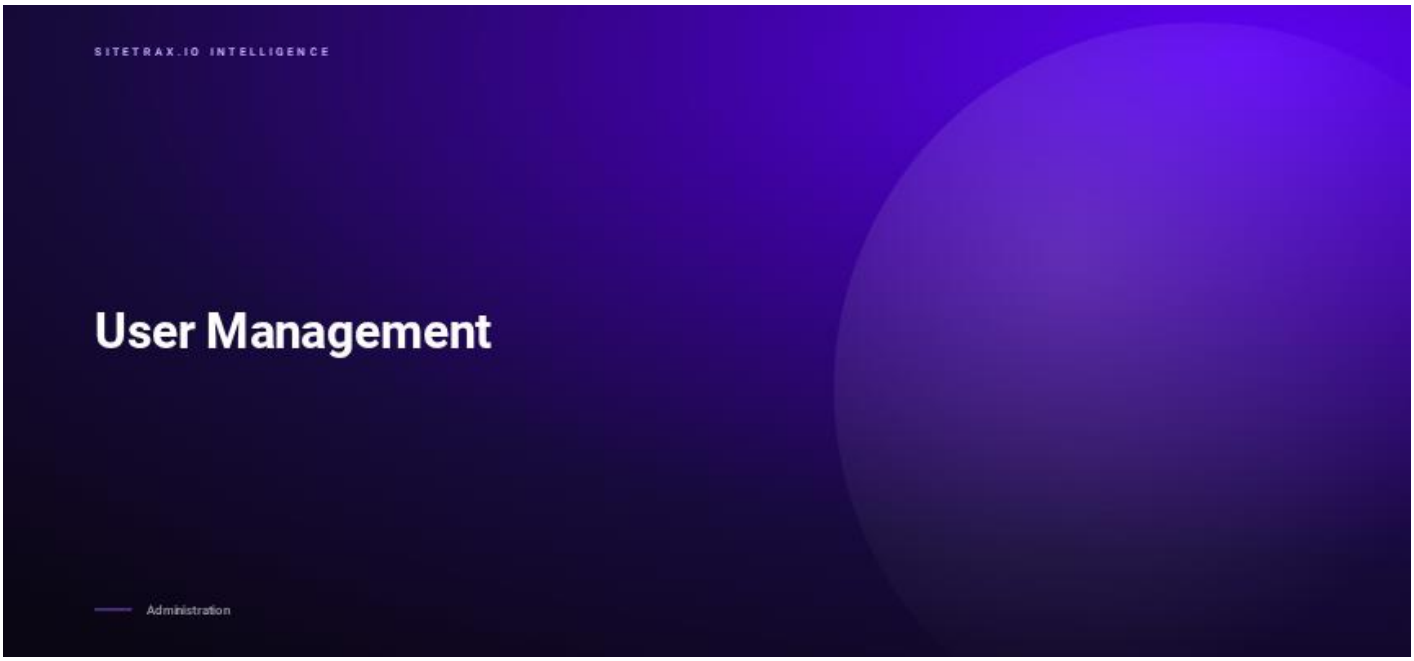
Administration

Manage project sharing, account requirements, permissions and Intelligence rollout. Project sharing controls access to operational projects; assistants also need OAuth authorization and the required scopes. Learn how profile ownership, media availability and notification permissions affect each workflow.

- User Management
- Permissions
- Organization Configuration
- Enabling Intelligence
- Best Practices

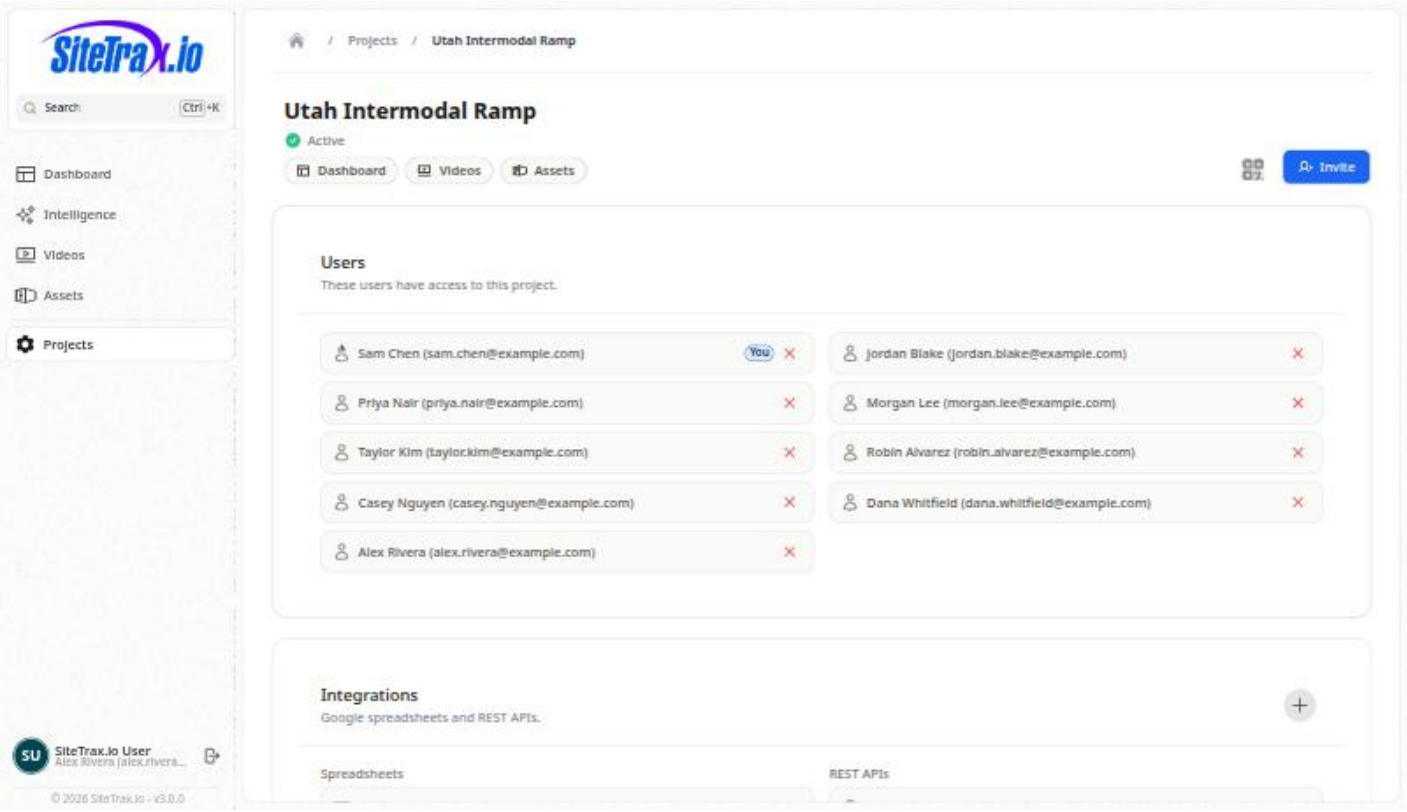
User Management



Access in SiteTrax.io is granted per project. A shared project makes its permitted operational information available to that account; media availability and redaction rules still apply. A project that is not shared with the account remains out of reach. External assistants also need that user to authorize a connection, and notification changes require the additional write permission.

See who has access

1. Open **Projects** and select the project.
2. The **Users** card lists everyone with access, with your own account marked **You**.



The addresses in this screenshot have been replaced with examples. Your own project will show real accounts.

Add someone

Select **Invite** on the project and supply the person’s address. They need a SiteTrax.io account; external assistant authorization also requires an active account with verified email. Once access is granted, the project appears in their application and becomes available to an assistant they authorize with that account. Complete account verification before starting the assistant connection.

Remove someone

Select the remove control beside their entry in the Users card. Removing access takes effect for the application and for connected assistants alike, because both resolve against the same project sharing.

Service and integration accounts

Projects commonly carry non-human accounts alongside staff, for automation and testing. Treat them like any other entry: review them periodically, and remove ones that are no longer needed.

They carry the same project access as a person.

What to review each quarter

- People who have changed roles or left.
- Service accounts nobody can now explain.
- External parties added for a project that has since ended.
- Whether anyone who needs Intelligence is missing a project they should have.

> Removing a person from a project also removes that project from future authorized assistant requests. Project sharing and disconnecting an assistant are different controls. SiteTrax.io does not currently provide a per-connection revoke screen; see Account Access and OAuth for the available access controls.

Permissions



How SiteTrax.io decides what a person, and any assistant acting for them, is allowed to see.

The model

Project sharing determines which operational projects an account can access. External assistants must also have valid authorization and the required scopes. Profile ownership and media availability apply their own controls. Connecting an assistant does not widen project access.

Layer	What controls it
Application access	The SiteTrax.io account sign-in; external assistants also require OAuth authorization with an active account and verified email
Which sites and yards are visible	Project sharing, managed on each project
What an assistant can reach	The projects shared with the account that authorized the connection
What an assistant is allowed to do	The OAuth scopes approved for that connection
Whose profile context can be retrieved	Selected facts and priorities from the published Intelligence profile of that same account; retrieval and use depend on the assistant

Assistant scopes

- **Read (`sitetrax:read`).** Projects, assets, analytics, review and exceptions, video, camera health, reference information and selected published profile context. It also covers listing your alerts and digests and reading their delivery history. These operations are read-only.
- **Notifications write (`sitetrax:notifications:write`).** Creating a detection alert, creating a scheduled email digest, or cancelling one of your notifications. These actions require read access plus this additional permission. A client may request it during the initial connection or later.

Grant the write scope only where the workflow needs it. A read-only connection does not receive it. Microsoft 365 Copilot connections can request it; Copilot then asks the user to approve each write action. See Account Access and OAuth for client-specific authorization and Alerts and Scheduled Digests for supported notification workflows.

Media

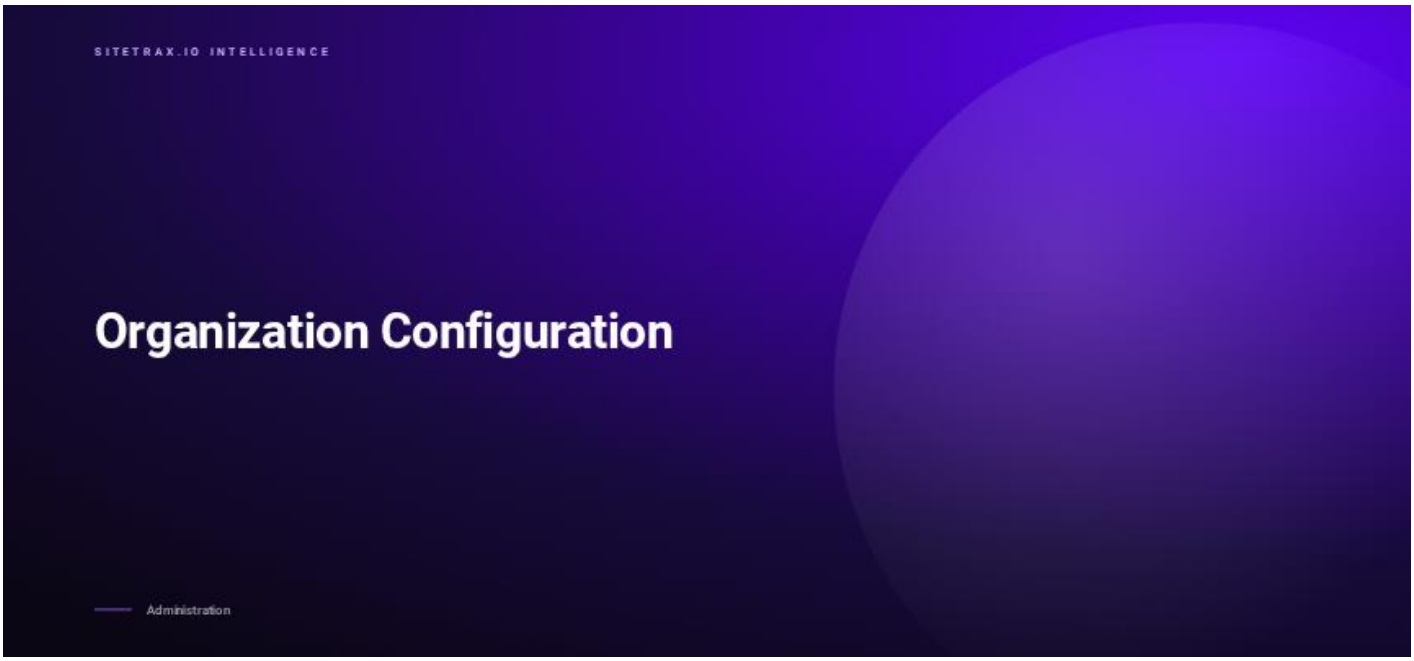
Images and video can be withheld independently of the record. Project configuration, retention, user permissions and redaction settings all affect availability, and a redacted record can return permitted operational metadata while withholding the media.

Profiles are personal

An Intelligence profile belongs to one user account. Each person completes their own interview for a personalized portal experience. Publishing it is not required for ordinary MCP access. An assistant can retrieve selected published facts and priorities, but the public profile tool does not return the saved working brief, custom instructions or response-style preferences. Projects selected in a profile provide context; current project sharing determines access, including later sharing changes.

> Project access is managed on each project. These instructions cover project sharing; contact SiteTrax.io for help with any additional administration arrangements used by your organization.

Organization Configuration



The settings that shape what SiteTrax.io captures and where that data goes are held on the project.

Project basics

Open **Projects** and select a project to see its status, shortcuts to its dashboard, videos and assets, its users, and its integrations. A project represents a site, yard, ramp, gate or facility.

Integrations

Each project can push its data outward through three routes.

- **Spreadsheets.** Configured spreadsheet destinations for operational output. Use the relevant provider section for setup.
- **REST APIs.** Endpoints that receive SiteTrax.io data for a downstream system.
- **Integration platforms.** Connections into the integration-platform network.

These outbound data destinations are separate from the MCP connection used by assistants. MCP provides authorized queries and analytics, plus narrowly permitted personal notification management. Connecting an assistant does not add or change spreadsheet, REST API, or integration-platform destinations.

Configuration guides for each live on the SiteTrax.io Integrations shelf.

Capture configuration

Processing settings, cameras, gate configuration, status filters and regex substitutions are stored per project. They determine what gets read, how identifiers are normalized, and whether direction is meaningful at that site. Because they shape every downstream number, record changes to them: a mid-period camera change moves volume for reasons unrelated to the business.

Capture hardware and installation guidance is on the SiteTrax.io Capture Solutions shelf.

Before rolling Intelligence out

1. Confirm each project has the capture its users assume it has, on both gate directions where dwell matters.
2. Confirm project sharing matches who actually needs each site.
3. Review integration destinations and remove any that are no longer used.
4. Agree internally how status codes will be described to customers.

Enabling Intelligence



What has to be true before a team gets value from Intelligence, in the order it makes sense to do it.

1. Confirm the accounts

Everyone needs their own SiteTrax.io account, with email verification completed before authorizing an external assistant. Share the projects they need. An account can authorize MCP without a published profile, but useful operational answers require shared projects; an empty project list is not itself an authentication failure.

2. Confirm the capture

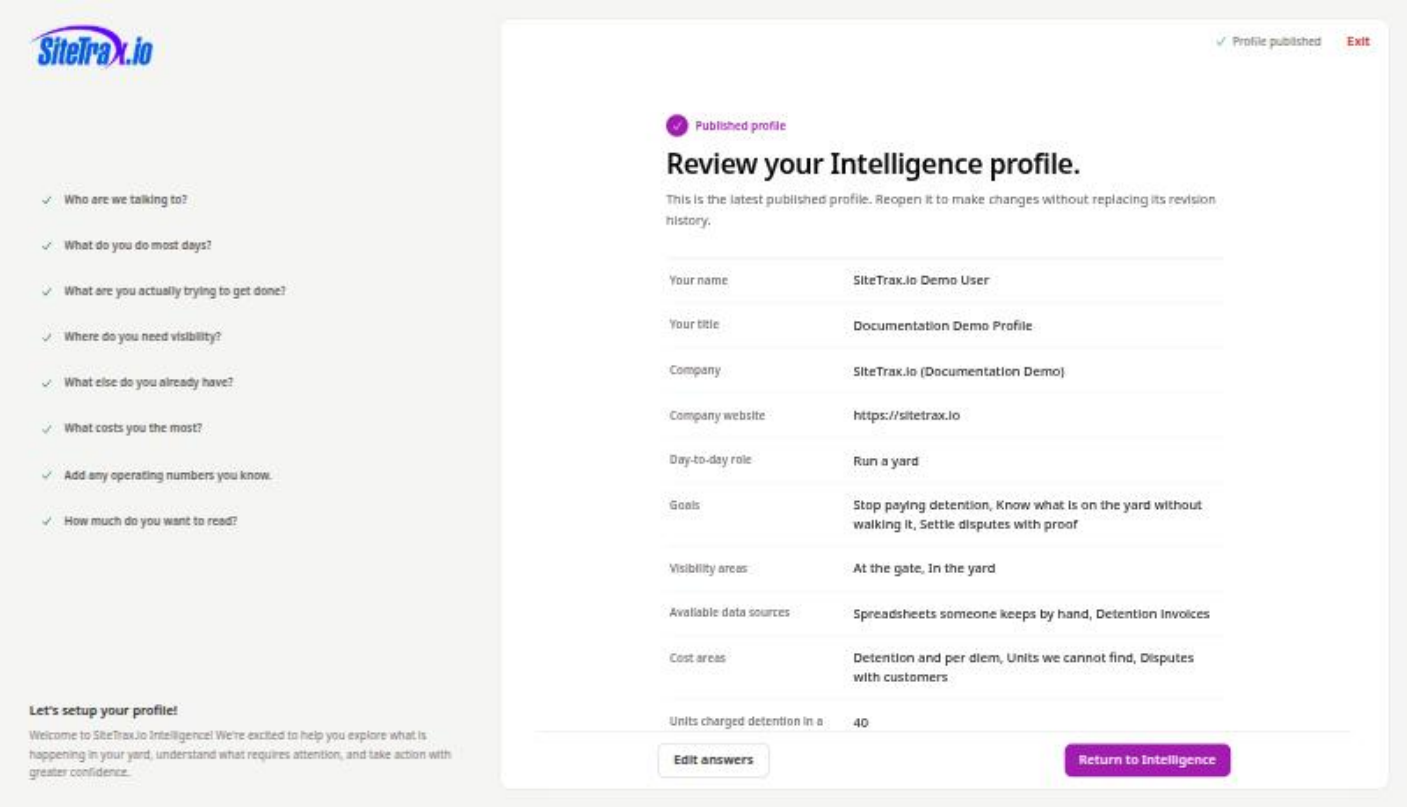
Intelligence reports what was observed. Before rollout, settle whether each gate has capture on both directions and which yard zones are covered. Doing this first prevents a team concluding the product is wrong when the real finding is a blind spot.

3. Have each person publish a profile

The personalized Intelligence hub becomes available once that account publishes the profile interview and Intelligence is enabled. Until publication, the normal hub route opens the interview

and the Intelligence navigation item is hidden. This portal setup is independent of OAuth: people can connect a supported external assistant and query their shared projects without publishing a profile.

Ask people to answer honestly rather than aspirationally. The interview asks what costs them the most and where they need visibility; an accurate answer produces a useful coverage review, and a flattering one does not.



4. Decide the assistant position

Your assistant workspace may require an authorized owner or administrator to enable a connection. Confirm the applicable requirements in your provider's dedicated setup section before rollout. Each user still authorizes the intended SiteTrax.io account.

Each person then authorizes their own assistant connection with their SiteTrax.io account. Decide whether they need to create or cancel alerts and digests; only those changes require the additional notifications write scope. Listing notifications and delivery history uses read access. The extra permission may be requested initially or later, depending on the client. See Account Access and OAuth and Alerts and Scheduled Digests.

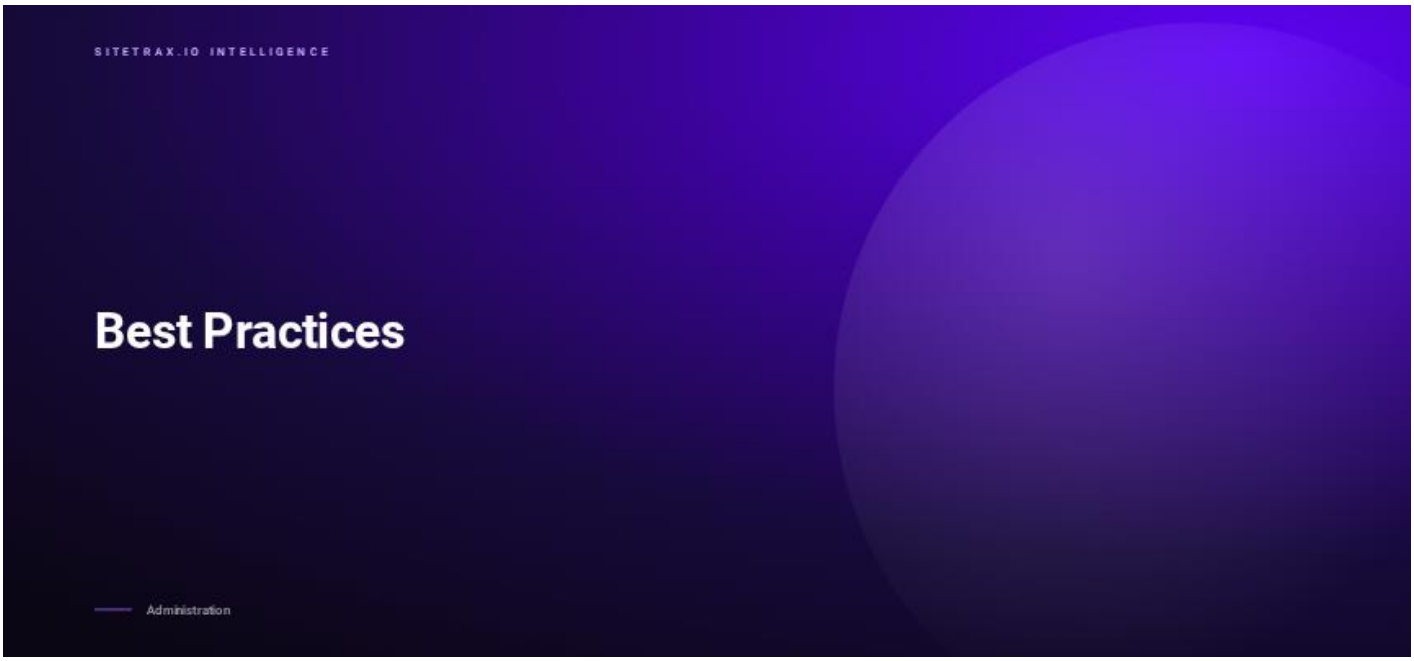
5. Retire the old references

Update runbooks, bookmarks, onboarding material and saved links that point at `service.sitetrax.io`. The current application is `app.sitetrax.io`.

A rollout that works

1. Start with one site and a handful of people who feel a specific pain, such as detention disputes.
2. Have them publish profiles and work the coverage review to a conclusion.
3. Choose one assistant platform for the pilot, then have each person authorize their own SiteTrax.io account and compare the returned project list with the application.
4. Compare an assistant answer against the application for the first week until the team trusts it.
5. Expand once they can explain the difference between a reading and an event.

Best Practices



What separates teams that get value from Intelligence from teams that stall.

Treat coverage as the foundation

Analysis cannot recover an observation that was never captured. When a result looks wrong, check coverage before questioning the analysis. Work the coverage cards on the Intelligence hub until each one is resolved rather than leaving them at needs confirmation indefinitely.

Keep profiles honest and current

- Answer the interview as the operation actually runs today.
- Republish when your role, sites or commercial terms change. A detention rate with a stale effective date quietly misleads.
- Give the assistant any terminology or response-style instructions it needs in the conversation or its own settings. The SiteTrax.io public profile tool returns selected published facts and priorities, not your saved working brief, custom instructions or response-style preferences.

Ask precisely

Name SiteTrax.io, the site, the period and the asset type. Most disappointing answers are underspecified questions rather than product limitations.

Verify anything that will be acted on

Before a charge is disputed, an invoice paid or a number published, open the underlying record and look at the image. The evidence trail is the reason to use SiteTrax.io rather than an estimate, so use it.

Use the language precisely

Say	Not
No observation of the unit in that period	The unit was not there
The reading could not be resolved	The container is damaged
The observed interval was 52 hours	The unit was delayed 52 hours
Stored readings	Units, when counting records

Give feedback on bad reads

Mark records correct or incorrect from the detail page. It takes a moment and it is the mechanism by which capture quality problems become visible.

Keep access tight

- Review project users quarterly, including service accounts.
- Grant the notifications write scope only to create or cancel supported alerts and digests. Listing them and reading delivery history needs only read access.
- Never put passwords or tokens in a prompt or a support email. Query results are shared with the assistant provider you choose; review your organization’s data-handling requirements. See Account Access and OAuth.
- Before connecting an assistant, confirm the intended account in the SiteTrax.io application and finish email verification. Use the account that holds the relevant project access and, if wanted, the published profile. After OAuth approval, ask the assistant to list your projects.