method for your team, you won't be able to sign in to 1Password Business account with your account password and Secret Key. To get more information about this policy and find out if the option to use the account password and Secret Key is available, please contact your 1Password administrator.