

AI Integrations

Connect an approved assistant or agent to SiteTrax.io. Start with account access and OAuth, then use the dedicated provider section for setup, availability and platform limits. Verify project access and one known asset before expanding to analysis or actions.

- [Account Access and OAuth](#)
- [Understanding MCP](#)
- [Using MCP with SiteTrax.io](#)
- [Supported AI Platforms](#)
- [Troubleshooting Connections](#)
- [Google](#)
 - [Google: Sheets, Gemini Enterprise and Custom Agents](#)
- [ChatGPT](#)
 - [Connecting ChatGPT](#)
- [Claude](#)
 - [Connecting Claude](#)
- [Microsoft](#)
 - [Microsoft: Connection Guide](#)

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

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.

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.

Follow [your provider's dedicated setup section](#) for provider-specific setup and support. Use your active, email-verified SiteTrax.io account, complete OAuth authorization and verify the returned project list against the application.

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.

If an authorization request does not specify permissions, SiteTrax.io defaults to read access. A client advertising support for notification management does not mean your connection has been granted it; check the actual scopes with authentication diagnostics.

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.

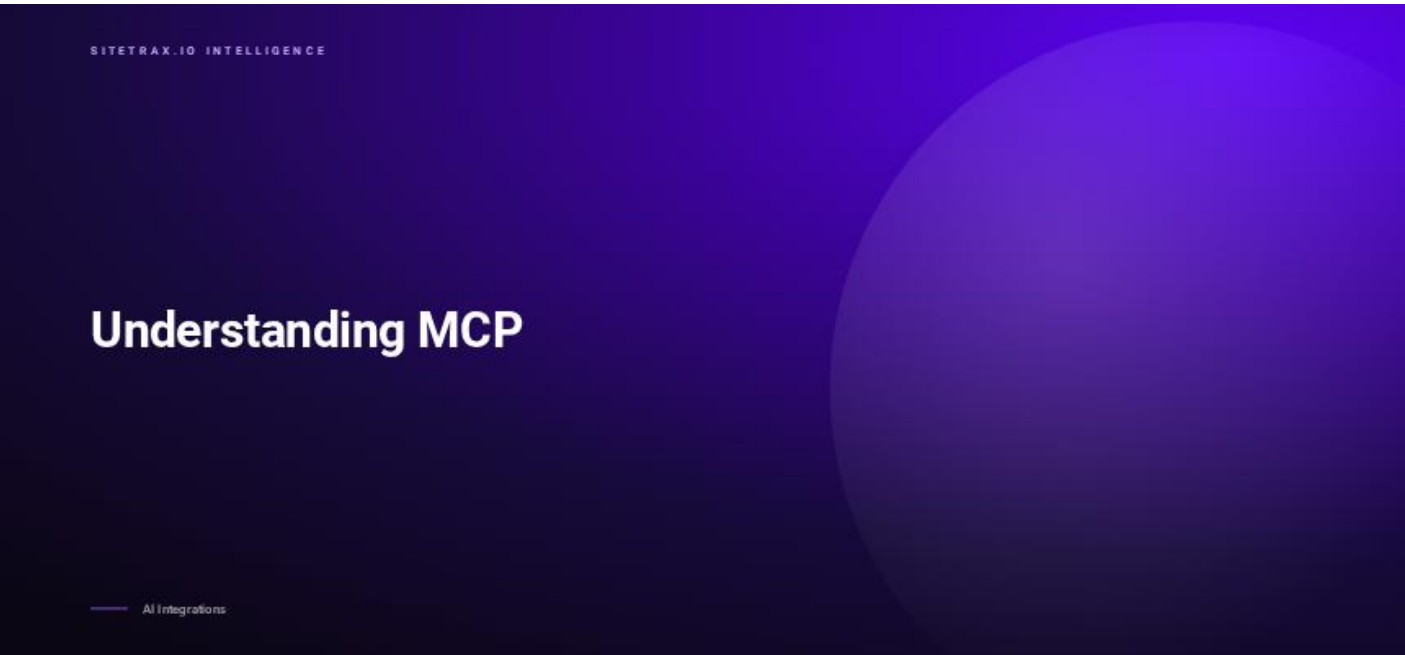
The public profile tool can retrieve selected confirmed facts and priorities from your latest published revision. It does not return drafts, the working brief, custom AI instructions, or preferred answer length. Ask the assistant to retrieve relevant published facts when needed; publication alone does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

Understanding MCP



Model Context Protocol, usually shortened to MCP, is an open standard that lets an AI assistant connect to an outside system and use it. SiteTrax.io implements it so that assistants can work with your operational data without anyone exporting it first.

Why it exists

Before MCP, getting an assistant to answer a question about your yard meant copying data into a prompt or building a bespoke integration for each assistant. Both approaches age badly. A copied extract is stale the moment it is pasted, and a bespoke integration has to be rebuilt for the next tool.

MCP replaces that with one connection the assistant understands. SiteTrax.io publishes what it can do once, and any compatible assistant can use it.

What it means in practice

Without MCP	With MCP
Export a report, paste it into a chat	The assistant can retrieve current records when it calls a SiteTrax.io tool

Without MCP	With MCP
The extract reflects one moment and one filter	A new tool call retrieves data for its requested scope and time period; a reply without one may use earlier context
The assistant cannot check its own answer	The assistant can retrieve the supporting record and permitted image links
Sharing the extract shares everything in it	Access follows the signed-in SiteTrax.io account

How SiteTrax.io implements it

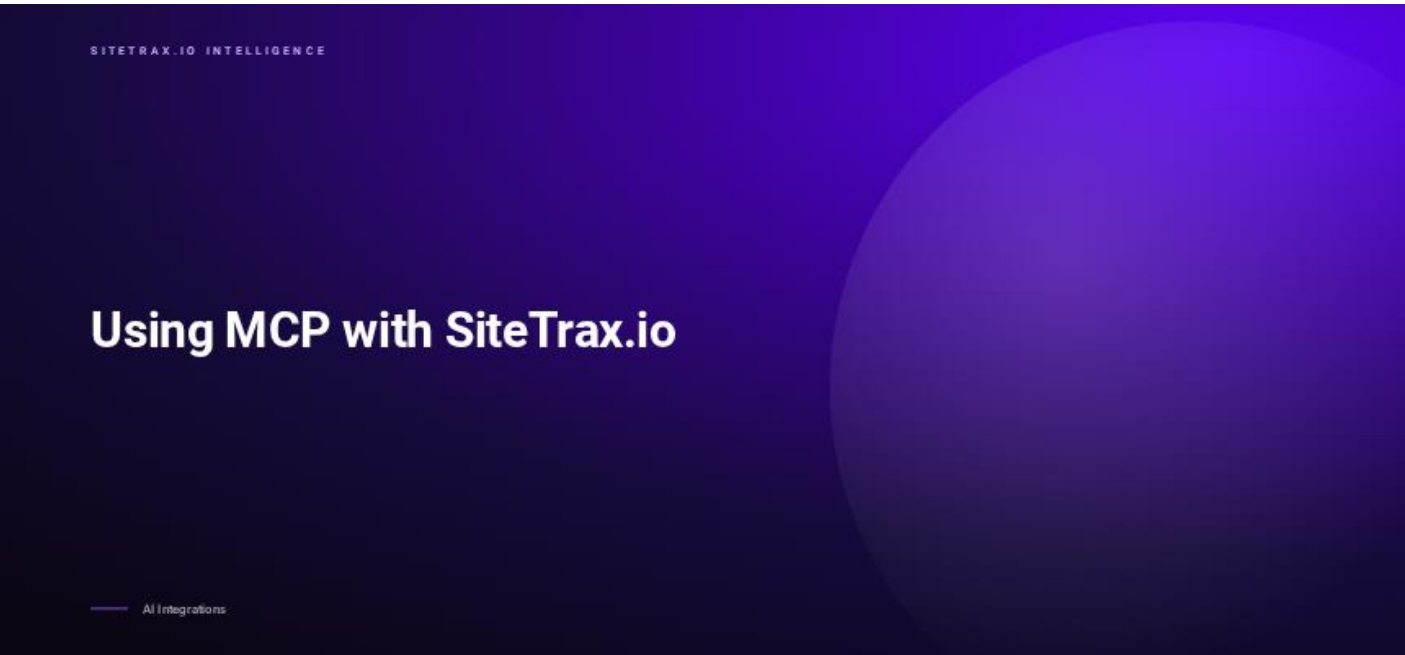
- **It is a remote server.** The endpoint is `https://mcp.sitetrax.io/mcp`. An assistant that only supports servers running on your own machine cannot reach it.
- **Authorization is OAuth-based.** You approve the assistant's access on the SiteTrax.io authorization screen using an active account with verified email. Application login alone does not grant an assistant access, and publishing an Intelligence profile is optional for ordinary MCP queries. No SiteTrax.io password is entered into the assistant.
- **Permissions are scoped.** Read access covers operational queries, selected published profile context, notification lists and delivery history. Creating an alert or digest, or cancelling one, needs read access plus an additional write scope. A client may request it during initial connection or later.
- **Analysis happens on the server.** SiteTrax.io calculates supported totals, groupings and durations itself, so the assistant does not need a large raw-data download for those calculations. It can separately retrieve permitted supporting records.
- **SiteTrax.io stays the system of record.** Operational records remain in SiteTrax.io. The assistant retrieves authorized results and can manage supported personal notifications when separately permitted and confirmed.

What it does not do

- It does not widen your SiteTrax.io permissions. A project not shared with you stays out of reach.
- It does not require a bulk export or a synchronized index. However, the records, summaries and any permitted evidence returned for a query are sent to the assistant provider you choose. Follow your organization's policies for using that provider.
- It does not make an unverified answer verified. Interpretation rules still apply.

See [Account Access and OAuth](#) for the account and authorization flow. For the full technical contract, including transport, scopes and response semantics, see the [SiteTrax.io MCP Server](#) reference.

Using MCP with SiteTrax.io



Once an assistant is connected and you have verified its project access, this page explains what to ask for and how to phrase it. For setup and permissions, see [Account access and OAuth](#). For tool names and response contracts, see the [SiteTrax.io MCP Server](#) reference.

What you can ask for

If you need to	Ask for
Locate one unit	The most recent observation of a specific identifier, with project, time and image
Understand a period	Activity across your sites for a date range, with totals and trends
Compare	A breakdown by project, camera, asset type, status code or time period
Measure dwell	Observed time between defined operational boundaries, such as gate-in to gate-out
Find problems	Records meeting review criteria, unreadable results, or unusual volume gaps
Check capture health	Camera activity and scan health across your projects

If you need to	Ask for
Get the evidence	The detection image, video metadata and saved audit feedback for a specific record, or supporting records behind an analytical result
Receive a recurring update	A new-detection watch or scheduled aggregate email digest, after confirming its conditions and approving the additional write permission
Check an existing notification	Its status and delivery history, using read permission

How to phrase it

Six things make the difference between a vague answer and a usable one.

1. **Name SiteTrax.io** so the assistant reaches for the connector rather than answering from memory.
2. **Name the site or project.** Without it, the answer spans everything you can see.
3. **Give a date or time range.** This is the single most common cause of a surprising number.
4. **Say the asset type** when it matters, such as containers rather than chassis.
5. **Confirm the complete identifier** when following one unit. Query search supports partial text and prefixes to discover candidates; exact latest-observation and identifier-based image/video lookups need the full identifier.
6. **Ask for the supporting record** whenever the answer will be used in an invoice, a dispute or a report.

A weak prompt

“ How busy were we?

The same question, answerable

“ Using SiteTrax.io, summarize container and chassis activity at the Utah site for the last seven days and break the results down by status code and asset type.

Reading the answer honestly

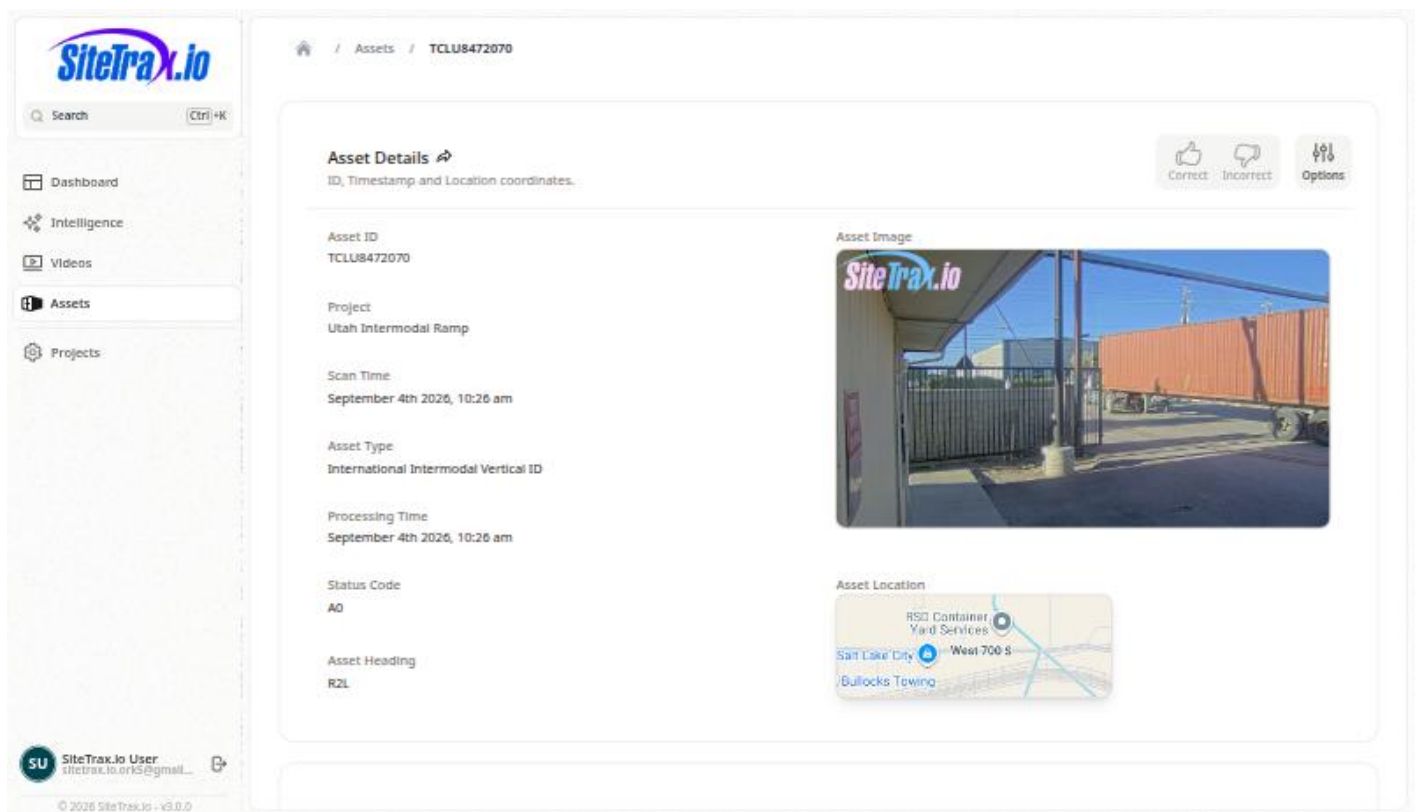
These are the mistakes that turn a good answer into a wrong decision.

- **A record is a stored processing result**, not a guaranteed physical event. Combined container and chassis processing can add a synthetic row for the paired side.
- **A processing status is not a condition report**. An unreadable result does not establish that the unit is damaged.
- **An observed interval is not an explanation**. Time between two camera observations is a measurement, not a cause.
- **A USDOT number identifies a carrier**, not an individual tractor.
- **Missing pairing is reported, not estimated**. Where a sequence cannot be paired reliably, SiteTrax.io says so instead of filling the gap.

When the answer will be acted on

Ask for the record. SiteTrax.io can return a link in the form

`app.sitetrax.io/dashboard/assets/view/{asset_id}`, which opens the same detail page you would reach in the application, with the image and the full payload. Verify there before an invoice is disputed or a charge is paid.



Creating a detection watch or digest, or cancelling one, requires your confirmation and `sitetrax:notifications:write` in addition to read access. A client may request that additional permission at initial connection or later. Listing notifications and reading history need read access only. See [Alerts and scheduled digests](#).

A connected assistant can retrieve selected published facts and priorities when relevant. The public MCP profile response excludes your working brief, custom instructions and response-style preferences, and publication does not guarantee retrieval or use. Ask directly for the level of explanation you need, such as: give the answer, explain the calculation and link to its supporting records.

Supported AI Platforms

Choose an assistant or agent platform your organization approves, then use that provider’s dedicated documentation section. Each section owns its connection status, setup instructions, platform limits and vendor references.

What every connection must support

- Remote HTTPS access to `https://mcp.sitetrax.io/mcp`.
- Streamable HTTP transport and SiteTrax.io OAuth authorization.
- The tools and permissions required for your intended task.

A provider’s MCP support alone does not establish that its connection to SiteTrax.io has been validated. A directory listing or setup button also does not prove a completed connection.

How to read availability

Status	Meaning	Next step
Documented connection	A SiteTrax.io setup route is published.	Follow the provider guide and verify your account’s project access.
Validation required	A technical route exists but SiteTrax.io end-to-end behavior has not been established.	Coordinate a scoped pilot before relying on it.
Pending release	The provider-specific guide reports a release or listing dependency.	Use that section for availability and next steps.
Custom implementation	A business workflow needs design, configuration and acceptance.	Agree scope, hosting, permissions and support.

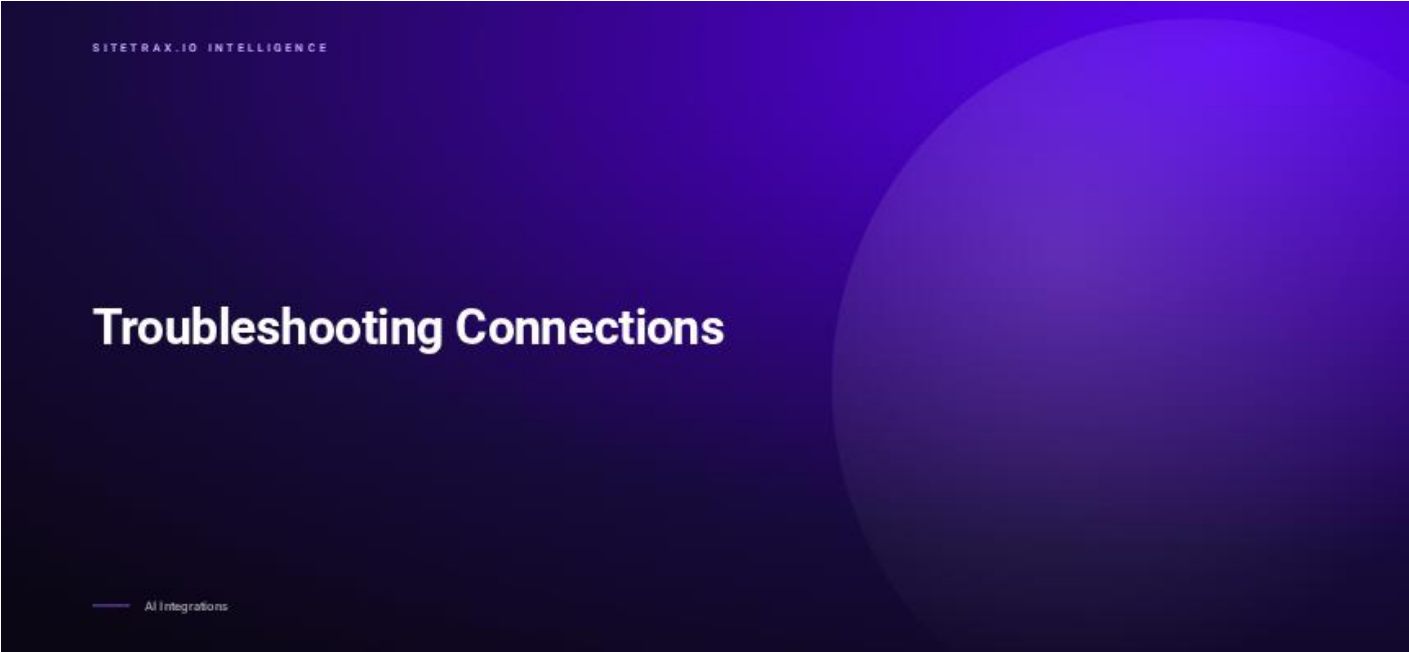
Verify the first result

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

Compare the result with the same account in the application, then query a known observation and open its record. Read access and notification-write permission are separate. Connecting an assistant does not expand project access.

Use the provider sections in this book for setup. For the shared technical contract, see [MCP Server](#).

Troubleshooting Connections



Connection problems, in the order they usually appear. For problems with the data in an answer rather than the connection itself, see the troubleshooting section of the [SiteTrax.io MCP Server](#) reference.

Setting up

What you see	Likely cause	What to do
The assistant cannot reach the server at all	The client does not support remote MCP servers, or a network control is blocking the endpoint	Confirm the endpoint is <code>https://mcp.sitetrax.io/mcp</code> , that the client supports remote servers over HTTPS with OAuth, and that no firewall or security tool blocks it
Nothing happens when authorization should start	The client only supports local servers running on your own machine	A local-only client cannot reach a remote endpoint. Use a client that supports remote MCP servers
There is no option to add a connector	Plan or role restriction	Check the applicable workspace role, supported surface and connection availability in your provider's dedicated setup section .

What you see	Likely cause	What to do
It works on a laptop but not on a phone	Platform limitation	Use a desktop browser for the documented setup flow. Check the current guidance for the published app or custom developer-mode connection you are using; availability can differ by surface and workspace.

Finish SiteTrax.io email verification before starting OAuth. If account creation or verification returns you to the dashboard while the assistant is still waiting, restart the connection from the assistant. An invalid or expired authorization link must also be restarted there. To use a different account, sign out in the SiteTrax.io application, sign in with the intended account, and start a fresh assistant connection. See [Account Access and OAuth](#).

After connecting

What you see	Likely cause	What to do
Authorization succeeded but no projects appear	No projects are shared with the account you used, or you signed in with a different account	Confirm which account you authorized with, and that at least one project is shared with it. This is a sharing question rather than an authentication one
Answers are generic and ignore your priorities	The wrong account is connected, no profile is published, the assistant did not retrieve it, or the expected instructions are outside the public profile contract	Confirm the account and publication in the application, then ask the assistant to retrieve your published profile context. It returns selected facts and priorities, not the saved working brief, custom instructions or response-style preferences. Reconnect when the account or grant is wrong; give response instructions in the assistant itself
Fewer projects than you expect	The assistant is scoped to a different account with narrower access	Compare the project list in the assistant against Projects in the application while signed in as the same user
A tool reports that another permission is required	The operation needs the notifications write scope	Check the actual granted permissions. Notification changes need <code>sitetrax:notifications:write</code> ; read-only connections cannot perform them. Use your provider's dedicated setup section for authorization steps.

What you see	Likely cause	What to do
The connector is present but does nothing in a chat	It is not enabled for that conversation	Enable the integration in the current conversation using the controls described in your provider's dedicated setup section .

Confirming a connection is healthy

Two checks settle most uncertainty.

For provider-specific loading errors, client restrictions and recovery steps, use [your provider's dedicated setup section](#). A client-side loading error alone does not establish a SiteTrax.io outage.

1. Ask the assistant to list the projects you have access to, and compare against **Projects** in the application.
2. Ask for the most recent observation of an identifier you can find yourself in the assets gallery, and compare the time and project.

If both match, those read requests reached the expected account and data. This does not prove that every tool or permission works, that profile context was used, or that a notification was delivered. Investigate any remaining failure against its specific tool, filter, permission and response.

Never paste SiteTrax.io passwords, OAuth tokens or client secrets into a prompt, a configuration field or a support email.

Getting help

When reporting a connection problem, include the assistant you are using, the approximate time, the SiteTrax.io account email, the project involved, what you attempted, and any error message shown.

Google

Google

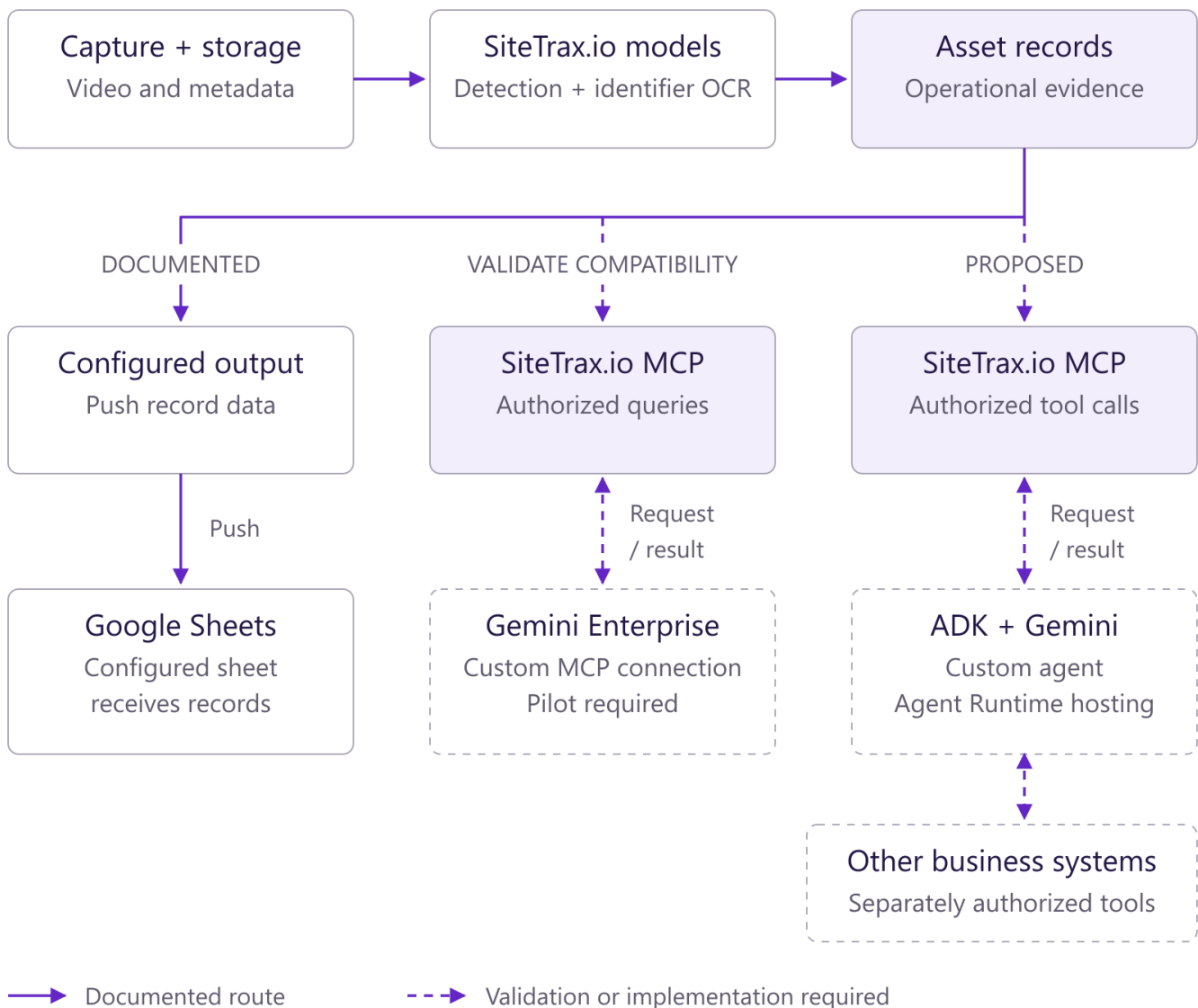
Google: Sheets, Gemini Enterprise and Custom Agents

Choose the Google product that matches the job. Sending records to Google Sheets, asking Gemini Enterprise a question and deploying a custom agent on Google Cloud require different setup.

Google reference architecture

SiteTrax.io + Google: integration routes

Three separate routes, each with its own setup and validation.



[Open the Google architecture diagram at full size](#). Solid arrows show the documented data path. Dashed paths require SiteTrax.io validation or a scoped implementation. The Google Cloud project owner, billing owner and support responsibilities must be agreed for a custom agent deployment.

Where Gemini fits

SiteTrax.io’s specialized detection and identifier-reading models create the asset observations. SiteTrax-managed processing can use Google Cloud compute, but that compute is separate from the agent layer. In the proposed agent path, Gemini interprets the task, ADK coordinates authorized tools, and Agent Runtime is a hosting option. The agent can combine SiteTrax.io evidence with separately authorized business data and actions.

For example, a user asks when an equipment identifier was last seen. The connected Google client requests permitted records through MCP, SiteTrax.io applies account and project access, and the returned observation supports the answer. An action in another system requires an additional defined workflow and permission.

Choose an integration route

Route	Use it for	SiteTrax.io status and next step
Google Sheets and My Maps	Receive operational records in a configured sheet; map available coordinates.	Documented data-delivery route. Confirm the project destination. My Maps requires reimport to reflect changes.
Gemini Enterprise custom MCP connection	Let an enterprise assistant query authorized SiteTrax.io information.	Google documents this capability. SiteTrax.io end-to-end compatibility has not been validated in this guide; coordinate a pilot.
Custom Google Cloud agent	Implement a defined business workflow using SiteTrax.io evidence and other authorized tools.	Proposed implementation route. Architecture, hosting, billing and support must be scoped.
Gemini in Gmail or the Gemini consumer app	Use a particular Google user interface.	Do not assume a Gemini Enterprise MCP configuration appears in these products. Confirm that exact surface before committing to a workflow.

1. Use data in Google Sheets and My Maps

Confirm the Google Sheets destination under your SiteTrax.io project integrations. Once records arrive, use [the existing My Maps guide](#) to import coordinates. Map markers describe recorded observations. Reimport the sheet to update the map; a sheet update alone does not refresh it.

2. Evaluate Gemini Enterprise access

Google’s [custom MCP data-store guide](#) documents Streamable HTTP and OAuth setup. That establishes a Google integration path, not a tested SiteTrax.io connection.

For a pilot, have your Google administrator and SiteTrax.io confirm:

- The Gemini Enterprise app, permitted users and required organization policies.

- The endpoint `https://mcp.sitetrax.io/mcp`, OAuth registration and redirect, requested scopes and allowed domains.
- Per-user project access, tool discovery and a read-only test before any notification write permission.

“ Using SiteTrax.io, list the projects I can access. Then find the latest observation of the equipment identifier I provide, including its time, project and supporting record.

Compare the answer with the same account in app.sitetrax.io. Test an inaccessible project and a missing identifier as well as a successful lookup. Publish a customer setup guide only after the actual connection, permissions and supported tools pass validation.

3. Build a custom agent on Google Cloud

Google's [Agent Development Kit supports MCP tools](#), and its [Agent Runtime guide](#) describes hosting ADK agents. A proposed SiteTrax.io implementation uses an agent to call permitted SiteTrax.io tools, apply a defined business process and request an approved downstream action. This does not require describing Gemini as the model that reads asset identifiers from video.

Scope one workflow first. Agree where it runs, who pays for the runtime, how each user or service is authorized, which data reaches Google, what actions require approval and who handles failures. Google Cloud Marketplace procurement is a separate workstream from validating this connection; this guide does not claim a SiteTrax.io listing or Google endorsement.

Start with a verifiable lookup

[Contact SiteTrax.io](#) with the Google product you use, one project and one question you need answered. Establish a reliable lookup before expanding to workflows that change business systems.

Provider documentation checked 7 October 2026. SiteTrax.io Google MCP setup remains unvalidated in this review.

ChatGPT

Connecting ChatGPT

Use ChatGPT to ask operational questions about the SiteTrax.io projects your account can access. SiteTrax.io returns authorized records and supported analytical results; ChatGPT uses those results in its response.

Before you start

- An active SiteTrax.io account with verified email and the relevant shared projects.
- A ChatGPT account where your organization permits the SiteTrax.io integration.
- A complete equipment identifier or known record for the first check.

A published Intelligence profile is optional for ordinary data queries. Sign in to the intended SiteTrax.io account before authorizing the connection.

Connect the published SiteTrax.io integration

1. Open [the SiteTrax.io listing in ChatGPT](#), or use **Open in ChatGPT** from the SiteTrax.io Intelligence hub.
2. Choose the connection option and complete authorization on the SiteTrax.io page. Review the permissions you are granting.
3. Return to ChatGPT, make SiteTrax.io available in the conversation and run the check below.

Verify access, then ask a useful question

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

Compare the list with Projects in app.sitetrax.io under the same account. Then ask:

“ Using SiteTrax.io, when was trailer [complete identifier] last observed at [project]? Include the observation time, timezone, project and supporting record. Explain if the available evidence does not establish its current location.

Use a custom MCP connection when your organization requires it

The endpoint is `https://mcp.sitetrax.io/mcp`. Use OAuth and Streamable HTTP. This route is separate from installing the published listing. OpenAI's current [custom MCP guide](#) describes adding a server from ChatGPT's Plugins interface; workspace controls apply. Follow the controls available in your account and the current vendor guide rather than an old developer-mode screenshot.

Understand the action boundary

Read permission covers permitted queries and notification history. Creating or cancelling a supported alert or digest also requires `sitetrax:notifications:write` and confirmation of the proposed change. That permission does not grant general edits to operational records or arbitrary actions in other systems. See [Alerts and Scheduled Digests](#).

If setup or an answer fails

An absent integration can be a workspace-policy issue. An empty project list can be an account-sharing issue. An answer without SiteTrax.io evidence can mean the assistant did not call the tools. If permission is insufficient, check the actual granted scopes; repeating the same read-only connection does not add write access. Use [Troubleshooting Connections](#).

Returned records and summaries are sent to OpenAI for the response. Follow your organization's provider and data-handling policies. For disconnecting and server-side access termination, see [Account Access and OAuth](#).

Vendor setup reference checked 7 October 2026. Customer-account installation was not exercised in this documentation review.

Claude

Connecting Claude

Use Claude to ask questions about authorized SiteTrax.io observations and analytics. The remote connector makes SiteTrax.io tools available to Claude; SiteTrax.io continues to enforce your account's project access.

Before you start

Use an active, email-verified SiteTrax.io account with the projects you need. A published Intelligence profile is optional. In managed Claude workspaces, a permitted owner or administrator must add the connector before members connect their individual accounts.

Add and authorize the connector

1. Use **Add to Claude** in the SiteTrax.io Intelligence hub, or open Claude's connector settings.
2. Add a custom web connector named **SiteTrax.io** with URL `https://mcp.sitetrax.io/mcp`.
3. Review the detected authentication settings and use the OAuth setup supported by SiteTrax.io. Supply a custom client ID only when SiteTrax.io provides one for your connection.
4. Complete SiteTrax.io sign-in and consent, then enable the connector for your conversation.

Anthropic's [current custom-connector guide](#) covers individual and managed-workspace setup. Labels and available authentication choices vary by account. Remote connector requests originate from Anthropic's cloud, including when you use Claude Desktop; a private-network-only endpoint needs compatible connectivity.

Check the connection

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

Compare the result with the same account in app.sitetrax.io. Then request a known equipment observation with its time, timezone, project and record link. An installed connector alone does not prove successful authorization.

Use the result in your work

“ Using SiteTrax.io, find the latest observation of trailer [complete identifier] at [project]. Draft a short customer-service response using only the returned evidence. Include the record link and identify any missing evidence. Do not send the response.

A draft is different from a sent message. Sending through another system requires a separately connected tool and authorization.

Permissions and troubleshooting

Read access supports authorized queries and notification history. Creating or cancelling supported alerts and digests additionally requires `sitetrax:notifications:write`. The client must request and receive that scope; reconnecting with a read-only request does not add it. Confirm the exact proposed notification before creation.

If Claude gives a general answer, confirm SiteTrax.io is enabled for the conversation and ask it to use the tools. If the project list differs from the application, check the connected account and sharing. See [Troubleshooting Connections](#).

Authorized results are returned to Anthropic. A published profile can supply selected facts and priorities, but it does not pass your saved working brief or response-style instructions to Claude.

Use [Account Access and OAuth](#) for scope and disconnect details.

Vendor reference checked 7 October 2026. Customer-account installation was not exercised in this documentation review.

Microsoft

Microsoft 365 Copilot setup, availability and permission limits are documented in the Microsoft section of the MCP Server reference. Use the connection guide below.

Microsoft

Microsoft: Connection Guide

Use the [Microsoft 365 Copilot connection guide](#) for current publication status, setup and federated read-only limits.

The guide remains at its original address so existing bookmarks continue to work. Its content is organized within a dedicated Microsoft section.