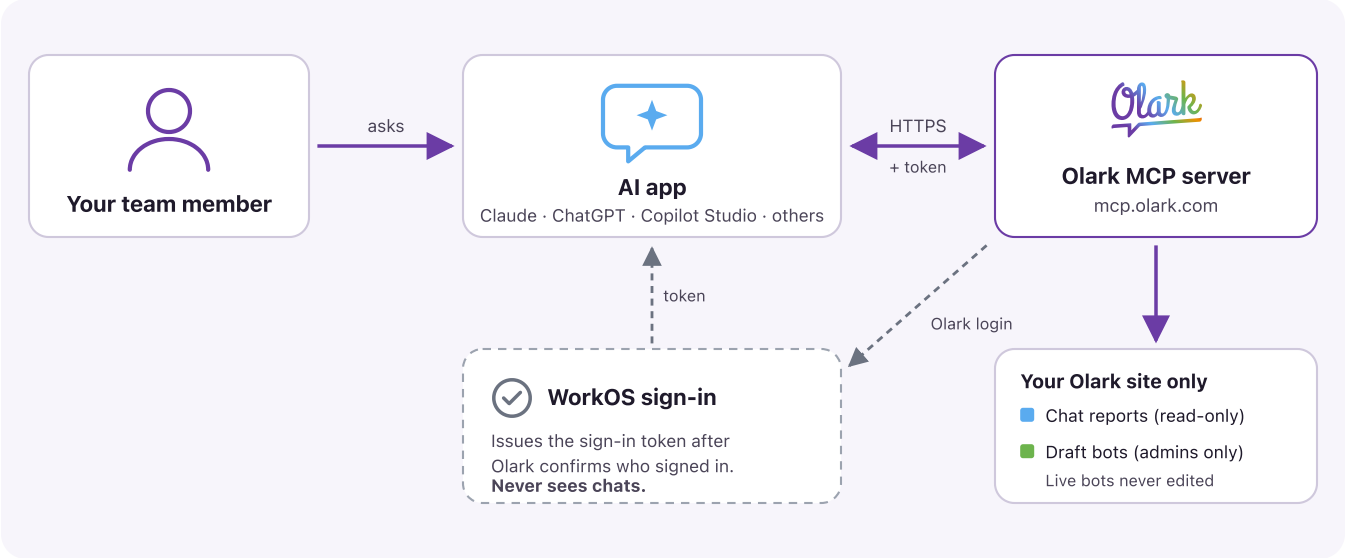
FOR IT AND SECURITY REVIEW

Olark MCP Server

A connector that lets the AI apps your team already uses pull chat reports from Olark and edit Olark bots. This packet explains what it can read and change, how sign-in works, the limits, and how personal information is handled.

Last updated: October 30, 2026 · Online version: olark.com/help/mcp-security



AI apps are shown by name only. Any app that supports remote MCP servers with OAuth sign-in can connect.

At a glance

Address
`https://mcp.olark.com/mcp`, HTTPS only.

Sign-in
Each person uses their own Olark login. No shared passwords, API keys, or service accounts.

Scope
One Olark site: the one that person belongs to.

Chat reports
Read-only. Can't change, delete, or send chats.

Bot changes
Admins and account owners only, and only on draft bots. Live bots are never edited in place.

Personal information
An Olark admin can turn on masking of names, emails, phone numbers, card numbers, and US Social Security numbers. Masking happens on Olark's servers, before results are sent to the AI app.

Terms used in this packet

AI app
The AI product a person chats with, such as Claude, ChatGPT, or Microsoft Copilot Studio. Another company makes it, not Olark.

Tool
One action an AI app can ask Olark to do, such as “search transcripts.”

Draft bot and live bot
A draft is a bot still being worked on. A live bot is turned on for your website. The MCP server can't change a live bot.

Olark site
One Olark account's chats, bots, and team. Each Olark login belongs to one site.

Masking
Replacing personal details, such as an email address, with a placeholder before data leaves Olark. Olark's settings call this **Redact personal information**.

MCP (Model Context Protocol)
An open standard that lets AI apps use tools from other products. The Olark MCP server is Olark's set of these tools.

Bot
An Olark chatbot that answers visitors on your website. Olark's own screens list bots under **AI Assistants**.

Knowledge source
Information a bot uses to answer questions, such as your website or a written FAQ.

OAuth and sign-in token
OAuth is the standard way an app gets permission to act for a signed-in person. The sign-in token is the proof of that permission, which the AI app sends with each request.

How a request works

1. A person asks their AI app a question, such as *“What did customers ask about pricing last week?”*
2. The AI app picks an Olark tool and sends a request to `mcp.olark.com` with that person's sign-in token.
3. Olark checks the token, looks up the person's Olark account and role, and only offers tools that role allows.
4. Olark runs the tool on that person's site. If masking is on, Olark masks personal information before the result leaves Olark.
5. The AI app receives the result and writes its answer.

Olark only sees the tool requests. It doesn't see the rest of the person's conversation with their AI app.

What the AI app can do

The AI app can only use the tools below. Which ones a person gets depends on their Olark role.

TOOL	WHAT IT DOES	TYPE	WHO GETS IT
Search transcripts	Chats filtered by words, visitor name, visitor email, tags, and dates. Includes conversation text, transcript links, times, tags, and the visitor's first page when known. Up to 100 chats per request.	Reads	Every Olark role
Transcript details	The same data as the dashboard's transcript CSV export: timing, visitor and agent fields, tags, custom fields, feedback, and transcript links. No message text. Up to 2,000 rows per request.	Reads	Every Olark role

TOOL	WHAT IT DOES	TYPE	WHO GETS IT
Agent activity	Availability, chats, missed chats, response times, ratings, and status history for each agent.	Reads	Every Olark role
Visitor funnels	Counts of website visitors who complete a series of steps, grouped by hour, day, or week.	Reads	Every Olark role
Read bots	List the site's draft and published bots, read a bot's settings (name, company name, tone, behavior, whether it is live), and list its knowledge sources.	Reads	Every Olark role
Create a draft bot	From a website address, a copy of an existing bot, or settings the person provides. Creating from a website reads that public website using OpenAI, which is already one of Olark's subprocessors.	Changes	Admins and account owners
Update a draft bot	Name, company name, tone, behavior, and settings such as contact-capture fields and proactive messages.	Changes	Admins and account owners
Knowledge sources	Add or remove a website domain the bot can search, or text written in Markdown, on a draft bot.	Changes	Admins and account owners
Preview link	A link to try a draft bot in a browser.	Reads	Admins and account owners
Publish a draft bot	Makes it available in Olark. It doesn't put the bot on your website. Someone still has to turn it on in Olark.	Changes	Admins and account owners

> **Important:** anyone with an Olark login on the site, including the basic Agent role, can use the reporting tools for the whole site.

Each tool tells the AI app whether it only reads or makes changes. Many AI apps use this to ask the person before making a change, and some let you turn individual tools off.

What it can't do

- Delete or edit chats, contacts, tags, agents, or account settings
- Send messages to website visitors
- Read or change anything on another Olark site
- Edit a live bot, or put a bot on your website
- Read data from your CRM or other apps

Limits

- **Reporting:** 60 requests per hour per Olark site, shared by everyone on the site and all four reporting tools. Olark raises it to 500 per hour for a small number of high-volume sites.
- If the limit can't be checked, reporting requests are refused rather than allowed through.
- Up to 100 chats per search and 2,000 rows per transcript details request.
- Up to 6 funnels and 500 time periods per funnel request.
- Agent activity is counted in whole days, in UTC.

Sign-in and WorkOS

Each person connects with their own Olark login, using OAuth, which is the standard way apps get permission to act for a signed-in person. Olark uses **WorkOS** to run the OAuth part of sign-in. WorkOS is a sign-in service used by many software companies.

- The person signs in on **Olark's own login page**, the same way they normally sign in to Olark: email and password, Google, Microsoft, or their company's SSO. WorkOS never sees their password or SSO credentials.
- After Olark confirms who they are, Olark tells WorkOS the person's Olark user ID, email address, and name.
- WorkOS then gives the AI app a signed sign-in token for that person.
- **WorkOS never receives chats, transcripts, reports, or bot settings.** Those go straight from Olark to the AI app.

On every request, Olark checks the token's signature and looks up the person's Olark account and role.

Personal information and masking

Chat transcripts often include visitors' names, email addresses, and phone numbers. By default, reporting results are returned as they appear in Olark. An Olark admin can turn on **Redact personal information** on the AI Connector page in Olark. It applies to the whole site. When it is on:

- Olark masks names, email addresses, phone numbers, card numbers, and US Social Security numbers in reporting results before they leave Olark.
- If masking fails for any reason, Olark returns an error instead of the unmasked result.

Masking reduces what reaches the AI provider, but it is automated and can miss details or mask the wrong text. It doesn't guarantee that no personal information reaches the AI provider. Masking doesn't apply to bot tools.

What happens to the data after Olark sends it

Olark sends each result only to the AI app that asked for it. After that, the AI provider's terms decide how the result is stored, how long it is kept, and whether it is used to train models. These usually depend on the plan your organization has with that provider: Claude privacy, OpenAI enterprise privacy, Microsoft Copilot privacy.

What Olark records

To run the service, Olark records each tool request: the site, the person's Olark user ID, the tool name, and the inputs the AI app sent, such as search words and dates. Olark also counts requests and errors by tool and by site. These records are not a report your team can view.

Common questions

Does the AI app get access to our whole Olark account?
No. It only gets the tools listed in this packet, for one site, under one person's login. It can't reach account settings, billing, agents, or other Olark sites.

Can a team member see more through the AI app than they can in Olark?
Possibly. The reporting tools cover the whole site for every Olark role, including the basic Agent role. If some agents shouldn't see all of your site's chats, decide whether to let them connect an AI app.

Can it change or delete our chats?
No. The reporting tools only read. Nothing in the MCP server deletes or edits chats.

Can we allow chat reports but block bot changes?
Yes. Bot editing is only available to admins and account owners. People with the Agent role get reporting and bot reading only. Some AI apps also let you turn off individual tools.

Can the AI app put a bot on our website?
No. It can publish a draft so it shows up in Olark, but turning a bot on for your website is a separate step someone has to take in Olark.

Is there a shared API key or service account?
No. Every connection is tied to one person's Olark login.

Can we stop people connecting a personal AI account?
Not from Olark. Olark checks who the person is, not which AI app or account they connect from. Anyone with an Olark login can connect any compatible AI app, including a personal account. Your organization's AI policy is what controls this. To cut off every connection on your site at once, email support@olark.com.

Does WorkOS see our chats?
No. WorkOS only handles sign-in. It receives the person's Olark user ID, email address, and name, never chat content.

Does Olark see our conversations with the AI app?
No. Olark only receives the tool requests the AI app sends, such as “search transcripts mentioning refunds from last week.” It doesn't see the rest of the conversation.

Will our data be used to train AI models?
Olark doesn't control that. Once the AI app receives a result, your agreement with that AI provider decides whether it can be used for training.

Could text inside a chat trick the AI app?
Chats are written by website visitors, so treat them as untrusted text. Someone could write instructions into a chat hoping an AI app will follow them. To limit the risk, reporting tools only read, bot tools can't change live bots, and each tool tells the AI app whether it makes changes. Ask people to review changes before approving them.

Is the connection encrypted?
Yes. The server only accepts HTTPS connections at `https://mcp.olark.com/mcp`.

What happens when a limit is reached?
The AI app gets an error that says the limit was reached, and reporting works again once the hourly limit allows. Bot tools aren't affected.

How do we disconnect?
Each person removes or disconnects the Olark connector in their AI app. That stops all new requests from it. To cut off every connection on your site at once, email support@olark.com.

Before your team connects

- [ ] Choose which AI apps your organization allows, and check their data retention and training terms. Olark can't limit which AI app or account someone connects, so make this part of your AI policy.
- [ ] Decide who should connect. Anyone with an Olark login can connect, and every Olark role can use the reporting tools for the whole site.
- [ ] Decide whether to turn on **Redact personal information** on the AI Connector page.
- [ ] If people only need reports, check whether your AI app lets you turn off the bot tools. People with the Agent role never get bot editing tools.
- [ ] Make sure people connect the official address, `https://mcp.olark.com/mcp`.

Questions from your IT or security team?

support@olark.com

Email us. We're happy to help with your review.

About this packet

This packet explains how the Olark MCP server works as of October 30, 2026. It is here to help with your review. It isn't a contract, and it doesn't change your agreement with Olark. Our Terms of Service (olark.com/tos) and Data Processing Agreement are what govern how Olark handles your data. The MCP server may change over time, and we'll update this packet when it does. Once your AI app receives data from Olark, your AI provider's terms apply to it.