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

Only 22% of teams treat agents as unique identities, with most relying on shared API keys

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 product/engg teams

- Securely expose your product APIs to AI agents.
- Define APIs as protected resources to enable scoped, delegated access at the user and / or tenant level.
- Leverage secure token exchange to support delegation chaining (e.g. agent → MCP server → API resource).

2 For MCP developers

- Securely expose MCP servers to AI agents with OAuth 2.1 and PKCE.
- Support flexible client registration (CIMD / DCR) with hardening and agent risk review controls.
- Define MCP servers as protected resources to enable scoped, delegated access.

3 For AI agent developers

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

4 For IT / security teams

- Define policies to govern how AI agents and MCP clients access corporate tools and backend APIs.
- Leverage context from the user / tenant, agent, MCP server, and downstream service.
- Enforce policies at the token boundary (issuance and exchange).

AI agent directory | Federation with workforce IdPs | Detailed audit trails and analytics | Complete AI agent identity lifecycle mgmt.

Popular use cases

Agent directory

Gain visibility into every agent connected to your product or MCP servers, their owners, permissions, and actions performed.

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

Granular access policies

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

Agent-readiness

Open up your product APIs to AI agents with time-bound, scoped, delegated access, while treating agents as principal identities along with human users.

AI agent identity lifecycle mgmt.

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

Benefits

- AI agents as first-class identities
- Agent-ready apps and APIs
- Secure and scalable remote MCP servers
- Complete AI agent auditability
- Reduced blast radius for AI agents
- Increased developer productivity

Some of our happy customers

you.com

"By unifying our user and MCP identity under Descope, we have an identity system that aligns with the unique security and experience needs of businesses, individuals, and AI agents."

- Saurabh Sharma, CPO

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

descope

www.descope.com | docs.descope.com | descope.ai