ATLORIA (SELF DOGFOOD)

Manage organization access

September 15, 2026

Manage organization access

Organization provisioning and SSO

Organization access settings connect your identity provider to Atloria. Use SCIM provisioning to synchronize users and their access, or use SAML single sign-on to let members sign in through your identity provider.

If you need to…	Go to
Connect an identity provider, create a SCIM token, or map groups to roles	Configure SCIM provisioning
Import SAML metadata, map attributes, or save SSO settings	Configure SAML single sign-on
Resolve a plan, permission, or configuration message	Resolve access configuration messages
Review organization activity after changing access	Organization audit

Before you start

Both provisioning and SSO are Business-plan features. You also need to be an organization admin to manage either configuration. Have your identity provider's connection details ready before you begin.

Prepare	What to have ready
Access	An organization-admin account
Plan	A Business plan
SCIM connection	The identity provider you are connecting and the group names you want to map
SSO connection	The IdP Entity ID (Issuer), IdP SSO URL (HTTP-Redirect), and IdP signing certificate

Prepare	What to have ready
SAML attributes	The assertion attribute names or claim URIs for `email`, `name`, `firstName`, `lastName`, and `groups`
Domain policy	The email domains that may be provisioned, if you want to restrict provisioning by domain

If you do not have the required plan, the provisioning page shows `SCIM provisioning is a Business-plan feature` and the SSO page shows `SSO is a Business-plan feature`. If you are not an organization admin, the pages show the corresponding permission message in Resolve access configuration messages.

Open the organization access settings

Use this procedure to open the surface for the access method you need.

Prerequisites

- You have an organization-admin account.
- You know whether you are configuring SCIM provisioning or SAML single sign-on.

Steps

1. Open the organization settings, then choose the provisioning surface for SCIM provisioning or the SSO surface for SAML single sign-on.

Result: The selected organization access settings surface opens.

Configure SCIM provisioning

Use this surface to connect the provider, create its access token, and map provider groups to Atloria roles.

Prerequisites

- You have an organization-admin account on a Business plan.
- You have the identity-provider setup details and the provider group names.

Steps

1. In **Identity provider**, choose one option.

If you are connecting…	Choose
Okta	**Okta**
Microsoft Entra	**Microsoft Entra**

The instructions below **Identity provider** change to match your choice.

2. In **Token label (e.g. Okta production)**, enter a label for the token.
3. Select **Generate token**.
4. Select **Copy** beside the displayed SCIM value, then select **I've saved it** after you have stored the token in your identity provider.

   The token notice says `Copy your SCIM token now`. The token is shown for this one-time copy step.
5. In **IdP group name (e.g. atloria-admins)**, enter the provider group to map.
6. In **role**, choose the role to grant to members of that group.

To grant…	Choose
Viewer access	**Viewer**
Contributor access	**Contributor**
Maintainer access	**Maintainer**
Administrator access	**Admin**

7. Select **Add mapping**.
8. To manage an existing entry, use the applicable action.

If you need to…	Select
Revoke an active SCIM token	**Revoke**
Remove a group-to-role mapping	**Remove**

Result: The selected provider instructions, token connection details, and group-to-role mapping are shown on the provisioning surface.

Configure SAML single sign-on

Use this surface to import or enter provider metadata, map attributes, set just-in-time provisioning defaults, and save the configuration.

Prerequisites

- You have an organization-admin account on a Business plan.
- You have the provider metadata URL or XML, or the values for the manual SSO fields.
- You have the IdP signing certificate when you are preparing to enable SSO.

Steps

1. Choose the metadata source you have, then use the matching alternative.

If you have…	Enter it in…	Then select…
A metadata URL	**Import from IdP metadata — URL**	**Parse URL**
Metadata XML	**metadata XML**	**Parse XML**

2. Review the values in **IdP Entity ID (Issuer)** and **IdP SSO URL (HTTP-Redirect)**.
3. Enter the provider certificate in **IdP signing certificate**.
4. In the Attribute mapping section, enter the assertion attribute name or claim URI for each field.

Field	Value to enter
email	The provider's email attribute or claim URI
name	The provider's name attribute or claim URI
firstName	The provider's first-name attribute or claim URI
lastName	The provider's last-name attribute or claim URI
groups	The provider's group attribute or claim URI

5. To fill a standard mapping, select **Okta preset** or **Entra preset**.
6. In **Default role for new users**, choose one option.

New users receive…	Choose
Viewer access	**VIEWER**
Contributor access	**CONTRIBUTOR**
Maintainer access	**MAINTAINER**

New users receive…	Choose
Administrator access	**ADMIN**

7. In **Allowed email domains**, enter a domain and select **Add**. Repeat for each domain you want to allow. Select **Remove** on a domain chip to remove it.
8. Complete the remaining SSO actions in this order.

Order	Action	Condition
1	Select **Test SSO login**.	Test the identity-provider connection before enabling or enforcing SSO.
2	Select **Enable SSO** or **Disable SSO**.	**Enable SSO** is available when the certificate and SSO URL are present; use **Disable SSO** when SSO is enabled.
3	Select **Save configuration**.	Save the SSO URL, entity ID, attribute mappings, default role, allowed domains, and entered certificate.
4	Select **Enforce SSO** or **Stop enforcing**.	Select **Enforce SSO** after a successful test; select **Stop enforcing** to allow password sign-in again.

Result: The SAML configuration is saved, and the connection status shows the available SSO and enforcement actions.

Handle access configuration branches

The surface changes what it shows according to your plan, permissions, saved configuration, and the provider you selected.

When…	Use this path
You choose **Okta** in **Identity provider**	Follow the Okta setup instructions.
You choose **Microsoft Entra** in **Identity provider**	Follow the Entra setup instructions.
The provisioning list has no token	Select **Generate token** to create the connection token.
The provisioning list has no group mappings	Enter a group and select **Add mapping**.
A new token is displayed	Select **Copy**, store it in the identity provider, and select **I've saved it**.
SSO settings are still loading	Wait for the SSO settings surface to finish loading.

When…	Use this path
No successful SSO test exists and SSO is not enforced	Run **Test SSO login** before selecting **Enforce SSO**.
The certificate or SSO URL is absent	Complete those fields before selecting **Enable SSO**.
SSO is enabled	Select **Disable SSO** to turn it off.
SSO is not enabled	Select **Enable SSO** to turn it on.

Resolve access configuration messages

Use the message on screen to choose the next action.

Message	What to do
`No tokens yet — generate one to connect your IdP.`	Enter a token label and select **Generate token**.
`No group mappings.`	Enter an IdP group name, choose a **role**, and select **Add mapping**.
`Copy your SCIM token now`	Select **Copy**, store the token in the identity provider, and select **I've saved it**.
`Only organization admins can manage provisioning.`	Sign in with an organization-admin account.
`SCIM provisioning is a Business-plan feature`	Use a Business plan before configuring provisioning.
`Only organization admins can manage SSO.`	Sign in with an organization-admin account.
`SSO is a Business-plan feature`	Use a Business plan before configuring SSO.
`Loading SSO settings…`	Wait for the SSO settings to load.
`SSO test succeeded — the IdP returned a valid assertion.`	Continue with the SSO configuration or select **Enforce SSO**.
`Metadata parsed. Review the values below, then Save.`	Review the imported values, then select **Save configuration**.
`Run a successful SSO test to unlock enforcement.`	Select **Test SSO login**, then select **Enforce SSO** after the test succeeds.

After configuring organization access

Review the values shown after you save. Provisioning displays token status, last-used time, sync counts, last sync, recent provisioning activity, and group mappings. SSO displays service-provider details, connection status, the last test result, and whether SSO is enabled or disabled.

For organization context, see Organization overview.
For activity review, see Organization audit.