



# Linx AI Access Control

The first inline governance layer built to control, audit, and enforce every MCP action — by humans and agents.

AI agents and the humans driving them are reading records, writing data, and calling APIs inside your most sensitive systems. Most enterprises have no enforcement layer for any of it. Linx AI Access Control changes that. Every MCP tool call passes through the Linx MCP Gateway and is adjudicated in real time against the identity behind it — human, non-human, or agent — before it executes. Most security tools generate alerts. Linx generates decisions.

## Governance at the call layer



### Tool-level decisions

Decide which specific read, write, and admin tools each identity can invoke inside an MCP — scoped by role, team, or persona. Server-level allow-lists become tool-level entitlements.



### Real-time enforcement

The Linx Gateway sits inline between every MCP client and the systems your AI touches. Every call is inspected and adjudicated before execution — approved, elevated through just-in-time access, or blocked — at machine speed.

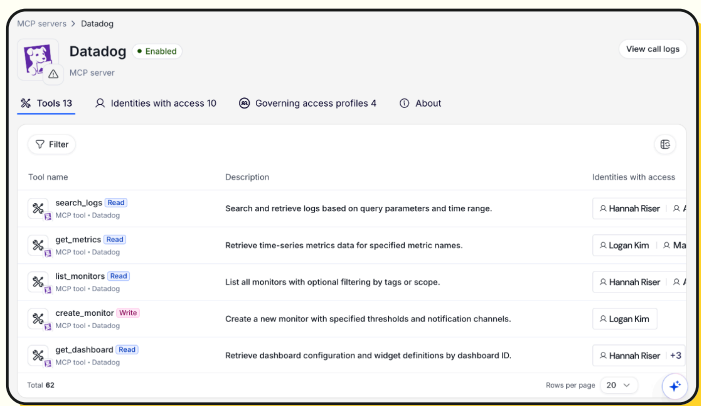


### Unified identity context

See the human invoking the call, the NHI it operates as, and the action being attempted — in one decision, one record, one platform.

## Inline. Every MCP. Every client.

The Linx Gateway sits between every MCP client your teams use — including Claude Desktop, Cursor, Claude Code, and others — and any MCP server they reach, whether SaaS, internal, or self-hosted. No client cooperation required. No hosting lock-in. If an agent calls an MCP tool, Linx governs it.



## Three decision states, one policy engine.

Not every call is allow-or-block. Linx adjudicates each tool call against the identity's access profile and routes it to one of three outcomes:



### Approved

The call matches the identity's standing entitlements. Forwarded to the target, logged, audit-ready.



### JIT Allowed

The call exceeds standing entitlements but qualifies for time-bound elevation. The gateway routes it through Linx's just-in-time approval flow; access expires automatically when the window closes.



### Blocked

The call violates policy. Stopped at the gateway with a clear reason returned to the client, logged for review.

## Tool-level access profiles, not server-level allow-lists

Define what each identity — human, NHI, or agent — can actually do inside an MCP. Read-only for one person, full admin for another, scoped writes for a third. The same access profile model that governs your employees now extends to the agents they deploy.

MCP servers > Datadog

**Datadog** • Enabled MCP server View call logs

Tools 13 | **Identities with access 10** | Governing access profiles 4 | About

Filter

Identity	Tools	Governing access profiles	Last used
<b>JD</b> Jared Devers jared@fincorp.com • Staff Engineer	% search_logs	SRE On-Call Engineering	May 12 2026 05:09
<b>AS</b> Amy Stewart amy@fincorp.com • SRE	% search_datadog_monitors +1	SRE Platform	May 12 2026 16:05
<b>MA</b> Mark Anderson mark@fincorp.com • Senior SRE	% get_datadog_incident +2	SRE On-Call Engineering	May 12 2026 05:23
<b>MT</b> Mary Tuckerman mary@fincorp.com • Platform Engineer	% get_datadog_metric	Platform Engineering	May 12 2026 05:14
<b>NL</b> Nick Lee nick@fincorp.com • Software Engineer	% search_datadog_spans	Engineering	May 12 2026 05:18

Total 62 Rows per page 20

**MCP gateway logs**

Filter

Identity	Tool called	Called at	AI client	Outcome
<b>JD</b> Jared Devers jared@fincorp.com • Developer	Notion Get Users <a href="#">Read</a> MCP tool • Notion	May 21 2026 17:31	Claude code jared@fincorp.com	Allowed
<b>AS</b> Amy Stewart amy@fincorp.com • Marketer	Notion Search <a href="#">Read</a> MCP tool • Notion	May 21 2026 17:30	Claude code amy@fincorp.com	Allowed
<b>MA</b> Mark Anderson mark@fincorp.com • Developer	authenticate_to_mcp <a href="#">Read</a> MCP tool	May 21 2026 17:29	Claude code mark@fincorp.com	Allowed
<b>MT</b> Monica Tuckerman monica@fincorp.com • Analyst	Get Attachment <a href="#">Read</a> MCP tool • Linear	May 21 2026 17:27	Claude code monica@fincorp.com	Allowed
<b>NL</b> Nick Lee nick@fincorp.com • Developer	Get Issue <a href="#">Read</a> MCP tool • Linear	May 21 2026 17:26	Claude code nick@fincorp.com	Allowed
<b>MA</b> Matthew Bernard matthew@fincorp.com • Developer	List Projects <a href="#">Read</a> MCP tool • Linear	May 21 2026 17:25	Claude code matthew@fincorp.com	Allowed
<b>RD</b> Richard Dryfus richard@fincorp.com • Developer	List Issues <a href="#">Read</a> MCP tool • Linear	May 21 2026 17:24	Claude code richard@fincorp.com	Allowed

Total 62 Rows per page 20

## A complete audit trail, attributed to identity

Every tool call — approved, elevated, or blocked — is captured with the arguments sent, the policy that decided it, and the identity that made it. Investigable for incidents. Defensible for audit. Queryable for governance reviews.

## Govern agents alongside humans and NHIs

Linx is one platform for every identity in your environment. Agent owners. Access reviews. Joiner-mover-leaver. The same workflows that already certify your employees' access now cover the agents they run — without standing up a separate stack or learning a new policy language.

**MCP Servers** Enable MCP server

Filter

MCP servers	Server status	Call count (7d)	MCP tools	Tools provisioned	MCP server owner
<b>Datadog</b> MCP server	Enabled	1842	<a href="#">Read 17</a> <a href="#">Write 2</a> <a href="#">Admin 0</a>	% Identity Domain ... +3	<b>JD</b> Jared Devers jared@fincorp.com
<b>Slack</b> MCP server	Enabled	256	<a href="#">Read 4</a> <a href="#">Write 1</a> <a href="#">Admin 0</a>	% All Staff % Tech Lead	<b>AS</b> Amy Stewart amy@fincorp.com
<b>AWS</b> MCP server	Enabled	2103	<a href="#">Read 6</a> <a href="#">Write 3</a> <a href="#">Admin 2</a>	% Cloud Admin +4	<b>MA</b> Mark Anderson mark@fincorp.com
<b>Okta</b> MCP server	Enabled	89	<a href="#">Read 3</a> <a href="#">Write 1</a> <a href="#">Admin 0</a>	% IT Admin +1	<b>MT</b> Monica Tuckerman monica@fincorp.com
<b>Jira</b> MCP server	Enabled	445	<a href="#">Read 5</a> <a href="#">Write 2</a> <a href="#">Admin 0</a>	% Developer +3	<b>NL</b> Nick Lee nick@fincorp.com
<b>Confluence</b> MCP server	Enabled	113	<a href="#">Read 3</a> <a href="#">Write 0</a> <a href="#">Admin 0</a>	% All Staff	<b>MA</b> Matthew Bernard matthew@fincorp.com
<b>Google Cloud</b> MCP server	Enabled	678	<a href="#">Read 5</a> <a href="#">Write 3</a> <a href="#">Admin 1</a>	% Cloud Admin +3	<b>RD</b> Richard Dryfus richard@fincorp.com

Total 14 Rows per page 20

“During our POV, Linx delivered visibility into identity risks and they were able to help us identify through its AI capabilities any suggestions or recommendations.”



**Brian Miller**  
Senior Director of Governance, Risk, and Compliance At Achieve

Ready to govern every agent action?

[Get a demo](#)

