1Password

Frequently Asked Questions

Unlock 1Password with SSO for Administrators

How secure is unlocking 1Password with SSO?

Unlock with SSO maintains our zero-knowledge architecture and end-to-end encryption, with decryption still happening on-device. That said, it's important to understand how the security model and risk considerations differ from the standard 1Password model when performing a risk assessment.

Unlocking with your identity provider provides an additional layer of identity-proofing on top of the existing 1Password security model. 1Password uses the employee's encrypted credentials and device key to Unlock with SSO, simplifying the enrollment process and eliminating the need for an account password.

For more information on the model and the risks associated, refer to the Unlock with SSO security model support article.

How does 1Password's approach to SSO compare to competitors?

Most enterprise password managers typically support SSO by taking one of two approaches.

The first is an auth bridge, which creates a large and attractive target for an attacker, and requires customers to maintain on-premise infrastructure. The second is a shared encryption key for every user's data, which means if a single employee is compromised, the entire company is put at risk. Neither of these approaches meet our stringent security requirements.

We opted to use a trusted device model, which means that if your identity provider credentials are ever compromised, attackers still won't have access to your 1Password data. Unlock with SSO removes the need for the Secret Key, but does so in a way that keeps all data secured on-device. A bad actor would still need a trusted device in order to prove your identity and access the data locked away inside your vaults. Your data remains protected – and now it'll be even easier to sign into new devices that you own.

Our approach maintains zero knowledge, and is end-to-end encrypted, as decryption still occurs on-device. **We don't store or have access to the keys needed to decrypt your data.**

Where should users who are scoped to unlock 1Password with SSO store their identity provider password if they previously stored it in 1Password?

When you enable Unlock with SSO, your 1Password login is replaced by your identity provider login. While identity providers don't have Emergency Kits like 1Password, users can still store their identity provider password in some similar ways as 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.

Does Unlock 1Password with SSO also do automatic provisioning, or is the SCIM bridge still needed?

The 1Password SCIM bridge is still required for automated user provisioning and you are still required to deploy the bridge within your environment.

Unlock with SSO will require a separate configuration and is not directly tied to the automated user provisioning that the 1Password SCIM bridge provides. You will not need to set up a separate infrastructure to use SSO to unlock 1Password.

While these features are configured separately, and you could use SSO to unlock 1Password without using the SCIM bridge for provisioning, we recommend using both for the best, most secure, and automated experience.

How does an existing user migrate from account password to Unlock with SSO and vice versa?

The migration process from moving from account password to unlock 1Password with SSO is simple. Once a user is required to unlock with SSO, they will see a pop-up the next time they sign in.

Then, they simply follow the instructions, including signing in to their identity provider and completing the migration. During migration, the user's device becomes their first trusted device. The next time they sign out and sign back in to 1Password, they will see the option to unlock with SSO rather than the account password. At that point, they will no longer have an account password, Secret Key, or Emergency Kit to maintain.

Disabling SSO and re-establishing an account password and Secret Key requires the user to go through account recovery. The user will receive an email to complete account recovery, set up a new account password, and get a new Secret Key and Emergency Kit. Please note that Account Owners cannot unlock 1Password with SSO; this prevents any accidental lockout.

Can I disable the SSO trusted device workflow and verification codes?

No, you cannot disable the SSO trusted device workflow. The trusted device enrollment process is fundamental to 1Password's end-to-end encryption.

Devices are defined as:

- Web Browsers (Safari, Firefox, Chrome, Brave, Arc, etc)
- 1Password 8 Desktop App (Windows, Linux, macOS)
- 1Password 8 for Android
- 1Password 8 for iOS

We recommend always signing in to two devices. Ideally this would be:

1. The browser the user created their 1Password account with.
2. 1Password for Windows, Mac, or Linux.

We've gone into detail on the security model and trusted device process behind Unlock with SSO on the 1Password blog. You can also refer to 1Password Support for instructions on setting up trusted devices.

Why can't 1Password use trusted device data from my identity provider or MDM tools?

There's a security/privacy risk with this approach. If we connect to your identity provider or MDM tools, we have visibility into your dataset, which would present a considerable responsibility on our end as well as violating our core privacy values.

Removing this functionality would also weaken security by removing our end-to-end encryption, making our solution susceptible to cyberattacks. Without device approval process, MITM (Man-in-the-Middle) attacks or malicious 1Password employees could replace requested keys and gain full access to user data.

Can a customer use two different identity providers for Unlock 1Password with SSO?

No, you'll need to pick one identity provider as your SSO provider. You won't be able to use multiple identity providers for SSO authentication. We recommend using the same identity provider you use for your account provisioning via SCIM bridge for the best experience.

Can I enable Unlock with SSO for some employees and not others?

Yes. You can designate which groups within your 1Password account can unlock 1Password with SSO, including custom groups and built-in default groups (i.e., Admins, Team Members), with the exception of Account Owners. You also have the option to exclude Guest users from using single sign-on.

Owners cannot unlock 1Password with SSO and must use their account password and Secret Key. This decision has been implemented to prevent accidental lockout and potential data loss if an Owner loses access and no one else can recover them.

Can employees still access 1Password if our identity provider goes down?

Users who have been scoped to Unlock 1Password with SSO and have biometrics enabled can access the 1Password client apps (desktop and mobile) offline or if the identity provider goes down. In the event of an identity provider outage, account owners will still be able to log in with their password and Secret Key. In an emergency, Owners can adjust SSO policies to require users to reestablish password and Secret Key authentication.

Can 2FA still be enforced in 1Password for users with Unlock with SSO enabled?

Users that you enroll in Unlock with SSO will no longer have 2FA enforced for them on the 1Password account.

Instead, your identity provider will now govern the 2FA requirements for your users. Any enforcement and settings set in your identity provider around 2FA will apply to users unlocking 1Password with the identity provider.

Can firewall rules be set-up in 1Password when Unlock with SSO is enabled?

Firewall rules will still be able to be applied within the 1Password Business account from the Security section of your account, even if users are scoped to unlock 1Password with SSO.

You can also set firewall rules in your identity provider that would apply when the user is unlocking 1Password with SSO, and therefore authenticating to the identity provider. After they have unlocked 1Password, then the firewall rules set in 1Password would apply.

How is the grace period for Unlock with SSO calculated?

For selected groups, the grace period will begin for a group when you add them in the configuration settings to Unlock with SSO. It's important to note that users can be added to a group after the grace period expires. In that case, users are placed into recovery and must complete the recovery process to configure single sign-on.

In the scenario that a group's grace period expires and you want to continue offering a migration grace period, you will need to create a new group and add it to your SSO policy.

If the "Everyone" option is chosen, then the grace period begins the day it is selected.

Why do I need to perform account recoveries in 1Password instead of my identity provider?

Account recovery occurs in your identity provider if a user no longer remembers their credentials to your identity provider. On the other hand, if users no longer have access to a trusted device for 1Password, recoveries would be performed in 1Password. This is primarily as a result of our trusted device security model.

The most common scenario we see for users needing account recovery in 1Password is when they only have a single trusted device set up. If they lose access to that trusted device, they'll need to reach out to a 1Password administrator to initiate account recovery. To avoid this, we recommend deploying the 1Password desktop applications to all users and enrolling the application as a new trusted device. If a second trusted device is set up, users will be able to retrieve a trusted device verification code to re-enroll an additional device that may have been deauthorized.

Our users log into new computers or virtual Windows environments every day. How can I prevent them from having to sign-in with SSO every time?

A lack of data persistence creates a difficult environment for 1Password, since our software depends on storing and processing data on a trusted device. This is part of balancing our security model. It may or may not be possible to run 1Password effectively in this kind of environment, but there are a few things to try on Windows. Sometimes companies that run computers like this can synchronize certain data so that it is available to the user every time they log in. There are a few directories customers can add to their user data sync system that may make life easier.

For the browser extension, ensure that the extension is installed in the browser automatically and can try to sync the following directories to potentially allow the user's account to show up:

- The path for Chrome (*%LocalAppData%\Google\Chrome\UserData\Default\IndexedDB*), and Edge is the same, just subbing in `Microsoft\Edge` for `Google\Chrome`

For the Windows desktop application:

- If installed using the .msi installer, 1Password is stored in *%ProgramFiles%*, along with all other applications
- If installed using the .exe installer, data will be stored in *%LocalAppData%*