ManageEngine Log360 Cloud

Zoho MCP

DATASHEET

Log360 Cloud MCP Server

Bring Log360 into your preferred AI client

Standardized AI access to Log360 Cloud through the Model Context Protocol (MCP). Query logs, investigate alerts, manage configurations, and drive response — from Claude, Copilot, Cursor, or any MCP-compatible client.

www.manageengine.com/cloud-siem

What it MCP

The Model Context Protocol is an open standard, that defines how AI clients discover and invoke external tools. It replaces bespoke, per-vendor integrations with a common wire format: an AI client speaks MCP, an MCP server exposes a set of tools, and the two negotiate what's available and how it's called — all through structured, auditable requests.

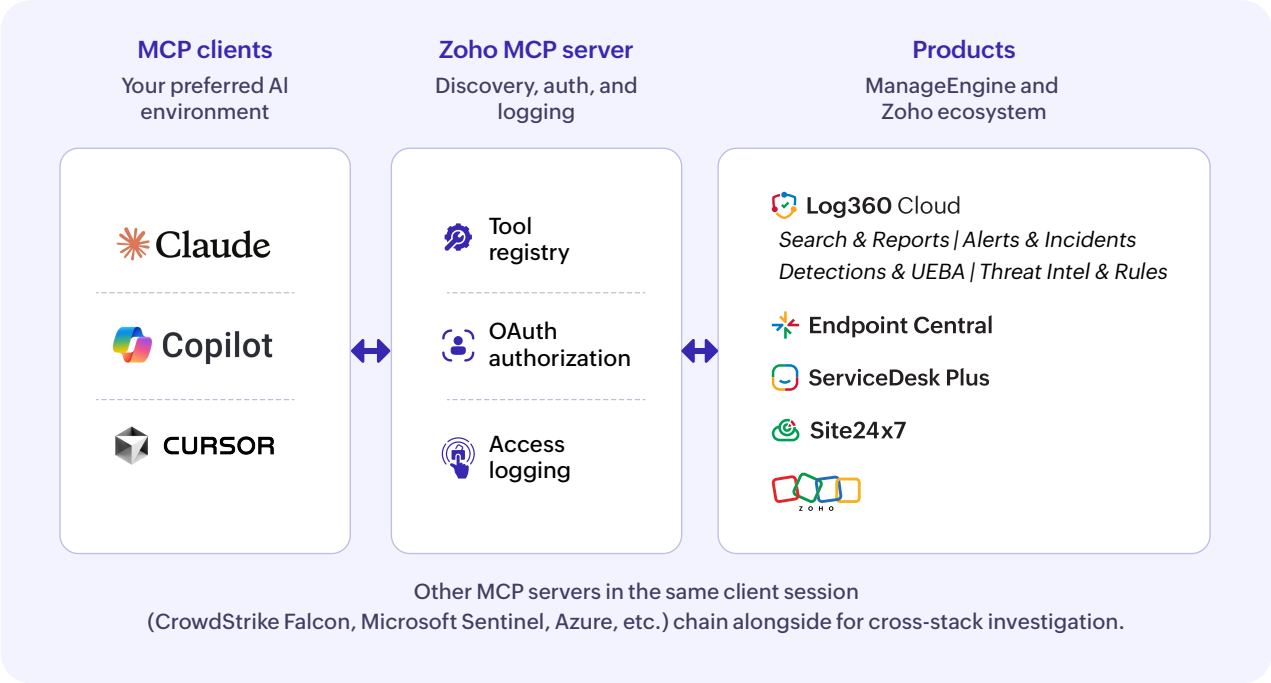
The Log360 Cloud MCP Server, delivered through the Zoho MCP platform, exposes Log360's operational surface as MCP tools. When an analyst prompts their AI client in natural language, the client discovers the available tools from the server, selects the right one for the request, calls it with structured parameters, and returns the response as reasoning material for the next turn.

Log360 becomes the data-and-action layer beneath the conversation. Any MCP-compatible client can query, correlate, and act on Log360 data without a custom integration.

How it works

The Zoho MCP Server connects to Log360 Cloud over its REST APIs and exposes prebuilt tools spanning log search, alerts, incidents, detections, UEBA, threat intelligence, reports, log sources, and the rule library. The server handles user authentication via OAuth and logs every tool invocation.

The same MCP server can include tools from other ManageEngine and Zoho products — Endpoint Central, ServiceDesk Plus, Site24x7, and Zoho business applications. One server, one connection, tools from across the stack.



Other MCP servers in the same client session, including CrowdStrike Falcon, Microsoft Azure, and others, can chain alongside, so a single conversation can span SIEM, EDR, cloud, and identity without switching tools.

What this changes for security teams

SIEM access outside the SIEM console

Log360 becomes a callable tool layer inside any MCP-compatible AI client. Analysts work from the environment they're already in. Log360 data and actions come to them.

End-to-end operations in a single session

One prompt thread can search logs, check threat intelligence, pull UEBA risk scores, review alert configurations, create an incident, and enable a detection rule — without switching consoles. Context carries across steps.

Read and write access

Log360's MCP tools cover search, retrieval, and action: create incidents, enable or disable alert profiles, manage log sources, build custom reports. Analysts investigate and act from the same session.

Skill barrier removed

Query syntax, module navigation, and platform-specific knowledge no longer gate what an analyst can extract. A Tier 1 analyst retrieves the same data a Tier 3 analyst would — through natural language.

Multi-product reach from a single server

The same Zoho MCP Server that carries Log360 tools can include tools from Endpoint Central, ServiceDesk Plus, Site24x7, and Zoho business apps. One prompt can pull a Log360 alert, check the device's patch status in Endpoint Central, and raise a ticket in ServiceDesk Plus.

Cross-stack investigation beyond ManageEngine

Chain additional MCP servers from your EDR, cloud security, and identity providers into the same AI client session. A single conversation correlates Log360 data with endpoint telemetry, sign-in risk, and cloud posture.

Scoped, logged, revocable

Each server exposes only the tools you add. Authorization is per-user via OAuth. Every invocation is indexed — user, tool, timestamp, status — retained 30 days, filterable from the Zoho MCP Console. Revoke access or disable a server at any time without losing configuration.

How to configure a MCP server for Log360 Cloud

To setup a Log360 Cloud MCP server, navigate to the Zoho MCP Console (mcp.zoho.com) with an active Log360 Cloud account.

1. Create the MCP server

- Open the Zoho MCP Console and create a new MCP server. Provide a name that identifies the server's purpose, such as "SOC-Log360" or "Security-Operations."

2. Add tools

- Navigate to the Tools section in the console and click Add Tools. Search for Log360 Cloud in the products list and select the tools you want to expose.
- To include tools from other products in the same server, click Add More Tools and search for Endpoint Central, ServiceDesk Plus, Site24x7, or any other available ManageEngine or Zoho apps. Only the tools you explicitly add are accessible to the AI client.

3. Connect to your AI client

- Go to the Connect section in the MCP Console and copy the MCP server URL. Add it to your AI client:
  - In Claude, paste the URL under Settings > Connectors > Add Custom Connector.
  - In VS Code, Cursor, and other MCP-compatible clients follow a similar process through their respective server configuration interfaces.

4. Authorize

- On first use, the AI client triggers an OAuth authorization flow. The user authenticates with their Zoho account and grants the scoped permissions required by the configured tools.

5. Verify

- Test with a prompt such as "Show me active alert profiles in Log360" to confirm the connection and tool access.

Use case

Scenario: A new security advisory describes active exploitation of scheduled task and service creation techniques for lateral movement. The analyst wants to assess coverage, check if anything has already fired, and investigate if needed.

1

Check detection coverage

"What detection rules do I have installed for lateral movement? Specifically anything covering T1053 and T1543."

Returns installed rules by MITRE technique, with severity, status, and gap between installed and available rules in the library.

2

Check alert profile coverage

"Do any of my alert profiles cover scheduled task creation or new service installation?"

Returns matching alert profiles with log sources, thresholds, and enabled/disabled status.

3

Pull recent detections

"Show me detections triggered in the last 7 days that map to T1053 or T1543."

Returns triggered detections with timestamps, hosts, users, an MITRE stage.

4

Investigate the flagged entity

"Pull the username and domain from detection [ID], then get that user's UEBA risk profile and anomaly history."

Returns risk score, anomaly count, and behavioral deviations for the user.

5

Enrich with threat intelligence

"Run the source IP from that detection through threat intel. Check both ATA and VirusTotal."

Returns reputation scores, geo/WHOIS data, and multi-vendor detection results.

6

Search surrounding logs

"Pull all activity from that host for the 30 minutes before and after the detection."

Returns matching log records from that host and time window.

7

Create an incident

"Create a Trouble-severity incident for these findings. Use the log search as evidence, put detection details in the description, and assign it to [analyst 2]."

Incident created with severity, linked evidence, and documented findings — assigned to a person.

8

Tighten coverage

"Enable the alert profile 'Suspicious Service Installation' that was disabled."

Profile enabled. Confirmation returned.

The session doesn't have to stop at Log360

If the same MCP server includes Endpoint Central tools, the next prompt can check whether the affected host has unpatched vulnerabilities or pending software deployments. If ServiceDesk Plus tools are configured, a ticket can be raised in the same conversation.

And if other MCP servers are connected to the AI client, the analyst can pivot into EDR telemetry, cloud security posture, or identity risk without leaving the session.

ManageEngine
Log360 Cloud

About Log360 Cloud

Log360 Cloud is a unified security platform designed to help organizations progress from log visibility to measurable security outcomes. The platform unifies log collection, correlation, behavioral analytics, and built-in SOAR to take security teams from detection through investigation to automated response in a single workflow. Zia, the AI layer inside Log360, turns raw alerts into analyst-ready context, replaces manual queries with natural language, puts prebuilt and custom AI agents to work on bounded SOC tasks, and connects the platform to external AI tools through MCP. Log360 Cloud helps security teams reduce dwell time, improve operational efficiency, and strengthen overall SOC maturity.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/ and follow the LinkedIn page for regular updates.

Sign-up for free

Get a personalized walk-through