Microsoft

- Connect SiteTrax.io to Microsoft 365 Copilot

Connect SiteTrax.io to Microsoft 365 Copilot

Use the SiteTrax.io connector to bring live SiteTrax.io operational intelligence into Microsoft 365 Copilot.

Availability. The SiteTrax.io Federated Copilot Connector is in submission to Microsoft and is not yet listed in the Copilot connectors gallery. This page documents how the connector works and how it will be enabled once Microsoft publishes it. Until then, SiteTrax.io operational data is available through any MCP client that supports remote HTTPS servers with OAuth, using the endpoint `https://mcp.sitetrax.io/mcp`. See the SiteTrax.io MCP Server page for that path.

Overview

The SiteTrax.io Microsoft 365 Copilot Connector lets authorized users query SiteTrax.io operational data directly from Microsoft 365 Copilot.

SiteTrax.io is implemented as a Microsoft Federated Copilot Connector using Model Context Protocol (MCP).

The SiteTrax.io federated connector does not maintain a synchronized Microsoft 365 index of operational records. When Copilot requests SiteTrax.io information, SiteTrax.io returns the authorized results to Microsoft for that response. SiteTrax.io remains the source system; query-time retrieval still shares the returned data with the assistant provider.

Access remains tied to the user's SiteTrax.io permissions.

What You Can Do

After SiteTrax.io is connected, users can ask Microsoft 365 Copilot questions such as:

> What SiteTrax.io sites do I have access to?

> Summarize SiteTrax.io asset activity for the last seven days.

> Where was container SITU 123456 7 last observed?

> Show today's detections at the Utah site by status code and asset type.

> Which SiteTrax.io records may require review today?

> Were there any unusual volume gaps across my sites this week?

> Compare SiteTrax.io activity this week with last week.

Copilot can use SiteTrax.io to retrieve and summarize authorized operational information without requiring the user to manually navigate through individual SiteTrax.io records.

Requirements

Before using the SiteTrax.io connector, you need:

- An active SiteTrax.io account with verified email. Finish verification before starting the Copilot connection.
- Access to at least one SiteTrax.io project, yard, facility, or site.

- A work or school Microsoft account in an organization where the SiteTrax.io connector has been enabled.
- A Microsoft 365 Copilot license that supports federated connectors.
- Permission from your Microsoft 365 administrator to use the SiteTrax.io connector.

Your Microsoft 365 administrator controls whether SiteTrax.io is available in your organization.

Your SiteTrax.io account controls which SiteTrax.io data you can access.

For Microsoft 365 Administrators

SiteTrax.io must be enabled for your Microsoft 365 organization before users can access it through Copilot.

Enable SiteTrax.io

Sign in to the Microsoft 365 admin center with an account that has the required Microsoft 365 administrative permissions.

Go to:

Copilot connectors → Connectors gallery

Find **SiteTrax.io** in the connectors gallery.

Review the connector information, including:

- Publisher
- Connector description
- Permissions
- Privacy policy
- Terms
- Support information

Approve or enable SiteTrax.io for the appropriate users or groups in your organization.

Microsoft can make connectors available through a staged rollout before organization-wide deployment. Your Microsoft 365 administrator determines who can use the connector.

If SiteTrax.io does not appear in the gallery, confirm that:

- The connector is available to your Microsoft 365 tenant.
- Federated connectors are enabled for your organization.
- Your administrator has the appropriate Microsoft 365 role.
- Any Microsoft release or tenant restrictions have been satisfied.

Changes to connector availability can require time to propagate through Microsoft 365.

Enabled connectors are managed under **Copilot connectors** → **Your connections**. To pilot SiteTrax.io with a limited group before a wider release, use **Add staging** and target a Microsoft Entra ID group. The **Staged Rollout** column shows which connectors are currently staged. Third-party federated connectors are a preview capability, so labels and placement can change.

For SiteTrax.io Users

After publication and your administrator's enablement, you must authorize your own SiteTrax.io account. Confirm the intended account in the SiteTrax.io application first. Application sign-in alone does not authorize Copilot, and a published Intelligence profile is optional for ordinary MCP access.

See Account Access and OAuth.

The SiteTrax.io federated connector uses user-level authentication. It does not use one shared SiteTrax.io account for the entire Microsoft 365 organization.

Connect Your Account

Open Microsoft 365 Copilot with your work or school account.

When Copilot asks to connect to SiteTrax.io, select the option to connect or sign in.

You will be redirected to the SiteTrax.io authorization process.

1. Sign in to your SiteTrax.io account.
2. Review the SiteTrax.io access requested for Microsoft Copilot.
3. Approve the connection.
4. Return to Microsoft 365 Copilot.

After authorization, Copilot can use the SiteTrax.io connector when it calls for SiteTrax.io information. Ask it to list your accessible SiteTrax.io projects and compare them with the application under the same account. An empty list can mean no projects are shared with that account.

You do not need to provide your SiteTrax.io password to Microsoft Copilot.

Read-Only Copilot Access

The SiteTrax.io Federated Copilot Connector is read-only.

The federated connector exposes permitted read-only tools, including search, retrieval and supported server-side analytics. SiteTrax.io also restricts its OAuth grant to `sitetrax:read`. Notification changes require the separate `sitetrax:notifications:write` scope, which is not granted to the Copilot connection.

The Copilot connector does not expose SiteTrax.io tools that:

- Create operational records.
- Modify SiteTrax.io data.
- Create notification automations.
- Cancel notification automations.
- Create recurring digest automations.
- Perform other cross-service write actions.

Microsoft Copilot can query authorized SiteTrax.io information, but the federated connector cannot use the connector to modify SiteTrax.io or create external automations.

This restriction is enforced by SiteTrax.io authorization in addition to the MCP tool configuration used by the Microsoft connector.

What Data Can Copilot Access?

Copilot can only access SiteTrax.io data that the signed-in SiteTrax.io user is authorized to access.

Depending on the customer's configuration, this can include:

Projects and Sites

- Sites
- Yards
- Facilities
- Projects
- Cameras
- Project activity

Asset Observations

- Intermodal container IDs
- Chassis IDs
- Trailer IDs
- USDOT numbers
- Other supported operational identifiers
- Observation timestamps

- Site and project information
- Camera information
- Direction information
- Processing status
- Available capture metadata

Operational Intelligence

- Activity totals
- Distinct stored identifier counts, with the returned eligibility and counting rules
- Trends
- Status breakdowns
- Asset-type breakdowns
- Site comparisons
- Camera activity
- Potential anomalies
- Review candidates
- Observed asset movement history
- Supported sequence and duration metrics

Supporting Evidence

Where permitted and available:

- Detection images
- Thumbnail information
- Capture metadata
- Asset record details

Project redaction policies and SiteTrax.io permissions continue to apply.

How Copilot Retrieves SiteTrax.io Data

SiteTrax.io uses Microsoft's federated connector architecture.

SiteTrax.io operational data remains in the source system and authorized query results are sent to Microsoft when Copilot calls the connector. Those returned results are processed by the assistant provider; consult your organization's Microsoft data-handling policies.

The connector does not operate as a Microsoft 365 synced connector and does not create a separate Microsoft 365 index of SiteTrax.io operational records.

SiteTrax.io remains the source system.

Permissions

There are two separate levels of access.

Microsoft 365 Access

Your Microsoft 365 administrator determines whether the SiteTrax.io connector is available to you.

SiteTrax.io Access

Your SiteTrax.io account determines which projects and operational data you can access.

Enabling the connector in Microsoft 365 does not grant additional SiteTrax.io project permissions.

For example, if your SiteTrax.io account can access three projects, Copilot can query those authorized projects. It cannot use the connector to access another customer's projects or a SiteTrax.io project that has not been shared with you.

Using SiteTrax.io in Copilot

Be specific when asking Copilot to use SiteTrax.io.

Name the Source

Instead of:

> What happened today?

Use:

> Using SiteTrax.io, summarize activity at the Utah site today.

Include a Time Period

Instead of:

> Show container activity.

Use:

> Show SiteTrax.io container activity for the last seven days.

Identify the Facility

Instead of:

> How many assets were scanned?

Use:

> Using SiteTrax.io, show asset activity at the Norfolk yard yesterday.

Identify the Asset

For an individual asset, use the complete identifier:

> Where was SITU 123456 7 last observed in SiteTrax.io?

Ask for a Breakdown

> Using SiteTrax.io, break today's detections down by asset type and processing status.

Ask for Comparisons

> Compare SiteTrax.io activity at my sites this week with last week.

Example Workflows

Morning Operations Review

> Using SiteTrax.io, summarize activity across my sites since yesterday morning. Identify unusual volume changes and records that may require review.

Asset Lookup

> Find the latest SiteTrax.io observation for SITU 123456 7 and tell me where and when it was observed.

Site Performance

> Using SiteTrax.io, show daily asset activity at the Utah site for the last seven days.

Exception Review

> Using SiteTrax.io, show today's results by status code and asset type and identify the categories I should investigate.

Camera Health

> Using SiteTrax.io, summarize camera activity and scan health for my sites today.

Equipment Flow

> Using SiteTrax.io, analyze observed trailer movement between the configured inbound and outbound gates this week.

Troubleshooting

Symptom	Likely cause	What to do
SiteTrax.io does not appear in Microsoft 365 Copilot	The connector is not yet publicly listed, or after publication your organization has not enabled it or included you in its staged group	The connector is currently in submission and not yet listed. After publication, ask your Microsoft 365 administrator whether it is available to your tenant and enabled for your account or group
SiteTrax.io appears but the connection fails	SiteTrax.io sign-in, the browser, or an organizational security control is blocking the authorization flow	Confirm you have an active SiteTrax.io account with verified email and can sign in normally, that your browser permits the authorization redirect, and that your organization allows the connection. If verification interrupted the flow or the request expired, restart from Copilot after completing verification. If it persists, contact SiteTrax.io support
Copilot says you need to authenticate	First use, expired authorization, revoked access, or a changed connector configuration	Complete the SiteTrax.io OAuth sign-in. No SiteTrax.io password is given to Microsoft
Copilot cannot find a project	The project is not shared with your SiteTrax.io account	Sign in to SiteTrax.io and confirm the project is shared with you. Microsoft Copilot cannot widen your SiteTrax.io permissions
Copilot cannot find an asset	The lookup expects an exact identifier, the filters exclude the record, or the prompt did not name SiteTrax.io	Use the complete identifier for an exact latest-observation or media lookup and name SiteTrax.io. Broader asset search can match partial identifiers. Add the site or approximate date and check project access if needed
Two users see different results	Expected. SiteTrax.io access is scoped per user	Nothing to fix. Two users with different SiteTrax.io project permissions correctly receive different answers

Symptom	Likely cause	What to do
Copilot cannot create an alert or change SiteTrax.io data	Expected. The connector is read-only	Creating or cancelling supported alerts and digests requires `sitetrax:notifications:write`, which this Copilot connection does not receive. Use a supported MCP client that can request that permission; see Alerts and Scheduled Digests. Use the SiteTrax.io application for operational actions available there
Results need more context	The prompt is too broad for the data available	Specify the site or project, a date range, the asset type, the identifier, the camera, the status, or the comparison you want

Disconnecting or Revoking Access

Your organization can disable the SiteTrax.io connector through Microsoft 365 connector administration.

Users can use the disconnect controls available in their Microsoft experience. SiteTrax.io does not currently provide an individual connected-app inventory or per-connection revoke control. Disconnecting in an assistant and invalidating issued credentials at SiteTrax.io are distinct actions; contact SiteTrax.io support if server-side access termination is required.

Current SiteTrax.io project sharing continues to apply to future requests. Removing a project share removes that project from the account's authorized reach, but is not the same as revoking the whole assistant connection. See Account Access and OAuth.

Known Issues and Limitations

- The connector is in submission to Microsoft and is not yet listed in the Copilot connectors gallery. Third-party federated connectors are a preview capability.
- The connector is read-only. Microsoft enables only MCP tools carrying the read-only annotation, and the SiteTrax.io write scope is not granted to the Copilot connection. Creating alerts, cancelling alerts and creating recurring digests are not available through Copilot.
- Availability is controlled by your Microsoft 365 administrator and can be staged to selected Microsoft Entra ID groups. Changes to connector availability can take time to propagate through Microsoft 365.
- Access is limited to the SiteTrax.io projects shared with the signed-in account. Enabling the connector grants no additional SiteTrax.io permission.

- Each user authorizes individually. There is no shared organizational SiteTrax.io login, so two users can correctly receive different answers to the same prompt.
- Detection images and video can be withheld by project configuration, record retention, user permissions or redaction, while permitted operational metadata is still returned.
- An asset record is one stored processing result. It is not necessarily one physical asset or one direct observation, and combined container and chassis processing can add synthetic pair-side rows.
- Sequence and duration results depend on camera placement and on observations that can be paired reliably. Where a required pairing is unavailable, SiteTrax.io reports the limitation rather than estimating a value.
- A Microsoft 365 Copilot licence that covers federated connectors is required. The surfaces and regions where approved federated connectors appear are determined by Microsoft and can vary by tenant and rollout ring.

Security and Privacy

SiteTrax.io access through Microsoft Copilot follows the authenticated user's SiteTrax.io permissions.

Do not include passwords, OAuth tokens, secrets, or other authentication credentials in Copilot prompts.

For information about how SiteTrax.io handles data, see:

SiteTrax.io Privacy Policy

`https://sitetrax.io/privacy-policy/`

SiteTrax.io Terms of Service

`https://sitetrax.io/tos/`

Support

For problems with your SiteTrax.io account, SiteTrax.io permissions, SiteTrax.io data, or the SiteTrax.io connector, contact:

`support@sitetrax.io`

When contacting support, include:

- Your SiteTrax.io account email.
- Your Microsoft 365 organization, if relevant.
- The site or project involved.

- The approximate time of the problem.
- The prompt you attempted.
- The error message shown by Copilot.

Do not include passwords, access tokens, OAuth secrets, or other credentials.

For Microsoft 365 tenant configuration or connector availability, contact your organization's Microsoft 365 administrator.

Frequently Asked Questions

Does SiteTrax.io copy my operational data into Microsoft 365?

The SiteTrax.io connector is federated: it does not maintain a synchronized Microsoft 365 index. Copilot requests authorized information from SiteTrax.io, and the returned records, summaries or permitted evidence are sent to Microsoft for the assistant's response.

Can Copilot see every SiteTrax.io customer?

No.

Copilot can only retrieve data available to the authenticated SiteTrax.io user.

Does enabling SiteTrax.io give a user additional SiteTrax.io permissions?

No.

SiteTrax.io project permissions remain authoritative.

Can Microsoft Copilot modify SiteTrax.io through this connector?

No.

Microsoft enables only read-only MCP tools in a federated connector, and the write scope is not granted to the Copilot connection.

Can Copilot create SiteTrax.io notifications or scheduled email digests?

Not through the Federated Copilot Connector.

Those capabilities require the SiteTrax.io write scope, which the connector does not receive.

Do users share one SiteTrax.io login?

No.

Federated SiteTrax.io access is authenticated at the user level.

Does a Microsoft administrator have to enable SiteTrax.io?

Yes.

The SiteTrax.io connector must be available and enabled for the user's organization before it can be used.

What Microsoft license is required?

Users querying federated data sources must have an applicable Microsoft 365 Copilot license.

Where can SiteTrax.io be used?

Microsoft can surface approved federated connectors in Microsoft 365 Copilot experiences supported by the connector platform. Availability can vary by Microsoft product, tenant configuration, and rollout.

Related SiteTrax.io Documentation

SiteTrax.io Documentation

`https://docs.sitetrax.io`

SiteTrax.io MCP Server

`https://mcp.sitetrax.io/mcp`

Privacy Policy

`https://sitetrax.io/privacy-policy/`

Terms of Service

`https://sitetrax.io/tos/`

Support

`support@sitetrax.io`