okta

The AI-Ready Identity Framework

Modernizing Product Architecture for the Model Context Protocol (MCP) Shift

From UI to Agentic Actions

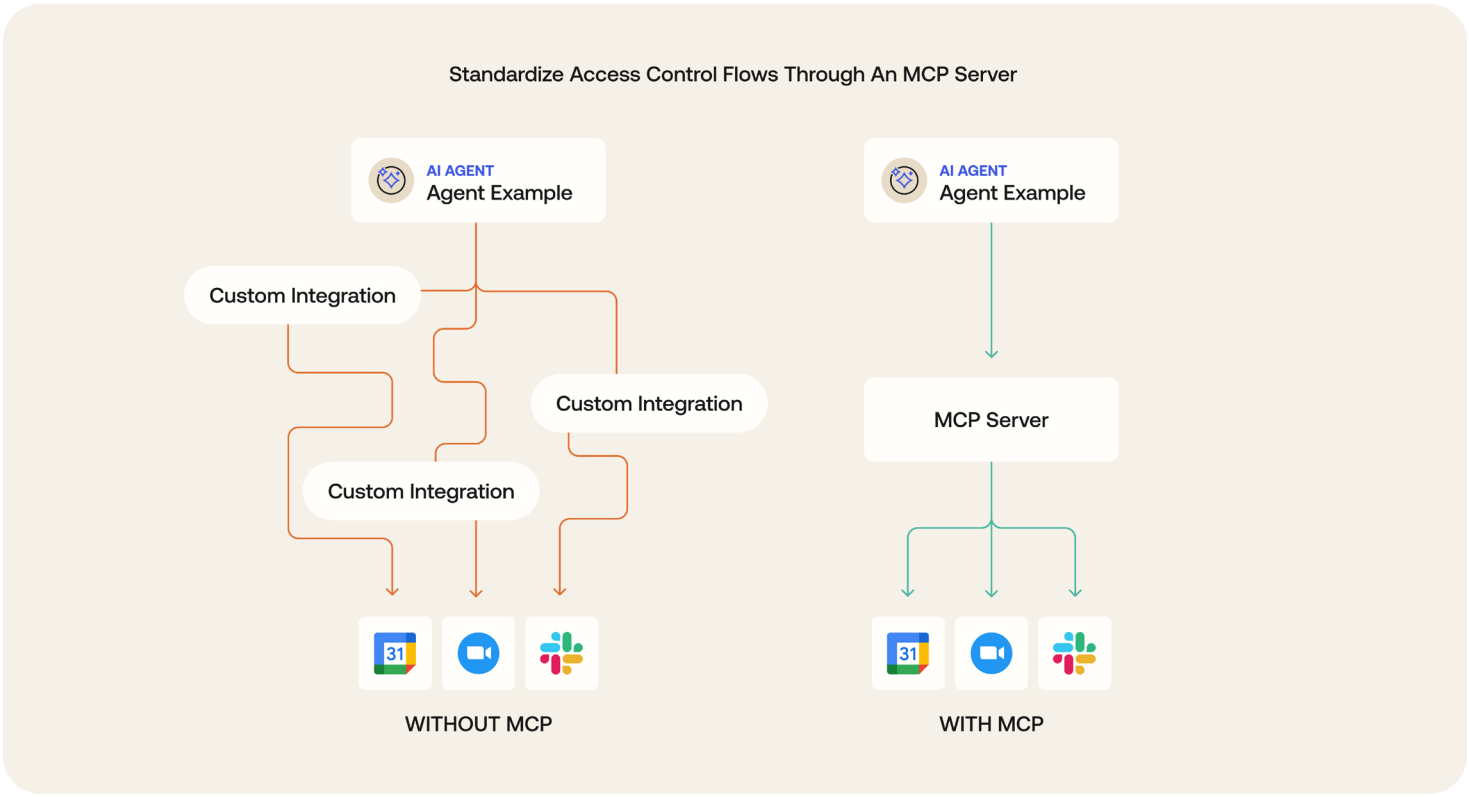
The industry is moving beyond generative AI toward autonomous agents that take action on behalf of human users. This transition is powered by the Model Context Protocol (MCP), a universal standard that replaces brittle, custom integrations with a unified interface for prompts, tool-calling, and data retrieval.

However, connectivity without identity is a liability. For your products to be truly AI-ready, they must solve two fundamental challenges at the protocol level:

1. When an agent connects to your MCP server, how do you verify exactly which human it is acting for, or does your server simply trust every request it receives?
2. When an agent acts on behalf of a user, how do you guarantee it only inherits the specific permissions of that individual, preventing it from accessing data beyond that user's authorized scope?

The Authorization Gap When Using MCP

While MCP provides the USB-C for AI connectivity, it is not a security protocol by design. The specification explicitly offloads authorization to an external authorization server, focusing on the communication layer rather than the security layer. Without a mature identity platform to handle these checks, connectivity quickly becomes a significant business liability.



A 3-Layer Framework

To bridge the Auth gap, an AI ready product must implement a layered security architecture. This promotes your product from a simple chatbot to an enterprise-grade agentic service. By exposing capabilities through the Model Context Protocol (MCP), you allow agents to act securely on behalf of your users within a global ecosystem using well known agents like ChatGPT or Claude.

PHASE 1

Register MCP clients so your server knows who's connecting.

- **Blocker:** For MCP clients to connect to your MCP server, they need to identify themselves. But how does your server trust a new client it's never seen? How do you get its name and logo for the consent screen? This is a key challenge for open ecosystems like MCP, where any client can connect to any server.
- **Solution:** The MCP spec recommends using Client ID Metadata Documents (CIMD) where each client hosts a document containing its metadata at a URL that serves as its digital identity. Your tenant admin simply provides that URL, your identity platform then fetches, validates, and presents the metadata for confirmation before any connection is established.
- **Result:** You get control over which clients can access your MCP server, ensuring no surprise registrations in your environment.

PHASE 2

Authenticate the user so every action is tied to a real human.

- **Blocker:** If an agent acts using a generic service account or without any user context at all, you lose accountability and the ability to distinguish an intern's request from a CFO's.
- **Solution:** A user must explicitly log in to the MCP server through the identity platform. This establishes the human context that the agent will inherit for all subsequent actions.
- **Result:** Every action becomes auditable. You know exactly which human the AI is acting on behalf of, and no agent can operate without an authenticated user behind it.

PHASE 3

Authorize agent actions so the agent can only do what the user is allowed to do.

- **Blocker:** A user's agent authenticates with your MCP server, then your server needs to call another API like a Salesforce instance or HR system to finish the job. The question is: how does that second API know the request is legitimate and who it's actually for?
- **Solution:** On-Behalf-Of Token Exchange lets your MCP server trade the user's access token for one that works with the downstream API, scoped correctly and still tied to the original user. No shared secrets, no service accounts with too much power.
- **Result:** The agent only gets to do what the user behind it is allowed to do with full auditing and visibility into every action. No over-reaching into data or systems the user shouldn't have access to.

okta

Implementing the Framework with Auth0

Building an identity layer for AI agents from scratch is a massive engineering undertaking that often distracts teams from their core mission. Auth0 simplifies this transition by providing a platform specifically designed for MCP. By using Auth0 for MCP, you can move away from manual identity plumbing and leverage a centralized system that handles the entire agent lifecycle. Auth for MCP automates the verification of client metadata through CIMD, the user login flows, the secure exchange of user tokens so permissions are always respected, and provides a more secure vault for credentials so your developers never have to hardcode a secret again. Essentially, Auth0 handles the complex security handshakes in the background, allowing your team to focus entirely on building the AI features that drive your business forward.

Imagine a user asking an AI agent, "Book a flight using my corporate card and add it to my calendar."

Step	Actor	Action
Client Registration	AI Agent	To authenticate against the `Travel-MCP-Server`, the AI agent must register itself as a client in Auth0. It sends its CIMD URL to Auth0 which creates the client.
User Login	User	The user provides their credentials and logs in to the MCP server.
Consent	User	The user sees a request: "Allow Travel-Agent to access Navan?" and they click approve. (Navan is a flight booking tool used by enterprises)
Execution	MCP Server	The MCP server receives a scoped token from Auth0. It calls the `Navan-Booking-API` on behalf of the user to secure the flight.

Conclusion

Adopting MCP authentication standards today isn't just about adding a feature, it’s about building the secure foundation for the future of work. By implementing this layered architecture, you help ensure that your product is ready for the enterprise where every action is auditable, every agent is more secure, and every user's data remains protected. As the industry moves toward a world where agents act on our behalf, the products that win will be the ones that prioritized security and identity from day one.

About Okta
Okta is the World’s Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We’re building a world where Identity belongs to you. Learn more at okta.com.