

Identity for the AI Era: Securing Customers, Employees, and AI Agents



Toby Allen

Senior Solutions Engineer, Okta

How many of you
have Agents in
production?

How many of you
believe your
machine identity &
secrets controls are
perfect?

You spent a decade securing humans. Agents are undoing it.

88%

of organizations report
confirmed or suspected AI
agent security incidents

97%

of AI breach victims had
no formal AI access
controls

AI SECURITY HAS THREE LAYERS

Security doesn't stop at the model layer.

The stronger models get, the more agent identity and data authorization become the critical layers.

MODEL SECURITY

Is this model sanctioned and in bounds?

VISIBLE

↑ MOST STOP HERE

AGENT IDENTITY

Is this agent authorized to act for this user?

GAP

DATA AUTHORIZATION

Should this action execute with these parameters, right now?

GAP



**Where are my
agents?**



**What can they
connect to?**

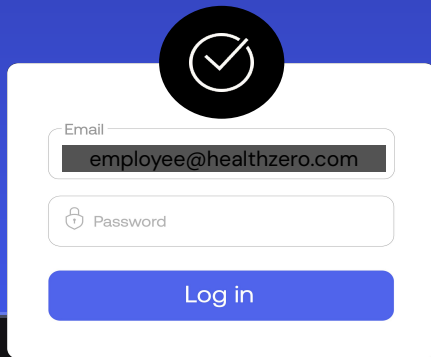


**What can
they do?**

Agentic Security for Applications

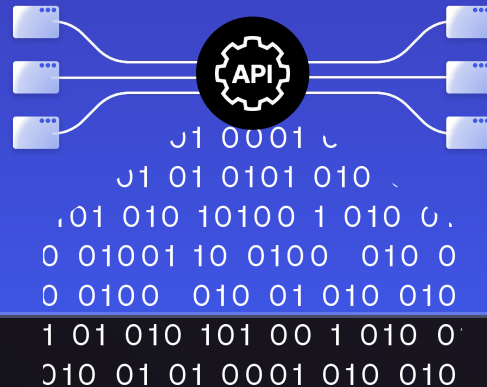
User Authentication

AI needs to know who I am



Token Vault

AI needs to call APIs on users behalf



Async Authorization

AI uses async interactions



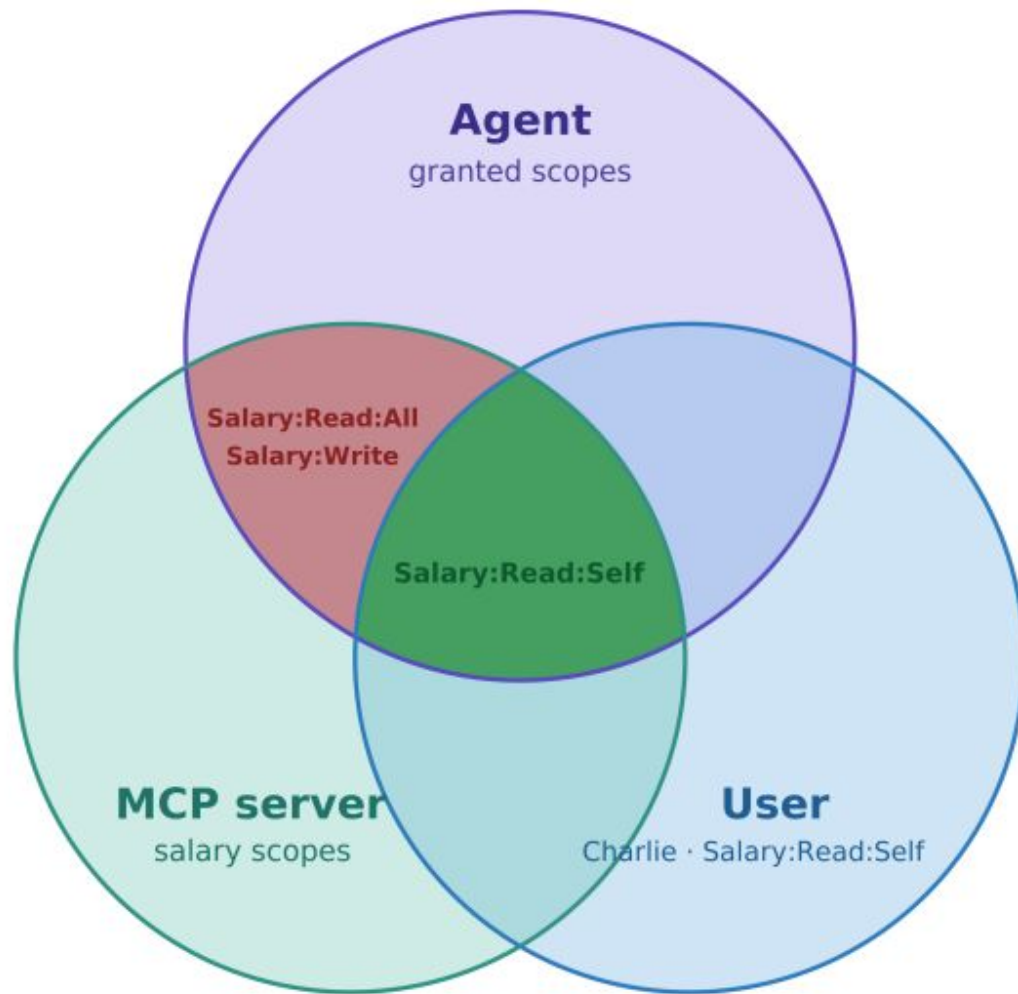
Fine-Grained Authorization

AI data access must consider user permissions



Are you securing AI
agents like service
applications?

Why service app architectures cause privilege escalation



✓ **Agent Modeled as First-class Identity**

Effective = the green center = Salary:Read:Self.
The agent does only what Charlie can do.
The over-scoped request is denied.

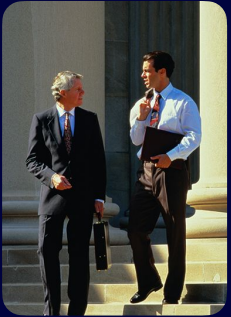
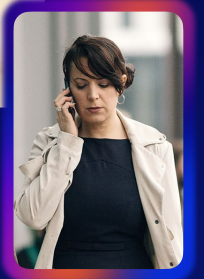
✗ **Agent Modeled as Service App**

The User circle drops out of the decision.
Effective grows beyond the green center
into the red region, Salary:Read:All and Salary:Write.
That added region is the escalation.

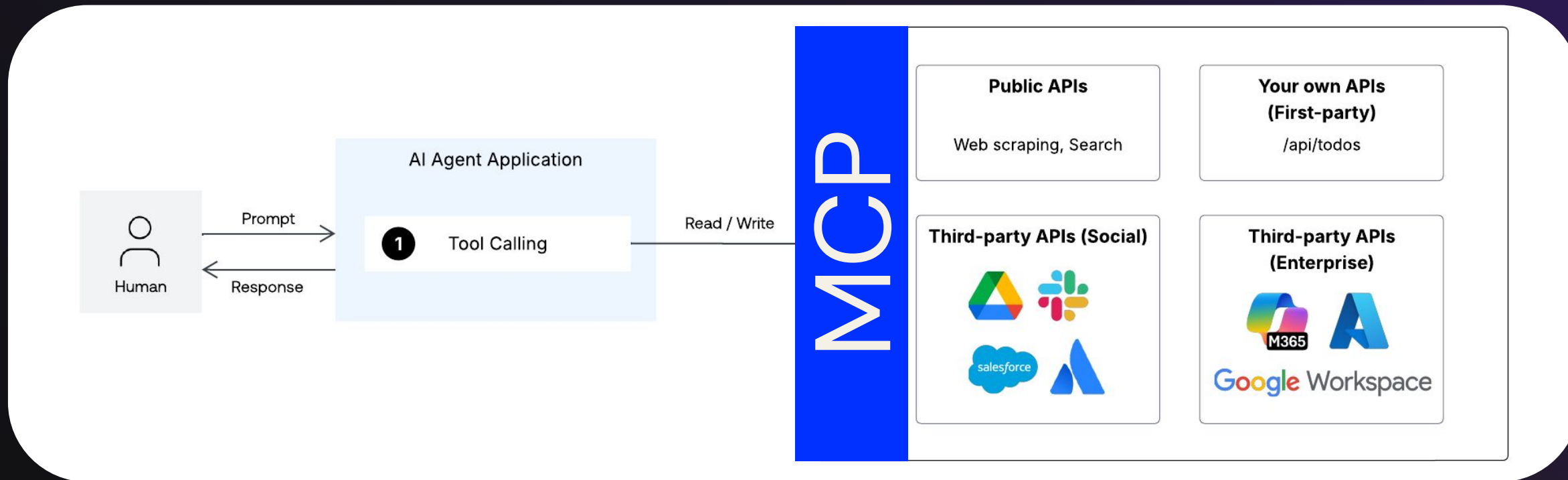
Bind the agent to the user and the effective set stays in the green center. Drop the user and it spreads into the red.



AI security *is*
identity security



Agents use Tools



On-Behalf-of Token Exchange

VS

Cross-App Access XAA

Wait, What is Cross-App access?



Allow the "Google Drive" app to access Slack

✓ App is approved by Slack

Apps are reviewed for quality before they are listed in the Slack Marketplace. [Learn more about app reviews.](#)

Workspace



Auth0



Review app permissions

[Manage permissions](#)

Information "Google Drive" can view



Content and info about channels & conversations



Content and info about your workspace



Actions "Google Drive" can take



Perform actions as you

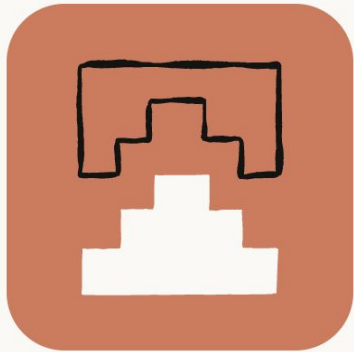


Perform actions in channels & conversations



↓ More permissions

Wait, What is Cross-App access?



**Centrally manage
authorization for
MCP connectors**

[Home](#) » [Posts](#)

Enterprise-Managed Authorization: Zero-touch OAuth for MCP

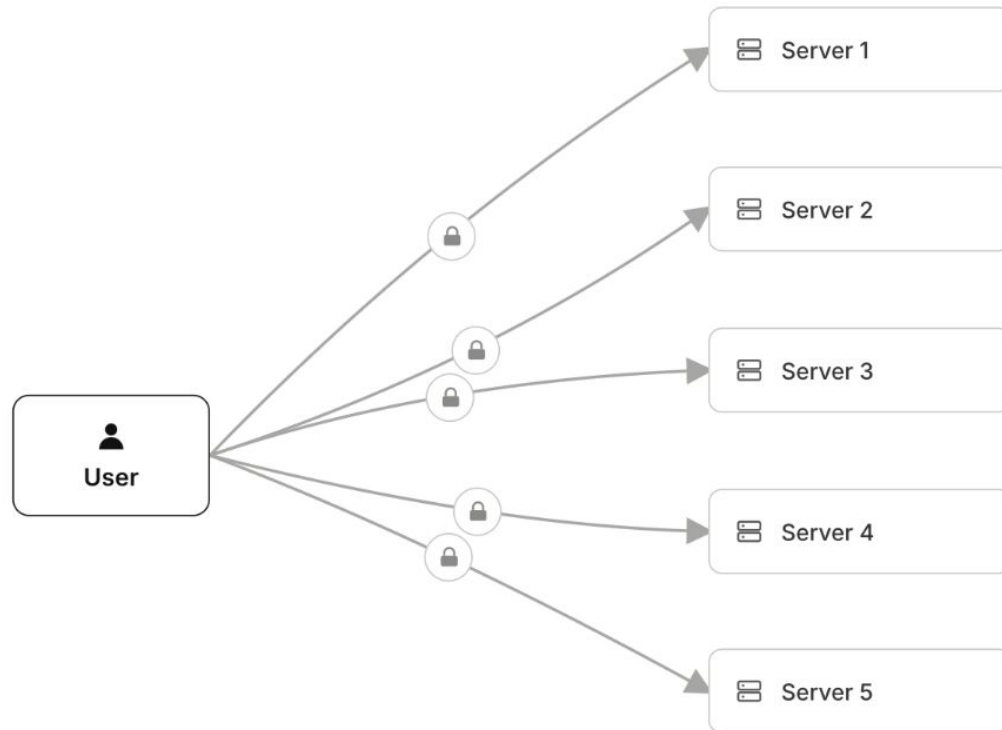
The Enterprise-Managed Authorization extension to the Model Context Protocol is now stable, enabling organizations to centrally provision MCP server access through their identity provider so users get connected servers on first login without per-app OAuth.

[All Collections](#) > [Connectors](#) > [General](#) > [Authorize MCP connectors for your entire organization](#)

Authorize MCP connectors for your entire organization

Updated over 3 weeks ago

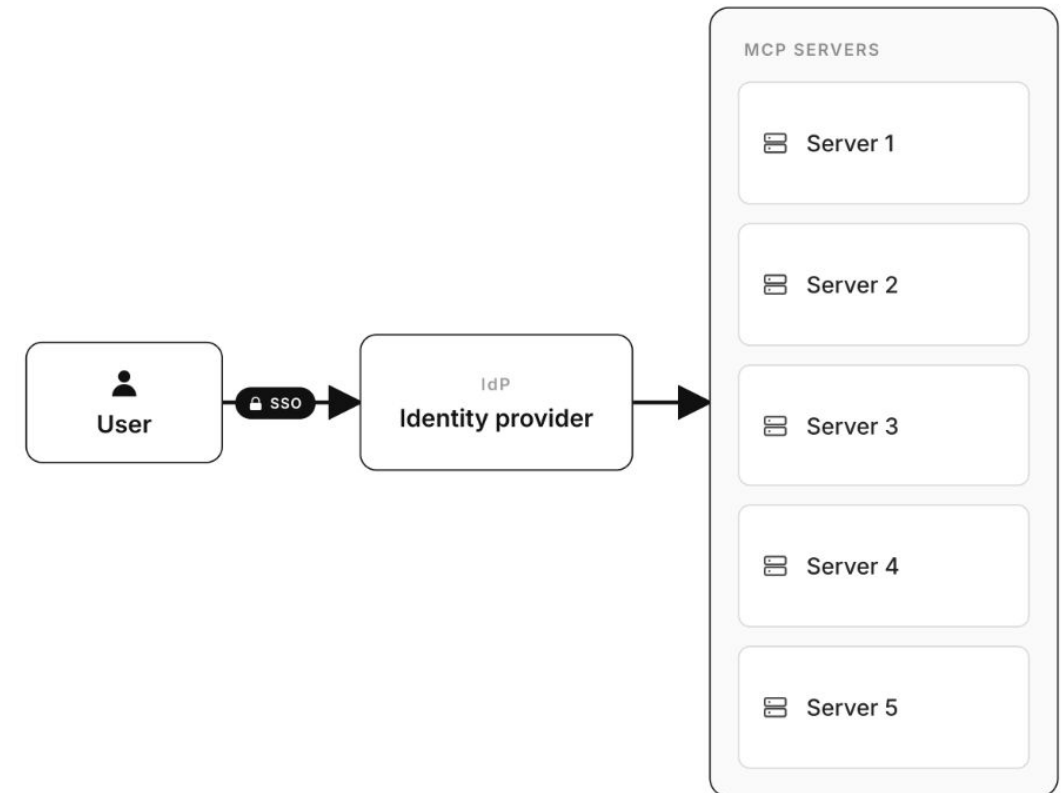
Standard MCP authorization



Authenticate to every server, one by one

A separate OAuth consent prompt for each connection. Nothing enforced or revoked centrally.

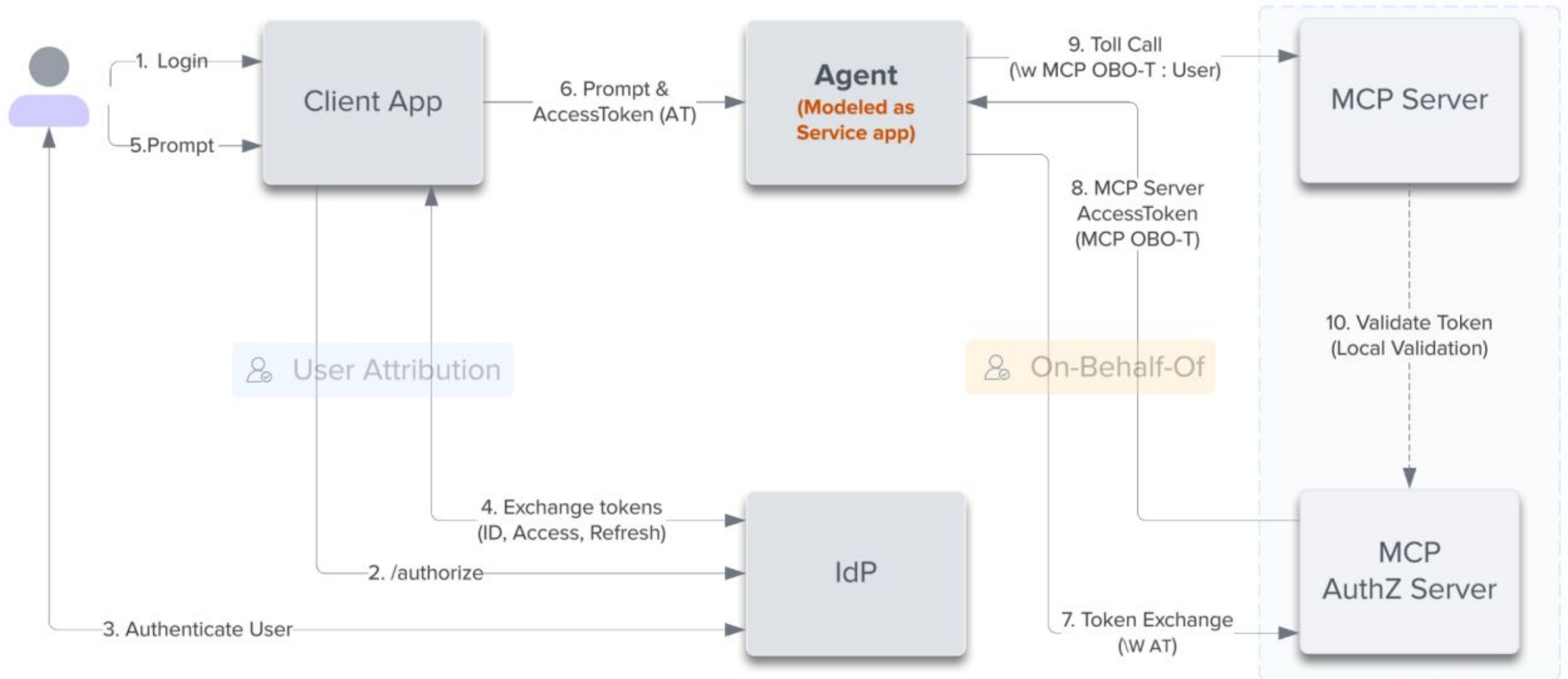
Enterprise-Managed Authorization



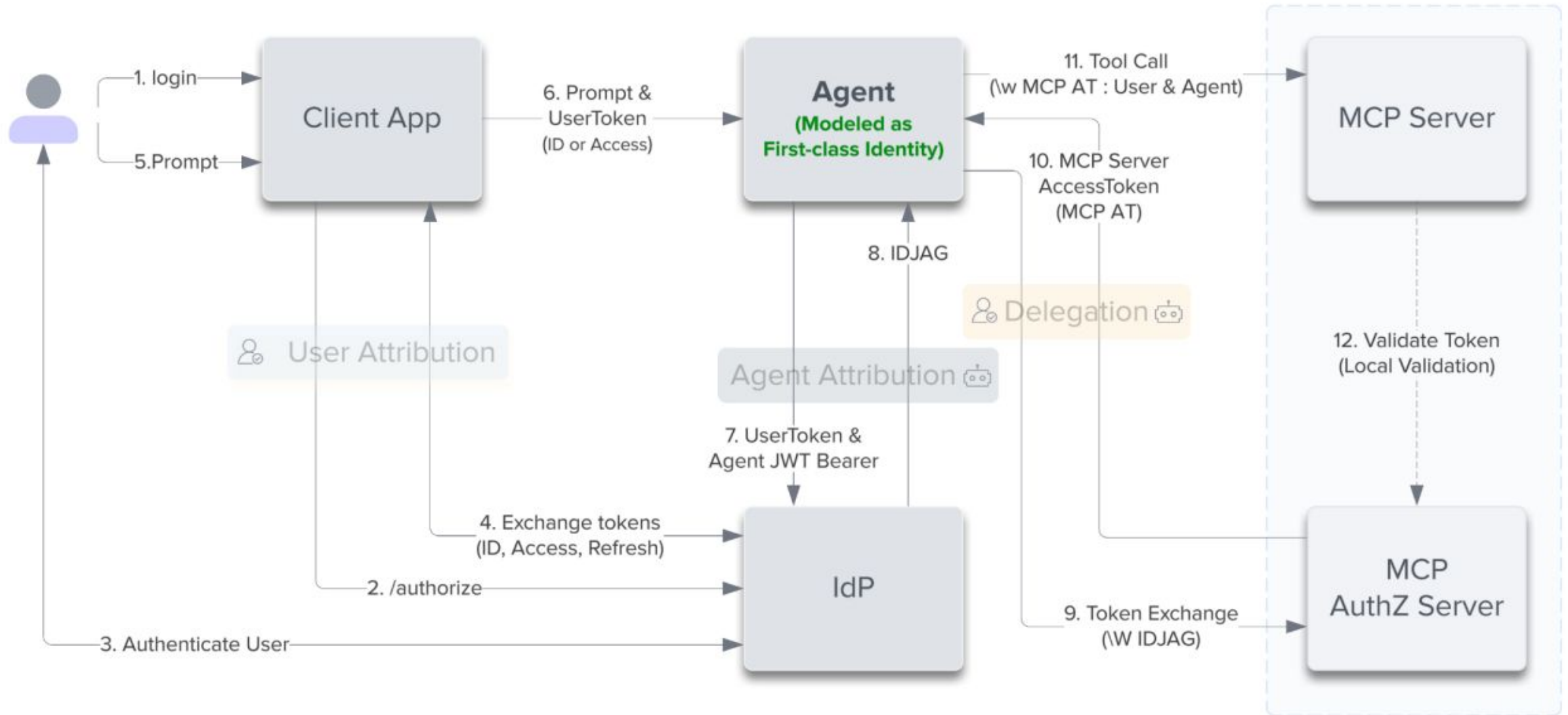
Authenticate once through your identity provider

Every server the admin authorized connects automatically. Scoped to the user's groups and roles.

An AI agent modeled as a service app using an OBO



An AI agent modeled as a first-class identity using XAA





**Where are my
agents?**



**What can they
connect to?**



**What can
they do?**



Unprecedented customer demand for security

