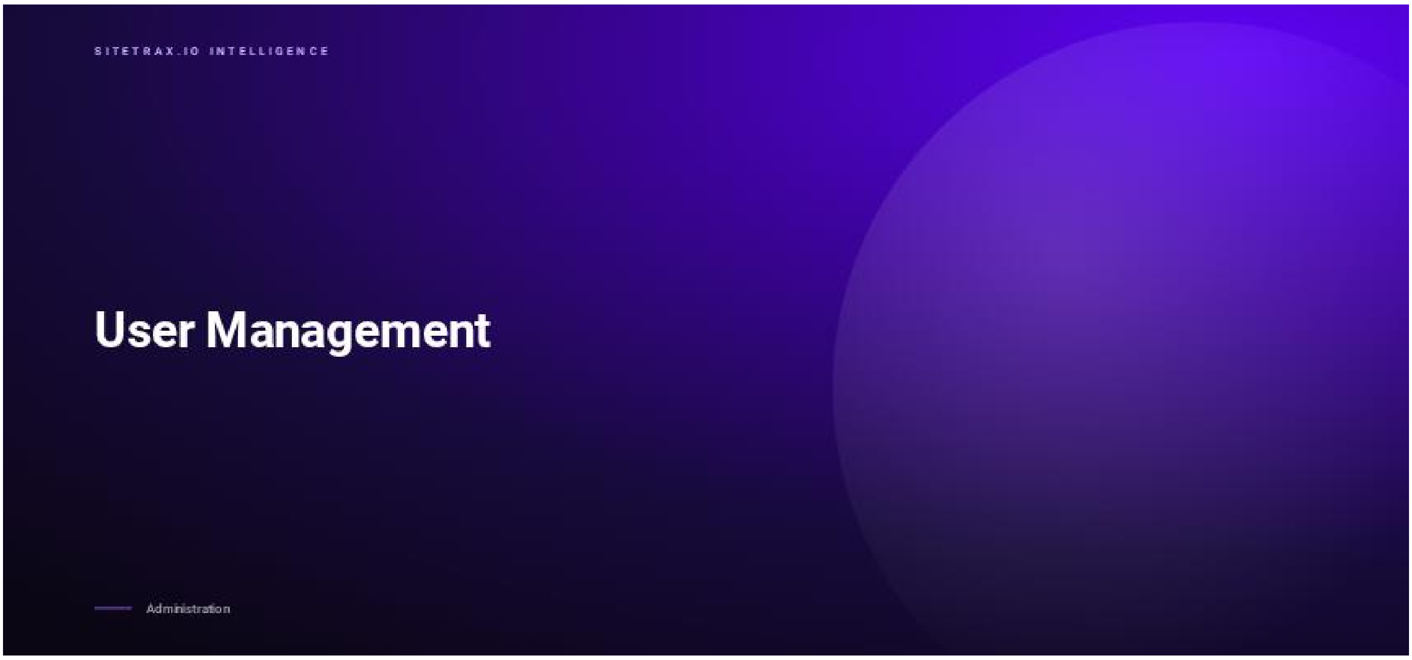
Administration

Managing users, permissions, project configuration and Intelligence enablement across an organization.

Access in SiteTrax.io is granted per project, and that single rule governs the application, the API and assistant access alike. This book covers reviewing and changing who can see each site, how permissions and OAuth scopes resolve, the project settings that shape what gets captured and where it is sent, what has to be true before rolling Intelligence out to a team, and the practices that separate teams who get value from it from teams that stall.

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

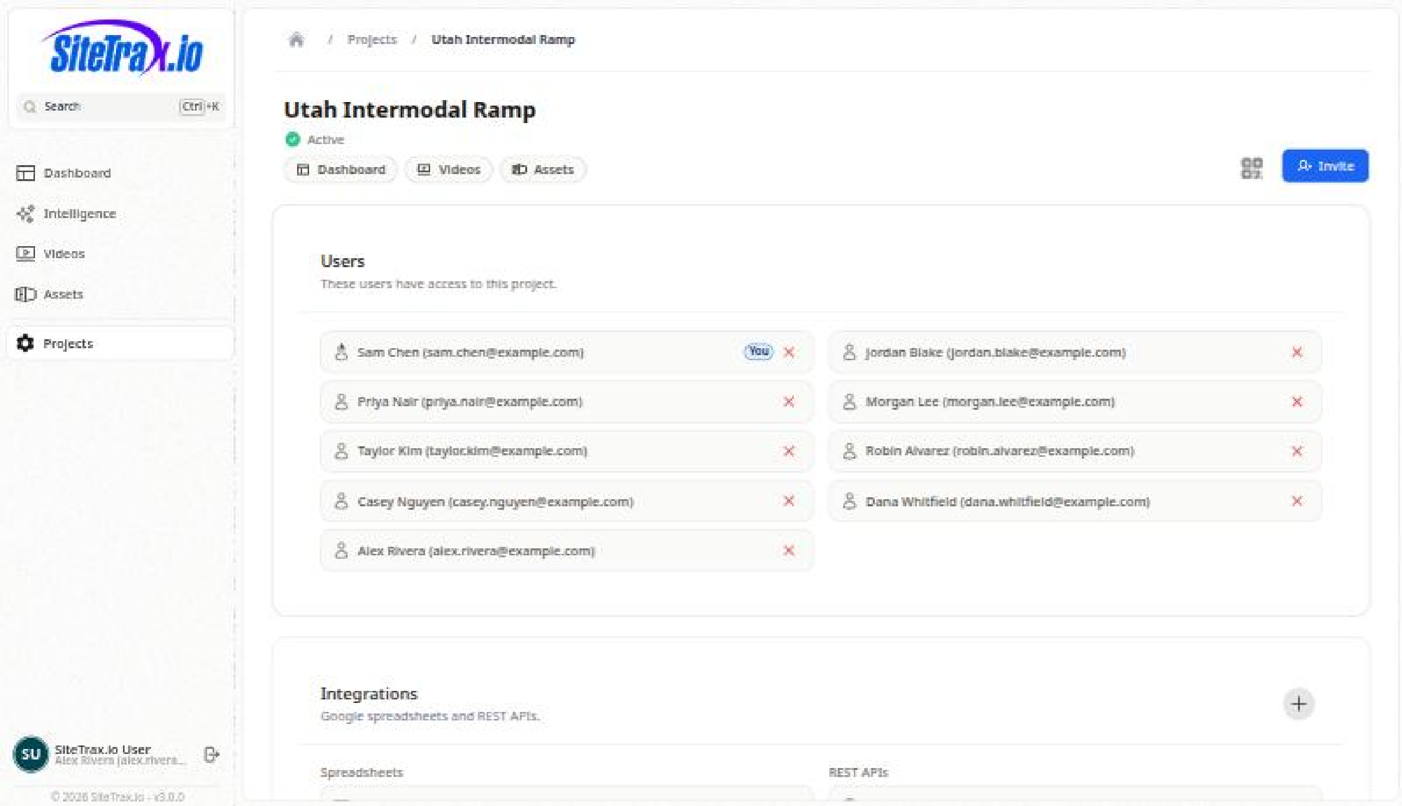
User Management



Access in SiteTrax.io is granted per project. A user who has been given a project can work with everything in it; a user who has not cannot see it at all. There is no separate Intelligence permission to grant.

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 address. They will need a SiteTrax.io account, and once invited the project appears in their application and in the scope available to any assistant they connect.

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 removes their reach through any connected assistant as well. There is no separate assistant access list to maintain.

Permissions

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

The model

Everything resolves to one question: which projects are shared with this account. That single rule governs the application, the API and the MCP server. Connecting an assistant does not widen it, and no prompt can talk past it.

Layer	What controls it
Application access	The account sign-in
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 priorities shape a response	The published Intelligence profile of that same account

Assistant scopes

- **Read.** Projects, assets, analytics, review and exceptions, video, camera health and reference information. This covers ordinary operational questions and is read-only.
- **Notifications write.** Creating, listing and cancelling alerts, and creating recurring digests. This is the only scope that changes anything, and it is approved separately.

Grant the write scope only where the workflow needs it. Integrations that expose SiteTrax.io through a read-only surface do not receive it.

Media

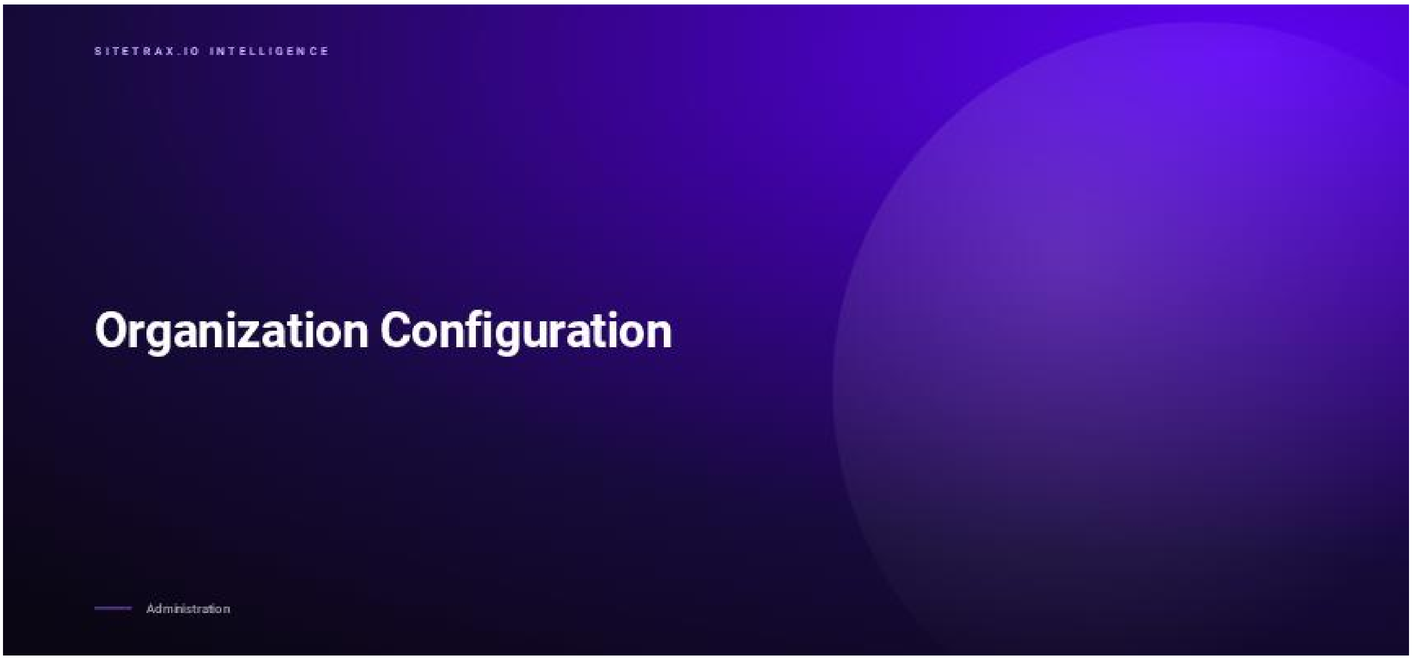
Images and video can be withheld independently of the record. Project configuration, retention, user permissions and redaction settings all affect availability, and a redacted record can return permitted operational metadata while withholding the media.

Profiles are personal

An Intelligence profile belongs to one user account. It is not an organization setting, it is not inherited, and one person answers do not shape another person results. Each person completes their own interview.

> Administration in the current application is scoped to individual projects. This account did not expose an organization-wide roles console, so role-level administration is not documented here. If your organization uses one, contact SiteTrax.io so this page can be extended.

Organization Configuration

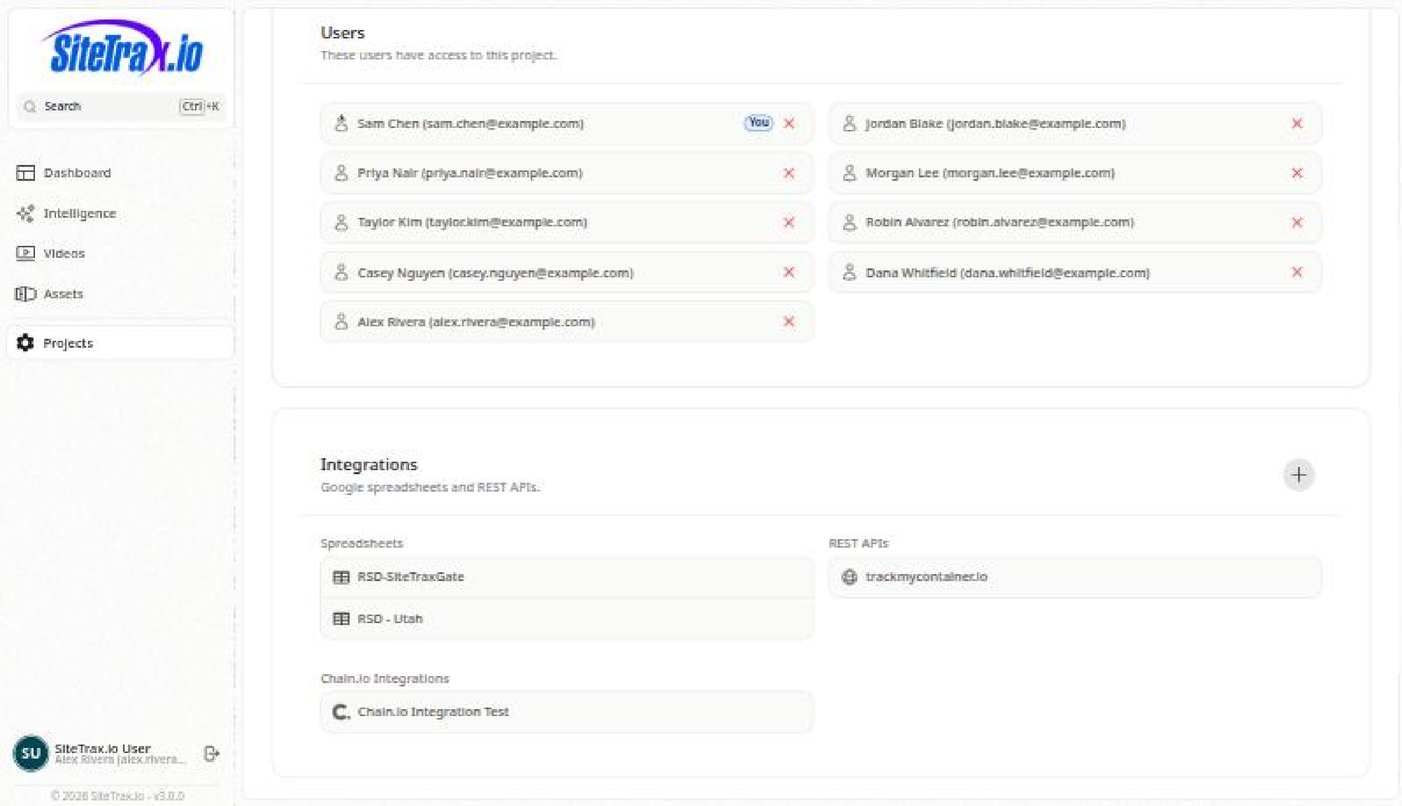


The settings that shape what SiteTrax.io captures and where that data goes are held on the project.

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.** Google Sheets destinations for operational output.
- **REST APIs.** Endpoints that receive SiteTrax.io data for a downstream system.
- **Chain.io integrations.** Connections into the Chain.io network.

These are outbound data destinations and are separate from the MCP server, which is an inbound read path for assistants. Adding an assistant connection does not change them, and removing a spreadsheet does not affect what an assistant can read.

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 who needs Intelligence needs a SiteTrax.io account and at least one shared project. Without a project there is nothing in scope, and the experience will look empty rather than broken.

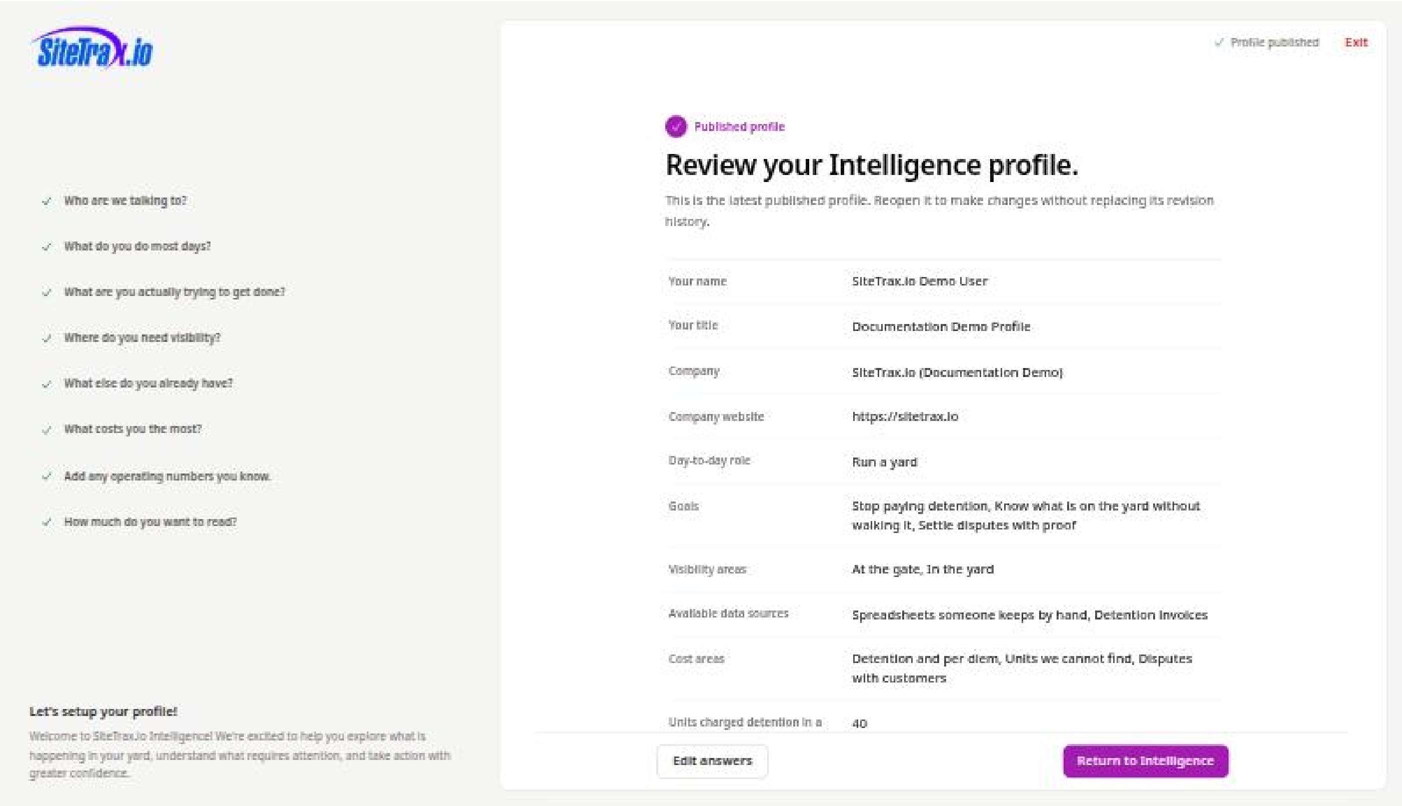
2. Confirm the capture

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

Intelligence becomes available to an account once that account publishes the eight-question interview. It is self-service and takes a few minutes. Until then the Intelligence item does not appear in that person navigation.

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

Decide whether assistant access is in scope, and which assistant. On Claude Team and Enterprise plans only Owners can add a custom connector; in ChatGPT workspaces an administrator controls whether apps may be added. Settle that before individuals try and fail.

Then decide whether anyone needs the notifications write scope. Most users do not.

5. Retire the old references

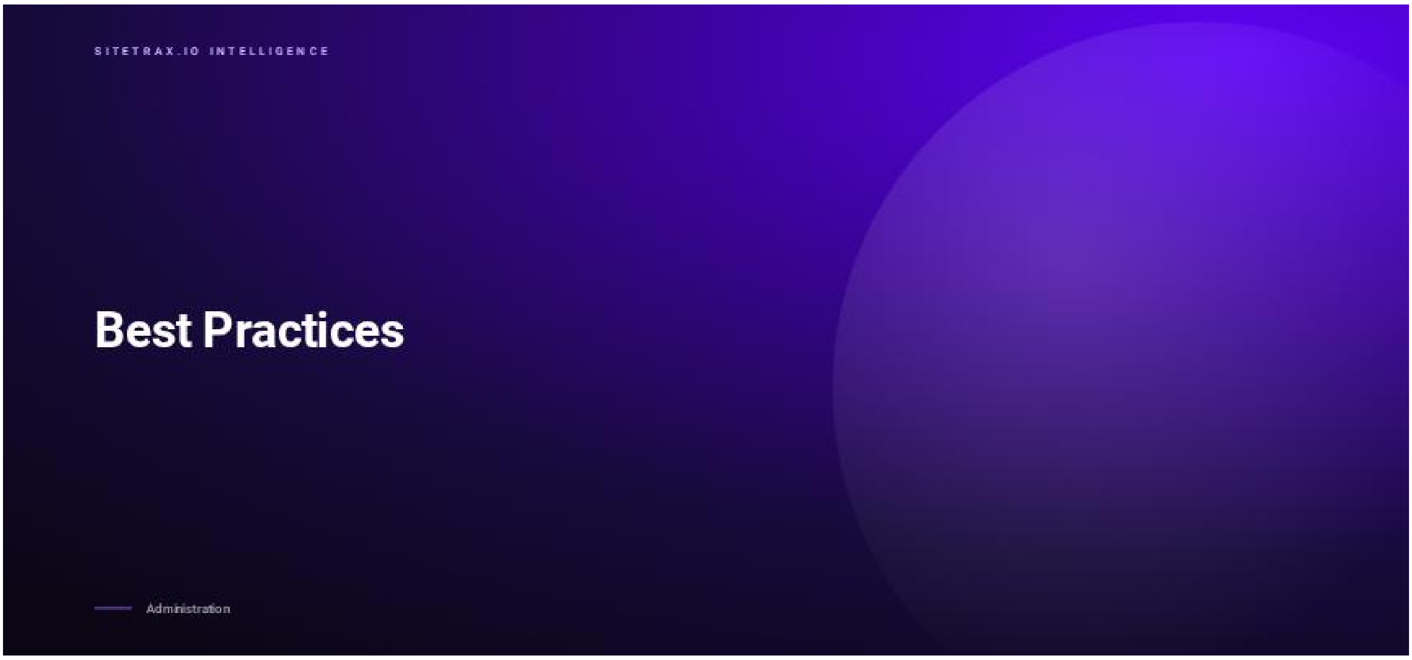
Update runbooks, bookmarks, onboarding material and saved links that point at `service.sitetrax.io`. The current application is `app.sitetrax.io`.

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. Connect one assistant for that group.
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.
- Use custom instructions for terminology your team actually uses, so answers come back in your language.

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 where a workflow needs it.
- Never put passwords or tokens in a prompt or a support email.
- Connect assistants with the same account that published the profile.