Configure Organization Member Access

September 10, 2026

Configure Organization Member Access

Use **Access Control** to configure the access information your organization uses for team members. This helps you assign and verify access for administrators, managers, writers, and contributors while keeping access configuration consistent across the team.

Overview

Organization member access is managed from the **Access Control** area. When you need to give a new team member access, update an existing member's authorization information, or confirm that access has been configured, begin here.

The access configuration flow includes a **Configure →** action and fields for supplying authorization information. Depending on your organization's setup, you may be asked to **Enter access token** or **paste a member JWT**. Use credentials issued by your organization's approved identity or access-management process.

After configuration is completed, the interface can show a **Configured** status. Treat this status as confirmation that the access setup has been recorded. If your organization uses role-based access control, ensure the member's assigned permissions match their work responsibilities, such as administration, management, writing, or contribution.

> 📷 *Screenshot pending: The Access Control area showing the Configure action and configured access status.*

Prerequisites

Before you configure member access, make sure you have:

- Permission to manage organization or team access.
- The correct member authorization information.

- An approved access token, if your organization uses tokens.
- A valid member JWT, if your organization uses JWT-based access.
- A clear understanding of the member’s intended responsibilities, such as administrator, manager, writer, or contributor.
- Confirmation that the member should be included in the organization or team.

Step-by-Step Instructions

1. Open the organization or team area where you manage members.
2. Select **Access Control**.
3. Review the current access information shown for the organization or member.
4. Click **Configure** →.
5. Select the access method requested by the configuration screen.
6. Enter the approved credential in the **Enter access token** field when your organization uses an access token.
7. Paste the member’s authorization value in the **paste a member JWT** field when your organization uses a member JWT.
8. Verify that the credential belongs to the intended team member before continuing.
9. Complete the on-screen configuration action provided after you enter the credential.
10. Return to **Access Control** after the configuration is complete.
11. Confirm that the access entry shows **Configured**.
12. Review the member’s access level and confirm it is appropriate for their responsibilities.

> 📷 *Screenshot pending: The configuration view with the Enter access token and paste a member JWT fields.*

Tips and Best Practices

- Use only credentials issued through your organization’s approved access process. Do not reuse a token or member JWT from another person unless your organization explicitly authorizes it.

- Match access to the member’s actual duties. Administrators typically need broader configuration authority than managers, writers, or contributors. Give each person only the access needed to complete their work.
- Verify the member identity before you paste a credential. A JWT or access token can grant access to the associated identity, so confirming the recipient before configuration helps prevent incorrect assignments.
- Check for the **Configured** status after completing the process. If that status does not appear, do not assume the access change was applied.
- Use **Share with Team** only when you need to communicate access-related information with the team. Avoid sharing sensitive authorization values in team notes or general team communications.
- If you add operational context for the team, use **Add any notes for the team...** for non-sensitive information, such as the reason access was configured or who should review it. Do not place access tokens or member JWTs in notes.
- Review access whenever a member changes responsibilities. For example, update access when a contributor becomes a writer, a writer becomes a manager, or an administrator no longer needs administrative responsibilities.

Related Pages

- **Manage Organization Members** — Add, review, and remove organization members.
- **Role-Based Access Control (RBAC)** — Understand role-based permissions for organization members.
- **Team Activity** — Review team-related activity and changes.
- **Share with Team** — Share relevant non-sensitive updates with team members.
- **Application Security & Access Control** — Review broader organization security practices.

Troubleshooting

The configuration screen asks for a credential I do not have

Request the required access token or member JWT through your organization’s approved access-management process. Do not create, guess, or reuse credentials from another member.

I entered a credential, but the access entry does not show “Configured”

Return to **Access Control** and start the **Configure →** flow again. Verify that the credential was pasted completely and belongs to the intended member. If the status still does not change, contact an organization administrator to confirm that your account can manage access.

I am unsure which access level to assign

Confirm the member’s responsibilities with the team owner or organization administrator. Assign the least amount of access necessary for the member to perform their work, and review the assignment if their responsibilities change.