Configure Single Sign On

September 10, 2026

Configure Single Sign On

This page explains how to verify whether single sign-on (SSO) configuration is available in Atloria's current administrator security experience. SSO helps you manage member access through your organization's identity provider, but the currently available Security screen does not show SSO-specific setup fields or identity-provider controls.

Overview

Single sign-on lets organization members sign in using an identity provider managed by your company. Administrators typically use SSO to centralize access policies, reduce password management, and ensure that access is removed when a member leaves the organization.

In the current Atloria Security experience, you can review security-related configuration and implementation information. The screen includes items such as **Security**, **Privacy**, **Infrastructure Security**, and **Application Security & Access Control**. It also displays a status reading **2. Configured** and provides **Configure →** actions.

However, the available screen evidence does not show fields for an SSO provider, sign-in domain, metadata URL, certificate, client identifier, or member-enforcement settings. Do not assume that the visible **Configure →** action configures SSO unless the next screen explicitly presents SSO settings.

> 📷 *Screenshot pending: The Security screen showing the Security and Privacy sections, the "2. Configured" status, and available Configure actions.*

Prerequisites

Before you begin, make sure you have the following:

- Administrator access to your Atloria organization.
- Authorization from your organization to manage member authentication settings.
- The name of the identity provider your organization intends to use, such as Microsoft Entra ID, Okta, Google Workspace, or another supported provider.
- Your identity provider’s SSO configuration details, if Atloria provides an SSO setup screen in your environment.
- A documented recovery method for administrators before requiring SSO for all members.
- A test member account that can be used to confirm the sign-in experience without risking administrator access.

Step-by-Step Instructions

1. Open the **Security** area in the Atloria administrator experience.
2. Review the status shown as **2. Configured** to understand that some security-related items are already configured.
3. Select **Configure** → only when it is associated with the security item you want to review.
4. Check the screen that opens for a section explicitly named **Single Sign On**, **SSO**, **Identity Provider**, or a similar authentication label.
5. Stop the configuration process if the screen does not display an SSO-specific option.
6. Do not use **Configure CI/CD** to configure member sign-in, because this action is labeled for CI/CD configuration rather than authentication.
7. Review **Application Security & Access Control** for access-control information that may affect organization member authentication.
8. Review **Privacy** when you need to understand privacy-related considerations for organization or member data.
9. Record the current security settings before requesting or enabling an SSO configuration feature.
10. Contact your Atloria administrator or support channel to request SSO setup guidance if no SSO-specific controls appear.

> 📷 *Screenshot pending: A future SSO configuration screen, showing the provider selection and required identity-provider fields, if this feature is made available.*

Tips and Best Practices

- Use the label on each action to determine its purpose. For example, **Configure CI/CD** is intended for continuous integration and delivery setup, not member authentication.
- Treat **2. Configured** as a status indicator for existing security configuration. It does not, by itself, confirm that SSO is enabled.
- Review the available security information before changing organization access practices. The Security area includes topics such as **Infrastructure Security**, **Application Security**, **Network Security**, **Kubernetes Security**, and **Database Security**.
- Keep at least one administrator recovery process outside the normal member sign-in flow. This helps prevent lockout if an identity-provider configuration is incomplete or unavailable.
- Test SSO with a non-critical user account before asking all organization members to use it.
- Do not share identity-provider secrets, certificates, or administrative credentials in general support messages. Use your organization's approved secure support process.

Related Pages

- Security Overview
- Privacy
- Application Security & Access Control
- Infrastructure Security
- Security & Trust Findings
- Manage Organization Members

Troubleshooting

No SSO option appears after selecting Configure →

The available Security screen does not currently show an SSO-specific setup option. Return to **Security**, confirm that you selected the relevant configuration action, and request assistance from your Atloria administrator or support channel. Include the name of the screen and the actions you can see.

You see Configure CI/CD but need to manage member sign-in

Do not use **Configure CI/CD** for SSO. This option is labeled for CI/CD configuration and is not evidence of an authentication setup workflow. Look for an option explicitly labeled **Single Sign On**, **SSO**, or **Identity Provider**.

You are unsure whether SSO is already enabled

Do not rely only on the **2. Configured** status. Confirm SSO only when you can view a dedicated SSO setting or when your organization has validated the sign-in process with its identity provider.