Account Access and OAuth

You use your existing SiteTrax.io account in the application. Connecting an external assistant adds a separate permission step: you authorize that assistant to retrieve the SiteTrax.io information your account can access. This guide helps you prepare the right account, complete that connection, and check that it works.

Choose the access you need

What you want to do	What you need
Use the SiteTrax.io application	Sign in with your SiteTrax.io account and complete email verification. No external-assistant OAuth connection is required.
Open the personalized Intelligence hub	Publish your personal interview in an application where Intelligence is enabled.
Query SiteTrax.io from an assistant	A verified SiteTrax.io account, a compatible assistant, and OAuth authorization. A published profile is optional for ordinary MCP queries.
Receive useful operational answers	Projects currently shared with your account. A valid connection with no shared projects can return an empty list.

1. Prepare your SiteTrax.io account

1. Sign in at app.sitetrax.io. Check the account shown in the application before starting the assistant connection.
2. Finish email verification if requested. If your organization has shared projects with a different email address, resolve that with the project administrator.
3. Open **Projects** and confirm that the sites you need are available. Publishing an interview does not add project access.
4. If you want to use your published priorities, use the same SiteTrax.io account that published them.

Complete registration and verification before connecting. If you finish them during an authorization attempt and arrive at the dashboard instead of returning to the assistant, go back to the assistant and start its connection again. The original request may have expired.

2. Add the assistant and authorize access

Follow Connecting ChatGPT or Connecting Claude. Your assistant workspace may require an owner or administrator to make the integration available. Each person still authorizes access with their own SiteTrax.io account.

The cards in the Intelligence hub open assistant setup pages. Opening a card does not establish a connection or confirm its success. You can also follow the direct setup route in those guides without publishing a profile first.

1. Start from the intended assistant's connection settings or the documented SiteTrax.io listing.
2. When directed to SiteTrax.io, sign in if necessary. An existing application session may take you straight to the consent screen.
3. Review the requested permissions and shared-project information. The project list describes your access; it is not a set of project-selection checkboxes. If this was not a connection you initiated, cancel.
4. Approve the intended access and return to the assistant. Enable SiteTrax.io in the conversation if that assistant requires it.

OAuth gives the assistant its own access token. Enter your SiteTrax.io password only on the SiteTrax.io sign-in page, never in a prompt or a connector configuration field. The current consent screen does not show your account email, so make the account check in the application first.

Understand the two permissions

- **Read access** (`sitetrax:read`) covers authorized projects, observations, analytics, available published profile facts, existing notifications, and delivery history.
- **Notification management** (`sitetrax:notifications:write`), together with read access, allows creating detection alerts or scheduled digests and cancelling them. It does not allow general operational-record edits or arbitrary email recipients.

The additional permission may be requested during initial connection or later, depending on the assistant. If an action reports insufficient permission, follow that client's authorization flow and check the resulting grant. Reconnecting with the same requested permissions may leave the problem unchanged. Microsoft's federated connection is read-only, and its public rollout remains pending.

Choosing projects for an Intelligence profile provides context; it does not narrow the assistant's OAuth grant. Current project sharing remains the access boundary, and later sharing changes affect what the account can retrieve.

3. Verify the connection

Start with a read-only check:

> Using SiteTrax.io, list the projects I can access. Do not create or change anything.

Compare the result with **Projects** in the application. If needed, ask:

> Use SiteTrax.io authentication diagnostics to show my masked account, verification status, granted scopes, and accessible-project count. Do not display credentials.

An empty project list can be a sharing issue. A different masked account points to account selection. Successful project access does not prove that an assistant has retrieved your profile or used its context.

The public profile tool can retrieve selected confirmed facts and priorities from your latest published revision. It does not return drafts, the working brief, custom AI instructions, or preferred answer length. Ask the assistant to retrieve relevant published facts when needed; publication alone does not guarantee personalized answers.

Disconnecting and getting help

Use the assistant's own controls to disable or disconnect SiteTrax.io there. SiteTrax.io does not currently provide a customer-facing connected-app inventory or individual server-side authorization-revocation control. Disconnecting in an assistant does not confirm that SiteTrax.io has invalidated previously issued tokens. Contact support@sitetrax.io if access must be stopped and you need help choosing the appropriate account or project action.

For connection problems, include the assistant, approximate time, account email, expected project, and visible error. Do not send tokens, passwords, client secrets, or full authorization URLs. See Troubleshooting Connections and Alerts and Scheduled Digests for the next steps.

Revision #1
Created 2026-09-08 13:03:09 UTC by SiteTrax.io Admin
Updated 2026-09-08 13:06:28 UTC by SiteTrax.io Admin