

AI agents · Cloudflare, managed by FirstNet

Let AI agents work. On your terms.

AI agents now reach company systems through MCP servers, the connectors that let them call tools and fetch data. Cloudflare MCP server portals give every agent one secured entry point, tied to your identity provider and fully logged.

1 entry point

for internal and third-party MCP servers

Your IdP

Microsoft Entra ID, Okta or Google sign-in

Per team

curated tools for each team, such as Sales, HR or Finance

Full log

of agent activity for audit and investigation

Sound familiar?

- Teams connect AI agents straight to internal systems
- No one can say which agents reach which data
- Every MCP server has its own credentials to manage
- Agents see more tools than they need, and answer worse for it
- Auditors ask who approved an agent's access

One portal, every connector. Agents connect once; policy, credentials and logging stay in one place.

One portal, three ways to govern agents

Authenticate

People sign in through Cloudflare Access with your identity provider before any agent reaches a tool.

[Cloudflare Access](#) · [OAuth](#) · [Entra ID](#), [Okta](#), [Google](#)

Curate

Choose which tools and prompts each team's portal exposes, without changing the MCP servers behind it.

[Tool curation](#) · [Per-team portals](#) · [Central policy](#)

Audit

Log every request through the portal, and send traffic through Gateway for DLP inspection where needed.

[Access logs](#) · [Gateway logging](#) · [DLP](#)

Start with one team's agents, then add servers and teams to the same portal.

What FirstNet does for you

1

Inventory

List agents, MCP servers and the data they reach.

2

Design

Agree portals, tools and access per team.

3

Deploy

Servers behind Cloudflare Access and your identity provider.

4

Integrate

Send logs to your SIEM or FirstNet monitoring.

5

Manage

Access reviews, changes and escalation into Cloudflare.

Why FirstNet

- ✓ **One accountable provider** for connectivity, cloud, security and voice, with one Rapid Response entry point.
- ✓ **Joined up with your AI.** Portals alongside AI Gateway, Zero Trust and Sovereign AI on one contract.
- ✓ **Local engineers** aligned to your change windows and South African working hours.
- ✓ **Cloudflare MSSP partner**, ICASA-licensed group, ISO 27001:2022 and ISO 9001.

Getting started

1

AI security assessment. Which agents and MCP servers are in use, and what they can reach.

2

Portal design. Teams, tools and access policies agreed with you.

3

Scoped pilot. One team's agents on a portal before a wider rollout.

What we will need from you: your identity provider details, the MCP servers and tools in use and a named technical contact.

Let's elevate your AI agents.

Book an AI security assessment with your FirstNet account team.

firstnet.co.za →

0861 989 896 · sales@firstnet.co.za

Cloudflare is a cloud platform and is not a managed SOC or MDR service. Features, availability and outcomes depend on solution design, scope and the signed customer agreement. These controls support, but do not guarantee, compliance with POPIA or ISO standards; compliance remains a shared responsibility. Agent and model behaviour is not guaranteed; the portal controls access and records activity. Cloudflare and the Cloudflare logo are trademarks of Cloudflare, Inc. All other names belong to their respective owners.