

HƯỚNG DẪN SỬ DỤNG TÍNH NĂNG CÔNG CỤ MCP CLIENT

1. Giới thiệu

Model Context Protocol (MCP) là một tiêu chuẩn mã nguồn mở cho phép kết nối AI Agent với các nguồn công cụ bên ngoài, nhằm tạo ra phản hồi chính xác và phù hợp hơn với ngữ cảnh nghiệp vụ.

Tính năng **Tạo Công cụ MCP Client** trên nền tảng FPT AI Agents cho phép:

- Kết nối tới MCP Server.
- Truy xuất và quản lý danh sách công cụ từ MCP Server cung cấp
- Sử dụng các công cụ này trong AI Agent để hỗ trợ xử lý nghiệp vụ, đảm bảo luôn cập nhật thông tin mới từ MCP Server.

2. Cách sử dụng chức năng

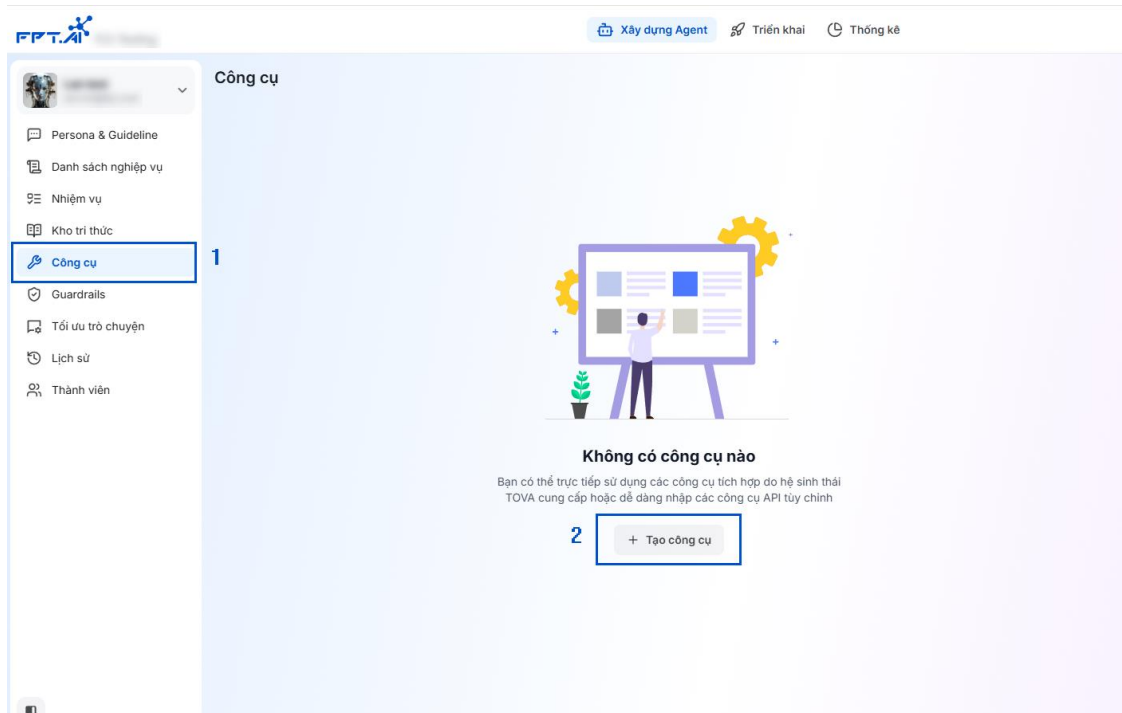
1. Tạo Công cụ MCP Client

Khi tạo Công cụ MCP Client, được hiểu là hệ thống FPT AI Agents sẽ thực hiện kết nối tới MCP Server và sử dụng các công cụ đã lựa chọn hỗ trợ cho AI Agent thực hiện nghiệp vụ.

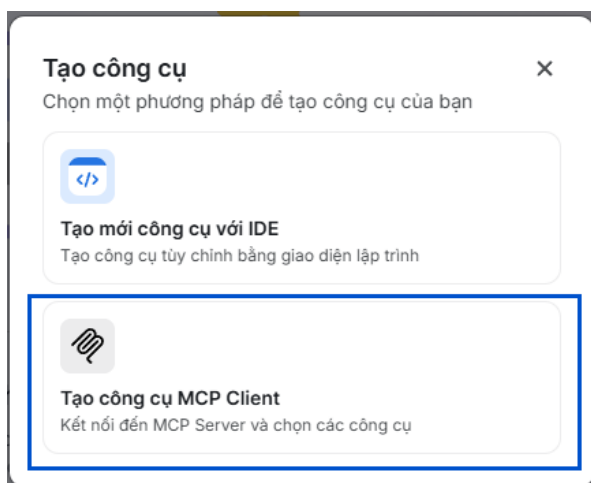
Cách thức tạo và kết nối như sau:

Bước 1: Truy cập menu “**Công cụ**”

Bước 2: Nhấn nút “**Tạo công cụ**”



Bước 3: Chọn phương thức “Tạo công cụ MCP Client”



Bước 4: Nhập thông tin kết nối và cấu hình sử dụng:

Thông tin kết nối

- **Tên (bắt buộc):** Tên định danh cho công cụ, tối đa 50 ký tự.
- **Mô tả:** Mô tả ngắn gọn về công cụ, tối đa 100 ký tự.
- **SSE Endpoint (bắt buộc):** URL Endpoint mà hệ thống sẽ gọi đến để lấy danh sách công cụ từ MCP Server.
- **Xác thực:** Chọn một trong hai phương thức:

- No Auth: Không yêu cầu xác thực.
 - Bearer Token: Nhập thêm trường Token để xác thực. Trường Token sẽ được mã hóa sau khi nhập.
- **Công cụ được sử dụng:** Lựa chọn công cụ để sử dụng
- Tất cả: Dùng toàn bộ công cụ từ Server.
 - Đã chọn: Chỉ định rõ tên công cụ cần dùng trong trường “*Công cụ đã chọn bên dưới*”. Sau khi chọn thông tin này, bạn cần chọn cụ thể công cụ cần sử dụng trong danh sách công cụ mà MCP Server cung cấp.
 - Tất cả trừ: Loại trừ các công cụ cụ thể khỏi danh sách bằng “*Công cụ loại trừ*”. Sau khi chọn thông tin này, bạn cần chọn cụ thể công cụ cần loại trừ trong danh sách công cụ mà MCP Server cung cấp.

Bước 5: Nhấn **[Tạo]** để xác minh kết nối và hoàn tất tạo công cụ MCP Client.

Tạo công cụ MCP Client

×

Kết nối đến MCP Server và chọn các công cụ

Tên *

Enter a name of MCP Client tool0/100

Mô tả

Enter a description of MCP Client tool0/800

SSE endpoint *

Ví dụ: https://my-mcp-server.ai/sse

Xác thực

No Auth

Công cụ được sử dụng

Tất cả

✓ Tất cả

Bao gồm tất cả các công cụ có sẵn từ MCP Server

Đã chọn

Bao gồm các công cụ cụ thể từ MCP Server trong trường "Công cụ đã chọn" bên dưới

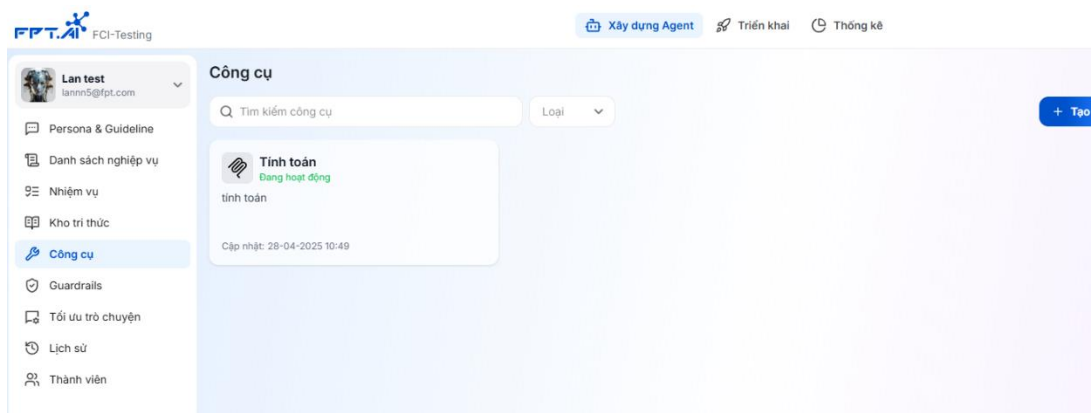
Tất cả trừ

Bao gồm tất cả ngoại trừ công cụ bạn chọn trong trường "Công cụ loại trừ" bên dưới

Hủy

Tạo

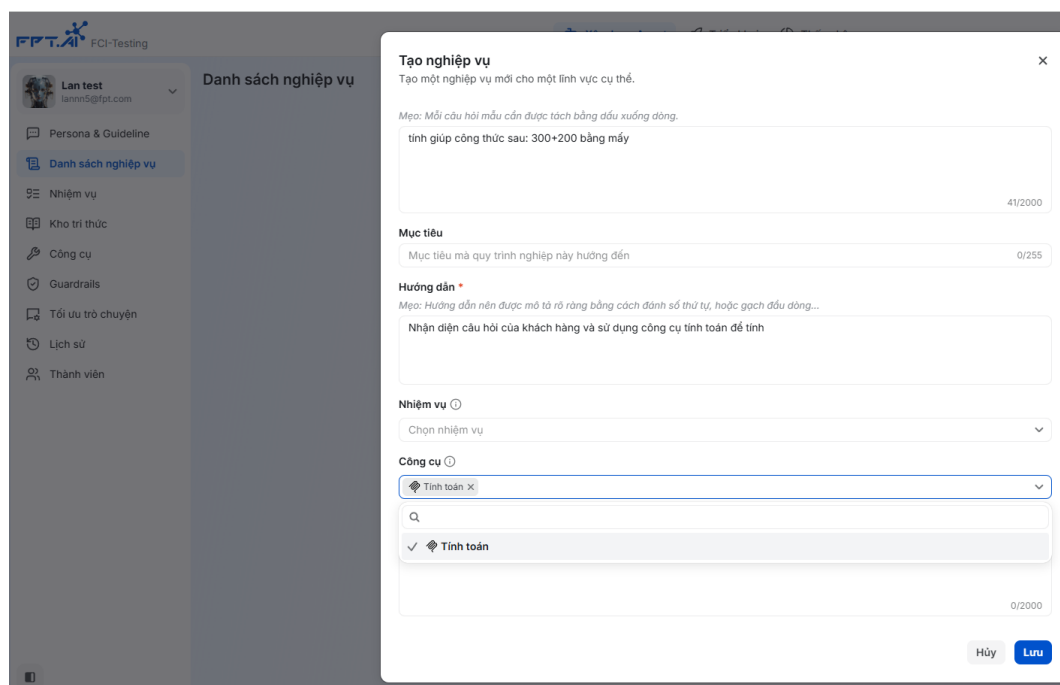
Bước 6: Hệ thống lưu thông tin, công cụ MCP Client vừa tạo sẽ xuất hiện trong **Danh sách công cụ**



2. Sử dụng Công cụ MCP Client trong “Danh sách nghiệp vụ”

Bước 1: Truy cập menu “Danh sách nghiệp vụ”

Bước 2: Khi tạo hoặc chỉnh sửa một nghiệp vụ, tại trường “**Công cụ**”, chọn công cụ MCP Client đã tạo trước đó để sử dụng. AI Agent sẽ xác định lựa chọn công cụ (nếu có nhiều công cụ nhỏ trong MCP Client đã tạo) và thực hiện công cụ.



Bước 3: Sau khi hoàn tất gắn Công cụ MCP Client trong luồng nghiệp vụ, kiểm tra luồng hoạt động tại “**Preview and Test**”

Lưu ý:

- Phương thức kết nối tới MCP Server mà FPT AI Agents hỗ trợ là **dạng SSE (Server-Sent Events)** – công nghệ cho phép Server chủ động gửi các cập nhật theo thời gian thực về Web Client qua HTTP.
- Nếu xảy ra sự cố kết nối với MCP Server, trạng thái Công cụ MCP Client sẽ hiển thị **“Fail”**. Người dùng cần vào kiểm tra và kết nối lại thủ công để tiếp tục sử dụng công cụ cho MCP Server cung cấp.