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.

Revision #3
Created 2026-09-04 15:22:37 UTC by SiteTrax.io Admin
Updated 2026-10-26 12:24:20 UTC by SiteTrax.io Admin