

Salt Claude Connect: Continuous MCP server visibility for Claude Enterprise

Know what's connected to your Claude organization — continuously, typically updated within one polling cycle

As AI adoption accelerates inside enterprises, security and IT teams are asking a foundational question: what exactly is connected to our AI, and what can it access? For organizations running Claude Enterprise, MCP (Model Context Protocol) servers are becoming a key surface area — enabling powerful tool integrations but also introducing new security exposure. Without a live inventory of what is connected, security teams are flying blind.

Salt Claude Connect links the Salt Security platform directly to Claude's Compliance API, providing continuous, read-only visibility into organization-managed MCP servers with recorded lifecycle activity in the Compliance API. With no agents, no traffic analysis, and no manual cataloging, security teams get a live picture of MCP server posture the moment the connector is activated.

The challenge: MCP server blind spots in Claude Enterprise

As organizations expand their use of Claude Enterprise, administrators regularly add MCP servers that give Claude access to internal tools, databases, APIs, and external services. Managing the growing inventory of these integrations introduces several challenges:

- **No centralized MCP inventory:** Administrators may add or remove MCP servers without a durable, auditable record. Security teams have no native view into what is connected at any given moment.
- **Delayed detection of unauthorized connections:** A rogue or misconfigured MCP server can sit in the connector directory for days before anyone notices. Without continuous monitoring, the window of exposure grows.
- **Manual processes that don't scale:** Periodically reviewing connector settings in the Claude admin UI is error-prone and labor-intensive, especially as organizations grow their Claude deployments across teams.
- **Compliance and governance gaps:** Security policies require organizations to know what systems their AI is authorized to access. Without a continuous inventory, demonstrating compliance is difficult.



Solution: Salt Claude Connect

Salt Claude Connect integrates the Salt Security platform with Claude's Compliance API, delivering a continuous, agentless inventory of the MCP servers connected to your Claude organization. In minutes following a simple four-step setup, security teams gain a live, always-current view of which MCP servers are active, when they were added or removed, and their current status — without requiring any traffic mirroring, agent deployment, or manual review cycles.

The connection is narrow by design. The integration requires a Compliance Access Key scoped to `read:compliance_activities` and polls Claude's Activity Feed on a regular cycle. It never sends prompts to Claude, never reads chat content, and never accesses file or project data. The only information flowing into Salt is MCP server lifecycle events.

Key features and benefits

- **Continuous, agentless MCP discovery:** Salt automatically surfaces organization-managed MCP servers that have recorded lifecycle activity within the Compliance API's activity window — no agents, no traffic, no manual exports required. The inventory reflects newly added, updated, or removed connectors, typically within one polling cycle.
- **Complete agentic attack surface visibility:** For the first time, security teams can see MCP servers alongside APIs, hosts, and other agentic surfaces in a single unified Salt inventory. This eliminates the blind spot between what Claude is authorized to access and what your security platform actually monitors.
- **Always-current server status:** Each discovered server shows its name, identity, current status (active or removed), and the timestamp of its most recent lifecycle event. Security teams can immediately act when an unexpected server appears or a known server changes state.
- **Least-privilege integration:** The key must be scoped to `read:compliance_activities` — the minimum scope needed for discovery. No content scopes are used. Your Compliance Access Key is stored encrypted and used only to authenticate against the Compliance API endpoint.
- **Governance and compliance enablement:** A continuously maintained, timestamped record of MCP server activity gives security and compliance teams the audit trail they need to demonstrate control over what their AI is authorized to access.

What the connector discovers

Surfaces in Salt inventory

- Organization-level MCP connectors added by administrators
- Server name, identity, and unique identifier
- Lifecycle events: when a server was added, updated, or removed
- Current status: active vs. removed

Not in scope

- Locally installed MCP servers (run on user devices; not reported to the Compliance API)
- Chat content, prompts, or project data
- User-level activity or personal workspace data

How it works

The connector authenticates to Claude's Compliance API using a Compliance Access Key scoped to `read:compliance_activities`. Salt polls the Activity Feed on a regular cycle. Each activity in the feed carries an `organization_uuid` that identifies your Claude organization, plus metadata about MCP server lifecycle events — server name, event type, and timestamp. Discovered servers appear in your Salt agentic inventory, labeled with the source Claude Compliance API, typically within one polling cycle of the event occurring.

Setup: four steps to connect

Getting the connector running requires a Claude Enterprise organization and Owner or Primary Owner permissions to create a Compliance Access Key.

STEP 1

Create a Compliance Access Key

In `claude.ai`, navigate to Organization Settings > Data and Privacy > Compliance access keys. Create a new key with the `read:compliance_activities` scope — the only scope required. Copy and store the key value securely.

STEP 2

Find your Organization ID

Your Organization ID is the UUID that identifies your org to Salt. Read it from your Claude organization settings, or retrieve it by calling the Compliance API directly with your new key. The `organization_uuid` field on any MCP server activity is your Organization ID. Some administrative activities are recorded without an organization — if the field is empty, use the next activity that has one.

STEP 3

Add the connector in Salt

Open the Data Source Hub in the Salt dashboard, click the Claude Connect tile, and enter your Compliance Access Key and Organization ID. Salt validates the key and runs an initial discovery scan. On success, the connector status changes to Connected.

STEP 4

Review your MCP server inventory

Discovered servers typically appear in your Salt agentic inventory within one polling cycle. From there, the connector is self-maintaining — it polls the Activity Feed continuously and reflects newly added, updated, or removed connectors automatically.

Security and privacy properties

Read-only

Salt reads activity data from the Compliance API only. It never writes back to your Claude organization, sends prompts, or changes any Claude settings or behavior.

Encrypted credentials

Your Compliance Access Key is stored encrypted and used only to authenticate against the Compliance API endpoint.

Single scope

Only `read:compliance_activities` is required. No content scopes are used or available — chats, files, and projects are never accessed.

Always current

The inventory refreshes each polling cycle. Changes to your organization's connectors are reflected shortly after they occur.

Get started with Salt Claude Connect

Don't wait for a security incident to reveal gaps in your AI inventory. Salt Claude Connect gives Claude Enterprise organizations immediate, continuous visibility into MCP server activity — with no agents, no traffic requirements, and no manual overhead. Visit salt.security/connect to learn more or request a demo.