

Manage Organization Users

September 10, 2026

Manage Organization Users

Use your organization's settings to control who can access Atloria and to review team access. Keeping user access current helps ensure that the right people can collaborate while former or unauthorized users do not retain access.

Overview

Organization user management is used when you need to add colleagues, share access with a team, review who belongs to the organization, or update a person's access level. In Atloria, you begin from the organization's settings area using the **Manage in Settings** action.

Access management is especially important when a team member joins, changes responsibilities, or leaves your organization. Review access regularly and limit administrative access to people who are responsible for managing the organization.

The available evidence confirms the **Manage in Settings** and **Share with Team** actions, as well as an invitation acceptance experience. It does not confirm the names of individual role options, user-list columns, or removal controls. Use the labels shown in your organization's Settings screen when completing those actions.



Screenshot pending: Organization Settings showing the area used to manage team access and organization users

Prerequisites

Before you start, make sure that you have:

- Access to the Atloria organization you want to manage.
- Permission to open and change organization settings.
- The work email address for each person you plan to invite.

- A clear understanding of the access each person needs.
- Approval from your organization's access-control owner, if your company requires it.
- A current list of people who should retain access.

Step-by-Step Instructions

1. Open the Atloria organization where you need to manage team access.
2. Click **Manage in Settings**.
3. Locate the organization access or user-management area in Settings.
4. Review the list of people who currently have access to the organization.
5. Select the control for adding or inviting a user.
6. Enter the new user's work email address in the invitation form.
7. Select the access level or role that matches the user's responsibilities.
8. Send the invitation using the confirmation button shown on the invitation form.
9. Ask the invited person to open the invitation they receive.
10. Have the invited person complete the available invitation acceptance steps.
11. Return to the organization access area after the invitation is accepted.
12. Confirm that the new person appears in the organization's user list with the intended access level.
13. Select an existing user when you need to review or change that person's access.
14. Choose the appropriate role or access setting for the user.
15. Save or confirm the access change using the button displayed on screen.
16. Select the organization's remove, revoke, or equivalent access control when a person should no longer have access.
17. Confirm the removal when Atloria asks you to verify the change.



Screenshot pending: Invitation form with email entry, available access options, and the action to send an invitation

Tips and Best Practices

- Use **Share with Team** when you want to begin sharing Atloria with colleagues, then review the resulting access in Settings. This helps you distinguish between sharing work with a team and maintaining the organization's ongoing access list.
- Assign the least access needed for each person's work. For example, reserve organization-management access for the small group responsible for team membership and security decisions.
- Use work email addresses rather than personal addresses. This makes it easier to manage access when employees change roles or leave the organization.
- Review organization membership after staffing changes, project handoffs, or access-policy updates. Remove access promptly when it is no longer needed.
- Verify invitations after they are accepted. An invitation sent successfully does not by itself confirm that the recipient has completed the acceptance process.
- Do not assume that every organization has the same role names. The available interface evidence identifies access-management functionality but does not confirm the exact role labels. Follow the role descriptions shown in your Settings screen and your organization's internal access policy.
- Limit use of **Manage in Settings** to authorized administrators. Changes made there can affect who can work with your organization's Atloria content.

Related Pages

- [Invite Team Members](#)
- [Share Content with Your Team](#)
- [Organization Settings](#)
- [Role-Based Access Control](#)
- [Application Security and Access Control](#)

Troubleshooting

You cannot find Manage in Settings

Confirm that you are working in the correct Atloria organization. If the action is not available, you may not have permission to manage organization settings. Contact an existing organization administrator to request the required access.

An invited user cannot join

Confirm that the invitation was sent to the correct work email address. Ask the recipient to check spam or filtered mail folders, then send a new invitation if your organization's Settings screen provides that option.

A user has more access than intended

Open the organization access area through **Manage in Settings**, select the user, and change their available access setting. If the correct access option is unclear, follow your organization's access-control policy before saving the change.