descope

Descope for Agentic AI / MCP

Identity Infra For Your AI Systems

Agentic identity challenges

Identity security

5 of the Top 10 OWASP for GenAI threats have authentication and authorization related mitigations

Access control

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

Production-readiness

Less than two-fifths of AI projects have successfully transitioned to production

Descope Agentic Identity Hub

1 For app developers

- Protect APIs with OAuth for seamless AI agent connectivity
- Add granular user / tenant level authorization to ensure scoped, secure access
- Create configurable user consent management flows

2 For MCP developers

- Add OAuth to remote MCP servers in 3 lines of code
- Easily connect MCP clients with external tools and MCP servers
- Call external APIs from MCP servers with full token management / storage

3 For AI agent builders

- Easily connect AI agents with external tools and enterprise systems
- Offload token management and storage
- Programmatically connect and fetch outbound tokens through SDKs

4 For security teams

- Govern how AI agents and MCP clients access external tools
- Restrict AI agent access based on user roles or JWT claims
- Ensure visibility with detailed, streamable audits and logs

Scalable, multi-tenant architecture

Multi-region data residency

Detailed audit trails and analytics

Plug & play connectors ecosystem

Popular use cases

Agent-compatible APIs

Turn your app into an OAuth provider for seamless API connections.

Secure MCP servers

Add enterprise-grade authorization, consent management, and tool connections to MCP servers.

Scope-based access control

Define granular user, tenant, and permission scopes for what AI agents can access.

Token management & storage

Enable AI agents to connect to 50+ external tools and enterprise systems.

Agentic AI security policies

Restrict AI agent access to specific scopes / tools based on user roles and claims.

AI agent identity lifecycle mgmt.

Create, manage, monitor, and revoke AI agent access control and permissions.

Benefits

- Modern, AI-compatible apps and APIs
- Secure and scalable remote MCP servers
- Purposeful, real-world AI agents
- Secure organizational AI adoption
- Increased developer productivity and focus
- Quick time to value with drag & drop workflows

Some of our happy customers

gofundme · databricks · NAVAN · you.com · Owens & Minor

DevRev · CEQUENCE SECURITY · BRANCH · Reco · AEG PRESENTS · MYRIAD360

whatfix · LUMBER · CARS24 · GradRight · bcm one · Wisdom AI

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