

MCP Registry and Gateway

TrueFoundry MCP Gateway

 Copy page



Centralized MCP gateway for enterprise AI agents—unified access, OAuth, security, observability, and guardrails for all your MCP servers.

Model Context Protocol (MCP) is an open standard that enables AI assistants to securely connect to data sources and tools. As AI systems evolve from simple chat interfaces to tool-using agents, MCP provides the standardized interface for these connections. Truefoundry MCP Gateway enables organizations to centralize access to MCP servers and provides a unified interface for AI agents to access them.

Why Enterprises Need an MCP Gateway

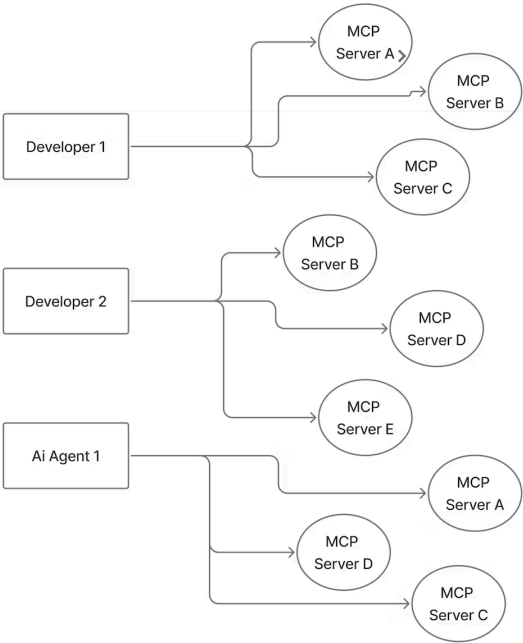
As AI agents become central to enterprise workflows, organizations face critical challenges when scaling MCP server adoption:

Fragmented Infrastructure
Security & Credential Sprawl
Zero Visibility
No Governance

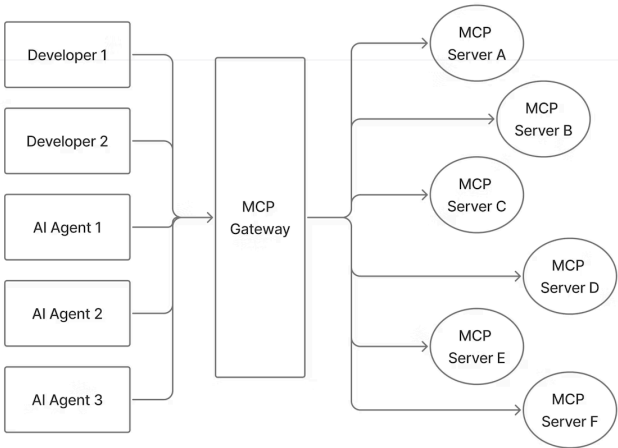
Before vs After: The MCP Gateway Difference



Without MCP Gateway



With MCP Gateway



Without MCP Gateway

With TrueFoundry MCP Gateway

Multiple Connections

AI agents require separate connections to each MCP server

Single Gateway Access

AI agents connect to one gateway, access multiple MCP servers

Fragmented Configuration

Each developer configures VS Code, Cursor, Claude Code individually

Unified Configuration

Single configuration point for all AI development tools

Local Server Management

Developers must install and manage MCP servers locally

Centralized Infrastructure

Central IT manages cloud-hosted MCP infrastructure via streamable HTTP

Ad-hoc Authentication

No standard authentication flow for enterprise tools

Standard OAuth Flows

Developers use standard OAuth 2LO/3LO flows for enterprise MCP servers

Credential Sprawl

Scattered API keys and credentials across tools

Secure Credential Management

Centralized credential management with secure vault integration

No Observability

No visibility into what tools teams are using

Full Audit Trail

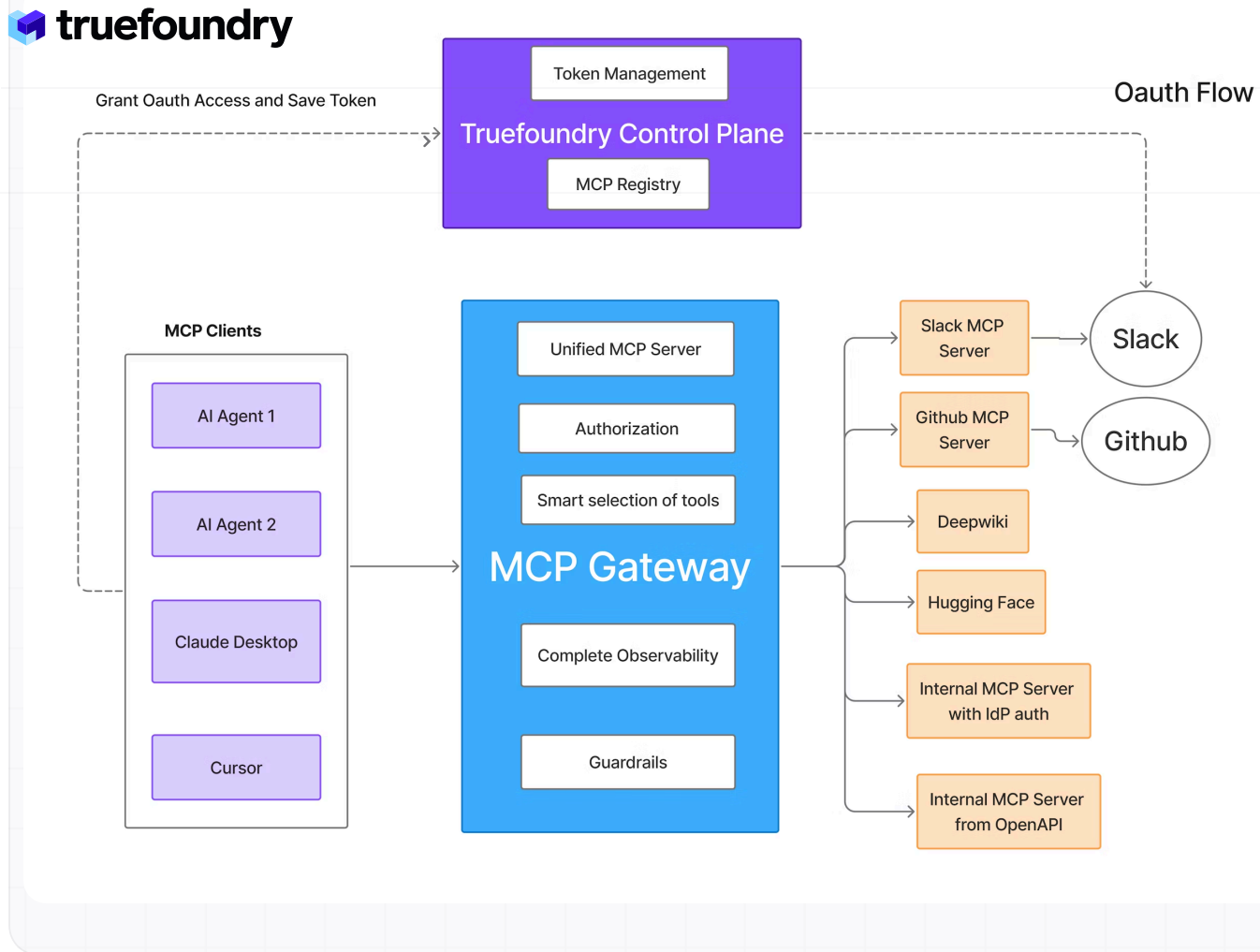
Complete visibility and audit trail for all tool usage

Without MCP Gateway	With TrueFoundry MCP Gateway
truefoundry Security Risks Security risks from unmanaged tool sprawl	Governed Access Enterprise-grade security with governed tool access
Static Tool Access No dynamic tool discovery for autonomous agents	Dynamic Discovery Dynamic tool discovery and invocation for autonomous workflows
No Catalog No curated tool catalog for multi-tenant environments	Curated Registry Registry provides discoverable, curated MCP servers for multi-tenant use

TrueFoundry MCP Gateway

TrueFoundry MCP Gateway is an enterprise-ready platform that centralizes access to AI development tools using the Model Context Protocol. Instead of managing hundreds of individual tool configurations across your development teams, provide secure, governed access to curated AI tools through a single platform.

Architecture



Key Features

1. Centralized MCP Registry

Register both public and self-hosted MCP servers in the TrueFoundry Control Plane. The control plane maintains the registry along with authentication mechanisms, handles user-specific OAuth2 flows, securely stores and refreshes access tokens, and ensures users can only access resources they are authorized for.

2. Unified Token Management

The AI Gateway stores and manages OAuth tokens for all MCP servers on behalf of each user. It maintains a mapping from user tokens to OAuth tokens for different MCP servers and

automatically refreshes them when they expire. Users interact with the Gateway using a single token without managing multiple credentials.

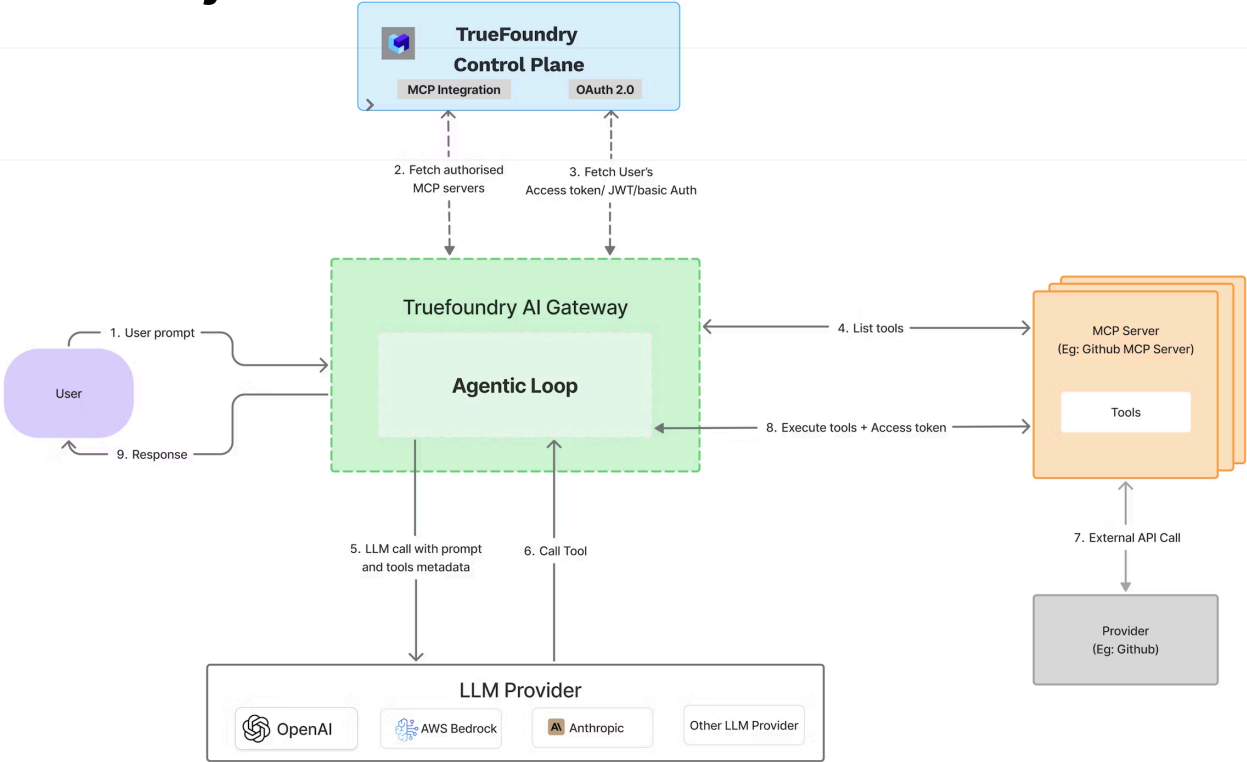
3. Enterprise Security & Access Control

Comprehensive security built for enterprise needs:

Capability	Description
Authentication	OAuth 2.0, SAML, and enterprise SSO integration—users authenticate once through your existing identity provider
Fine-grained Permissions	Tool-level RBAC and ABAC policies for different teams, controlling access down to specific tools and read vs. write operations
Unified Access Keys	Generate a single Personal Access Token (PAT) to access all authorized models and MCP servers, or Virtual Account Tokens (VAT) for application-level access
Secure Credential Management	API keys and credentials stored in a secure vault—developers never handle raw credentials

4. Agent Playground & Code Integration

Build and test agents directly in the browser using the playground. Experiment with prompts and MCP tools like Websearch, WebScraping, document extraction, and code execution. The gateway streams the agentic loop in real-time so you can watch LLM reasoning, tool calls, and responses as they happen. Ready-to-use code snippets help you integrate MCP servers into your applications quickly.



5. MCP Guardrails

TrueFoundry offers MCP guardrails that apply before and after tool calls to enforce security best practices:

Guardrail Type	Description
Pre-execution Checks	Validate tool inputs, check for sensitive data, and enforce policies before any tool runs
Real-time Blocking	Block suspicious or unauthorized tool usage as it happens—prevent risky operations before they execute
Post-execution Validation	Inspect tool outputs for PII, secrets, or policy violations before returning results
User Approval Workflows	Require explicit approval for high-risk operations like deletions or write actions

6. Observability & Audit

 truefoundry

Full visibility into your AI tool usage across the organization:

>

Capability	Description
Request Logging	See exactly what tools AI assistants are calling, when, and with what parameters
Cross-Platform Monitoring	Unified visibility across Claude Code, Cursor, ChatGPT, and other AI clients through a single dashboard
Audit Compliance	Complete request/response logging for regulatory requirements, with every tool call available for compliance audits

Was this page helpful?

 Yes

 No

< Log Feedback

Getting Started >

Powered by 