1Password

# Unlock 1Password with Single Sign-On Adoption Kit

This kit includes everything you need to successfully enable, roll out, and manage Unlock 1Password with Single Sign-On (SSO) across an entire organization.

1Password

# Awareness

Let's start with an overview of the business value, key benefits, and security considerations of unlocking 1Password with Single Sign-On (SSO).

## *Identity provider integrations: SSO vs SCIM*

1Password Business offers two types of integrations with identity providers:

- The SCIM bridge for automated user lifecycle management and role-based access control.
- Single Sign-on (SSO) using the OpenID Connect (OIDC) protocol to let end-users unlock 1Password with their identity provider credentials. Configuring these integrations is done by setting up two distinct applications in most identity providers.

These integrations serve two different functions and interact with your 1Password tenant in distinct ways.

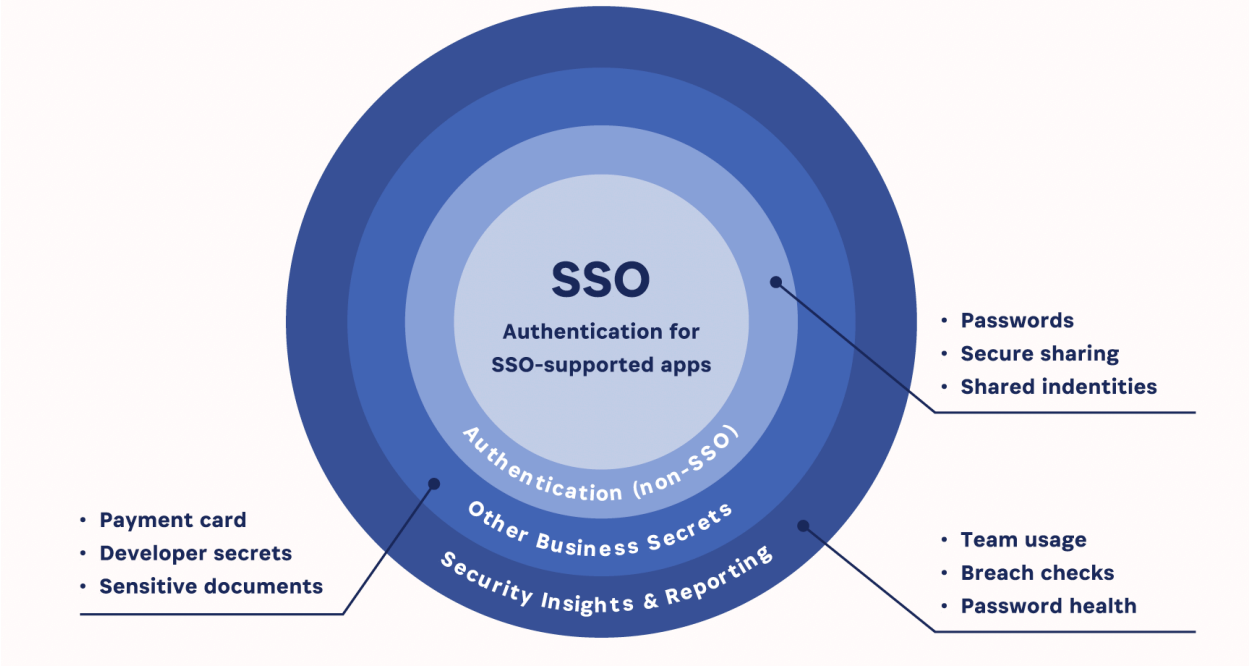
The 1Password SCIM bridge operates as an API endpoint to continue communicating with the 1Password servers via an encryption protocol (SRP).

Single Sign-on (SSO) uses a direct API integration with the 1Password servers to let an end user authenticate using their SSO credentials. This results in the local 1Password application being given authorization to unlock the local database.

## *Business value*

Using a Single Sign-On (SSO) solution is a reasonable way to strengthen password security by simplifying account access. It does, however, have security limitations. When using SSO alone, many websites or applications may not be protected because they aren't compatible with the necessary authentication protocols. 1Password protects the company assets and resources when SSO can't.

Employees can use 1Password to create strong, unique passwords for apps and services that aren't covered by the identity provider. That gives the company more comprehensive access and security, and the ability to safeguard secrets that aren't covered by the identity provider, like documents, secure notes, and SSH keys.




Unlock 1Password with Single Sign-On let's 1Password Business users sign in to their 1Password accounts using their identity provider credentials instead of their account password and Secret Key.

- Without Unlock with SSO, users sign in to their 1Password account on any device using their account password and Secret Key.
- With Unlock with SSO, users sign in to their 1Password account on their first trusted device using their identity provider credentials. Users then sign in to their 1Password account on a new device using their identity provider credentials and by entering a verification code sent to their trusted device.

---

With Unlock with SSO enabled, your 1Password login is now 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, eliminating the need to store the password anywhere other than in their memory. This is now the only password they need to remember. 1Password can generate memorable passwords by changing the password type from "random password" to "memorable password."

## *Key benefits*

**Designed with a security-first approach to minimize risks and possible threats.** Integrate with your identity provider to access 1Password using Single Sign-On with zero-knowledge and end-to-end encryption preserved. See the Security overview for more information.

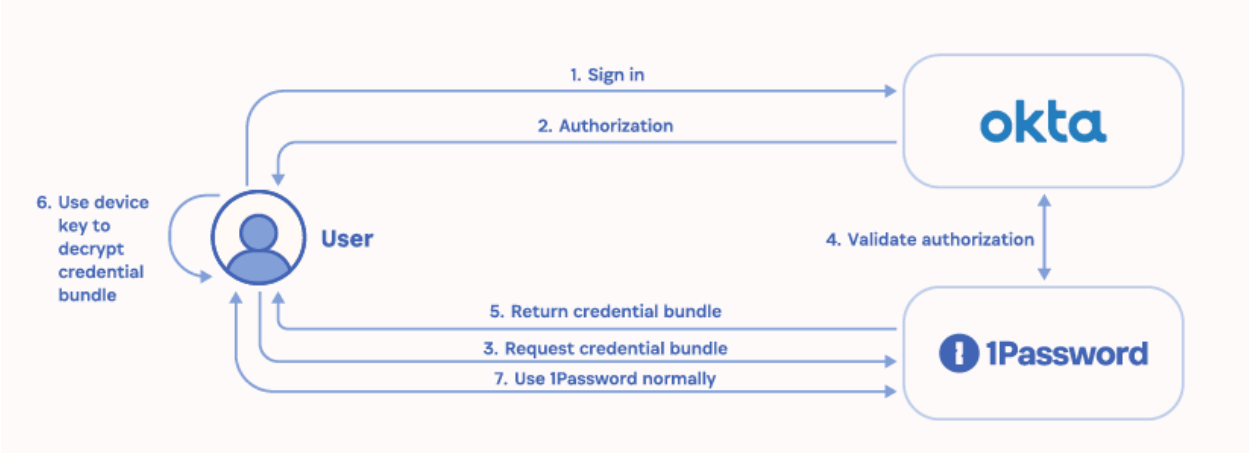
**Secure access to passwords and sensitive information.** Let employees use their identity provider to authenticate 1Password so they can access their vaults without the need for an account password. Take advantage of secure biometrics for more flexibility on how employees access vaults.

**Simple admin management.** Use the setup wizard to set policies and roll out Unlock with SSO in just a few clicks.

## *Security overview*

Unlock with SSO acts as an additional layer of identity-proofing on top of the existing 1Password security model. That model requires an account password and Secret Key to access and unlock your account. The account password is a secret that you remember and should only be stored in your brain.

Unlock with SSO works differently. 1Password first confirms that a team member has authenticated to their identity provider, then downloads the team member's encrypted credentials. The team member's device key, which is stored on each device set to Unlock with SSO, is used to decrypt the credentials and access their 1Password data. When this process is complete, Unlock with SSO works just like 1Password with traditional unlock.




**Fundamentals of the Unlock with SS0 security model:**

- **Zero-knowledge architecture and end-to-end encryption** is maintained by the fact that decryption occurs on device. We still do not have access to the keys needed to decrypt a user's data.
- **The trusted device model authorizes the initial device and new devices to securely access your 1Password Business account.** This is fundamental to 1Password's end-to-end encryption, letting the new device sign in to their account and decrypt the 1Password data while keeping their secrets safe.

When they enter the verification code, 1Password securely transfers a credential bundle from the existing trusted device to the new device. The new device then uses the bundle to sign in to the 1Password account, register itself as a new trusted device, and encrypt the credential bundle with its own device key. This allows the new device to sign in to the account and decrypt the 1Password data independently while keeping the secrets safe. The trusted device enrollment process is not a form of multi-factor authentication, nor is it a replacement for existing device management programs the organization may have in place.

Learn more about the Unlock with SSO security model and the risk considerations

1Password

# Customer stories

Discover how 1Password customers use Unlock with SS0 to easily access their vaults by signing in with their identity provider.

1,400 employees secured in weeks: How 1Password's SSO integration helped Frontiers protect its global workforce

How Airwallex is using 1Password to eliminate all passwords at work

---

To learn more about customer experiences on 1Password, visit - https://1password.com/resources/

# Training Resources

## *Articles and PDFs*

[Article] How 1Password and SSO fit together - and what comes next
[Article] 1Password and SSO: A perfect match
[Article] Unlock with SSO: Under the Hood
[Article] Unlock 1Password with Duo, Onelogin, and More
[Article] Passkeys vs. SSO: What are the differences?
[PDF] Unlock with Single Sign-On: 1Password vs. LastPass
[PDF] Pair 1Password with your existing 1AM infrastructure

## *Support documentation*

About 1Password Unlock with SSO security
Get started with 1Password Unlock with SSO
Administrator: Set up Unlock 1Password with SSO for your team
Configure Unlock 1Password with JumpCloud
Configure Unlock 1Password with Microsoft Entra ID
Configure Unlock 1Password with Okta
Configure Unlock 1Password with SSO using OpenID Connect
Sign in to 1Password with SSO
Set up trusted devices to unlock with SSO
If you're having trouble unlocking 1Password with SSO

1Password

## *On-demand webinars*

Unlock 1Password with SSO: What you need to know

1Password

# Planning and change management

## *Rollout plan*

### Align on the rollout goals and stakeholders

What does the customer hope to accomplish with the rollout of Unlock 1Password with SSO? For example, the goal might simply be to validate that Unlock with SSO works for the company use cases in a certain amount of time. Pinpoint how to monitor and measure the success, and track against the goals.

With a firm understanding of the goals, engage the stakeholders. Consider adding stakeholders to the table below to get started:

**SO:** Sign-off on the rollout, **R:** Review project and provide input, **I:** Informed of this project

| | | |
|---|---|---|
| Enter name and email | **MSP Administrator/Technician**<br>A representative from the MSP organization who can provide input from an admin and help desk perspective. | **SO** |
| Enter name and email | **Security Owner**<br>A representative from the security team that can sign off that the plan will meet the security requirements of the organization. | **SO** |
| Enter name and email | **Managed Company**<br>A representative from the managed company that can sign off that the plan will meet the use case of the organization. | **SO** |
| Enter name and email | **Enter role** | **Enter ownership** |

Ensure each stakeholder has the appropriate access to the *Policies* tab in 1Password to access the *Unlock with Identity Provider* configuration page. By default, admins and owners have access to the page, which is required to complete an SSO integration.

## *Consider the implementation approach*

Once Unlock 1Password with SSO is enabled, it will be required for enrolled users. Users who are required to sign in with SSO will get an email once the configuration is saved. The email will prompt the team to connect their 1Password accounts with the identity provider. A user who has not yet linked their 1Password account to the identity provider will be prompted to link them at their next login, or if they're already logged in, they'll see a sign-in page when they try to access their vaults or items. If not planned and communicated clearly, your rollout could cause confusion and disruption for team members.

**Consider these best practices:**

**Plan which users will be unlocking 1Password with SSO**

If they are  just getting started with 1Password and would like all users to Unlock 1Password with SSO from day one, we recommend configuring your settings to enroll everyone but guests. All existing users will be prompted to switch to Unlock with SSO, and all new users will use their identity provider username and password when joining 1Password.

If they're migrating from traditional 1Password unlock (account password and Secret Key) to Unlock 1Password with SSO, we recommend taking a phased approach to rolling out by selectively enabling and testing specific groups of users at a time. This will allow you to identify and solve any roadblocks with minimal impact and make training smoother for the employees.

**Consider whether or not; users will be able to access data stored in 1Password while offline**

Enabling biometrics for Unlock with SSO allows users to authenticate to 1Password using biometrics, giving them access to their vaults and data even if they're offline. If they choose not to enable biometrics, users will only be able to

unlock 1Password with SSO when they are online to make the connection to the identity provider.

**Determine your grace period**
Users who already have 1Password accounts will need to switch to Unlock with SSO. They have the option to specify a grace period, or the number of days before users must make the switch. The default is 5 days, but you have the option to set it to 1 to 30 days. Review these considerations when determining a grace period.

**Plan to deploy the 1Password desktop application**

The most common scenario we see for users who need account recovery in 1Password is when they only have a single trusted device set up, or they clear the cache of the browser where they first signed into 1Password. This is primarily a result of our trusted device security model. To avoid this, we recommend deploying the 1Password desktop application 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. Learn more about implementing a recovery plan for the team.

**Communicate frequently with users ahead of time**

While SSO can simplify signing in to 1Password, change management is always a challenge. Be sure to let them know why this change is happening and how it will benefit them. The change communication templates in the roll out section below is a good place to start.

**Timeline**

Tracking the rollout plan is an important aspect of the project's success. Consider creating a task list for the rollout to monitor and schedule the timelines and key stakeholders to help keep everyone on track.

1Password

# Design and configuration

There are several considerations and ways to configure Unlock 1Password with SSO. Be sure to review the Set up 1Password Unlock with SSO support article and the Before you begin section for important considerations when configuring this feature.

Additional getting started and configuration support articles are also linked below:

- Get started with 1Password Unlock with SSO
- Administrator Setup Unlock 1Password with SSO
- Configure Unlock 1Password with JumpCloud
- Configure Unlock 1Password with Microsoft Entra ID
- Configure Unlock 1Password with Okta
- Configure Unlock 1Password with SSO using OpenID Connect

1Password

# Testing your configuration

Create a list of test scenarios for Unlock with SSO on various devices and browsers. These test cases should reflect the specific business use cases. See example test scenarios below:

| | | |
|---|---|---|
| Owner attempts to enroll in Unlock with SSO | Owners accounts will be unaffected by the SSO configuration and will continue to be required to use their account password and Secret Key to log in. | Did your actual result match the expected result? |
| End user logs into 1Password.com on their browser for the first time | The end user navigates to 1Password.com and signs in with their identity provider credentials, creating their first trusted device.<br>The admin confirms their enrollment. | |
| End user attempts to log into 1Password.com on their first trusted device, but the admin hasn't confirmed their enrollment | The admin confirmation will not block the end user enrollment.<br>They can continue to log in uninterrupted. | |
| End user signs into the 1Password application on a new device | The end user will sign into 1Password with their identity provider credentials on a new device or browser. The user is then prompted to acknowledge the enrollment by unlocking 1Password on any existing trusted devices and entering the verification code. | |
| End user attempts to log into 1Password with SSO but enters the incorrect password for their identity provider | The end user will see a sign-in error message and will be prompted to enter the correct password. | |
| End user signs into the 1Password application on the same device where they first signed in to 1Password.com | The end user will sign in to the 1Password application with their identity provider credentials. The user is then prompted to acknowledge the enrollment by unlocking 1Password on their existing trusted device (1Password.com) and entering the verification code. | |
| End user attempts to add a new trusted device but enters the incorrect verification code | The end user will see an error message and will be prompted to re-enter the correct verification code. | |

After you complete all of the testing based on the test cases above, you're ready to roll out Unlock with SSO to additional users.

# Rolling out Unlock with SSO

After you complete the planning, configuration, and testing, it's time to roll out Unlock with SSO to the rest of the organization.

## *Provide change communication to end users*

The end user experience is going to change when they access 1Password moving forward. You can distribute the readiness materials to the users before the SSO rollout. Educating them on the feature and the changes will help reduce help desk tickets and drive positive adoption for the deployment of Unlock with SSO.

- SSO Frequently Asked Questions for Administrators
- SSO Frequently Asked Questions for End Users
- Deployment email and communication templates are available in the MSP Launch Kit for download and use

## *Turn on Unlock 1Password with SSO for additional users*

Return to the 1Password admin console and make sure you've added all of the users to 1Password. Navigate back to the Unlock with SSO settings page in the 1Password account and choose or adjust who you'd like to enroll. Typically it's easiest to set "everyone except guests" to unlock with SSO, since this ensures that new team members invited to the account will receive an SSO invite.

Once you save the configuration changes, the employees will receive an email with instructions on how to sign into 1Password using SSO. They will no longer be able to use their account password and Secret Key to sign in to 1Password unless they are an Owner of the 1Password account. Keep in mind that any users who have not signed in to 1Password using SSO at the end of your grace period will require account recovery from an administrator.

1Password

# Management and operations

How do I manage and maintain Unlock 1Password with SSO? This section provides resources for troubleshooting information, operation, and ongoing management details.

## *Errors, warnings, and troubleshooting*

In this section you'll find troubleshooting guides for common scenarios that can be useful for MSP Administrators/Technicians.

| | | |
|---|---|---|
| User is unable to sign in | Verify that the user has entered the correct credentials and is on the correct URL - If they're using my.1password.com as a sign-in address, they need to switch to your team's unique web address on 1Password.com instead. Learn how to find yours.<br>Verify the user's email used for their identity provider matches the one used in 1Password.<br>Verify the user is on 1Password 8. If they are on 1Password 7 or earlier, they won't be able to sign in with SSO. | Upgrade from 1Password 7 to 1Password 8 for Mac or Windows and 1Password 8 for iOS or Android.<br>Make sure they have the following releases installed on their computer and mobile device:<br>• 1Password browser extension<br>• 1Password 8 for iOS or Android 1Password 8 for Mac, Windows, or Linux<br>• 1Password CLI (optional)<br>If the user's email is different between your identity provider and 1Password, update the email to make sure they match.<br>If the user still can't sign in, you can recover their account. Once account recovery is complete, the user will need to re-enroll their trusted devices. |
| **User is asked for an account password and Secret Key** | Verify that they accepted the invitation to join Unlock with SSO | Wait 30 minutes and try again. |
| **User sees "unable to sign in because grace period is expired" message** | Verify the user hasn't migrated to SSO by navigating to the Group Details page. "Needs recovery" will be displayed next to users in that group who passed their grace period deadline. | Recover their account. |

| | | |
|---|---|---|
| User is signed out of their account after closing their browser | Check the cache clearing policies. If browsing data is cleared when the browser is closed, users will lose access to their trusted device. | Option to exclude the team's sign-in address from that policy to make sure team members won't lose access to their trusted device.<br><br>Encourage users to set up other trusted devices, like the 1Password desktop app, after they sign up or switch to unlock with SSO |
| User's device is lost or stolen | Verify the device location if possible | Start account recovery and deauthorize the lost or stolen device.<br><br>Once account recovery is complete, the user will need to re-enroll their trusted devices. |