descope

Descope for Agentic AI / MCP

Identity Provider For Your AI Agents

Agentic identity challenges

Identity security

Every OWASP Top 10 Threat for Agentic Applications has at least one identity-related mitigation.

Access control

57% of IAM decision-makers are worried about AI agents accessing unauthorized data.

Production-readiness

While 88% of orgs have adopted or want to adopt AI agents, only 37% have moved past pilot phases.

Descope Agentic Identity Hub

1 For MCP developers

- Secure internal and external-facing MCP servers with OAuth 2.1 compliant auth.
- Support DCR and CIMD based registration with agent risk assessment flows.
- Provide granular authorization scopes at the agent and tool level.

2 For AI agent developers

- Manage, store, and refresh credentials for AI agent connections to third-party services.
- Choose from 50+ app templates and presets for third-party MCP servers.
- Use ephemeral credentials purpose-built for AI agents.

3 For IT / security teams

- Define policies to govern how AI agents and MCP clients access corporate tools and backend systems.
- Leverage context from the user / tenant, agent, MCP server, and downstream service.
- Ensure visibility with detailed, streamable audits and logs.

Dedicated agentic identity management	Integration with workforce IdPs	Detailed audit trails and analytics	Complete AI agent identity lifecycle mgmt.

Popular use cases

Purpose-built agentic identities

Issue portable, revocable tokens designed specifically for agents, independent of platform or downstream auth requirements.

Secure MCP servers

Add user auth and consent, client registration, scope-based access control, and tool connections to MCP servers.

AI agent credential mgmt.

Securely store and refresh the API keys and OAuth tokens your agents need to connect to external services and MCP servers.

Enterprise-grade access policies

Define policies that use context from the agent, user / tenant, MCP server, and target service to govern access to enterprise resources.

Complete agent observability

Gain full visibility into every agent across your organization, with audit trails that stream to our dashboard or your SIEM.

AI agent identity lifecycle mgmt.

Register AI agent identities, manage and monitor access, identify potential misconfigurations, and revoke permissions.

Benefits

- Purpose-built AI agent identities
- Secure organizational AI adoption
- Secure and scalable remote MCP servers
- Modern, AI-compatible apps and APIs
- Purposeful, real-world AI agents
- Increased developer productivity and focus

Some of our happy customers

WisdomAI

"Our customer-facing MCP server uses Descope as the auth layer–helping us show the value of our AI-powered analytics platform while having the confidence that identity controls are baked-in."

- Soham Mazumdar, Co-Founder and CEO

CEQUENCE SECURITY

"Descope's flexible, developer-friendly handling of MCP auth has played an important role in helping Cequence AI Gateway customers securely expose their APIs to AI agents."

- Shreyans Mehta, Co-Founder and CTO

daylight

"Our MCP server is very popular with larger customers, with security analysts using it to uncover analytics about our MDR platform. Adding Descope as the auth layer was a breeze."

- Asaf Rosentswaig, Senior Software Engineer