



#Milano



Renderere un MCP server enterprise-ready: autenticazione, Azure API Management e Microsoft 365 Copilot

Matteo Pagani

Cloud Solution Architect @ Microsoft



#Milano

improve



TD SYNnex

Grazie ai nostri sponsor 🙏



#Milano

Understanding Model Context Protocol

What is MCP?

- Model Context Protocol
 - Open-source standard for connecting AI applications to external systems
- MCP is like a “universal plug”
 - Allows AI models connecting to tools, apps, and data
 - Just like USB-C connects your phone to anything else
- Helps AI agents do more
 - Calling APIs, reading files, sending messages, etc.
 - Without needing custom code for each task
- Developers save time
 - Making AI solutions more powerful, flexible, and easier to maintain



MCP Host

(Copilot, GitHub Copilot, IDEs, Chat UI, etc.)

MCP Client

- Discovers and connects to MCP servers
- Handles 1:1 communication with one server
- Invokes Tools
- Queries for Resources
- Discovers and supplies Prompts arguments

LLM/Orchestrator

MCP Servers

(Any technology)

MCP Server

Tools

Resources

Prompts

MCP Server

Tools

Resources

Prompts

Transport & Security

Transports: stdio (local), Streamable HTTP (remote). JSON-RPC 2.0 message schema

AuthN: anonymous, API key, OAuth 2.1

Microsoft ❤️ MCP

MCP at Microsoft

MCP servers across Microsoft



Azure



Foundry Tools



GitHub



Azure Logic Apps



Agent 365

Build your own and publish



Logic Apps



Azure API Center



Azure Functions



Azure App Service



Azure Container Apps

Call from MCP clients anywhere



Foundry agents



Copilot Studio



VS Code



GitHub Copilot

Secure access and governance



Azure API Management



Entra ID

What we'll see today



Authentication

Protecting the MCP server using Microsoft Entra and the OAuth 2.0 protocol



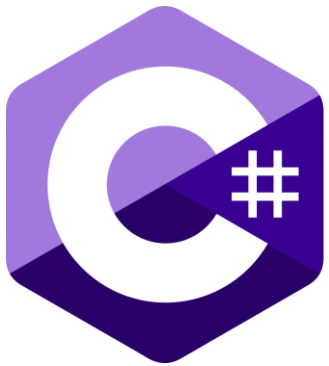
Support for enterprise agentic platforms

Building agents connected to a protected MCP server with:

- Microsoft 365 Agents Toolkit
 - Copilot Studio
 - Microsoft Foundry

Building an MCP server

- If you already have an API, the hard part is already done 😊
- You expose your API endpoints as MCP tools
- Key difference with APIs: you must describe the purpose of the functions and the input parameters, so that the agent knows when and how to use it





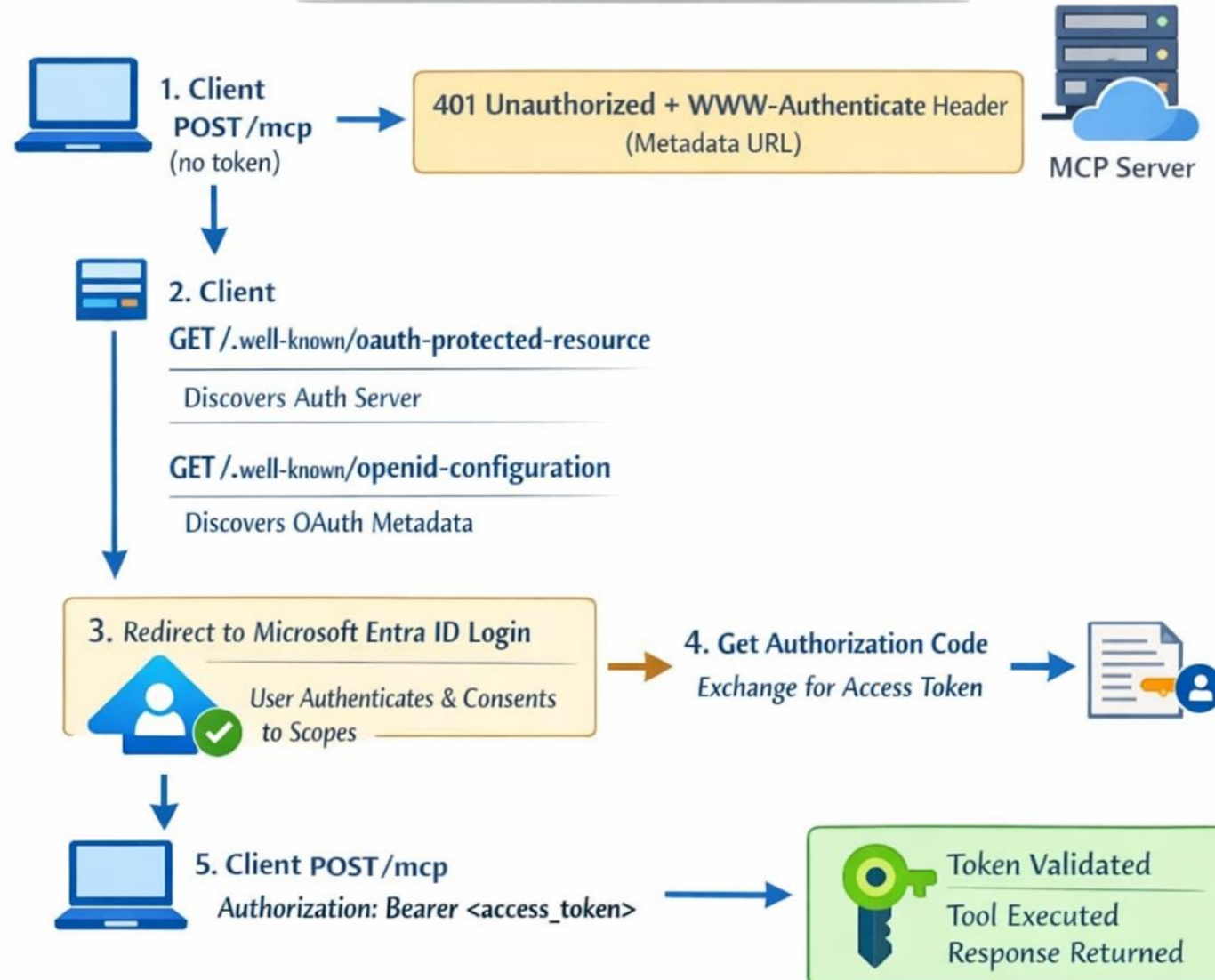
#Milano

An MCP server to manage flights

Demo

The MCP authorization chain

OAuth Authentication for MCP Servers





#Milano

The MCP authorization chain

Demo

Three ways to build this infrastructure

Code



Most flexible, but more work and harder to maintain

Azure App Service



Simple to implement, but least flexible option

API Management




In between the other options: more work to implement it than App Service, but more flexible

You need an app registration in Entra (server)


Edit a scope ×

 Save  Discard  Delete

Scope name * 

access_as_user


api://2eff18e0-1ca3-4943-a691-2bd63313692c/access_as_user

Who can consent? 


Admins and users Admins only

Admin consent display name * 


Access Flights API

Admin consent description * 

Allows the app to access the Flights API on behalf of the signed-in user

User consent display name 

Access Flights API

User consent description 

Allows the app to access the Flights API on your behalf

State 

Enabled Disabled

- It's used only to protect the MCP server
- No need to configure secrets or redirect URI
- You must expose a scope to enable clients to access to the MCP server

Azure App Service



1. You deploy your MCP server (with no authentication code) to the App Service
2. You enable Easy Auth
3. You set an environment variable called **WEBSITE_AUTH_PRM_DEFAULT_WITH_SCOPES** with the scope exposed by the app registration used to protect the App Service (e.g. `api://5643e255-1c40-4eb5-98fd-255148bad97b/user_impersonation`)

Your app service will automatically expose the `.well-known/oauth-protected-resource` endpoint with the required information



#Milano

Azure App Service and MCP

Demo

API Management



1. You deploy your MCP server (with no authentication code) to an App Service or Azure Container Apps
2. You restrict traffic so that only APIM can access to the service
3. You use the validate-azure-ad-token policy to restrict access to clients authenticated with Entra
4. If the authentication fails, you return a 401 and the WWW-Authenticate header with the .well-known/oauth-protected-resource URL
5. You manually implement the .well-known/oauth-protected-resource endpoint using policies

Two options for APIM

Expose MCP tools in code



You use APIM only to enforce the authentication layer

Turn APIs into MCP tools



You use APIM to turn your APIs into MCP tools without changing the code



#Milano

API Management and MCP

Demo

You need an app registration in Entra (client)

+ Add a permission ✓ Grant admin consent for Contoso

API / Permissions name	Type	Description
▼ Flights API (1)		
access_as_user	Delegated	Access Flights API
▼ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Redirect URI configuration Supported accounts Settings

A redirect URI, or reply URL, is the location where the Entra authorization server sends the user and delivers tokens once the user has successfully signed in.

+ Add Redirect URI Delete

i If you want to view or change implicit grant and hybrid flows settings or front-channel logout URL, please visit the settings tab.

Start typing a reply url to filter these results

<input type="checkbox"/> Platform Type ↑↓	Redirect URI ↑↓
<input type="checkbox"/> ▼ Web	Edit
<input type="checkbox"/> Web	https://teams.microsoft.com/api/platform/v1.0/oAuthConsentRedirect
<input type="checkbox"/> Web	http://127.0.0.1:33418/
<input type="checkbox"/> Web	https://teams.microsoft.com/api/platform/v1.0/oAuthRedirect

- It's used to authenticate against the MCP server
- It's a proper OAuth registration
- You expose a client id and client secret
- You set up the redirect URIs for your calling platform
- You add permission for the scope you created for the MCP server



#Milano

Consuming MCP from Declarative Agents

Empowering every developer to build agents

Build on the M365
Copilot Stack

Build on your own
AI Stack

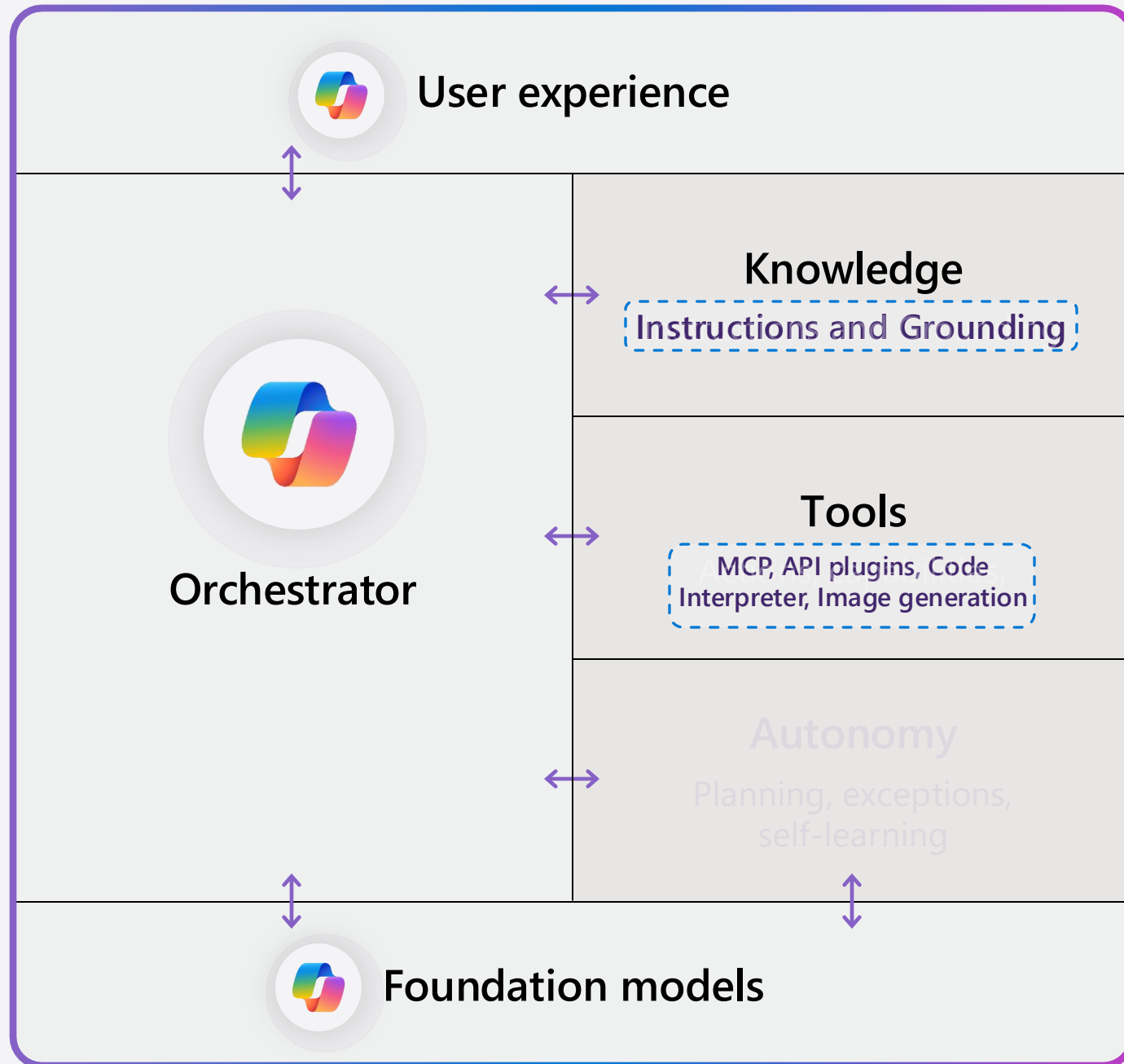
Build for your
own app




Declarative agents

Deliver powerful solutions on
the Copilot AI stack.

Declarative agents



 Microsoft provided

 Developer provided



#Milano

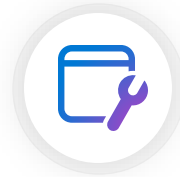
Consuming MCP from Copilot Studio

Empowering every developer to build agents

Build on the M365
Copilot Stack

Build on your own
AI Stack

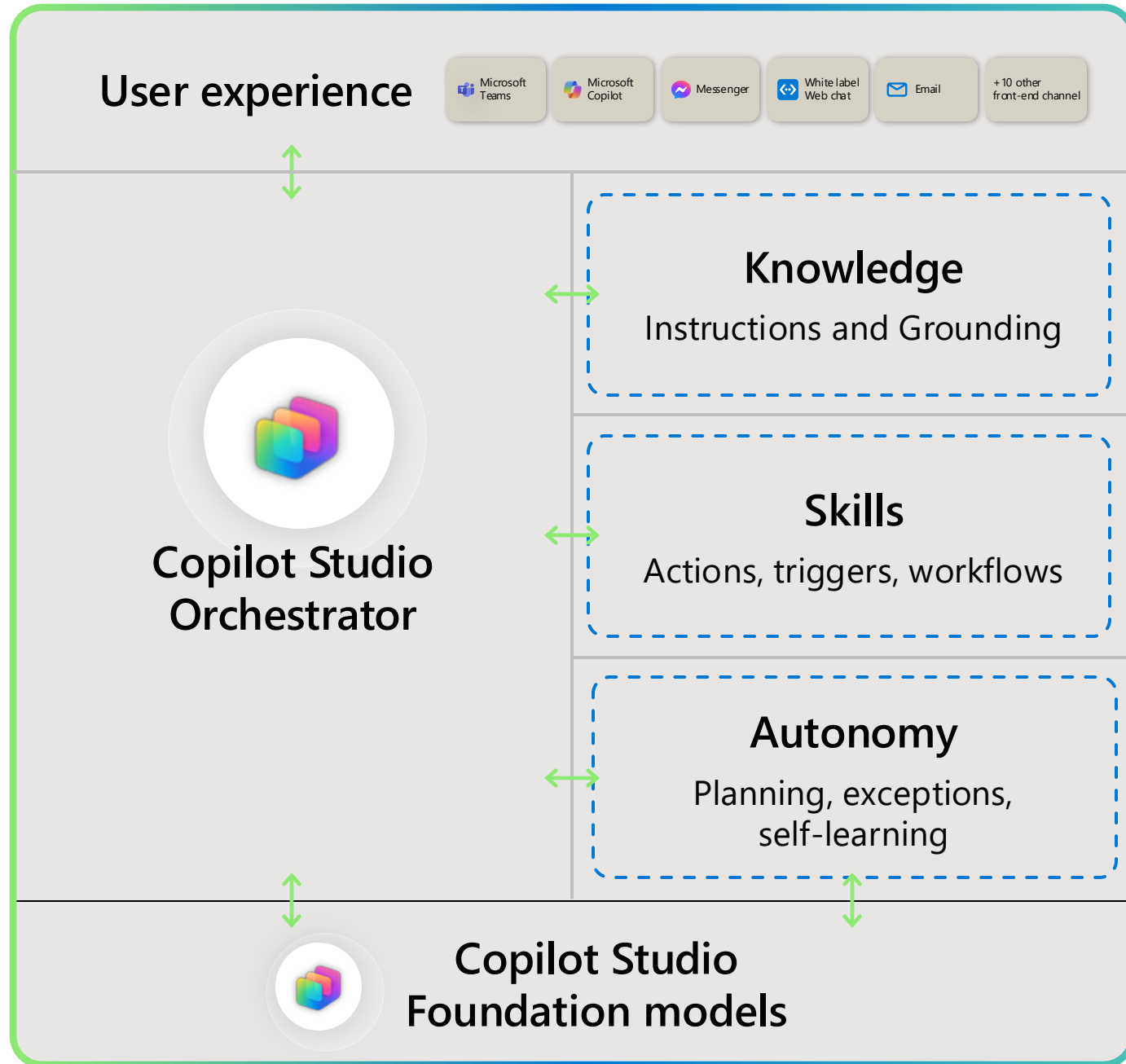
Build for your
own app




Custom Engine

Bring your own agent, custom models, orchestration and logic

Copilot Studio Full agents



 Microsoft provided

 Maker designed

Adding an MCP server to a Copilot Studio agent

Add tool

Let your agent do more. [Learn more](#)

Create new [See all](#)

Agent flow
These predictable automations run the same way each time, giving you more control when you need it.

Prompt
Analyze and transform text, documents, images, and data, with natural language and AI reasoning.

Model Context Protocol
Open standard for connecting your agent to data, designed with AI in mind.

Computer use [Preview](#)
Empower your agent to directly use web and desktop apps.


All [Connector](#) [Prompt](#) [Flow](#) [REST API](#) **[Model Context Protocol](#)**

Almanac by PassBy Almanac by PassBy	Azure Databricks Genie Azure Databricks	Bigdata.com MCP endpoint Bigdata-com	Box MCP Server Box MCP Server
CData Connect AI CData Connect AI	Celonis MCP Server Celonis MCP Server	Contact Management MCP S... Office 365 Outlook	Contesso Contesso
D365 Sales MCP Server (dep... Microsoft Dataverse	D365 Service MCP Server (D... Microsoft Dataverse	Databricks Genie Databricks	Dataverse MCP Server (Depreca... Microsoft Dataverse
DocuSign MCP Server DocuSign Demo	Draup MCP Server Draup MCP Server	Dynamics 365 Business Cent... Dynamics 365 Business Central	Dynamics 365 Contact Center A... D365 Contact Center Admin MCP

How is your experience with adding tools?

Suggestions and search will include AI-generated results. [See terms](#)

Add a Model Context Protocol server



Model Context Protocol

Used to represent the server. Icon should be in PNG format and less than 30 KB in size.

Server name *

Server description *

Server URL *****

Enter the complete server path to continue

Authentication
 None API key OAuth 2.0



#Milano

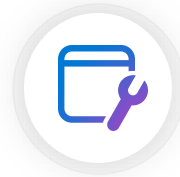
Consuming MCP from Foundry Agent Service

Empowering every developer to build agents

Build on the M365
Copilot Stack

Build on your own
AI Stack

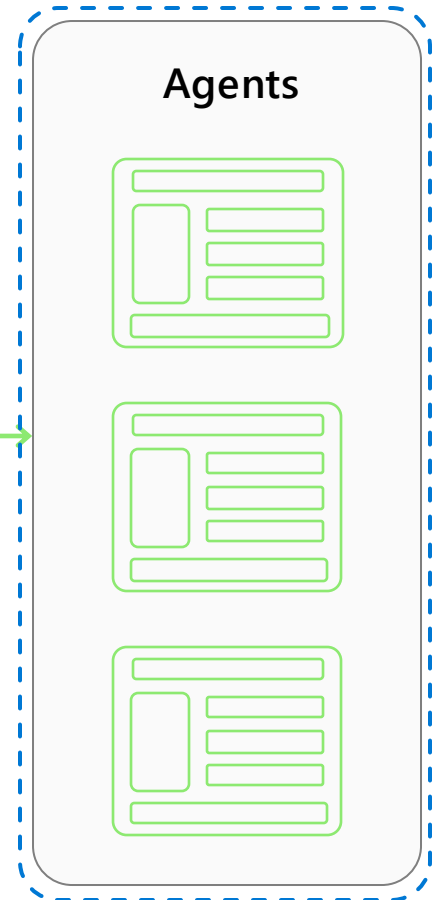
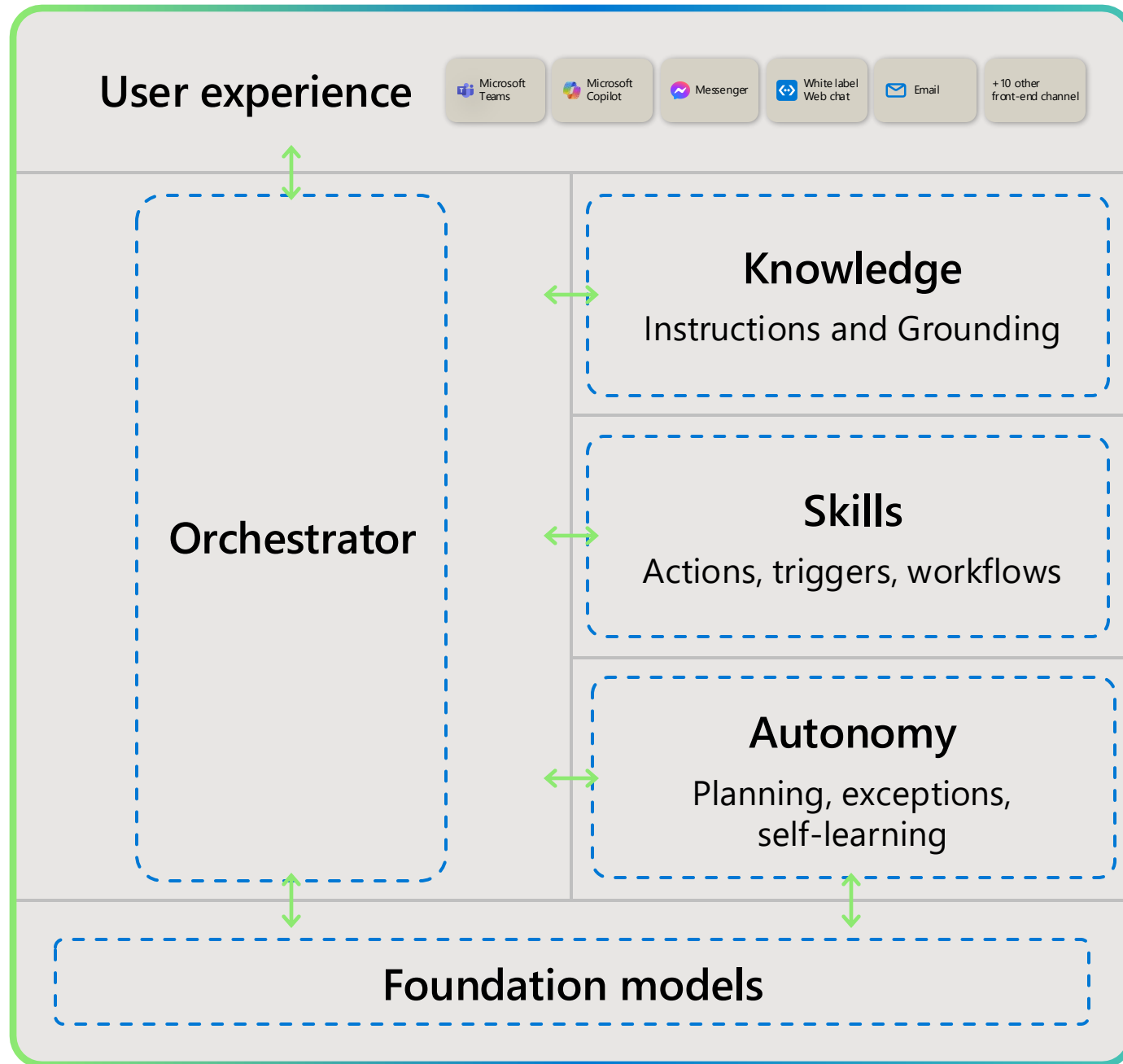
Build for your
own app



Custom Engine

Bring your own agent, custom models, orchestration and logic

Custom engine agents



Microsoft provided

Developer provided

Adding an MCP server to Foundry agent

Select a tool

Configured **Catalog** Custom

Browse tools from the public or organizational Foundry Tool Catalog. Some tools may require setup before use. [Learn more](#)

Search

Featured

Type Provider Category Registry Supported auth

MongoDB MCP Server MongoDB MCP Server allows any MCP-aware LLM to connect to MongoDB Atlas for admin tasks and to... Local MCP	Azure SQL MCP Server A secure, self-hosted MCP for interacting with SQL data (Azure SQL, SQL MI, SQL DW, SQL Server). Local MCP Preview	Foundry MCP Server (preview) Foundry MCP Server (preview) offers instant access to model exploration, deployment of models and agents... Remote MCP Preview
Elasticsearch Search, retrieve, and analyze Elasticsearch data in developer and agentic workflows. Remote MCP Preview	Work IQ Mail Work IQ Mail MCP Server which enables Microsoft Outlook email actions (create, send, reply, search) for... Remote MCP Preview	Pinecone Assistant MCP Server Pinecone Assistant MCP server helps prototype and deploy assistants that retrieve context-aware answers... Remote MCP
Work IQ Calendar Work IQ Calendar MCP Server which enables core Outlook calendar actions (create, update, manage, an... Remote MCP Preview	Work IQ Copilot Work IQ Copilot MCP Server which enables core Microsoft Copilot chat actions, including starting... Remote MCP Preview	Azure Database for PostgreSQL Enables Agents to interact with and retrieve data from Azure Database for PostgreSQL resources using natura... Local MCP Preview
GitHub Access GitHub repositories, issues, and pull requests through secure API integration. If you need the GitHub... Remote MCP	Work IQ Word Work IQ Word MCP Server which enables Microsoft Word document creation, retrieval, and commenting actions... Remote MCP Preview	Vercel With Vercel MCP, you can explore projects, inspect failed deployments, fetch logs, and more right from your AI... Remote MCP Preview
Work IQ Teams Work IQ Teams MCP Server which enables core Microsoft Teams actions, including chat, channel, and... Remote MCP Preview	Azure Cosmos DB Enables Agents to interact with and retrieve data from Azure Cosmos DB accounts. Local MCP Preview	Microsoft Dataverse Enables Dataverse data and schema operations (query, table & record management, API invocation). This... Remote MCP Preview
Azure Managed Redis Azure Managed Redis MCP Server provides a natural language interface for agentic apps to interact with Azu... Local MCP Preview	Azure Databricks Genie Azure Databricks Genie MCP server lets AI agents connect to Genie spaces so users can ask natural... Remote MCP Preview	Factory RCA MCP Toolset for manufacturing root-cause analysis, anomaly detection, and telemetry-driven recommendations. Remote MCP

< Prev Next >

Add Model Context Protocol tool

Third-party services you connect to via Model Context Protocol are Non-Microsoft Products under the Product Terms. Use third-party services at your own risk and subject to third-party license terms and privacy policies.

Name *

Provide a unique name

Remote MCP Server endpoint * [i](#)

Provide the remote MCP server endpoint

Authentication * [i](#)

Key-based

Credential * [i](#)

E.g. "key1" : E.g. "{{value}}"

+ Add key value pair

Connect Cancel



#Milano

Copilot Studio and the Flight MCP server

Demo



#Milano

Slide e video:

<https://www.globalazuremilano.it>