ATLORIA (SELF DOGFOOD)

Claim Organization Access

September 10, 2026

Claim Organization Access

Use the organization claim screen to request or confirm access to an organization using the access token provided to you. Completing this process helps ensure that organization ownership and team access are assigned through the correct authorization flow.

Overview

Organization access claims are used when you need to establish access to an organization that has been shared with you or when you are asked to verify your authorization. The claim screen uses an access token to associate your request with the intended organization.

You may also be able to include information for other administrators or reviewers during the claim process. Where available, the **Add any notes for the team...** area lets you provide context, such as why access is needed or who supplied the token.

This task is especially important for administrators managing enterprise access, including areas such as **Access Control**, **Application Security & Access Control**, and 👤 **Role-Based Access Control (RBAC)**. Complete the claim carefully, because the access token determines which organization access request is being processed.

> 📷 *Screenshot pending: Organization claim screen showing the Enter access token field.*

Prerequisites

Before you start, make sure you have:

- A valid organization claim link or invitation from an authorized administrator.
- The access token supplied with the claim request.
- Permission to request or manage access for the organization.

- Any details you may need to share with reviewers, such as your role or reason for requesting access.
- A secure way to handle the token; do not send it in public chat channels or include it in unrelated tickets.

Step-by-Step Instructions

1. Open the organization claim link provided by your administrator or organization contact.
2. Review the organization and access context displayed on the claim screen before entering any information.
3. Click the **Enter access token** field.
4. Enter the access token exactly as it was provided to you.
5. Check the token for missing characters, extra spaces, or an incorrect copied value.
6. Add an explanation in **Add any notes for the team...** if you need to provide context for the request.
7. Describe only the information needed to help the reviewing team understand your request, such as your business role or the reason you need organization access.
8. Use the submission action displayed on the claim screen to send the token and any notes for review.
9. Read the confirmation, validation message, or next-step message displayed after you submit the claim.
10. Select **Share with Team** if the screen offers this action and you need to notify your team about the claim or its outcome.
11. Follow any follow-up instructions shown on the screen if additional authorization or review is required.

> 📷 *Screenshot pending: Claim screen showing the Add any notes for the team... area and Share with Team action.*

Tips and Best Practices

- Treat the access token as sensitive authorization information. Share it only through approved organization channels.
- Copy and paste the token when possible. This reduces the risk of mistyping characters.
- Do not add unnecessary confidential information in **Add any notes for the team...**. Keep notes focused on the access request.
- If you are requesting access for a specific enterprise area, state that clearly in your note. For example, identify whether your work relates to **Access Control**, 👥 **Access Control**, or 👤 **Role-Based Access Control (RBAC)**.
- Use **Share with Team** only when the relevant team needs visibility into the request. Sharing broadly can expose information that is not needed by all recipients.
- Do not assume that access is active until the screen confirms the outcome or your organization's access administrators notify you. The available interface labels do not identify separate on-screen stages such as Draft, Approved, or Paid, so rely on the confirmation shown after submission.
- If your organization uses separate access areas, make sure you are claiming the correct organization context before you submit the token.

Related Pages

- Access Control
- Application Security & Access Control
- Role-Based Access Control (RBAC)
- Team Activity
- Version Access Control

Troubleshooting

The access token is not accepted

Re-enter the value in **Enter access token** and verify that it matches the token you received. Check for leading or trailing spaces that may have been included when copying the token. If it still fails, request a new token from the administrator who initiated the claim.

I do not know what to write in the notes field

The **Add any notes for the team...** field is optional context for reviewers. Include your role, the organization you need access to, and the business reason for the request. Do not include passwords, unrelated credentials, or confidential information that reviewers do not need.

I need other people to know about the claim

Use **Share with Team** when it is available on the claim screen. Share the request only with the team members responsible for access decisions or follow-up work.